



AI in risk management

A board perspective

Board Leadership Center (India)

June 2026

kpmg.com/in

KPMG. Make the Difference.



Introduction

For most of its history, risk management has been a discipline of assembly. Risk teams gathered data from across the organisation, consolidated it into reports, reviewed it in committees, and produced assessments that reflected the state of the organisation at a particular point in time. The process was thorough. It was also slow, labour-intensive, and — by the time a board reviewed the output — already a view of the past.

AI is changing risk management at its core. The way risks are identified, assessed, monitored, and acted upon is shifting from periodic and judgement-led to continuous and signal-led. AI can surface anomalies before they appear in any report, run Anti-Money Laundering (AML) and Know Your Customer (KYC) checks at a scale no team could sustain manually, generate consistent risk ratings across the enterprise, and — in more advanced organisations — execute parts of the risk workflow with limited human involvement.

The board that has not engaged with this shift is governing with an incomplete picture of where consequential decisions are being made, and where accountability therefore sits. India's regulators are moving in this direction across financial services, capital markets, and beyond. The board that waits for formal obligation to engage will have already fallen behind.



What AI is doing across the risk lifecycle

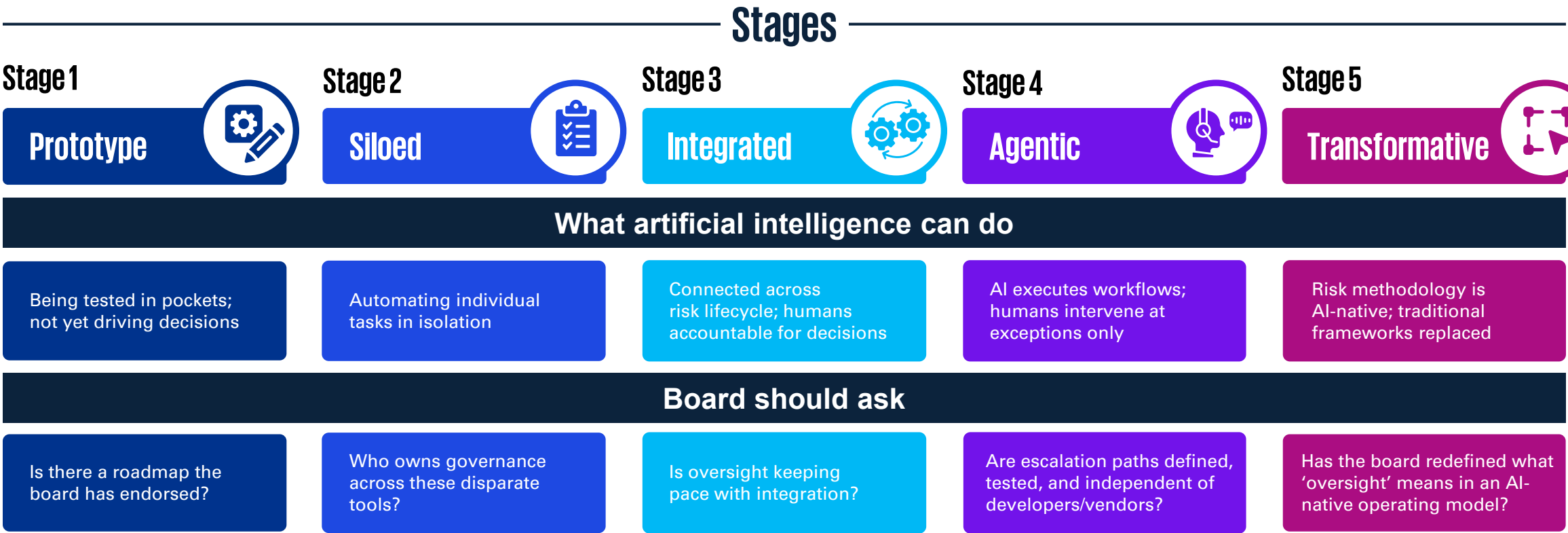
AI's impact is not uniform. It varies by stage of the risk lifecycle and by organisational maturity. The table below summarises what changes and what boards should focus on at each stage.

Stage	Before AI	What AI changes	Board implication
Risk identification 	Manual scanning, periodic reviews, analyst-dependent	Continuous pattern detection across operational and financial data; earlier and probabilistic signals	Ensure management can evidence signal quality, false positives, and escalation thresholds
Risk assessment 	Qualitative ratings, committee judgement, point-in-time	More consistent ratings at scale — but dependent on training data and embedded assumptions	Treat model assumptions as governance: who approves them, tests them, and revises them?
Risk mitigation 	Issue logs, manual root cause analysis, slow response cycles	Faster root-cause hypotheses, control mapping, and prioritisation of remediation based on signals	Define where automation is allowed vs where human sign-off is mandatory
Risk monitoring 	Periodic dashboards, static thresholds, backward-looking KRIs	Continuous control testing; anomaly detection on every transaction; dynamic thresholds	Require monitoring of the model itself (drift, bias, performance under stress)
Risk reporting 	Manually compiled reports, inconsistent formats, significant analyst time	Near real-time dashboards and automated narratives; algorithmic visibility thresholds	Know what is being excluded: ensure auditability and explainability of reporting logic
Testing and validation 	Sample-based testing, resource-constrained, infrequent coverage	Automated testing across full data sets; continuous anomaly learning; faster validation cycles	Mandate independent validation, model change control, and periodic AI red teaming

Read together, these shifts describe something important: risk management is increasingly evolving into a more continuous and forward-looking discipline. The board's role — historically calibrated to a quarterly rhythm of reports and committee reviews — may need to evolve accordingly. The question is not whether to embrace this change, but how to govern it wisely.

What boards should see as AI gets embedded in risk operations

There is a meaningful difference between deploying AI and genuinely embedding it. Deployment is the easy part. Embedding requires connecting AI tools into the organisation's Governance, Risk and Compliance (GRC) and ERP systems, governing the data they depend on, and ensuring the humans remaining in the loop are adding real judgment rather than simply approving outputs at speed.



What the board is expected to own

The board's role is to ensure that the organisation is making considered choices about how AI is used in risk management, that those choices are governed appropriately, and that accountability is clear. With that in mind, there are four areas where board engagement is most consequential.

The human in the loop — by design, not by default

One of the most important design choices in an AI-enabled risk function is defining where human judgment must remain present. This is to do with institutional accountability. An AI that flags a potential control failure is a tool. An AI that determines the organisation's response to that failure — without human review — is something quite different. Well-designed risk functions treat the human-in-the-loop not as a reluctant concession to governance, but as a deliberate architectural feature. They have mapped the moments in the risk lifecycle where automated decision-making is appropriate, and the moments where it is not. The board is expected to know whether its own organisation has made these choices explicitly or whether the boundaries have simply evolved as capability has expanded.

Data — the foundation that determines everything

AI in risk management is only as sound as the data that informs it. That is a governance issue, not merely a technical one. Fragmented or poorly owned data does not become accurate when fed into a model; it becomes more confidently wrong. Boards should ask whether risk data is owned, standardised, lineage-tracked, and quality-controlled across entities and systems — especially where group structures and multiple geographies increase complexity.

The workforce that risk management now requires

Future risk functions will require new capability alongside traditional expertise: model validators, AI governance specialists, and data professionals embedded in risk teams. This is not about replacing experienced risk managers; it is about ensuring they can challenge AI systems with confidence. The board's interest is practical: does the organisation have a credible talent plan, and are staff trained to interrogate outputs, detect anomalies in model behaviour, and escalate appropriately?

Regulatory expectations are arriving — not approaching

Indian regulators have been clear in their direction of travel. The Reserve Bank of India, SEBI, and central government bodies have each turned attention to AI governance, with frameworks, consultation papers, and guidelines that signal a shift from voluntary good practice to expected standard. Transparency in how AI decisions are made, explainability of model outputs, and evidence of board-level engagement are moving from aspirational to required. The organisation that has built its AI governance deliberately — that can show a regulator how its risk AI is supervised, challenged, and accountable — is in a fundamentally stronger position than one that has deployed capable technology without equivalent governance. The board's role is to ensure the organisation is building for that standard, not waiting to be asked for it.



The double edge: AI as risk manager and risk creator

AI has the potential to improve risk management substantially: it can reduce cost, automate elements of compliance, and increase the speed, consistency, and breadth of monitoring and insight. However, these benefits come with new model-related risks that warrant dedicated oversight. Boards may therefore need to treat AI as both an enabler of risk management and a distinct risk source—one that may not fit neatly within traditional governance patterns.

Model drift embeds historical patterns into future decisions at scale, invisibly in aggregate reporting and undetected by standard GRC controls. Model drift causes systems that performed well in stable conditions to fail precisely when accurate risk assessment matters most.

Third-party AI dependency — a growing concern as organisations rely on external vendors for core risk functions including credit scoring, AML monitoring, and regulatory reporting — means a vendor changing a model's underlying logic can compromise processes in ways difficult to detect from inside. And as Indian enterprises integrate with national digital platforms and interconnected financial infrastructure, a failure in one AI system can **cascade through the network** in ways no individual ERM model was designed to anticipate.

The board that governs only the benefits of AI in risk management, while leaving its failure modes to management, has an incomplete governance posture. These are not operational concerns. They are accountability questions that belong at the board table.

Board decision points

To make oversight operational, boards may consider agreeing a small number of decision points that management brings for approval and periodic review

- **AI inventory:** a register of AI systems influencing risk decisions (including vendor tools), with owners and purpose
- **Autonomy boundaries:** which decisions may be automated, which require human sign-off, and what triggers escalation
- **Model risk appetite:** acceptable thresholds for false positives/negatives, customer impact, and control failures
- **Change control:** how model updates (internal or vendor-driven) are approved, tested, and communicated
- **Independent assurance:** who validates models, how often, and how results reach the board or its committees
- **Incident readiness:** tested response playbooks for model failures, data breaches, and regulatory challenge.



