AI Governance Benchmarking Study 2026

Insights from 175 Senior Leaders, AI Specialists & Practitioners
16 Industries | 27 Countries | 4 Risk Pillars

Prepared by Hexagrow Consultants Pvt Ltd
May 2026

For Authorised Distribution Only

Contents

Executive Summary

This report presents findings from the AI Governance Benchmarking Study 2026, conducted by Hexagrow Consultants. We surveyed 175 senior leaders, AI specialists and practitioners across 16 industries and 27 countries to understand how organisations are governing AI today and where the biggest gaps lie.

Findings are organised under four risk pillars: Governance & Oversight, Technology & Operational, Data & Privacy, and Ethical & Social. Every quantitative finding excludes non-responses. Section 9 provides the full methodology.

175	16	27
Respondents	Industries	Countries

1

Governance lags adoption by a wide margin

77% of organisations have moved beyond minimal AI use, but only 11% report Systemic or Leading governance maturity. The pace of adoption is outstripping the pace of governance build-out.

2

Data & Privacy is the only pillar that clears the bar

Data & Privacy maturity averages 3.27/5 — the only pillar above the 3.0 benchmark. Governance & Oversight is weakest at 2.75/5. Existing privacy regulations are providing a transferable foundation; AI-specific governance is not yet doing the same.

3

Foundational policies are the single biggest gap

RP1 (AI policies and cross-functional collaboration) has the worst net top-box score (-16pp). 46% rate their organisation weak (1-2) on this, only 29% rate it strong (4-5). Every downstream control suffers when foundational policies are missing.

4

The mid-market is the weakest segment

Organisations with 5,000–20,000 employees report the lowest maturity across every pillar (1.89–2.25). Large enterprises (>100k) lead at 3.39–3.88. Small firms benefit from simplicity; large firms benefit from resources; the middle is squeezed.

5

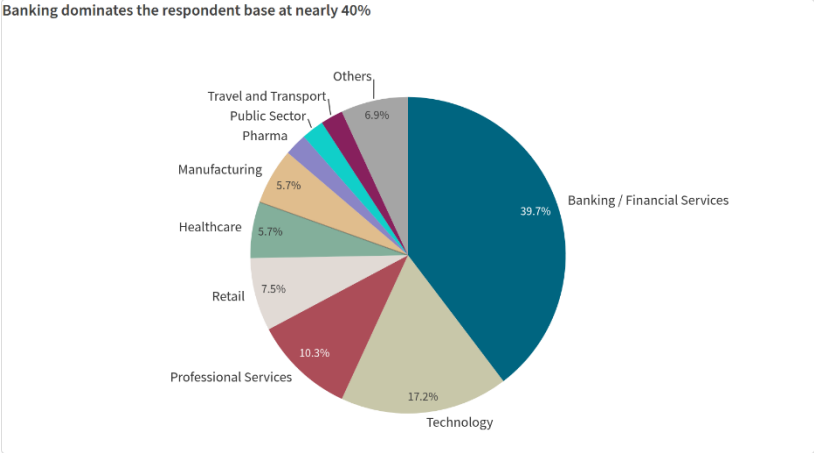
Boards see governance very differently from practitioners

Board members rate governance maturity at 2.10/5; Risk/Compliance professionals rate it at 3.07; Technology specialists at 3.15. The gap between oversight bodies and operational teams is a structural risk in itself.

1. Who Responded

Three demographic patterns shape the data: banking dominance, large-enterprise weighting, and India-centric geography.

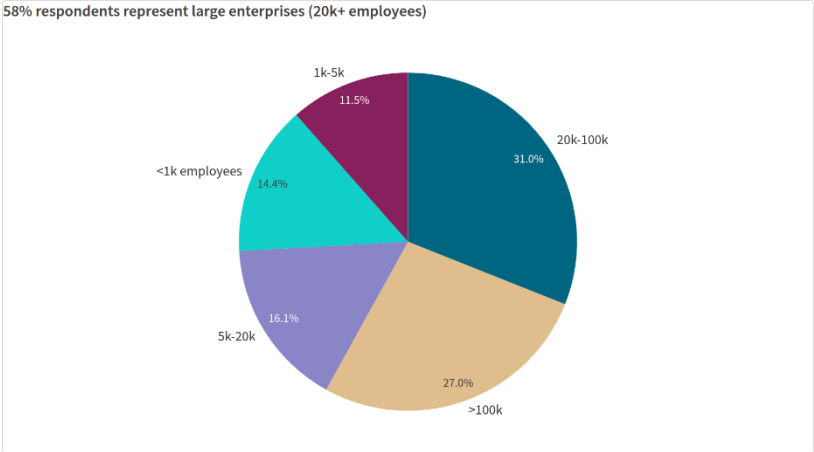
1.1 By Industry



Respondent distribution by industry

Banking & Financial Services dominates at 40% (69 respondents), reflecting the sector's regulatory intensity and early AI adoption. Technology (17%) and Professional Services (10%) follow. Together, these three sectors account for two-thirds of the sample.

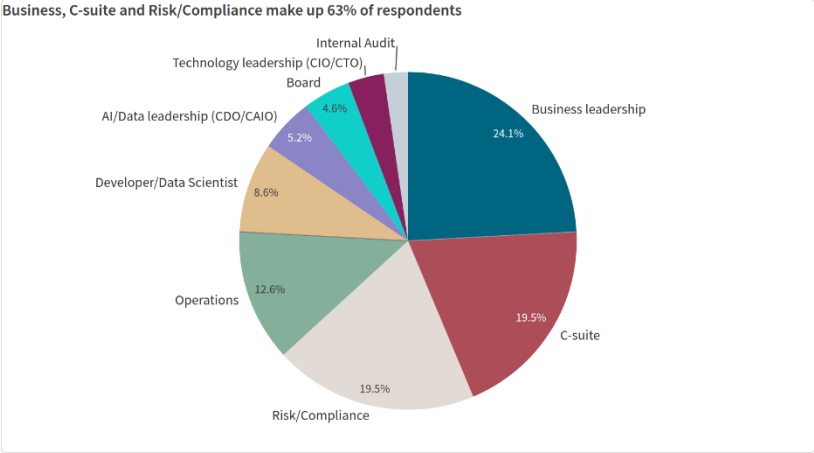
1.2 By Organisation Size



Respondent distribution by organisation size

58% of respondents come from organisations with 20,000+ employees. This skew matters because larger firms have more resources for governance but also more complex AI ecosystems. Smaller firms (<1k and 1k–5k employees) make up 26% combined.

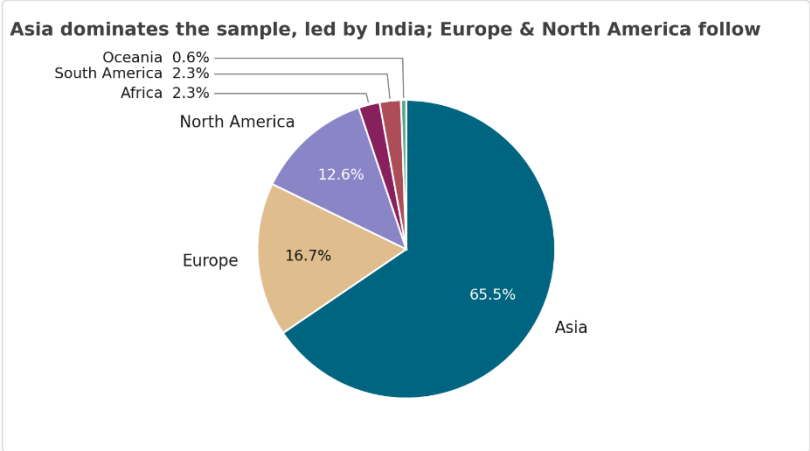
1.3 By Role



Respondent distribution by role

Business leadership (24%), C-suite (19%), and Risk/Compliance (19%) together represent 64% of respondents. Importantly, the survey captures perspectives from both strategic decision-makers (Board, C-suite) and operational practitioners (Developers, Risk teams). This enables comparison across organisational layers.

1.4 By Geography

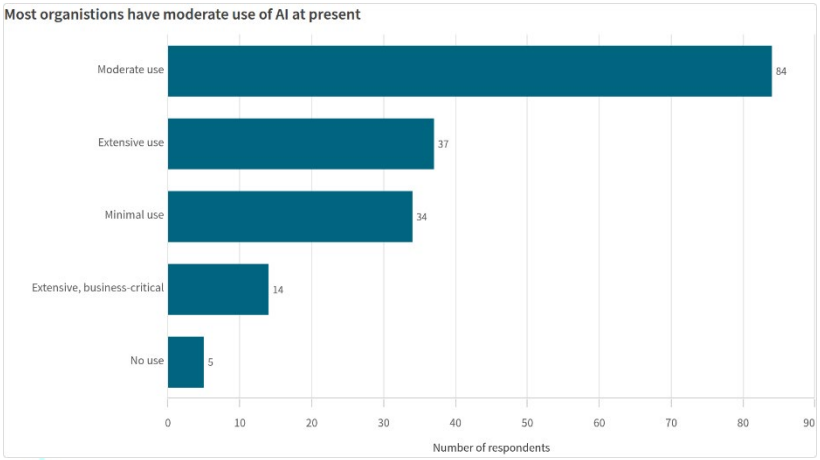


Respondent distribution by geography

India represents 55% of respondents (96 responses), followed by the UK (11%) and US (10%). The sample spans 27 countries in total. Findings should be read with this geographic concentration in mind.

2. The AI Adoption Landscape

2.1 How Widely is AI Being Used?

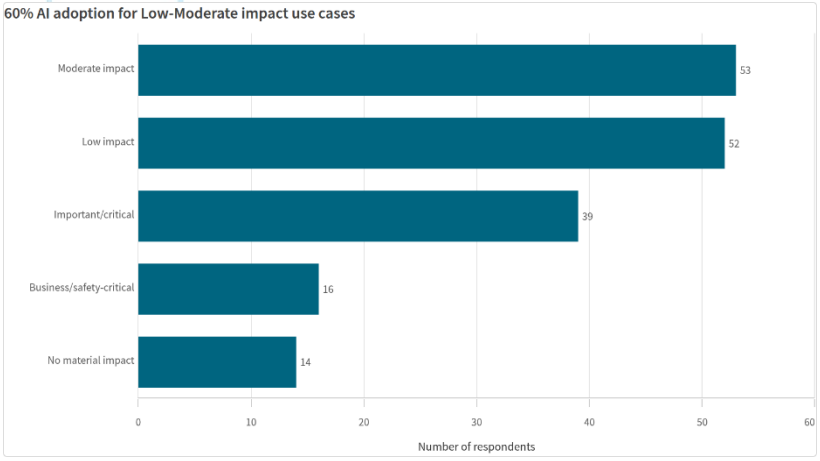


Extent of AI adoption across organisations

77% executives report moderate to extensive AI adoption across organisations with only 3% reporting no AI use at all. AI adoption is already significant with minimal AI usage across a much smaller proportion of businesses – 19%.

With AI adoption moving at pace and crossing past thresholds, governance is no longer an emerging concern. The risks AI creates are pervasive at present with long-term implications for industries and society at large.

2.2 How Critical Is AI?

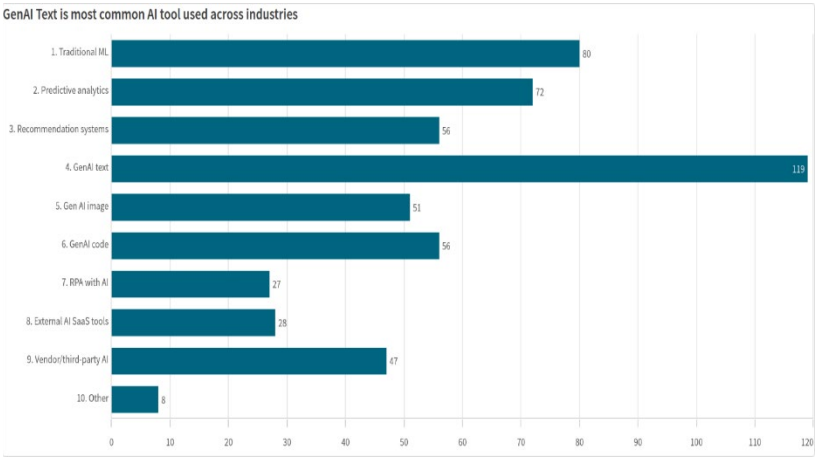


Reported criticality of AI systems

While AI adoption has critical mass now, 60% AI usage is reported to be in low to moderate impact use cases. Only a third of the executives recognise AI systems as having important to critical business impact.

As AI use scales from low impact to critical business functions, investment and focus on building structured governance frameworks will also have to increase proportionately. At present though, as a bulk of AI impact is perceived to be low to medium, it could be that organisations are systematically underinvesting in controls.

2.3 What Types of AI Are in Use



Types of AI technologies in use

GenAI text is the dominating AI technology at 68% (119 respondents). Traditional ML (46%) and Predictive Analytics (41%) remain widely used. Despite the benefits, traditional ML raises bias and explainability issues and GenAI adds hallucination, IP leakage, and prompt injection risks to the LLMs. Given that both generative and traditional AI create different types of risks they need independent controls for mitigation.

In 32% use cases GenAI is applied for code generation, and vendor or third-party AI services are used in 27% cases. These two combined introduce supply-chain risks that classical AI governance frameworks are not designed to address.

3. The Four Pillar View

3.1 Creation of the Four Risk Pillars

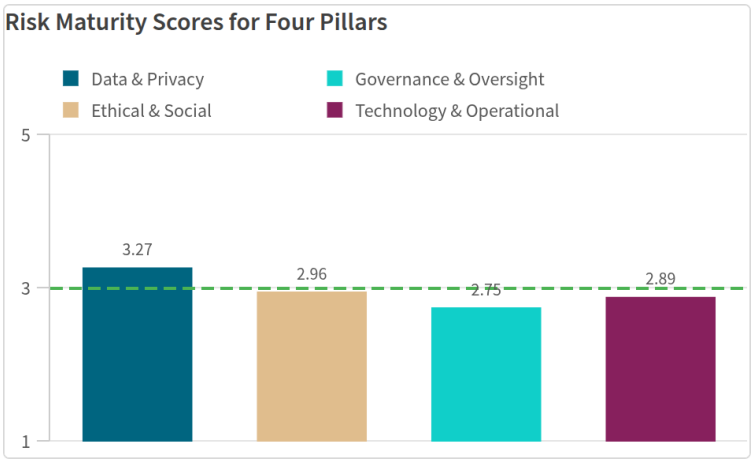
Across the survey we asked specific questions (see below) to inform the contents of our 4 core risk pillars (RPs).

Code	Question / Practice
RP1	AI-related policies in place and supported by cross-functional collaboration
RP2	Central inventory of AI systems and pre-deployment review gates
RP3	Ongoing production monitoring and continuous risk monitoring
RP4	Compliance review against applicable privacy and data protection requirements
RP5	Technical and organisational controls applied to protect personal data used by AI systems
RP6	Responsible AI principles articulated and endorsed by senior leadership
RP7	Structured review and testing to assess potential unfair bias
RP8	Employee training or awareness — AI uses, policies, and expectations

Risk Pillar	Composed of
Governance & Oversight	RP1 + RP2
Technology & Operational	RP3 + RP8
Data & Privacy	RP4 + RP5
Ethical & Social	RP6 + RP7

Each was rated on a 1–5 Likert scale (1 = lowest maturity, 5 = highest), with "Don't Know" excluded from numeric calculations.

3.2 Pillar Scores

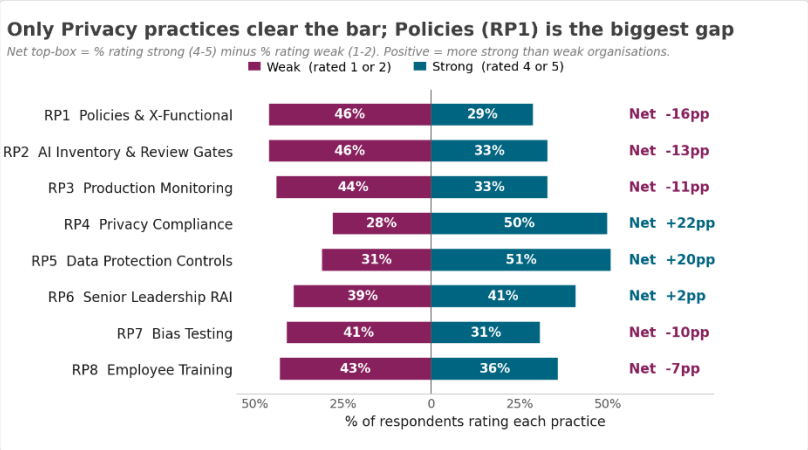


Maturity scores across the four risk pillars

The overall risk maturity score across industries averages at 2.95/5 which is below the maturity midpoint across all four pillars. The four risk maturity pillars are – Data & Privacy, Ethical & Social, Governance & Oversight, and Technology & Operations. Out of all, Data & Privacy maturity is the highest (3.27) followed by Ethical and Social maturity (2.96) followed by Technology & Operations (2.89). Individually, Data & Privacy risk maturity score is the highest likely due to a sustained regulatory focus related to data governance, data security and data protection.

Management of Governance & Oversight risk is however lagging as executives focus on the more tangible risks related to technology implementation, operational challenges and data privacy/security risks. Governance and oversight risk maturity is key for future-proofing and ensuring any blind spots are identified and mitigated through formalised controls and governance structures.

3.3 Net Top-Box: Where Practices Are Genuinely Strong or Weak



Strong (4-5) vs Weak (1-2) ratings across the eight risk practices

Pillar means tell only part of the story. A mean of 3.0 could come from a polarised population (half strong, half weak) or a uniformly mediocre one. The net top-box chart resolves this by separating, for each practice, the proportion of organisations rating it strong (4 or 5) from those rating it weak (1 or 2). The net top-box — strong minus weak, in percentage points — is the most diagnostic single number for each practice.

Three practices show a positive net: RP4 Privacy Compliance (+22pp), RP5 Data Protection Controls (+20pp), and RP6 Senior Leadership RAI (+2pp).
Only the two privacy practices have a clear majority of strong responses; RP6 is essentially split. Every other practice has more weak organisations than strong, with RP1 (AI Policies & Cross-Functional Collaboration) the worst at -16pp — 46% of organisations rate this weak, only 29% rate it strong. This is the single biggest foundational gap in the dataset.

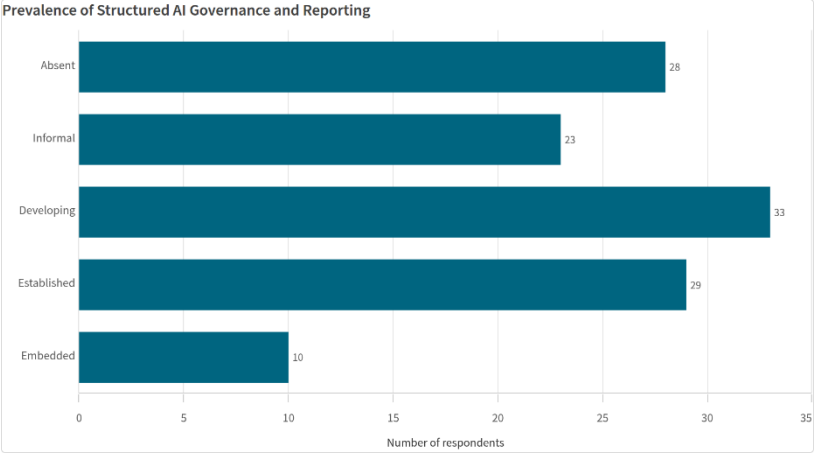
Later sections delve in which practices are weak as a population (RP1, RP2, RP3, RP7, RP8) versus where the average score hides genuine strength (RP4, RP5).

4. Deep Dive — The Four Pillars

4.1 Governance & Oversight (Score: 2.75/5)

This pillar covers AI policies, central inventories, governance forums and committees, accountability structures, and framework alignment. It is the weakest of the four pillars.

Governance Structures Today

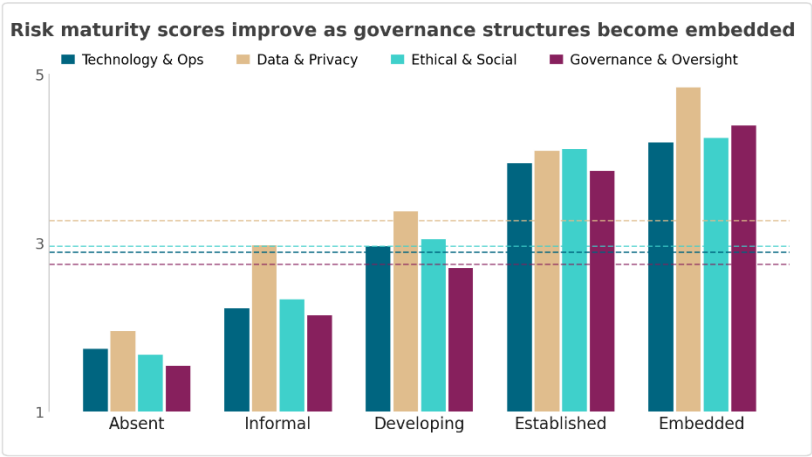


Maturity of structured governance roles, forums and committees

41% of executives report that governance roles and committees specifically for reviewing AI-related topics are either absent or informal. According to 27% respondents, organisations are in the process of formalising/developing AI governance roles and forums for regular and effective reviews. A similar proportion of respondents concede that where formal structures already exist, they are being inconsistently applied. As a result, a majority of businesses may risk having patchy AI inventories, ambiguity around decision ownership, and poor traceability of decisions to AI/AI Agents.

Only 8% executives claim that governance is embedded and is a default part of how the organisation operates with regards to AI.

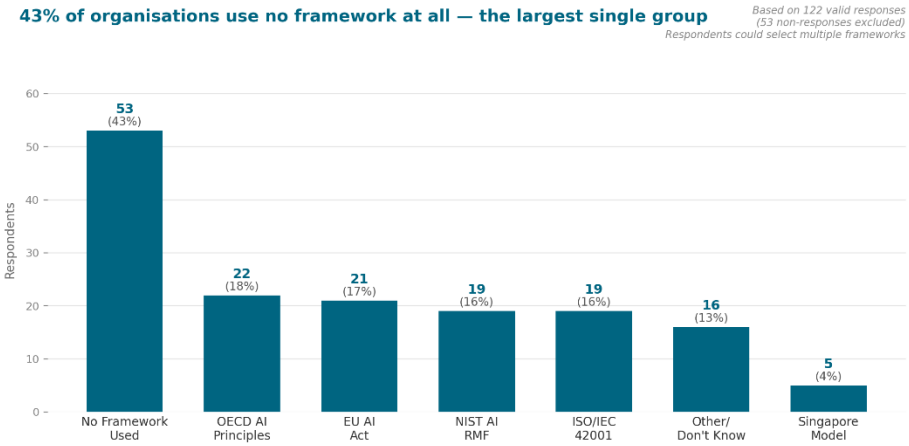
Governance Structure Drives Everything Else



Risk maturity scores by structured governance level

As governance structure moves from Absent to Embedded, every risk pillar score climbs from approx.1.7 to approx. 4.4. There is a direct correlation here, every step up in governance structure delivers higher risk maturity across all four pillars. Structure is the prerequisite for everything else.

Framework Adoption



AI governance frameworks referenced (122 valid responses)

The largest single group of respondents (53) explicitly report using no AI governance framework at all. Among those who do use a framework, the four major frameworks/ guidelines specified in the survey, namely OECD AI Principles, NIST AI RMF, ISO/IEC 42001 and EU AI Act, have nearly equal prevalence and reach (19–22 references each).

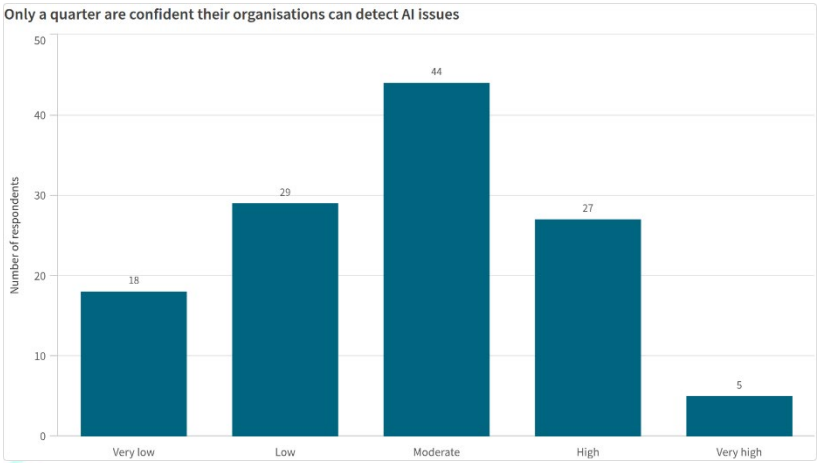
Even though these frameworks are globally applicable, there is a natural alignment for businesses located/operating in the geographies from where these frameworks have originated. While most frameworks provide guiding principles for responsible AI without punitive regulatory actions, the EU AI Act is by far the most comprehensive one including penalties for non-compliance.

From the survey data, nearly half of all organisations are not following any of these globally known AI frameworks. As AI's reach and scope cuts across industries, supply chains and geographies, risks due to inconsistent and non-standard practices in one region/jurisdiction can quickly expand to other areas as well. So, to ensure global adoption of responsible AI there should be a uniform code or globally-accepted policies that can complement organisation level governance frameworks.

4.2 Technology & Operational (Score: 2.89/5)

This pillar covers production monitoring, continuous risk monitoring, and employee training. It sits just below the 3.0 benchmark.

Confidence in AI Issue Detection and Resolution

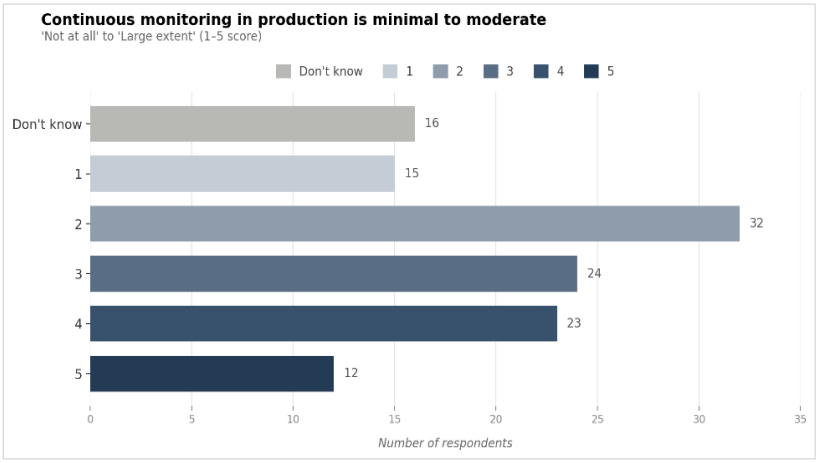


Confidence in AI-issue detection and resolution

Out of all the respondents surveyed, 38% executives have very low to low confidence in their organisations' capability to quickly detect and effectively manage any AI-related issues or incidents.

Erroneous or harmful outputs, bias and security issues can go undetected until they start impacting individuals and have material consequences in the real world. Therefore, any gaps in incident response management and AI monitoring infrastructure will need to be addressed by companies to reassure both internal and external stakeholders.

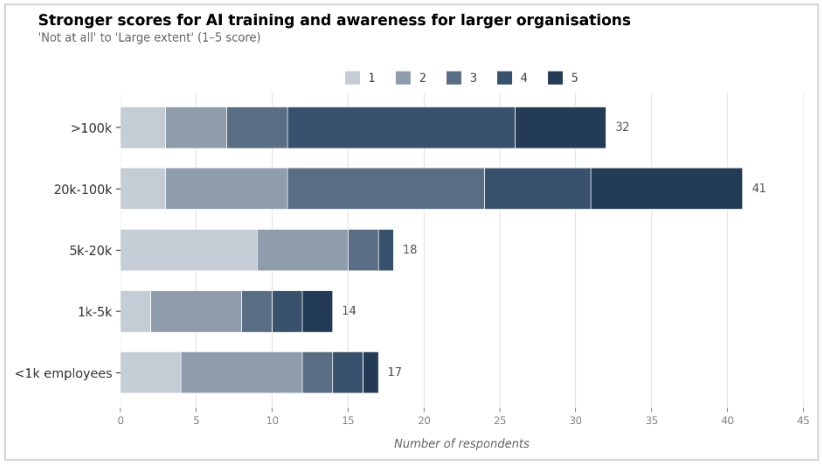
Production Monitoring at a Practice Level



Extent of ongoing production and continuous risk monitoring

The chart reflects responses when asked "to what extent are AI systems subject to ongoing production monitoring and continuous risk monitoring (for example, performance, drift and key risk indicators)?". Production monitoring clusters in the low-to-mid range: 48% of respondents score 3 or above, but the single largest group sits at the lower end of the scale.

The Training Multiplier



AI-related training and awareness maturity by organisation size

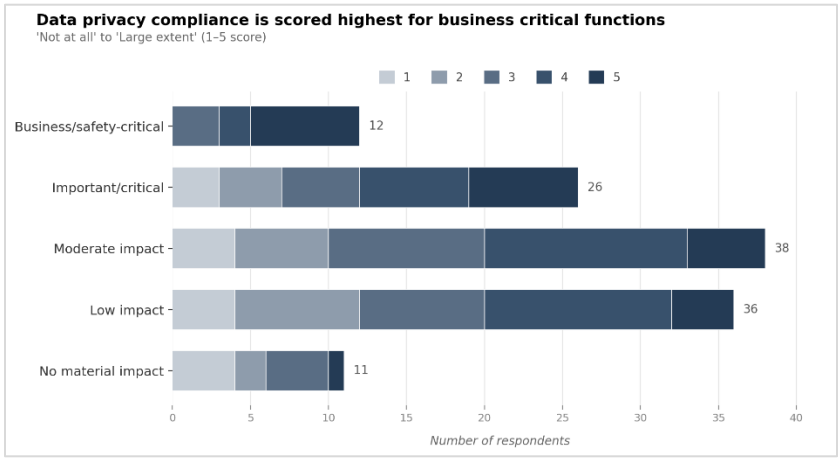
While respondents are equally split across the spectrum with regards to scoring AI-related training and awareness policies, there is a strong correlation between organisation size and training maturity. Respondents from bigger organisations (20K-100K and >100K employees) rated their AI-related training and awareness policies higher compared to their counterparts in relatively smaller firms.

Unsurprisingly, large well-established organisations have invested in AI literacy faster and more effectively. Small firms are however behind the curve and will need to equip their workforce to adapt to AI as well as guard against AI risks which could emanate from their external environment.

4.3 Data & Privacy (Score: 3.27/5)

This pillar covers compliance reviews against privacy and data protection requirements and technical/organisational controls for personal data used by AI systems. It is the strongest of the four pillars and the only one above the 3.0 benchmark.

Compliance with data privacy and protection requirements



Data privacy compliance maturity by AI criticality

From the survey data, as the criticality of AI systems increases the data privacy compliance scores increase in tandem. Highest proportion of respondents scored a perfect '5' for data privacy compliance where AI systems are used for more important or critical business functions. Similarly, organisations with low-moderately critical AI use also had the highest proportion of respondents scoring data privacy strongly at '4'. Data privacy and security requirements have been front and centre for many decades and remain critical for the safe deployment of AI as well.

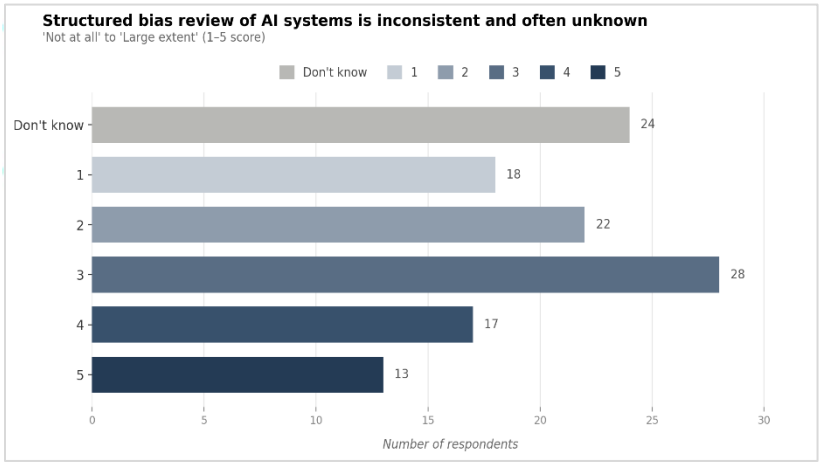
The "Shadow AI" Risk Surfaces in Comments

Open-ended responses surface a concern that the quantitative scores partially mask. Multiple respondents flagged unauthorised employee use of public GenAI tools as a data privacy concern. One business respondent wrote: "My biggest concern is the number of non-firm AI services which exist, and the risk these pose for our data — through smartphones, smart glasses or just web AI tools where the data lineage is unclear." This is a privacy challenge that traditional data protection frameworks were not built to address.

4.4 Ethical & Social (Score: 2.96/5)

This pillar covers senior leadership endorsement of Responsible AI principles and structured review/testing for bias. It sits just below the 3.0 benchmark.

Bias Testing — The Awareness Problem

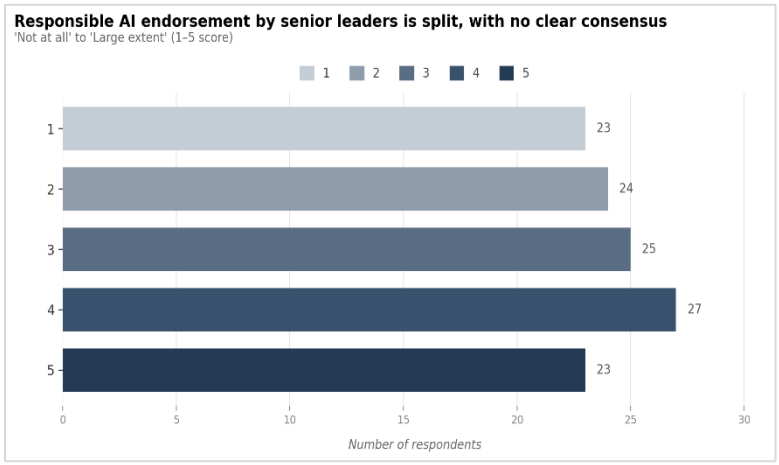


Structured review and testing for unfair bias

According to the survey results, more than half respondents score their bias testing capability and review structures in the low-mid range with scores of '1', '2', and '3'. Only 25% executives have rated this capability highly. Also, 20% have marked 'Don't know' showing a gap in knowledge dissemination and awareness.

While AI is data-driven and objective, underlying bias can seep through from the data samples (from the real-world) used to train the AI models. Developers may prioritise specific objectives such as maximise accuracy or optimise computations thereby allowing for human bias and subjectivity to shape the AI output. So, in order to mitigate these risks and nurture trust in AI, it is important to follow 'Trust by Design' principles at the outset and also create awareness to remove any governance blind spots.

Senior Leadership Endorsement — Polarised



Endorsement of Responsible AI by senior leaders

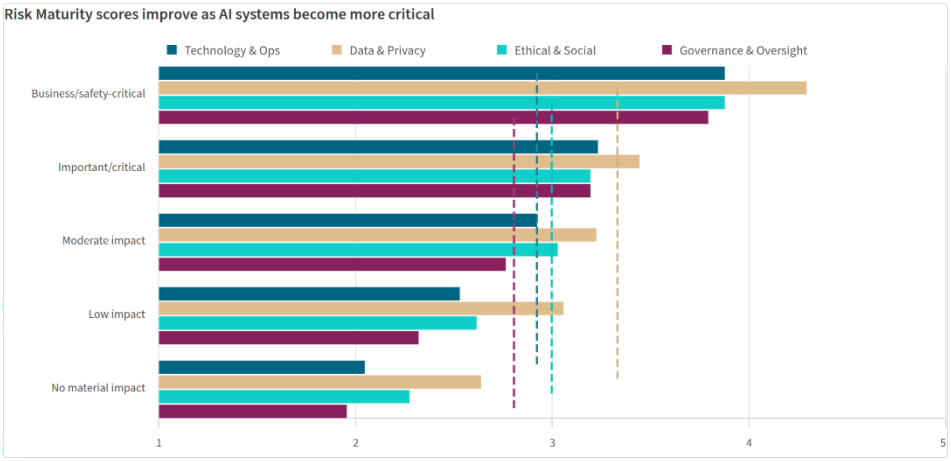
Senior leadership endorsement of Responsible AI principles scores 3.02/5 on average — but this average masks a strikingly polarised picture. Responses are spread almost evenly across the entire scale. In net terms, 39% rate leadership endorsement weak (1-2) while 41% rate it strong (4-5), with very little clustering around the middle.

This is near-uniform distribution - organisations either have visible, active senior sponsorship for Responsible AI or they have almost none. Endorsement appears to be driven by individual leadership conviction rather than systemic governance design. Responsible AI only gets traction where a senior leader owns it. This makes leadership endorsement one of the most fragile pillars of the governance system, because it depends on individuals rather than embedded structures.

5. Cross-Cut Analysis

5.1 Maturity by AI Criticality

Where the criticality story breaks down



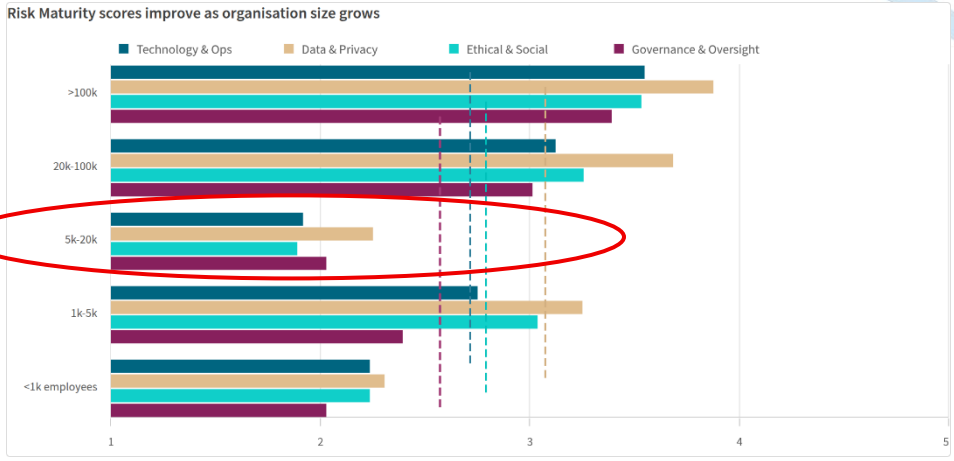
Risk maturity by AI criticality across pillars

Risk Maturity nearly doubles from 2.20 to 3.95 as AI moves from no material impact to safety-critical. Organisations rightly invest more in high-stakes systems but it raises a strategic question: are organisations correctly assessing criticality? If a system rated "low impact" is actually feeding aggregated business intelligence or influencing customer outcomes, the underinvestment in governance becomes a hidden risk.

The bar chart shows that even for Business/Safety-Critical AI systems, Governance & Oversight is the weakest pillar (3.79) — lower than Data & Privacy (4.29). Even when organisations recognise high stakes and invest accordingly, governance structures lag the data privacy controls. There is a structural problem with AI-specific governance that exists at every level of risk perception.

5.2 Maturity by Organisation Size

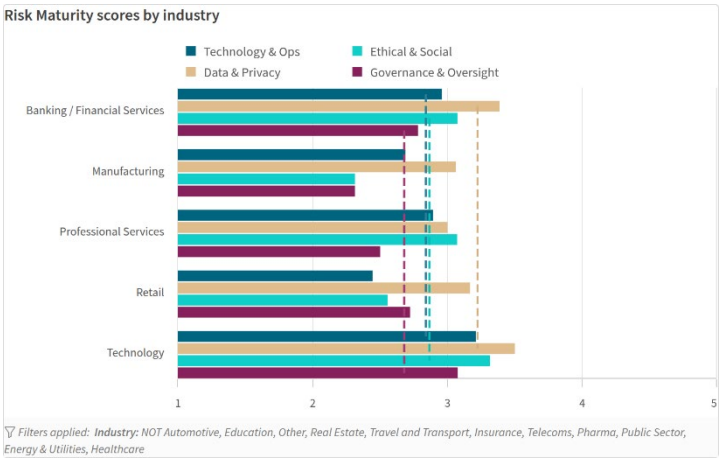
The missing middle



Risk maturity by organisation size across pillars

From the survey results, small-mid sized firms (5k–20k employees) report the lowest risk maturity among all different sized businesses. They have enough AI complexity to create risk but not enough scale to justify dedicated AI governance teams. They are too large for ad-hoc oversight and too small for institutional governance. This is the most exposed segment in the study.

5.3 Maturity by Industry

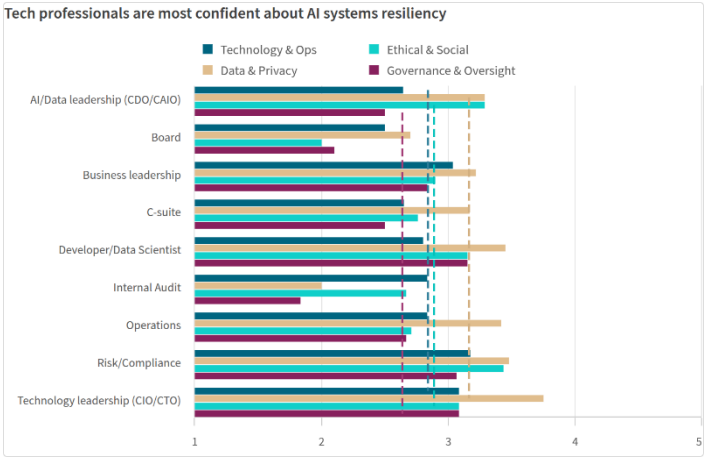


Risk maturity by industry across pillars

Technology (3.31 overall) and Banking (3.02) lead the major industries. Manufacturing (2.56) and Retail lag. Banking's leadership in Data & Privacy (3.39) is notable, it reflects decades of regulatory infrastructure. But Banking's Governance & Oversight score (2.78) shows the same AI-specific gap as other industries: regulatory investment does not automatically translate to AI governance.

5.4 Maturity by Role — What Different Voices Are Saying

Finding 1: Board members report the lowest maturity



Risk maturity by role profile across pillars

Board members rate governance at 2.10/5 and ethical maturity at 2.00/5 — the lowest of any role. They sit below Risk/Compliance (3.07 governance) and Developers (3.15). The people responsible for oversight have the least visibility into how AI is governed. This is a structural risk.

Finding 2: Risk/Compliance and Developers see the same picture

Risk/Compliance professionals and AI/Data specialists report similar maturity scores. Risk/Compliance rate overall maturity at 3.29/5 (Governance 3.07, Technology 3.17, Data & Privacy 3.48, Ethical 3.43); AI specialists rate it at 3.14/5 (Governance 3.15, Technology 2.80, Data & Privacy 3.45, Ethical 3.15). Both groups sit well above the Board and C-suite. This convergence is reassuring: the people closest to building and controlling AI systems share a broadly consistent view of how mature the organisation actually is.

Finding 3: C-suite sits below Risk/Compliance

The C-suite rates overall maturity at 2.77/5 — materially below Risk/Compliance (3.29) and Business leadership (3.00), and only modestly above the Board (2.33). C-suite scores are weakest on Governance & Oversight (2.50) and Ethical & Social (2.76). This is a notable disconnect: the executives who set strategy and allocate budget

rate the organisation's AI maturity lower than the practitioners who run it day to day. Oversight layers and operational layers do not yet share a common picture of AI governance.

5.5 What Different Voices Are Asking For

The survey included role-specific open-ended questions. Across 97 substantive responses, four themes recurred:

- **Awareness and training (most common):** "Increasing awareness of AI at all levels", "democratising AI policies", "awareness trainings proportional to impact" — this is the most consistently requested intervention across every role.
- **Clearer accountability and ownership:** Board respondents explicitly asked for "clear ownership in the C-Suite" and "updated boards with contemporary tech savvy talent". Risk/Compliance respondents flagged "fragmented ownership — AI governance split across tech, business, risk, and legal teams with no single accountable owner".
- **Better board reporting, not more:** One Board respondent captured the tension exactly: "Board reporting is well documented and comprehensive — almost too comprehensive — so finding a far more streamlined and relevant report with KPIs in dashboard form would provide for more meaning."
- **Shadow AI is the unspoken risk:** Multiple Business and Operations respondents flagged unauthorised employee use of public GenAI tools, smart device AI, and web-based AI services. This concern appears qualitatively but is barely measurable in the quantitative data — a known unknown.

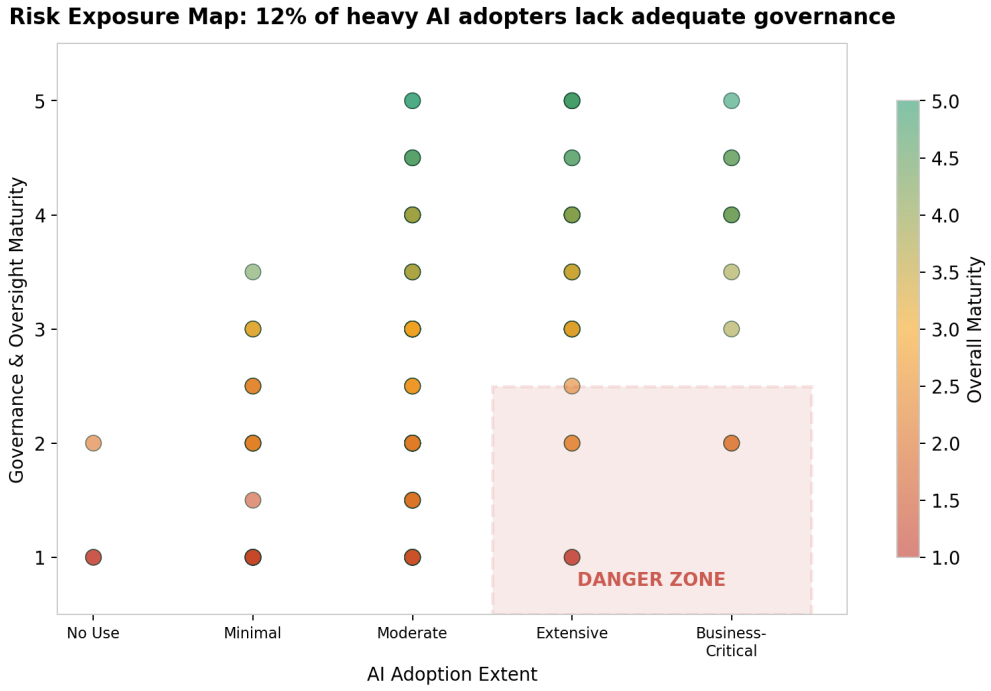
6. Key Insights — The Big Picture

Pulling the analysis together, five insights stand out as the most important takeaways.

Insight 1: Governance & Oversight is the binding constraint

Across every cut — by criticality, size, role, framework adoption — Governance & Oversight is the weakest pillar in the data. RP1 (Policies) is the weakest single practice. The Board has the lowest visibility. This is not a coincidence. AI governance maturity is bottlenecked by governance structure, and governance structure is bottlenecked by foundational policies. Until that base is fixed, downstream investments under-perform.

Insight 2: Risk Exposure is concentrated where adoption outpaces governance



Risk exposure map: AI adoption vs governance maturity

This chart maps every respondent by their AI adoption extent (x-axis) and governance maturity (y-axis). The red “danger zone” identifies organisations with extensive or business-critical AI use but governance maturity of 2 or below. 12% of heavy AI adopters fall into this zone — material AI dependencies without structural controls. These organisations are the most exposed to regulatory, operational, and reputational risk.

Insight 3: Training is the highest-leverage single investment

Training stands out as a priority for three independent reasons. First, RP8 sits within a tightly clustered set of governance practices — every pair of practices in this dataset correlates closely, meaning maturity tends to move together rather than in isolation. Second, training is the most consistently requested intervention in open-ended responses: it was the single most common ask across all five role-specific questions. Third, it is the practice with the fewest external dependencies — organisations can act on it unilaterally, without waiting for

regulators, vendors, or board-level mandates. That combination of cross-practice alignment, qualitative demand and unilateral actionability makes it a high-leverage starting point.

Insight 4: The Risk/Compliance blind spot is real

Risk/Compliance professionals have the highest “Don't Know” rates on the three most technical practices (RP3 -Production Monitoring, RP5 -Data protection, RP7 -Bias testing). 29% don't know whether their organisation tests for bias. This is not a knowledge deficiency on their part; it reflects a structural failure to integrate technical practices into oversight reporting.

Insight 5: Frameworks work — but most organisations aren't using them

Organisations that reference any named framework (OECD, NIST, ISO 42001, EU AI Act) score 1.04 points higher overall (3.42 vs 2.38). The lift is consistent across all four pillars, and framework users clear the 3.0 benchmark on every pillar while non-users fall below it on every pillar. Yet 43% of respondents who answered this question explicitly use no framework at all. Framework adoption is the lowest-cost intervention with the highest measurable impact in the dataset.

7. Remediation Roadmap

Ten priority actions, sequenced from foundational to advanced. Organisations should identify their starting point based on current maturity and address gaps in order.

1

Establish foundational AI policies with cross-functional ownership

RP1 (policies and cross functional) has the worst net top-box (-16pp). Develop clear AI use policies with explicit cross-functional accountability spanning technology, risk, legal, and business. This is the highest-impact single action in the report.

2

Build a central AI inventory

Governance & Oversight is the weakest pillar (2.75/5), and RP2 (AI Inventory) contributes directly. Register every AI system, model, and third-party AI service. Include risk classification, data lineage, and ownership.

3

Reference an established framework

Organisations using an established AI Framework users score +1.04 points higher overall (compared to those using No framework) and clear the 3.0 benchmark on every pillar; the 43% who use none fall below it everywhere. Stop debating frameworks; Pick one and use it

4

Stand up structured governance forums

Only 8% have Embedded governance. Establish AI governance committees with charters, regular cadence, and escalation authority. Include Risk, Legal, Technology, and Business.

5

Implement pre-deployment review gates

Require formal risk assessment, bias testing, and compliance review before any AI system enters production. Include third-party and vendor-supplied models.

6

Invest in employee training

Training (RP8) is the most consistently requested intervention in qualitative responses and the practice organisations can act on without external dependencies. Tiered delivery: executive awareness for board/C-suite, governance protocols for risk teams, technical standards for developers, responsible use for all employees.

7

Close the Risk/Compliance visibility gap

29% of Risk/Compliance professionals don't know whether their organisation tests for bias. Establish reporting flows from technical teams to oversight functions for monitoring, bias testing, and data controls.

8 **Build continuous production monitoring**

38% report low or very low confidence in detecting AI issues. Real-time monitoring, drift detection, and incident response are now operational requirements, not nice-to-haves.

9 **Adapt data protection for AI-specific risks**

Privacy controls score well but were not designed for training data leakage, prompt injection, model memorisation, or shadow AI use. Extend existing frameworks to cover these.

10 **Bridge the Board perception gap**

Board members rate governance at 2.10/5 vs practitioners at 3.15. Invest in board-level reporting that translates technical AI risk into strategic and fiduciary language.

8. Methodological Disclosure

8.1 Data Collection

Survey Period	January – March 2026
Total Responses	175 individual respondents across 16 industries and 27 countries.
Collection Method	Structured online survey distributed through professional channels.
Question Types	Quantitative Likert-scale (1–5) for eight risk practices (RP1–RP8); categorical for demographics, criticality, framework usage, and governance structure; open-ended (max 350 characters) for role-specific perspectives.
Scale Direction	All Likert scales: 1 = lowest maturity / weakest controls; 5 = highest maturity / strongest controls. Higher = better. The same direction applies to all pillar scores and the overall maturity score.

8.2 Analytical Methodology

Non-Response Treatment	Non-responses, blanks, and “Don't Know” selections are excluded from all calculations. Means and percentages use only valid numeric responses. Response counts (n) are reported throughout.
Central Tendency	Arithmetic means of valid responses. Likert-scale data is treated as interval data, which is standard practice for samples of this size (n=175) in applied survey research.
Cross-Tabulations	Where sub-group sample sizes fall below 10, findings are characterised as directional signals rather than statistically representative conclusions.

8.3 Pillar Score Composition

The dataset includes four pre-calculated pillar scores plus an overall maturity score. Verified compositions:

Governance & Oversight	Average of RP1 (Policies & Cross-functional Collaboration) and RP2 (AI Inventory & Review Gates)
Technology & Operational	Average of RP3 (Production Monitoring) and RP8 (Employee Training)
Data & Privacy	Average of RP4 (Privacy Compliance Review) and RP5 (Data Protection Controls)
Ethical & Social	Average of RP6 (Senior Leadership RAI Endorsement) and RP7 (Bias Testing)
Overall Maturity	Average of the four pillar scores above

8.4 Limitations and Caveats

Self-Report Bias	All data is self-reported. Respondents may over- or under-estimate maturity depending on role, knowledge, and interpretation.
Sample Composition	Weighted toward Banking (39%), India-based respondents (55%), and large organisations (58% with 20k+ employees). Findings may not generalise to all sectors, geographies, or organisation sizes.
Sub-Group Sizes	Technology Leadership (n=6), Board (n=8), Internal Audit (n=4) are small sub-samples. Findings for these groups are directional, not statistically robust.

---------- End of Report ----------

If AI governance isn't on your agenda yet or if you would like to review your existing controls, now is a good time to start. You can reach us at info@hexagrow.com, or head to https://hexagrow.com/resources to download our proprietary risk and controls toolkit and run a self-assessment against your current AI maturity.