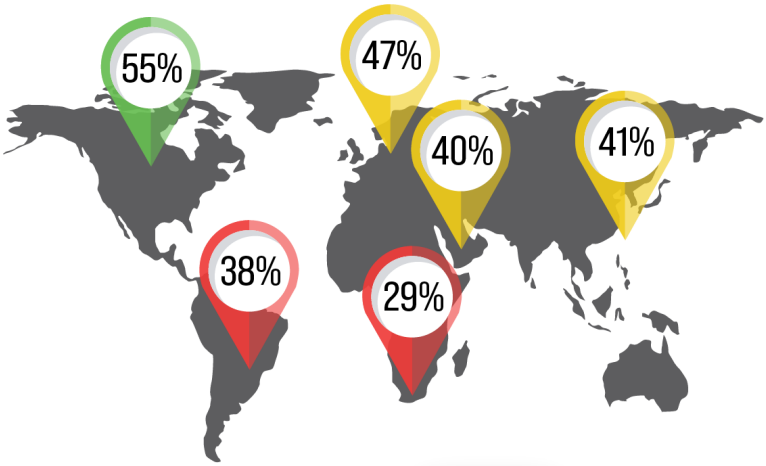
AI Standards Index™ 2025

Global Benchmark of AI Standards Adoption, Governance, and Readiness

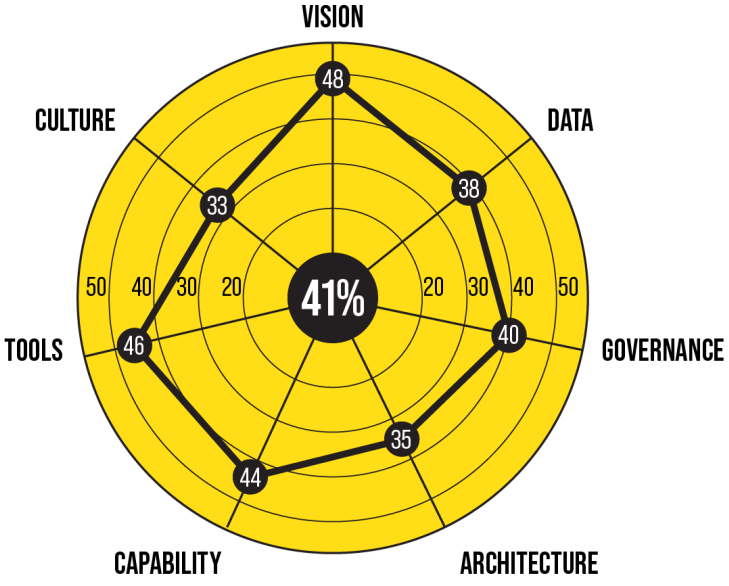
First Edition, December 2025

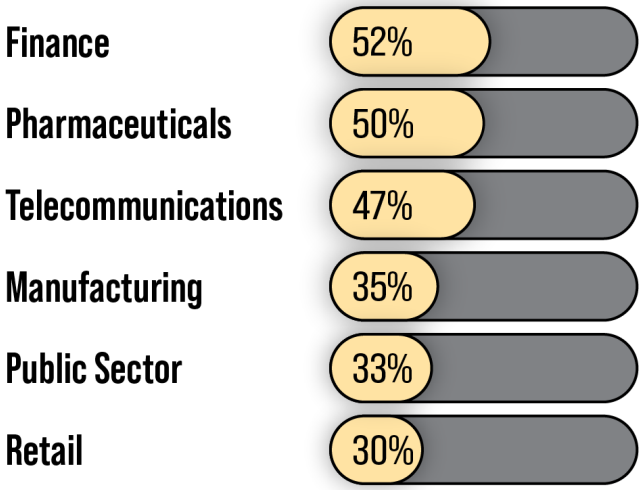
Published by
Kadir Özbayram, The Standards Effect™



41% **AI Standards Index™ 2025**

41% Operational Maturity across 7 dimensions, aligned with ISO/IEC SC 42, NIST AI RMF, OECD AI Principles, and the EU AI Act.





https://thestandardseffect.com/index

Disclaimer & Legal Notices

This report is provided solely for informational and research purposes and does not represent the views of any public authority, regulatory body, or standardization committee.

The AI Standards Index™ is **not** a certification program, audit, regulatory assessment or legal compliance tool. All maturity scores and benchmarks reflect the AI Standards Index™ methodology and the analysis of participating organizations. The author makes no warranties regarding accuracy, completeness or fitness for any particular purpose and assumes no liability for decisions made based on this material.

This publication is independent and is not affiliated with, endorsed by or approved by ISO/IEC, NIST, OECD, the European Commission or any regulatory authority.

Readers should apply professional judgment when interpreting the findings and should not rely on this material as a substitute for regulatory, legal or compliance advice.

All trademarks, service marks and product names referenced in this report remain the property of their respective owners.

This publication is made available through **thestandardseffect.com.**

Research Conducted: May–December 2025
Publication Date: December 2025

Author's Introduction: The Standards Effect™ Movement

In my work with global enterprises, the same pattern kept appearing. AI initiatives advanced quickly until they hit the same structural walls: missing documentation, inconsistent terminology, fragmented architectures, and unclear ownership. The technology was rarely the limiting factor. The absence of standards was.

I wrote *The Standards Effect™* to articulate this problem: organizations underestimate the power of shared standards. When AI scales faster than governance, the result is friction, rework, and avoidable risk. But a philosophy alone was not enough. Leaders needed a measurable way to understand where they stand—and how far they are from what international standards require.

The AI Standards Index™ was created to close that gap in 2025.

It translates the principles in *The Standards Effect™* into measurable indicators aligned with ISO/IEC SC 42, the NIST AI RMF, OECD AI Principles, and the EU AI Act. It defines the foundation for a discipline that has been missing in enterprise AI: **AI Standards Management™**.

This Index is more than a benchmark. It represents a shift toward disciplined, evidence-based AI—a move away from intuition and speed toward clarity, accountability, and structural integrity. Leaders who adopt this approach are not only improving governance; they are shaping how AI will operate at scale.

The Standards Movement starts here.
This report provides the first global measurement of it.

December 2025
Kadir Özbayram

About the AI Standards Index™

The AI Standards Index™ provides a measurable baseline for how well organizations implement the controls required by modern AI Standards. It evaluates not only the existence of policies, but whether teams apply them with the discipline demanded by ISO/IEC 23053 lifecycle requirements and EU AI Act documentation obligations. The Index covers 30 countries and exposes gaps that are not visible through adoption surveys alone.

The Index is grounded in internationally recognized standards and regulatory expectations, including:

Foundational Standards & Regulations

- ISO/IEC SC 42: Technical standards for Artificial Intelligence
- ISO/IEC 22989: Concepts and Terminology
- ISO/IEC 23053: AI System Life Cycle Framework
- ISO/IEC 23894: AI Risk Management
- ISO/IEC TR 24028: Trustworthiness
- ISO/IEC TR 24027: Bias in AI Systems
- NIST AI Risk Management Framework (Govern, Map, Measure, Manage)
- EU AI Act: Evidence, traceability and conformity requirements for high-risk AI

External Research References

- OECD AI Policy Observatory
- Stanford AI Index
- WEF AI Governance Research
- McKinsey Global AI Survey

The Index assesses maturity across seven dimensions: Vision & Leadership, Data Quality, Governance & Process, Architecture & Reuse, Capability & Skills, Tools & Automation, and Culture & Behavior. The lowest-scoring dimension in 2025 is Culture (33%), a signal that many organizations treat standards as recommendations rather than enforceable controls. Data Quality (38%) shows similar strain, often due to missing lineage, inconsistent documentation, or risk controls that fail ISO/IEC 23894 transparency expectations.

By consolidating these dimensions into a single maturity baseline, the AI Standards Index™ offers an unfiltered view of global readiness. It shows where organizations meet standards, where they fall short, and the specific structural weaknesses that prevent AI from being governed, audited, and scaled with confidence.

About the Author

Kadir Özbayram
CEO & Co-Founder, **ins-pi**

Kadir Özbayram is an enterprise architecture and AI governance specialist with nearly two decades of experience designing the structures and controls that large organizations rely on to manage technology at scale. His work focuses on the practical implementation of AI Standards—ISO/IEC SC 42, NIST AI RMF and emerging EU AI Act requirements—within real enterprise environments where documentation gaps, architectural drift and weak oversight routinely obstruct AI maturity.

He is the creator of the AI Standards Index™, a global benchmark measuring how well organizations operationalize AI governance, data quality and lifecycle discipline. He is also the author of *The Standards Effect™*, a framework that explains how standards reduce complexity and improve decision-making inside modern enterprises.

Kadir leads ins-pi, a company focused on enterprise architecture and transformation tooling. His research brings together formal standards, architectural rigor and the operational realities of large-scale AI programs, providing organizations with methods that close the gap between policy intent and actual implementation.

Executive Summary

Global AI Standards maturity sits at **41%**, a level where organizations deploy AI at scale but cannot consistently prove how those systems were built, validated, or governed. The Index exposes the structural gap between policy and execution: most enterprises reference ISO/IEC 23053 lifecycle principles and the documentation expectations of EU AI Act Articles 10–12, but few enforce them. The result is predictable. AI systems run in production while evidence of lineage, risk controls, and design rationale sits in disconnected tools—or does not exist at all.

The dimensional scores show where the system breaks down. Vision & Leadership reaches **48%**, supported by clear executive intent. Tools & Automation (**46%**) and workforce capability (**44%**) also show investment. But the operational core is weak. Data Quality drops to **38%** because many teams still manage lineage in spreadsheets or undocumented pipelines, violating ISO/IEC 24028 transparency expectations. Architecture & Reuse sits at **35%**, reflecting inconsistent design patterns and one-off integrations that make reproducibility difficult. Culture is the lowest at **33%**. Standards are written, but teams bypass governance gates when deadlines hit.

Industry results follow the same pattern. Finance (**52%**), Pharmaceuticals (**50%**) and Telecommunications (**47%**) perform better because regulators require traceability and documented controls. Retail (**30%**) has the lowest maturity; most environments lack the data discipline or architectural consistency required for ISO/IEC 23894 risk management. Manufacturing and the Public Sector remain stalled by fragmented accountability and legacy systems that prevent any meaningful enforcement of lifecycle evidence.

Regional performance exposes another layer of imbalance. North America leads at **55%**, with Western Europe close behind at **47%** due to earlier regulatory pressure and higher readiness for conformity documentation. Asia-Pacific (**41%**) and the Middle East (**40%**) show progress but inconsistent standard adoption inside organizations. Latin America is lower at **38%**, with significant documentation and capability gaps. Africa establishes the lower boundary at **29%**, highlighting how documentation, lineage evidence, and governance practices remain at early-stage maturity. This uneven foundation makes global interoperability difficult.

The consequence is straightforward. With AI scaling faster than lifecycle governance, organizations accumulate risk they cannot easily unwind. Many would struggle to satisfy EU AI Act conformity assessments because evidence is incomplete or scattered. Architecture drift makes reproducibility unreliable. Cultural resistance turns standards into optional guidance rather than enforceable rules. These maturity levels do not reflect a lack of funding or talent; they reflect inconsistent oversight.

To move beyond the **Operational** plateau, leadership must treat standards as conditions for deployment—not advisory material. Lifecycle documentation must be mandatory. Data controls must meet evidence requirements. Architectural divergence must stop.

Governance gates must hold, even when delivery pressure rises. Without these changes, maturity will not improve, and AI will remain a high-exposure capability rather than a governed one.

The AI Standards Index™ 2025 establishes the first empirical baseline for this readiness gap across 30 countries. It shows where organizations stand, where they fall short, and what must be corrected before AI can be governed, audited, or scaled responsibly.

Key Metrics at a Glance

The following summary distills the essential metrics of the Index, where global maturity stands today, where the strongest and weakest capabilities lie, and which regions and industries are leading or lagging.

Key Metric	Score	Description
AI Standards Index 2025:		
Global Maturity Score	**41%**	Operational maturity; standards exist but are inconsistently applied.
Lowest-Maturity Dimension:		
Culture & Behavior	**33%**	Indicates weak adherence to standards in day-to-day decision-making.
Highest-Maturity Dimensions:		
Vision & Leadership	**48%**	Leadership alignment and clear role definitions improve consistency of standards.
Tools & Automation	**46%**	Unified toolchains reduce manual work and enforce lifecycle controls.
Industry Leaders:		
Finance	**52%**	Strong governance pressure and mandated documentation drive maturity.
Industry Laggard:		
Retail	**30%**	Fragmented data practices and limited standardization.
Regional Leader:		
North America	**55%**	Highest structural readiness and governance depth.
Regional Laggard:		
Africa	**29%**	Early-stage standards adoption and limited documentation maturity.
Dataset Size:		
Organizations	**250**	Representing C-level, governance, architecture, and AI leadership roles.
Countries	**30**	

Table of Contents

How to Interpret the Index

The AI Standards Index™ measures whether organizations apply the controls defined in modern AI standards with enough consistency to produce evidence. It does not evaluate model quality or technical performance. It evaluates whether leaders, architects and developers follow the lifecycle, documentation and accountability requirements described in ISO/IEC 23053, ISO/IEC 23894, the NIST AI RMF and the EU AI Act. Every score in this Index reflects operational behavior, not stated policy.

Figure 1: Five-Level AI Standards Maturity Model

The Index uses a five-level maturity scale ranging from **Chaos** to **Transformational** (*see Scoring Framework page 34*). These levels map to observable practices. Chaos indicates that evidence is missing or fragmented. Foundational means policies exist, but teams bypass them. Operational—the global average at 41%—means controls are partially used but not enforced. Integrated maturity appears only when lifecycle steps follow one standard pattern. Transformational maturity requires cultural adoption: teams treat standards as the default, not an obligation.

Scores are normalized to a 0–100 scale to expose differences across dimensions, industries and regions. The interpretation is straightforward: the spread matters more than the average. A high score in one dimension does not offset a low score in another. Strong performance in Vision & Leadership or Tools & Automation often reflects investment, not discipline. Conversely, weak Data Quality or Culture scores show where standards fail in practice—missing lineage, undocumented assumptions, inconsistent approvals or drift monitoring that exists only on paper.

Comparisons across industries and regions should be read as indicators of **evidence discipline**, not compliance. A higher score means an organization can more reliably demonstrate how AI systems were designed, validated and deployed. It does not imply full conformity with EU AI Act Articles 10–12 or with ISO/IEC 23053 lifecycle requirements. Regionally, high scores reflect earlier regulatory pressure or more mature digital infrastructures; lower scores reflect gaps in documentation, capability or execution. Africa's lower bound at 29% is offering a clearer picture of global variability.

The Index is a benchmark, not a certificate. It highlights where organizations can produce consistent lifecycle evidence and where they rely on informal practices. A strong score indicates readiness for scale; a weak score indicates structural risk. Interpreting the Index correctly means understanding that maturity is not about ambition or tooling. It is about whether standards are applied reliably enough that an external reviewer could reconstruct decisions, assess risks and trace model behavior without guesswork.

Why Standards Matter in 2025

By 2025, AI systems sit inside processes that decide credit limits, diagnose patients, trigger operational workflows and influence public services. Most enterprises built these systems faster than they built the controls required to govern them. The pattern repeats across organizations: undocumented model assumptions, missing lineage, approvals handled informally and risk assessments produced only when someone asks for them. The pace of deployment has outstripped the discipline needed to make AI verifiable, traceable and defensible.

Regulators have already codified what "good" must look like. The **EU AI Act** requires documented data quality, traceability and lifecycle oversight for high-risk systems (Articles 10–12). **ISO/IEC 23053** defines the lifecycle evidence organizations must produce, not just reference. **ISO/IEC 23894** demands risk controls that can be demonstrated, not implied. The **NIST AI RMF** assigns accountability to leadership, not to individual developers. These expectations are explicit, and they expose the gap between what enterprises believe they are doing and what standards require them to prove.

Inside organizations, the failure is structural, not conceptual. Policies exist, but adoption is inconsistent. Documentation standards vary by team. Architecture decisions lack traceability. Cultural resistance turns governance into an optional step. This is why the Index registers **Data Quality at 38%**, **Architecture at 35%**, and **Culture at 33%**. These numbers reflect how work is actually done: lineage tracked in spreadsheets, model decisions left undocumented, governance gates bypassed to meet sprint deadlines.

Standards matter because they remove ambiguity. They specify when evidence must be created, how it must be maintained and who is accountable for approving it. They force consistency across teams so that AI systems can be audited, monitored and reproduced. Without standards, organizations cannot meet regulatory scrutiny, cannot defend high-impact decisions and cannot scale AI without accumulating risk that eventually becomes unmanageable.

The AI Standards Index™ quantifies this gap. It measures the distance between the formal requirements defined by global standards and the operational reality inside enterprises. It shows where governance collapses, where documentation is unreliable and where leaders rely on assumptions rather than evidence. The Index does not measure ambition. It measures whether organizations can operate AI systems in a way that survives audit and scale. In 2025, that capability is no longer optional. It is the baseline for responsible AI deployment.

Objectives of the AI Standards Index™

Most organizations deploy AI faster than they establish the controls required to govern it. Standards from ISO/IEC SC 42, the NIST AI RMF, the OECD Principles and the EU AI Act define what trustworthy AI demands, but they do not tell enterprises how far they are from meeting those requirements. Policies exist on paper, tooling is implemented unevenly and documentation varies by team. Leaders rarely have a reliable way to see whether standards are applied with enough consistency to support scale, audit or regulatory scrutiny.

The AI Standards Index™ was created to close this gap. It provides a measurable, evidence-based assessment of how deeply AI standards are embedded into seven operational dimensions: leadership alignment, data quality, governance processes, architecture, skills, tooling and culture. The Index translates formal standards into indicators that can be observed, scored and compared, turning abstract requirements into practical maturity signals. It is not concerned with ambition or stated policy; it measures whether organizations can produce the lifecycle evidence required by modern AI regulation and international standards.

Fragmentation is the core issue the Index confronts. Documentation is incomplete, governance gates are inconsistent and risk reviews are often retrospective rather than systematic. Many high-impact AI failures originate not in the models but in these gaps: missing assumptions, undocumented data lineage, architectural drift or unclear accountability. By providing a unified scoring model, the Index enables cross-industry and regional comparison and establishes a baseline that can be tracked over time. It gives organizations a grounded understanding of where their operational discipline breaks down.

This report explains the purpose and methodology of the Index and the logic used to convert global standards into a repeatable maturity model. It describes how maturity scores are derived, how each dimension functions and how leaders should interpret the results when assessing readiness for scale or exposure to regulatory requirements.

The Index is guided by three research questions:

RQ1: What is the global state of AI Standards maturity across industries and regions?
RQ2: Which dimensions show the largest readiness gaps, and what operational behaviors drive those gaps?
RQ3: How do industry characteristics, regulatory pressure and organizational scale influence maturity?

To answer these questions, the AI Standards Index™ aims to:

- Define measurable indicators that reflect how reliably organizations apply standards in practice.
- Benchmark enterprises against internationally recognized lifecycle, documentation and risk-management requirements.
- Give leaders objective insight into where structural weaknesses exist and where investment will have the most impact.

Through these objectives, the Index establishes a reference point for enterprises and policymakers seeking to build the operational discipline required for responsible, auditable and scalable AI.

Limitations

The AI Standards Index™ measures whether organizations apply the controls defined by international AI standards with enough consistency to produce evidence. It does not certify compliance, assess legal readiness or evaluate the quality of AI models. The Index focuses on operational behavior: how organizations document lineage, manage risk, approve lifecycle stages and maintain architectural discipline.

Several limitations define the boundaries of this assessment. In some regions and industries, publicly available information is limited, requiring modeled estimates based on expert review. Self-reported inputs introduce bias, especially when organizations overstate documentation quality or the consistency of governance processes. Evidence is often incomplete; many enterprises maintain policies but lack the artifacts needed to validate adherence. Regulatory maturity differs sharply across regions, which affects comparability: an organization operating under the EU AI Act faces obligations that do not yet exist in other markets. There is also a timing gap between new standards and operational adoption; many organizations update policies long before they update practice.

These constraints define the boundaries of what the Index measures; they do not diminish its ability to expose structural weaknesses. It is a directional benchmark that exposes structural gaps in governance, data discipline, architecture and culture. It should inform prioritization, investment and oversight—not be used as proof of conformity with EU AI Act requirements or ISO/IEC lifecycle controls. As standards evolve and future editions incorporate broader datasets, the precision and granularity of the Index will increase.

Benchmark Overview

Public data from the OECD, ISO/IEC SC 42, NIST and EU regulatory bodies all indicate the same structural issue: AI deployment is rising faster than the governance needed to support it. Adoption now exceeds 55%, yet fewer than 20% of organizations report lifecycle controls or documentation practices aligned with ISO/IEC 23053, ISO/IEC 23894 or the EU AI Act. Most enterprises operate production models with incomplete lineage, informal approvals or inconsistent monitoring.

To measure how this gap operates inside real organizations, the AI Standards Index™ 2025 combines global data with **direct inputs from 250 organizations across 30 countries**, including North America, Western Europe, Asia-Pacific, the Middle East, Latin America and Africa. This dataset provides operational evidence that has been largely missing from public reporting: how standards are applied in practice, how often documentation is incomplete and where governance steps break down.

Until now, no unified maturity assessment existed to compare organizational readiness against international standards or to evaluate differences across industries and regions. The Index addresses that gap. It translates the requirements defined by ISO/IEC SC 42, the NIST AI RMF, the OECD AI Principles and the EU AI Act into a structured measurement model and applies it consistently across all 250 organizations. The result is the first empirical baseline of global AI Standards maturity—evidence of how organizations actually operate, not how they describe their intentions.

Global Results

The AI Standards Index™ 2025 establishes a global maturity score of **41/100**, placing most organizations at the **Operational** level. This reflects partial adoption of standards-aligned practices without consistent enforcement. Policies exist, tools are in place and leadership intent is visible, but lifecycle discipline, documentation quality and cultural adherence remain unreliable across environments.

The distribution across the seven dimensions exposes where operational breakdowns occur:

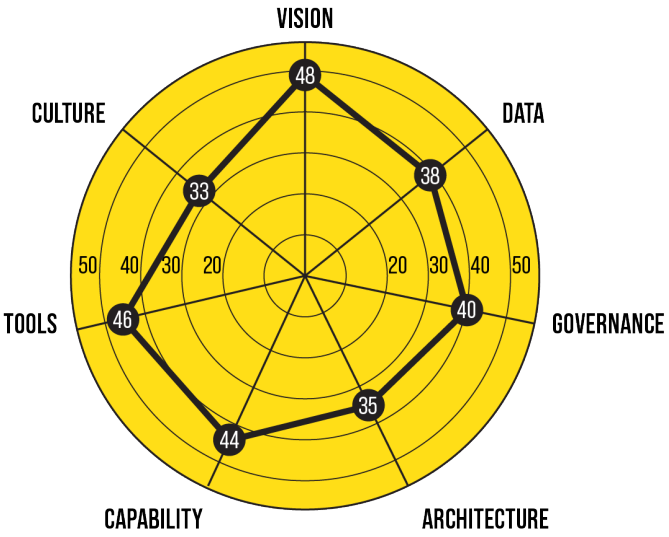


Figure 2: Global AI Standards Maturity by Dimension (n=250)

Dimension	Score
Vision & Leadership Alignment	48
Tools & Automation	46
Capability & Skills	44
Governance & Process	40
Data Quality & Documentation	38
Architecture & Reusability	35
Culture & Behavior	33
Global Average (7 Dimensions)	**41**

Vision & Leadership, Tools & Automation and Capability & Skills form the upper tier, showing where organizations have invested. The lower tier—Data Quality, Architecture and Culture—shows where standards fail in practice. Missing lineage, informal approvals, inconsistent design decisions and weak behavioral adherence remain persistent friction points.

The global score does not describe aspiration; it describes the level of evidence organizations can produce. A maturity of 41% means AI is deployed widely, but the controls required by ISO/IEC 23053, ISO/IEC 23894, NIST AI RMF and EU AI Act Articles 10–12 are only partially implemented and rarely enforced with consistency.

Industry Benchmark Results

Maturity varies sharply across industries, driven by differences in regulatory pressure, operational risk and the level of discipline required to maintain audit-ready evidence. The Index shows the following distribution:

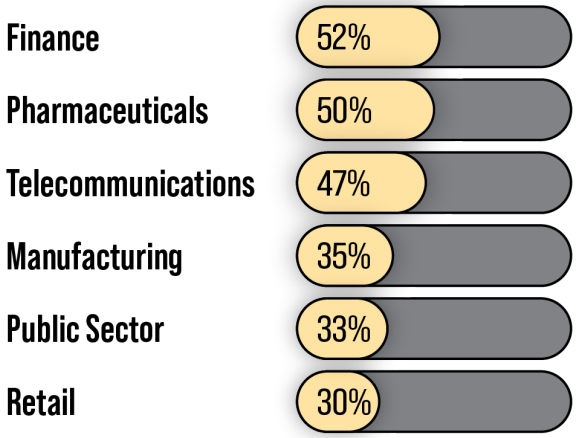


Figure 3: Industry Maturity Scores (n=250)

Industry	Score
Finance	52
Pharmaceuticals	50
Telecommunications	47
Manufacturing	35
Public Sector	33
Retail	30
Industry Average	**41**

The upper tier—Finance, Pharmaceuticals and Telecommunications—reflects sectors where regulators expect traceability, documented controls and clear accountability paths. These industries already maintain evidence for audits, so lifecycle documentation and risk reviews are less likely to be optional or improvised. Their higher scores indicate that standards are enforced, not merely referenced.

The lower tier shows the opposite pattern. Manufacturing and the Public Sector operate with fragmented processes and legacy systems that make consistent documentation difficult. Retail anchors the bottom at **30%**, where data quality varies widely, architectural patterns are inconsistent and governance steps are often bypassed to meet operational demands. In these sectors, standards fail not because they are unclear, but because the underlying processes cannot support them.

The gap across industries shows that readiness is determined less by AI ambition and more by whether an industry has the structural discipline to generate and maintain evidence.

Regional Benchmark Results

Regional maturity reflects how consistently organizations can produce the evidence required by international AI standards. The Index shows wide variation:

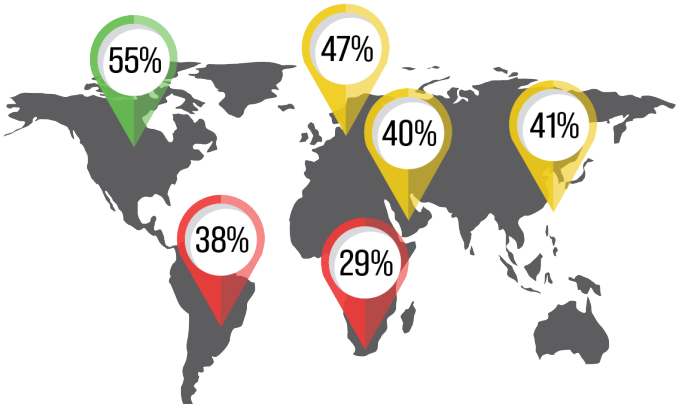


Figure 4: Regional Maturity Scores (n=250)

Region	Score
North America	55
Western Europe	47
Asia-Pacific	41
Middle East	40
Latin America	38
Africa	29
Region Average	**41**

North America leads at **55%**, driven by earlier adoption of formal governance processes and stronger pressure to document model lineage, risk controls and lifecycle decisions. Western Europe follows at **47%**, influenced by the requirements introduced through the EU AI Act, which has pushed organizations to strengthen documentation and traceability even before full enforcement.

Asia-Pacific and the Middle East sit near the global baseline but for different reasons. Asia-Pacific includes markets with mature digital ecosystems alongside others where documentation and architectural consistency remain uneven. In the Middle East, investment is high, but standards adoption varies by sector and by the degree of central oversight.

Latin America scores **38%**, where governance structures and documentation practices are still developing. Africa enters the Index for the first time at **29%**, establishing a clear lower bound. In both regions, lineage evidence, risk logs and architectural documentation are either incomplete or inconsistently maintained, making it difficult to satisfy the lifecycle controls defined in ISO/IEC 23053 or the data requirements of EU AI Act Articles 10–12.

Regional differences do not measure ambition or innovation. They measure how reliably organizations can demonstrate the controls that international standards require.

Key Findings

The Index exposes five structural patterns that define the current state of AI Standards maturity:

1. Governance, Data and Culture anchor the bottom of the maturity curve.
Scores of **40%** for Governance & Process, **38%** for Data Quality and **33%** for Culture show where standards break down in practice. Missing lineage, informal approvals and inconsistent documentation reveal that organizations struggle most at the points where standards require evidence. These weaknesses make lifecycle evidence incomplete and fail the expectations defined in ISO/IEC 23053 and EU AI Act Articles 10–12.

2. Regulation is the strongest driver of maturity.
Finance (**52%**) and Pharmaceuticals (**50%**) lead because they already operate under environments where traceability and documentation are non-negotiable. Their higher scores reflect enforcement, not ambition. Less regulated sectors—Retail (**30%**) and Manufacturing (**35%**)—show how quickly maturity drops when evidence discipline is optional.

3. Culture remains the most persistent obstacle.
The 15-point gap between Leadership (**48%**) and Culture (**33%**) demonstrates that organizations adopt tools and policies faster than they change behavior. Governance collapses when teams bypass documentation to meet delivery deadlines. Culture lags technical capability by **25–40%**, creating a predictable pattern: standards exist, but they are not followed when pressure increases.

4. The global enterprise landscape is not prepared for high-risk AI deployment.
A global maturity of **41%** indicates that most organizations cannot yet demonstrate the lifecycle evidence required for high-risk systems. Even the strongest regions and industries fall short of integrated maturity. The gap is not technical—it is structural. Most enterprises can build AI; far fewer can prove how those systems were designed, validated or monitored.

5. Standards adoption is the clearest predictor of scalable and resilient AI.
Where data controls, reference architectures, governance gates and cultural accountability are enforced, organizations show higher scores and greater readiness for scale. Where these foundations are weak, AI initiatives remain fragile, difficult to audit and exposed to operational and regulatory failure.

Taken together, these findings show that the constraints organizations face are not model-related. They are documentation-related, process-related and culture-related. The Index makes these constraints visible and defines the priorities leaders must address to move from isolated AI efforts to governed, auditable and enterprise-wide AI systems.

Leadership Implications

The Index shows a simple reality: AI fails when standards are optional. The maturity gaps across Data, Architecture and Culture are not technical problems. They are leadership problems. Executives must decide whether standards are enforced or ignored, because the data makes clear that organizations drift toward inconsistency when governance depends on individual teams.

The first requirement is **accountability**. Without a single function that owns AI standards, lifecycle controls fracture. Documentation formats differ by team, risk assessments are inconsistent and approvals occur informally. An AI Standards Office, or an equivalent governance authority, is the only structure that can create uniformity across development, validation and deployment. ISO/IEC 23053 and the NIST AI RMF assume centralized oversight; most organizations do not have it.

The second requirement is **data discipline**. A score of 38% in Data Quality shows how often lineage is incomplete, assumptions go undocumented and dataset decisions are not reviewable. Leaders cannot delegate this to IT. AI systems cannot meet the evidence expectations of EU AI Act Articles 10–12 if the underlying data is unreliable or undocumented. Executives must elevate data governance to a board-level concern.

Architecture is the next structural gap. A maturity of 35% indicates that organizations are still building one-off solutions with no standard patterns, no reuse and no traceability. This prevents audit, slows scale and increases risk. Leadership must mandate reference architectures and enforce reuse. Without architectural discipline, no governance framework can hold.

Capability development also becomes a strategic obligation. Governance fails when teams do not understand the standards they are expected to follow. Training cannot focus only on technical roles. Business leaders, risk teams, compliance officers and operators must all understand lifecycle evidence, risk controls and documentation requirements. Without this breadth of literacy, standards remain theoretical.

Finally, **culture** is the hardest—and most critical—leadership responsibility. The 15-point gap between Leadership and Culture shows that teams know what should happen but do not do it consistently. Documentation is skipped under deadline pressure. Governance gates are treated as advisory. Ethical considerations surface only when raised explicitly. Leaders must enforce a culture where evidence is routine, not extraordinary; where undocumented models cannot ship; and where accountability is shared, not avoided.

The implication for executives is direct: organizations that institutionalize standards will scale AI with control and resiliency. Those that continue treating standards as guidance will face mounting regulatory exposure, operational fragility and limited ability to deploy high-risk AI systems. Maturity begins with leadership choices, not technical capability.

What Organizations Should Do Next

Raising AI maturity requires replacing informal practices with enforceable systems. Most organizations already know what should happen; the Index shows how often it fails to happen. Closing that gap begins with operational discipline, not new technology.

The first step is to strengthen the foundations that support lifecycle evidence. Documentation must be standardized and mandatory. Model decisions, data assumptions and validation steps must be recorded in formats that can be reviewed, audited and reproduced. Data lineage must move out of spreadsheets and into controlled processes. Without this baseline, organizations cannot meet the requirements of ISO/IEC 23053 or the evidence expectations of the EU AI Act.

Architecture must be the next point of correction. Fragmented patterns create fragmented governance. Reference architectures, component reuse and controlled integration standards are essential for eliminating unnecessary variation and ensuring that AI systems behave consistently across teams. Architectural enforcement is what allows governance to scale.

Organizations also need mechanisms for continuous adjustment. Standards evolve, and governance systems must evolve with them. Lightweight checkpoints, automation of documentation tasks and embedded compliance signals inside development workflows reduce friction and expose failures early. These changes do not add bureaucracy; they prevent the chaos that emerges when governance is retrofitted after deployment.

Capability development is equally non-negotiable. Teams cannot follow standards they do not understand. Training must expose non-technical leaders to the evidence obligations they ultimately approve. Shared language and shared expectations remove ambiguity and reduce the need for governance escalation.

Culture determines whether any of this holds. A maturity of 33% in Culture shows that documentation is skipped when deadlines tighten and governance gates collapse when challenged. Leaders must create conditions where undocumented models cannot ship, where risk discussions are routine and where accountability is distributed rather than avoided. Without cultural adherence, every other investment remains fragile.

The organizations that act on these structural requirements will progress from Operational maturity to Integrated maturity. Those that continue relying on informal practices will not. The path forward is defined not by ambition, but by the consistency with which standards are applied.

AI Standards Roadmap for Enterprises

The AI Standards Index™ 2025 shows that AI adoption is accelerating faster than the structures required to govern it. Organizations can deploy models, but most cannot demonstrate how those models were designed, validated or monitored. “Good” in enterprise AI is defined not by algorithmic sophistication but by the reliability and repeatability of the standards that guide lifecycle decisions. Mature enterprises build systems where evidence is created automatically, decisions are traceable and governance is applied the same way every time.

This chapter outlines what strong standards-aligned practice looks like under ISO/IEC SC 42, the NIST AI RMF, the OECD AI Principles and the EU AI Act, and provides a roadmap for progressing from Operational maturity to Integrated and Transformational maturity.

Characteristics of a Mature AI Enterprise

Enterprises with high AI Standards maturity behave differently across leadership, data, governance, architecture, tooling, skills and culture. What follows are **observable conditions**, not aspirational statements.

1. Vision & Leadership Alignment

Observable Conditions

- Leadership sets the direction for AI and enforces it.
- Decision rights and accountability for AI risk, approval and oversight are assigned to named roles.
- AI terms and concepts follow **ISO/IEC 22989**, eliminating ambiguity across functions.
- Investment, risk and design decisions move through a structured governance path.

Standards Basis

- **NIST AI RMF – Govern** requires accountable leadership.
- **OECD Accountability Principle** links leadership involvement to trustworthiness.

2. Data Quality & Documentation Standards

Observable Conditions

- Data lineage, metadata and documentation exist for every dataset used in training, validation and monitoring.
- Bias controls and data constraints are recorded and reviewable.
- Documentation artifacts are consistent across teams and reusable across projects.
- Evidence logs are maintained—data changes, assumptions, exclusions.

Standards Basis

- **EU AI Act Articles 10–12** require traceability and documented data quality.
- **ISO/IEC 23894** defines risk management evidence.
- **ISO/IEC 24027** requires bias detection and mitigation documentation.

3. Governance & Process Standards

Observable Conditions

- The AI lifecycle follows one pattern across the enterprise: ideation → data → model → validation → deployment → monitoring → retirement.
- Every phase contains a formal checkpoint.
- Approval gates are mandatory, documented and enforced.
- Risk assessments are routine and publicly reviewable internally.
- Decisions are traceable: requirements to output, output to decision, decision to documentation.

Standards Basis

- **ISO/IEC 23053** defines the lifecycle and evidence required at each stage.
- **ISO/IEC 24668** assigns process management obligations.
- **NIST AI RMF** requires continuous oversight (Map → Measure → Manage).

4. Architecture & Reusability Standards

Observable Conditions

- A reference architecture governs how AI systems are designed, integrated and monitored.
- Models, features, pipelines and interfaces are built as reusable components.
- Integration patterns are standardized; exceptions require approval.
- Architectural drift is monitored and corrected.
- Decisions on architecture are documented in a consistent format.

Standards Basis

- **ISO/IEC 23053** requires architectural traceability.
- **ISO/IEC 22989** defines modularity and conceptual clarity.

5. Capability & Skills Alignment

Observable Conditions

- Roles are defined to separate development, validation and operation.
- Teams understand the lifecycle, documentation requirements and risk obligations.
- Training covers governance, not just model development.
- Business, compliance and operations teams share the same vocabulary and expectations.

Standards Basis

- **NIST AI RMF – Govern** requires human competence for trustworthy AI.
- **OECD Principles** reference the need for organizational capability.

6. Tooling & Automation Standards

Observable Conditions

- Tooling enforces governance; it does not rely on human discipline alone.
- Versioning, monitoring and validation are automated where possible.
- Documentation is generated as part of the workflow, not after the fact.
- Model lineage, metrics and risk logs are stored in durable systems, not in personal files or ad-hoc tools.
- Compliance signals appear in the development pipeline and block deployment when missing.

Standards Basis

- **EU AI Act** requires durable documentation and automated risk logging for high-risk AI.
- **ISO/IEC 23053** mandates consistent pipeline and monitoring practices.

7. Culture & Behavioral Standards

Observable Conditions

- Teams follow standards even under delivery pressure.
- Undocumented models do not ship.
- Risk discussions are routine and surfaced early.
- “Shadow AI” is detected and reduced.
- Documentation and verification are treated as part of the job, not administrative work.

Standards Basis

- **OECD Principles** emphasize accountable human behavior.
- **NIST AI RMF** identifies culture as the determining factor in whether governance holds.

Standards-Aligned Enterprise AI Rollout Roadmap

The Index makes it clear that AI maturity improves only when organizations replace informal practices with enforceable systems. The roadmap below outlines how enterprises progress from experimentation to sustainable, standards-driven AI. It mirrors the four maturity transitions measured in the Index—**Standardize, Build, Scale, Sustain**—and embeds expectations from ISO/IEC SC 42, the NIST AI RMF, the OECD AI Principles and the EU AI Act.

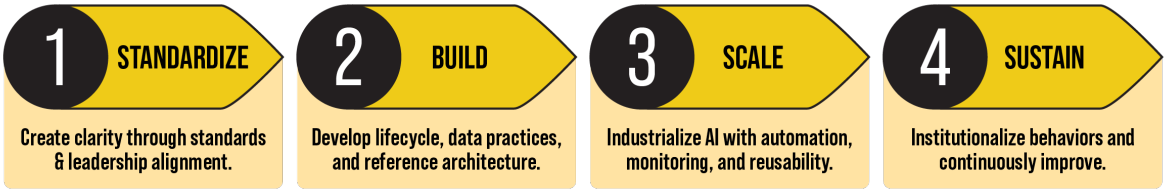


Figure 5: Enterprise AI Rollout Roadmap (Standards-Aligned)

Stage 1 — Standardize (Chaos → Foundational)

Objective: Create clarity, define ownership and establish non-negotiable standards.

Required Actions

- Define enterprise AI terminology according to **ISO/IEC 22989**.
- Assign accountable executive ownership as required by **NIST AI RMF – Govern**.
- Establish baseline AI policies, risk statements and lifecycle expectations.
- Inventory all AI, analytics, automation and decision-intelligence systems.
- Form an AI Standards Office or equivalent body to enforce consistency.

Structural Indicator

Work is no longer ad hoc. Language, ownership and expectations stabilize.

Stage 2 — Build (Foundational → Operational)

Objective: Establish lifecycle discipline, data controls and architectural coherence.

Required Actions

- Formalize the AI lifecycle with mandatory documentation and checkpoints (**ISO/IEC 23053**).
- Implement standardized data documentation, lineage and quality controls aligned to **EU AI Act Articles 10–12**.
- Introduce governance gates for approvals, risk reviews and traceability checks.
- Create the first version of the enterprise AI reference architecture.
- Deliver mandatory governance and risk training across technical and non-technical roles.

Structural Indicator

Lifecycle evidence exists. Documentation and governance steps are performed consistently, not optionally.

Stage 3 — Scale (Operational → Integrated)

Objective: Industrialize AI with automation, monitoring and disciplined reuse.

Required Actions

- Automate compliance tasks and risk logging consistent with **NIST AI RMF – Manage**.
- Implement drift, bias and anomaly monitoring pipelines following **ISO/IEC 24027**.
- Standardize and reuse components—pipelines, features, interfaces, models.
- Deploy a unified toolchain that enforces versioning, traceability and documentation.
- Establish cross-functional capability frameworks that define roles and reduce ambiguity.

Structural Indicator
AI development follows the same lifecycle steps regardless of team. Systems are scalable, auditable and reproducible.

Stage 4 — Sustain (Integrated → Transformational)

Objective: Institutionalize standards and create continuous, evidence-driven improvement.

Required Actions

- Embed standards into investment, budgeting and portfolio decisions.
- Use incidents, monitoring data and audit findings to drive routine adjustments.
- Reinforce and reward adherence to documentation and lifecycle discipline.
- Ensure all AI initiatives follow the same lifecycle without exception.
- Adopt **AiPM™** (Artificial Intelligence Portfolio Management) to control prioritization and scale.

Structural Indicator
Standards hold under pressure. AI becomes predictable, defensible and sustainable.

The Ideal Enterprise AI Rollout Model

A mature AI enterprise operates with the following characteristics:

1. AI is aligned to business strategy and bounded by risk appetite.
2. Every AI initiative and model enters through a governed portfolio (AiPM™).
3. A single lifecycle governs design, development, deployment and monitoring.
4. Documentation is generated automatically as part of the workflow, not recreated later.
5. Reference architectures enforce reuse and interoperability.
6. Monitoring pipelines maintain trustworthiness throughout the lifecycle.
7. Culture reinforces transparency, accountability and disciplined execution.

This model reflects the requirements of ISO/IEC SC 42, the NIST AI RMF, the OECD Principles and the EU AI Act and represents the operational conditions needed to scale AI responsibly.

Why Organizations That Implement This Roadmap Win

Organizations that follow this roadmap gain structural advantages:

- Lower operational and regulatory risk.
- Higher reliability in deployment and fewer project failures.
- Creation of reusable assets instead of isolated experiments.
- Readiness for EU AI Act evidence requirements and audits.
- Greater trust from regulators, auditors, customers and internal stakeholders.
- Improved ability to attract and retain skilled AI and data professionals.

Most importantly, they convert AI from isolated activity into a governed, enterprise-wide capability that can scale without accumulating unmanaged risk.

Methodology

Purpose of the AI Standards Index

The AI Standards Index™ provides a measurable way to determine whether organizations apply the controls defined in international AI standards. It does not evaluate model performance. It evaluates whether leadership, data teams, architects and operators produce the evidence required for lifecycle traceability, documented risk management and accountable decision-making. The Index converts the requirements of ISO/IEC SC 42, the NIST AI RMF, the OECD AI Principles and the EU AI Act into a score from 0 to 100 that reflects operational readiness, not stated intent.

Organizations across industries publish policies but rarely measure how consistently those policies are followed. The Index was created to expose that gap. It offers a standardized maturity model that reveals where standards break down—in data practices, governance, architecture, tooling, skills and culture. The score enables comparison across industries and regions and provides a baseline for understanding whether enterprises can meet international evidence expectations.

The Index is designed to:

- Establish a global baseline for evaluating the operational use of AI standards.
- Provide comparability across industries, regions and organizational sizes.
- Identify structural weaknesses in data lineage, documentation, architecture, governance and culture.
- Help leaders allocate investment toward controls that reduce risk and increase reproducibility.
- Track changes in maturity over time as standards evolve and regulatory pressure increases.

By transforming formal standards into observable maturity indicators, the Index defines the discipline of **AI Standards Management**—the consistent application of evidence, documentation, control points and lifecycle rigor across enterprise AI systems.

Foundation in International Standards

The AI Standards Index™ is built on requirements drawn directly from the world's primary AI governance frameworks. These standards define the evidence organizations must produce to demonstrate traceability, responsible risk handling and lifecycle discipline. The Index operationalizes these requirements into questions that can be scored consistently across organizations.

ISO/IEC JTC 1 SC 42 – Artificial Intelligence

ISO/IEC 22989 — Concepts & Terminology
Establishes unified terminology needed for consistent governance and architectural clarity.

ISO/IEC 23053 — AI Systems Machine Learning Framework
Defines the lifecycle and the artifacts required at each stage, providing the basis for process governance.

ISO/IEC 23894 — AI Risk Management
Specifies documentation expectations for risk handling, incident evidence and control measures.

ISO/IEC TR 24028 — Trustworthiness in AI
Addresses robustness, transparency and reliability requirements.

ISO/IEC 24027 — Bias in AI Systems
Defines expectations for identifying and documenting data and model bias.

ISO/IEC 24668 — AI Process Management
Formalizes requirements for reproducibility and process-level evidence.

NIST AI Risk Management Framework (AI RMF 1.0)

NIST provides the most widely referenced operational model for risk management:

- **Govern** — Assigns accountability and oversight.
- **Map** — Defines system context and purpose.
- **Measure** — Assesses risk, trustworthiness and impact.
- **Manage** — Implements controls, monitors and adjusts.

These functions form a practical structure for evaluating whether an organization applies governance obligations consistently.

OECD AI Principles

Globally recognized expectations for responsible AI:

- Human-centered values
- Transparency and explainability
- Robustness and safety
- Accountability

These principles set the ethical floor for standards-aligned operations.

EU AI Act (2024/2025)

The EU AI Act introduces binding legal obligations for high-risk AI:

- Documented risk management
- Data governance and quality evidence
- Traceability and lifecycle documentation
- Conformity assessment
- Post-market monitoring and reporting

These obligations reinforce the requirement for durable evidence—not policy statements. Together, these frameworks define the global baseline for responsible AI. The Index translates their requirements into maturity indicators that reveal how far organizations are from consistent, repeatable and enforceable standards adoption.

Methodology Overview

The AI Standards Index™ applies a structured, multi-stage method to convert international AI standards into a measurable maturity score. The methodology evaluates whether organizations produce consistent, auditable evidence across leadership, governance, data, architecture, tooling, workforce capability and culture.

1. Data collection through questionnaire, interviews and documentation review

Organizations provide structured responses, supporting documentation and expert insights. Cross-validation reduces reliance on any single source and exposes inconsistencies between stated and observed practice.

2. Maturity scoring using a five-level scale (1–5)

Each item is scored on observable behavior, not aspiration (*see Scoring Framework page 34*).

- Level 1: Evidence missing or inconsistent
- Level 3: Evidence exists but is not routinely enforced
- Level 5: Evidence is complete, traceable and continuously maintained

3. Aggregation into seven dimension averages

Scores for individual items are grouped under the seven dimensions of the Index. This reveals patterns of weakness—such as documentation gaps or architectural inconsistency—that cannot be seen in isolated questions.

4. Normalization to a 0–100 scale

Scores are normalized to create a common benchmark across dimensions, industries and regions. This ensures meaningful comparison even when organizations have different internal structures.

5. Weighting based on standards-driven risk priorities

Dimensions are weighted to reflect their importance in international standards and regulatory requirements. Data quality, documentation, lifecycle governance and accountability carry higher weight because failures in these areas produce the largest operational and regulatory risks.

6. Composite score generation and maturity classification

Weighted scores are combined into a single maturity rating and mapped to one of five levels: Chaos, Foundational, Operational, Integrated or Transformational. The level reflects the degree to which standards are applied with consistency and enforceability across the enterprise.

Global Data Coverage & Sample Distribution

The AI Standards Index™ 2025 is based on data from **250 organizations across 30 countries**. The sample reflects entities most affected by international AI standards and regulatory requirements, including ISO/IEC SC 42, the NIST AI RMF, the OECD AI Principles and the EU AI Act. The dataset focuses on organizations where AI governance is not theoretical but operational—where decisions about traceability, documentation, risk controls and lifecycle oversight must occur in practice.

Inputs come from senior leaders responsible for AI governance, enterprise architecture, data oversight and operational risk. This ensures that results reflect how decisions are made and enforced, not how they are described in policy documents.

Role Breakdown

- C-Suite Executives (CIO, CDAO, CAIO, CTO) — **15%**
- VP / Director of AI, Data, or Analytics — **45%**
- Enterprise Architects & Governance Leaders — **25%**
- Lead Data Scientists / ML Engineers — **15%**

These roles are directly accountable for lifecycle documentation, architectural decisions, governance gates and data controls—the areas where standards adoption succeeds or fails.

Enterprise Size

- Large enterprises (revenue > $1B) — **55%**
- Mid-size enterprises — **30%**
- Public sector agencies — **15%**

The distribution reflects organizations with the greatest exposure to regulatory scrutiny and the highest operational dependence on AI.

Regional Distribution

Region	Organizations	Percentage	Rationale
Western Europe	75	30%	Highest regulatory readiness (EU AI Act), advanced governance adoption
North America	63	25%	Mature AI ecosystems, strong corporate governance structures
Asia-Pacific	45	18%	Mixed maturity across advanced and emerging markets
Middle East	30	12%	Rapid AI scaling and strong investment in governance
Latin America	25	10%	Early-stage standards adoption and documentation maturity
Africa	12	5%	Growing interest in AI frameworks, emerging regulatory efforts
TOTAL	**250**	**100%**	

Country-Level Representation
Each region includes organizations from multiple countries:

- **Western Europe:** UK, Germany, France, Netherlands, Switzerland, Sweden, Austria
- **North America:** United States, Canada
- **Asia-Pacific**: Singapore, Australia, Japan, South Korea, India
- **Middle East:** Bahrain, UAE, Saudi Arabia, Qatar, Turkey
- **Latin America:** Brazil, Mexico, Chile, Argentina
- **Africa:** South Africa, Angola, Kenya, Nigeria

This distribution captures differences in regulatory exposure, governance culture and operational discipline, ensuring the Index reflects real-world variability rather than a single regional perspective.

The Seven Dimensions of the AI Standards Index

The AI Standards Index™ evaluates whether organizations apply international AI standards in practice—not whether they reference them in policy. Each dimension captures a structural requirement drawn from ISO/IEC SC 42, the NIST AI RMF, the OECD AI Principles and the EU AI Act. Together, these dimensions expose where lifecycle evidence is produced reliably and where it breaks down.

1. Vision & Leadership Alignment

This dimension examines whether leadership defines clear expectations for AI and enforces them. It evaluates the presence of accountable roles, decision rights, risk ownership and standardized terminology based on **ISO/IEC 22989**. Organizations with high scores exhibit consistent leadership oversight; organizations with low scores defer decisions to individual teams, creating fragmentation.

Leadership alignment is the strongest predictor of standards adoption. Without explicit ownership, governance collapses into isolated efforts that cannot scale.

2. Data Quality & Documentation Standards

This dimension evaluates whether data used for AI can be traced, reviewed and defended. It assesses documentation quality, lineage transparency, labeling practices and the presence of bias controls. It reflects the evidence required by **EU AI Act Articles 10–12**, **ISO/IEC 23894** and **ISO/IEC 24027**.

Poor scores indicate missing lineage, undocumented assumptions or data stored without metadata—conditions that make auditability impossible and violate international standards.

3. Governance & Process Standards

This dimension measures whether AI follows a consistent lifecycle aligned to **ISO/IEC 23053** and the functional model of the **NIST AI RMF**. It evaluates the presence and enforcement of checkpoints, risk reviews, policies and decision records.

Weaknesses in this dimension show where teams bypass governance gates, where approvals occur informally and where risk assessments happen only after deployment. Organizations with strong scores produce lifecycle evidence that can withstand regulatory scrutiny.

4. Architecture & Reusability Standards

This dimension assesses whether architectural decisions are documented, reproducible and aligned to a reference architecture. It evaluates component standardization, reuse, integration patterns and interface consistency.

Organizations with low architecture maturity rely on one-off solutions that cannot be governed uniformly. These environments accumulate technical debt quickly and fail to provide the traceability demanded by **ISO/IEC 23053** and the modularity principles of **ISO/IEC 22989**.

5. Capability & Skills Standards

This dimension evaluates whether teams understand the standards they are expected to implement. It examines competency frameworks, skills development, role clarity and segregation of duties.

Low maturity indicates confusion about responsibilities, inconsistent understanding of lifecycle controls and limited capacity to apply governance requirements. Standards cannot function without competent practitioners, as emphasized in the **NIST AI RMF – Govern** function.

6. Tooling & Automation Standards

This dimension measures whether tooling enforces governance. It evaluates unified toolchains, versioning, monitoring, documentation automation, CI/CD processes and automated compliance signals.

Organizations with weak tooling maturity rely on manual processes, which creates inconsistent evidence and increases the likelihood of undocumented changes. High maturity indicates durable infrastructure capable of supporting repeatable AI development and satisfying EU AI Act documentation requirements.

7. Culture & Behavioral Standards

This dimension evaluates whether teams follow standards when pressure increases. It examines behavioral consistency, accountability mechanisms, resistance patterns, “shadow AI” prevalence and adherence to documentation expectations.

Low scores reveal environments where governance is treated as administrative overhead rather than mandatory practice. Culture is the differentiator: without it, standards degrade into checklists that are ignored when delivery deadlines compete with governance requirements.

Scoring Framework

The AI Standards Index™ evaluates organizational maturity using a five-level scale applied consistently across all seven dimensions. The scale reflects the depth, consistency, and institutionalization of AI standards adoption.

Level	Label	Meaning	Score
1	Chaos	No standards; unpredictable, inconsistent behaviors	0-20
2	Foundational	Basic standards exist but are not adopted	21-40
3	Operational	Standards documented and partially adopted	41-60
4	Integrated	Standards integrated across functions	61-80
5	Transformational	Standards embedded culturally and behaviorally	81-100

Figure 6: Five-Level AI Standards Maturity Model

Each dimension is assessed using **3 to 6 scored items**, derived directly from ISO/IEC, NIST, OECD, and EU AI Act criteria. This ensures alignment between global standards requirements and the real-world operational behaviors they are meant to govern.

Normalization of Scores

To ensure comparability, each maturity level is normalized to a 0–100 scale:

```
Normalized Score = (Maturity Level − 1) x 25
```

Examples:

- Level 1 → 0
- Level 2 → 25
- Level 3 → 50
- Level 4 → 75
- Level 5 → 100

This linear transformation enables consistent weighting and cross-dimension benchmarking.

Weighting Model

The AI Standards Index™ uses a weighted composite scoring model based on priorities defined in international standards and regulatory frameworks. Dimensions most strongly associated with **risk management**, **documentation**, and **lifecycle governance** receive higher weightings, reflecting their importance in ISO/IEC, NIST, and EU AI Act requirements.

Dimension	Weight
Vision & Leadership Alignment	15%
Data Quality & Documentation	20%
Governance & Process	20%
Architecture & Reusability	15%
Capability & Skills	10%
Tools & Automation	10%
Culture & Behavior	10%

Data and governance receive the highest weights because global standards consistently identify them as the foundational controls for risk mitigation, transparency, and auditability.

Final Index Score Calculation

The overall Index score is calculated through a weighted aggregation of normalized dimension scores:

$$\text{AI Standards Index Score} = \sum (\text{Normalized Dimension Score} \times \text{Weight})$$

The resulting composite score yields a rating on a 0–100 scale mapped to the Index's maturity levels:

- **0–20** → Chaos
- **21–40** → Foundational
- **41–60** → Operational
- **61–80** → Integrated
- **81–100** → Transformational

Annual Update Mechanism

To maintain long-term relevance, the Index is recalibrated annually to reflect:

- New and updated **ISO/IEC** standards
- Revisions to the **NIST AI RMF**
- Implementation learnings from the **EU AI Act**
- Emerging OECD policy guidance
- Shifts in global industry maturity and adoption patterns
- Expansion of industry-specific benchmarks

By updating the scoring model, weighting logic, and questionnaire items annually, the Index remains aligned with the evolving nature of AI standards, governance practices, and regulatory expectations.

Data Sources & Validation

The AI Standards Index™ draws on multiple data sources to ensure a balanced, evidence-based assessment of organizational readiness. The methodology combines self-reported inputs, qualitative interviews, and objective documentation reviews to reduce bias and capture a comprehensive view of how AI standards are applied in practice.

Primary data sources include:

- **Self-assessment surveys** that evaluate maturity across the seven dimensions of the Index
- **Leadership and subject-matter expert interviews** to validate interpretations, clarify practices, and assess cultural adoption
- **Reviews of policies, architectural artifacts, and lifecycle documentation** to confirm the existence and quality of standards-aligned practices
- **Compliance and risk reports** where available, providing insight into audit readiness and regulatory expectations
- **Training, certification, and competency records** to assess organizational capability and workforce preparedness

These inputs collectively provide a multi-perspective view of governance, process maturity, and standards adoption.

Target populations include:

- **Enterprises deploying AI at scale**, particularly those integrating AI into core business processes
- **Public sector agencies**, where transparency, accountability, and lifecycle governance requirements are expanding rapidly
- **Regulated industries**, such as finance, healthcare, pharmaceuticals, and manufacturing, where governance expectations and standards adoption are typically more advanced

This approach ensures the Index reflects the realities of organizations operating under diverse regulatory environments, architectural constraints, and cultural contexts. It also enables cross-industry and cross-regional comparisons that highlight the structural factors influencing AI readiness.

Validation mechanisms—including cross-functional review, standards alignment checks, and independent expert oversight—further strengthen the reliability and credibility of the findings.

Conclusion

The AI Standards Index™ 2025 exposes a structural problem that is now visible across every region and industry: organizations are deploying AI faster than they are building the controls required to govern it. A global maturity score of **41%** makes this unavoidable. Most enterprises have policies, templates, and review steps, but they do not operate with the consistency required for high-risk AI. Standards exist on paper; they fail in execution.

The weakest dimensions—data documentation, architecture, and culture—show where the breakdown occurs. Teams build models before data lineage is defined. Architectural decisions are rarely recorded with sufficient traceability. Documentation is treated as an afterthought, not as mandatory evidence. Culture is the most persistent failure point: when delivery pressure increases, governance is the first thing teams abandon. These gaps violate the expectations set in ISO/IEC 23894, 23053, and the evidence requirements of the EU AI Act.

Industry and regional variation confirms that maturity is driven by external pressure more than internal discipline. Finance, Pharmaceuticals, and North America score higher because their oversight systems demand defensible evidence. Even these sectors, however, are far from Integrated maturity. No region demonstrates lifecycle consistency or portfolio-level governance strong enough to support the scale of AI that organizations are attempting to deploy.

Closing this gap requires operational changes, not new slogans. Enterprises must enforce lifecycle controls, standardize architectural decisions, build reusable components, and treat documentation as a production asset rather than administrative work. Leadership must remove ambiguity about ownership. Teams must stop bypassing validation gates. Without these changes, AI portfolios will continue to expand while governance remains static, increasing both operational and regulatory exposure.

For many organizations, the most practical entry point is **Artificial Intelligence Portfolio Management (AiPM™)**. AiPM™ forces AI work into a governed intake, creates traceability across initiatives, and exposes where documentation, data, and architecture are breaking down. It converts standards from isolated rules into portfolio-level requirements. This is the mechanism that turns intent into repeatable behavior.

The AI Standards Index™ sets the baseline. Future editions will measure whether organizations are closing the structural gaps identified here or whether AI adoption continues to advance without the controls required to support it. Capability will not determine leadership in the next phase of AI. Standards will. The organizations that build these foundations now will be the only ones able to operate AI at scale without losing control.

APPENDIX

AI Standards Index™ Questionnaire

The following questionnaire forms the official assessment instrument for the AI Standards Index™ 2025. Each question is scored on a five-level maturity scale from 1 (not at all) to 5 (fully institutionalized). Respondents should provide evidence where available, including policies, documentation, architectural artifacts, logs, and records. All items map directly to international AI standards (ISO/IEC, NIST, OECD, EU AI Act).

Scale for each item
1 = Not at all
2 = Partially / Ad-hoc
3 = Defined but inconsistently applied
4 = Consistently applied across most teams
5 = Fully institutionalized & continuously improved

1. Vision & Leadership Alignment

Purpose: Determine whether leadership provides clarity, direction, and ownership for AI Standards.

Weighting: 15%

Q#	Question	Reference
1.1	Our organization has a clearly documented AI vision and strategy aligned with corporate objectives.	ISO/IEC 22989 §5; NIST RMF Govern §1
1.2	Leadership recognizes that standards (data, process, governance) are required for AI scale.	NIST RMF Govern §3
1.3	Roles and responsibilities for AI oversight are clearly defined (CIO, CDAO, Chief Architect, etc.).	NIST RMF Govern §4
1.4	Teams use a shared, standardized terminology for AI concepts.	ISO/IEC 22989 (entire standard)
1.5	AI investment, risk, and governance decisions follow a defined approval model.	OECD Accountability Principle
1.6	Leadership reviews AI risks, dependencies, and standards adoption through a documented, recurring process.	NIST RMF Govern §5

2. Data Quality & Documentation Standards

Purpose: Assess the organization's ability to provide trustworthy, transparent, consistent data for AI.

Weighting: 20%

Q#	Question	Reference
2.1	Training and validation datasets meet documented quality, integrity, and completeness criteria.	EU AI Act Art. 10; ISO/IEC 23894 §6
2.2	Data lineage, metadata, and documentation follow an organizational standard.	ISO/IEC 22989; ISO/IEC TR 24028 §7
2.3	Data governance processes identify and mitigate bias, drift, and representativeness risks.	ISO/IEC 24027; ISO/IEC 23894 §7
2.4	Sensitive or high-risk data is processed under defined compliance controls.	EU AI Act Art. 9–15
2.5	Standardized documentation templates exist for datasets, model inputs, and assumptions.	ISO/IEC 23053 §8
2.6	Data teams follow a standardized validation workflow with documented evidence and approvals before model training.	NIST RMF – Measure/Manage

3. Governance & Process Standards

Purpose: Evaluate whether AI development follows a formal lifecycle with governance gates.

Weighting: 20%

Q#	Question	Reference
3.1	A standard AI lifecycle is used (idea → training → deployment → monitoring).	ISO/IEC 23053 §6
3.2	Governance gates (approvals, documentation checks, risk reviews) are consistently enforced and evidenced.	ISO/IEC 24668 §5; NIST RMF Govern
3.3	Requirements, model decisions, and outputs are fully traceable.	EU AI Act Art. 12; ISO/IEC 23894
3.4	AI risks are regularly assessed, documented, and managed.	ISO/IEC 23894 §7
3.5	Ethical, safety, security, and compliance checks are part of the deployment workflow.	OECD Principles; NIST RMF Manage
3.6	The organization has defined incident response and monitoring procedures for AI failures.	NIST RMF Manage §3

4. Architecture & Reusability Standards

Purpose: Establish whether technical foundations enable scalable and reliable AI.

Weighting: 15%

Q#	Question	Reference
4.1	Standard architecture patterns are used for AI components (pipelines, APIs, storage, monitoring).	ISO/IEC 23053 §5
4.2	AI components—models, features, pipelines—are reusable across teams and products.	ISO/IEC 22989 (modularity principle)
4.3	Architectural decisions are consistently documented in a standardized format.	ISO/IEC 23053 §8
4.4	Technical debt in AI systems is identified, documented, and remediated through a structured lifecycle process.	ISO/IEC 23894
4.5	Integration between AI systems and enterprise platforms follows defined standards.	ISO/IEC 22989 §6
4.6	The organization maintains a reference architecture for AI systems.	ISO/IEC 23053 Annex C

5. Capability & Skills Standards

Purpose: Measure the organization's readiness in skills, roles, and professional consistency.

Weighting: 10%

Q#	Question	Reference
5.1	Skills and competency frameworks exist for AI-related roles.	NIST RMF Govern §4
5.2	Teams use a standardized vocabulary aligned with ISO/IEC 22989.	ISO/IEC 22989
5.3	Employees receive training on AI standards, governance, and ethics.	OECD AI Principles
5.4	Roles are clearly separated (developers, validators, operators).	EU AI Act governance requirements
5.5	Capability gaps are identified through structured assessments.	NIST RMF Map §3
5.6	AI-related new hires are onboarded using standardized governance and lifecycle practices.	NIST RMF Govern – organizational culture

6. Tooling & Automation Standards

Purpose: Evaluate how automation supports consistent, high-quality AI delivery.

Weighting: 10%

Q#	Question	Reference
6.1	Documentation, testing, and validation use standardized templates and checklists.	ISO/IEC 24668 §5
6.2	Model versioning, experiment tracking, and monitoring are standardized across teams.	ISO/IEC 23053 §4
6.3	CI/CD or CI/ML workflows are consistently applied.	ISO/IEC 23053 (pipeline principles)
6.4	Compliance and governance tasks (approvals, risk logs) are automated where possible.	NIST RMF Manage §2
6.5	Teams use a standardized toolchain for data, pipelines, monitoring, evaluation, and documentation.	ISO/IEC 23053 ecosystem consistency
6.6	Automated checks surface bias, drift, anomalies, and model degradation.	ISO/IEC 24027

7. Culture & Behavioral Standards

Purpose: Assess the human and organizational willingness to adopt and respect standards.

Weighting: 10%

Q#	Question	Reference
7.1	Teams consistently follow defined AI standards without escalation or forced enforcement.	NIST RMF Govern §5
7.2	Employees understand why standards matter for AI safety, quality, and scalability.	OECD Principles
7.3	Ethical and responsible AI considerations influence daily decision-making.	OECD; NIST Map–Measure
7.4	Resistance to standardization—including “shadow AI”—is identified, monitored, and reduced.	NIST RMF – organizational culture
7.5	The organization recognizes and reinforces adherence to standards.	NIST RMF Manage
7.6	Lessons learned from AI incidents are documented and shared across teams.	NIST RMF Manage – continuous improvement

Definitions & Terminology

Term	Definition
AiPM™	Artificial Intelligence Portfolio Management — the discipline for prioritizing, governing, and monitoring AI initiatives using standardized controls.
AI Standards	Technical, organizational, and ethical requirements defined by ISO/IEC SC 42, NIST AI RMF, OECD AI Principles, and the EU AI Act guiding responsible and trustworthy AI.
AI Governance	Processes, roles, and controls ensuring AI systems are safe, compliant, ethical, transparent, and aligned with policy and business objectives.
AI Lifecycle	The end-to-end sequence from data collection to model development, validation, deployment, monitoring, and decommissioning (ISO/IEC 23053).
Architecture (AI Architecture)	The structure and standards that define how AI systems are designed, integrated, scaled, reused, and documented across the enterprise.
Bias	Systematic errors that lead to unfair or harmful outcomes; defined and managed through ISO/IEC 24027.
Conformity Assessment	A mandated EU AI Act process for high-risk AI systems requiring documented evidence, testing, risk controls, and evaluation before deployment.
Culture & Behavior	The organizational mindset, habits, and accountability mechanisms that determine whether standards are consistently followed.
Data Governance	Policies, controls, and processes ensuring data quality, documentation, security, and responsible use throughout the lifecycle.
Data Lineage	The ability to track data origins, transformations, and lifecycle changes to ensure transparency and auditability (ISO/IEC 24028).
Documentation	Structured evidence describing data, processes, decisions, risks, design choices, and model behavior required across the AI lifecycle.
Drift (Model Drift)	Degradation in model performance as data or environments change; monitored in ISO/IEC 24027 and NIST guidance.
Ethical AI	AI aligned with fairness, transparency, accountability, and human-centered values as defined by OECD AI Principles.
Explainability	The extent to which the internal logic, decisions, and outputs of an AI system can be understood by stakeholders.
Governance Gate	Formal lifecycle checkpoint (e.g., risk review, documentation check) required before progressing to the next stage.
High-Risk AI	AI systems classified under EU AI Act Articles 6–51 requiring enhanced controls, documentation, and monitoring.

Term	Definition
Integrated Maturity	A maturity level where AI standards are applied consistently across teams, processes, and lifecycle stages.
Lifecycle Traceability	The ability to track requirements, data, decisions, and model outputs across the full lifecycle (ISO/IEC 23053, EU AI Act Art. 12).
Maturity	The depth, consistency, and institutionalization of AI standards adoption across the seven dimensions.
Maturity Level	The five-stage maturity scale: Chaos, Foundational, Operational, Integrated, Transformational.
Model Monitoring	Ongoing observation of model accuracy, bias, drift, anomalies, and risk signals in production.
Operational Maturity	A state where AI standards are documented and partially applied but not yet fully institutionalized.
Post-Market Monitoring	Continuous oversight of deployed AI systems as required by EU AI Act, including incident logging and corrective actions.
Reference Architecture	A standardized blueprint defining reusable design patterns, interfaces, and lifecycle controls for AI systems.
Reusable Component	An AI feature, model, dataset, pipeline, or tool that can be applied across multiple solutions.
Risk Management	Processes for identifying, mitigating, and monitoring risks across the AI lifecycle (ISO/IEC 23894; NIST AI RMF).
Shadow AI	Unapproved or undocumented AI usage outside formal governance processes, posing compliance and security risks.
Standard Operating Procedure (SOP)	Documented instructions describing how tasks must be executed to ensure consistency and compliance.
Standards Adoption	The degree to which global AI standards are embedded into processes, decisions, documentation, architecture, and culture.
Toolchain (AI Toolchain)	The unified set of tools for data preparation, ML pipelines, model training, deployment, monitoring, and documentation.
Traceability	The ability to track data, assumptions, decisions, dependencies, and outputs across the lifecycle for auditability and compliance.
Transformational Maturity	The highest maturity level where AI standards are fully institutionalized, culturally embedded, and continuously improved.
Trustworthy AI	AI meeting global standards for safety, robustness, fairness, transparency, and accountability.
Versioning	Tracking changes in datasets, models, features, and code to ensure reproducibility and auditability.
Region (Benchmarking)	Geographical grouping used for regional maturity comparison (e.g., Western Europe, North America, Asia-Pacific).
Score (Index)	The normalized 0–100 rating derived from weighted maturity assessments across the seven dimensions.

References

OECD AI Readiness Report 2024
https://oecd.ai/en/news/ai-readiness-2024

NIST Trustworthy AI Survey 2024
https://www.nist.gov/artificial-intelligence

EU AI Act (2024)
https://artificialintelligenceact.eu/

ISO/IEC SC 42 Standards Library
https://www.iso.org/committee/6794475.html

Gartner AI Transformation Survey 2023
https://www.gartner.com/en/research/artificial-intelligence

ISO/IEC 22989: Artificial Intelligence — Concepts and Terminology
https://www.iso.org/standard/74296.html

ISO/IEC 23053: Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
https://www.iso.org/standard/74438.html

ISO/IEC 23894: Artificial Intelligence — Risk Management
https://www.iso.org/standard/77304.html

ISO/IEC TR 24028: Trustworthiness in Artificial Intelligence
https://www.iso.org/standard/77608.html

ISO/IEC TR 24027: Bias in AI Systems and AI-Assisted Decision-Making
https://www.iso.org/standard/77607.html

ISO/IEC 24668: Process Management Framework for AI Systems
https://www.iso.org/standard/78368.html

NIST AI Risk Management Framework (AI RMF 1.0)
https://www.nist.gov/itl/ai-risk-management-framework

OECD AI Principles
https://oecd.ai/en/ai-principles

EU AI Act (2024/2025) – Regulatory Texts and Implementation Guidance
https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
& https://artificialintelligenceact.eu/

Stanford AI Index Report (2024/2025)
https://aiindex.stanford.edu

WEF (World Economic Forum) AI Governance Reports
https://www.weforum.org/centre-for-the-fourth-industrial-revolution/artificial-intelligence/

McKinsey Global AI Survey
https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

The Standards Effect, Kadir Özbayram, 2025
https://thestandardseffect.com