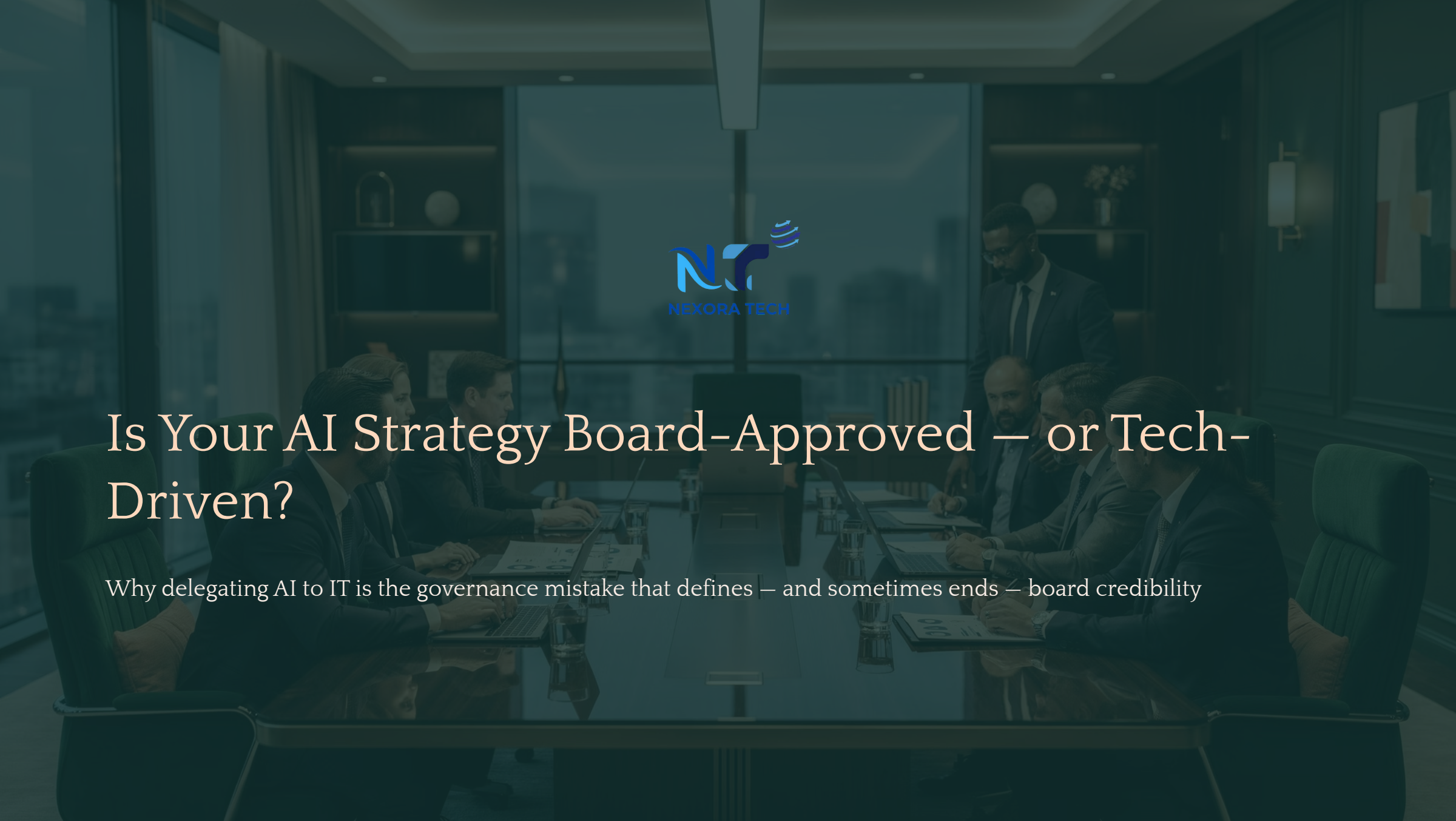


NEXORA TECH

Is Your AI Strategy Board-Approved — or Tech-Driven?

Why delegating AI to IT is the governance mistake that defines — and sometimes ends — board credibility

Contents

01 Executive Summary

02 Context & Urgency Framing

03 Risk Taxonomy

04 Regulatory Landscape

05 Strategic & Capital Implications

06 Operating Model Considerations

07 Maturity Framework

08 Board-Level Questions to Ask Management

09 Case Illustrations

10 12–24 Month Action Roadmap

11 Strategic Conclusion

Executive Summary

There is a pattern across industries in how AI decisions are being made, and it should concern every board. The decision to deploy a large language model in a customer-facing product, to procure a third-party AI system for credit decisioning, to build proprietary models on proprietary data — these are choices that carry material legal, financial, and reputational consequences. Yet in most organisations, these decisions are being made by technology leadership, endorsed by executive committees, and presented to boards as accomplished facts rather than strategic choices pending approval.

The distinction between a board-approved AI strategy and a tech-driven one is not semantic. A board-approved strategy means that the organisation's AI investment portfolio, risk appetite, prohibited use cases, and success criteria have been explicitly reviewed and sanctioned at the highest level of governance. A tech-driven strategy means that technology leaders — with the best of intentions — are making consequential choices about what AI the organisation uses, at what scale, on what data, and in what contexts, without a governance mandate that holds them accountable to the organisation's values, risk tolerance, and regulatory obligations.

> The strategic risk exposure is direct. An AI programme that is not board-governed is a programme whose failure — operational, reputational, or regulatory — cannot be defended on governance grounds. Boards that have not approved an AI strategy have, in practice, approved everything management chooses to do, without the oversight structures that would limit liability or enable timely intervention.

The regulatory urgency is accelerating. The NIST AI Risk Management Framework explicitly connects AI technical decisions to organisational values and strategic priorities through its GOVERN function — making clear that governance is not a layer added on top of technology decisions but the precondition for making them responsibly. The EU AI Act reinforces that transparency and governance controls are obligations, not choices, for high-risk AI systems. India's regulators are closely watching deployment patterns, and the sector-specific guidance from RBI and MeitY signals that the expectation of accountable AI governance is moving from advisory to mandatory.

The board that has not approved its organisation's AI strategy has, by default, approved every risk that strategy entails.

The capital implication is equally clear. AI washing enforcement by the SEC has established that the narrative organisations tell about their AI to investors, analysts, and the market must be governed with the same rigour as any material disclosure. The gap between the AI story being told externally and the AI governance reality internally is a liability that markets are beginning to price.

Context & Urgency Framing

The Governance Vacuum at the Centre of AI Deployment

The velocity of AI deployment in enterprises has created a structural governance gap. Technology teams move at the pace of model releases, vendor capability updates, and competitive pressure. Governance structures — boards, committees, risk frameworks — move at the pace of quarterly cycles, annual strategy reviews, and deliberative process. In the space between these tempos, AI systems are entering production in volume, carrying risks that governance has not assessed and in contexts that strategy has not addressed.

This is not a criticism of technology leadership. It is a structural observation about where decision rights sit. The question of which AI systems the organisation deploys, in what contexts, with what controls, and at what pace, is a strategic and governance question — not merely a technical one. When boards delegate this entirely to IT, they are not simply being deferential to technical expertise. They are abdicating governance responsibility for decisions that directly affect the organisation's legal exposure, regulatory standing, and enterprise value.

The Diagnostic Question

The most useful diagnostic a board can apply is simple: has the board explicitly approved what AI the organisation is building, buying, and using — including its dependence on general-purpose AI and large language models from third-party providers? Has the board defined where AI is prohibited — the use cases that should not proceed without validated controls, regardless of commercial opportunity? Has the board set success criteria that go beyond deployment speed to include safety, fairness, and compliance measures?

> If the answer to any of these questions is no, the organisation does not have a board-approved AI strategy. It has a technology programme operating in a governance vacuum.

Tech-Driven vs. Board-Approved AI — Signals

Tech-Driven AI — Signals

- Board learns of AI deployments after the fact
- No explicit prohibited-use list approved at the board level
- Success metrics are deployment velocity and feature count
- Risk appetite for AI is not documented or board-approved
- AI vendor decisions made by procurement and IT alone
- No standing board agenda item for AI portfolio review

Board-Approved AI — Signals

- The board has reviewed and approved the AI investment portfolio and risk appetite
- Prohibited use cases are explicitly defined and enforced
- KPIs and KRIs are paired for every material AI initiative
- Quarterly AI portfolio review is a standing board item
- Audit Committee governs AI claims in investor materials
- Incentives reward safe, compliant value — not just deployment

Why Boards Cannot Delegate This

> AI is not an IT project with IT consequences. It is a strategic capability with board-level risk exposure.

The cases that have produced regulatory action, shareholder litigation, and reputational damage in the AI space are not cases of technical failure alone. They are cases of governance failure — of decision-making structures that placed the authority to deploy AI systems ahead of the accountability structures designed to govern the consequences. Boards that treat AI as a technology matter delegate not just a decision but a liability.

Risk Taxonomy

The risks arising from an ungoverned AI strategy are distinct from those of individual AI system failures. They are structural risks — arising from the absence of a governance framework — rather than operational ones. The following taxonomy maps these risks to the oversight domains that boards are constituted to address.

Strategic

Investment Misalignment & Capability Overhang

AI spend not mapped to board-approved use cases creates investment portfolios with no defined success criteria, no exit discipline, and no accountability for value realisation. The organisation builds AI capabilities that it cannot govern or defend.

Operational

Hallucination Persistence & Model Collapse Risk

Hallucination in large language models cannot be eliminated through calibration alone — mitigation requires post-training controls, context grounding, and human oversight design. Additionally, training pipelines contaminated by synthetic content ("model collapse") degrade model quality over time. Without board-level awareness, these known hard problems are treated as engineering challenges rather than risk management obligations.

Regulatory

Governance-Gap Liability

Regulators assess governance as a precondition for deployment, not as a parallel track. NIST's GOVERN function, the EU AI Act's risk management requirements, and India's sector guidance all expect documented, accountable governance structures. Organisations that cannot demonstrate board-level AI oversight face elevated regulatory risk regardless of whether individual systems have caused harm.

Risk Taxonomy (Continued)

Cyber & Data

AI-Specific Vulnerabilities Without Governance Mandate

Data poisoning, adversarial examples, model inversion, and training data contamination are AI-specific cyber risks. The EU AI Act explicitly identifies these as cybersecurity obligations for high-risk AI systems. Without a board-level mandate that includes AI in the cyber risk framework, these vectors remain outside traditional IT security governance.

Reputational

Narrative Incoherence Between AI Claims and Reality

When the AI story told to investors, media, and customers is not governed by the same rigour as the AI reality inside the organisation, the gap becomes a reputational liability. The speed at which AI failures become public events makes narrative incoherence a board-level risk, not a communications problem.

Capital

AI Washing Liability & Misallocated Investment

SEC enforcement actions have established that misleading AI claims in investor communications carry securities liability. Simultaneously, ungoverned AI investment portfolios — where spend is not mapped to approved use cases or measurable outcomes — represent a failure of capital allocation discipline that institutional investors are increasingly scrutinising.

These risks compound. A strategic risk — investment in AI without a board-approved thesis — creates operational risk (ungoverned deployment), which creates regulatory risk (absence of documented governance), which amplifies reputational risk (when failures occur), which crystallises capital risk (investor concern about governance quality). The cascade is not theoretical. It is the documented pattern of major AI governance failures.

Regulatory Landscape

India: A Principles-Based Governance Expectation

India's AI regulatory environment does not yet operate through prescriptive AI-specific legislation at the scale of the EU AI Act. What it does operate through is sector-specific guidance, principles-based oversight, and a supervisory approach that increasingly expects documented governance. The RBI's model risk management guidance — applicable to financial institutions — requires explainability, independent validation, and ongoing performance monitoring for AI-driven models. This is a governance expectation at the board level, not merely a technical standard. SEBI's attention to algorithmic accountability in securities markets reinforces the theme. MeitY's advisory on synthetic media and deepfakes — requiring labelling and metadata for AI-generated content on platforms with consumer exposure — represents the first explicit generative AI governance obligation in India's regulatory environment, with direct implications for boards of organisations operating consumer-facing AI applications.

Critically, the Digital Personal Data Protection Act 2023 constrains what data AI systems can be trained and operated on when that data includes personal data of Indian residents. Board-approved AI strategy must account for these constraints as a governance requirement, not as a legal compliance afterthought.

Global Frameworks as the Governance North Star

The NIST AI Risk Management Framework's GOVERN function provides the clearest articulation of what board-level AI governance requires: organisational values and risk tolerance must be explicitly connected to AI deployment decisions. The framework is explicit that accountability structures must be established before deployment, not retrofitted after failure. The EU AI Act codifies this as law for high-risk AI systems: risk management must be documented, human oversight must be designed in, and robustness and cybersecurity obligations — including protections against data poisoning and adversarial attacks — must be met. The WEF AI Governance Alliance's "shift-left" framing captures the operational implication: safety and governance must be built into AI systems at the design stage, not added as controls after deployment.

> For boards, the fiduciary implication is clear. These frameworks define what "reasonable governance" for AI looks like. A board that has not reviewed its organisation's AI strategy against these frameworks cannot demonstrate reasonable governance if called to account by a regulator, investor, or court.

Strategic & Capital Implications

The enterprise value implications of AI governance quality are no longer speculative. The governance quality of an organisation's AI programme affects its regulatory approval timelines, insurance and capital provisioning requirements, standing with institutional investors, and competitive position relative to peers that have built governance-enabled deployment capacity.

On the investment side, the discipline question is whether AI spend is mapped to board-approved use cases with defined success criteria and risk controls. Organisations that cannot answer this question do not have an AI investment thesis — they have an AI spending pattern. The difference matters to investors, who are increasingly asking for evidence that AI investment is generating value rather than being deployed at pace without accountability. The concept of "AI value realisation" — measurable in terms of time-to-value and adoption — is becoming a standard line of inquiry for investors alongside the more familiar cyber and data governance questions.

> An AI investment thesis without a governance framework is a wager. A board that has approved the thesis but not the governance has approved the wager without setting the odds.

The AI washing risk carries a specific capital dimension. SEC enforcement has set a precedent that investor-facing AI claims require evidentiary substantiation equivalent to that required for any material disclosure. For boards operating in jurisdictions where securities regulators are developing similar frameworks — including India — this means that the process by which the organisation's AI narrative is constructed and approved is itself a governance obligation. Boards that have not established a pre-clearance process for AI claims in investor communications are carrying an undisclosed securities liability.

Long-term competitiveness also depends on governance maturity. Regulatory approval for new AI use cases in financial services, healthcare, and infrastructure will increasingly require demonstrated board-level oversight. Organisations that have invested in governance infrastructure will move through approval processes faster and with lower compliance costs than those that have not.

Operating Model Considerations

Making AI a Standing Board Agenda Item

The single most consequential operating model change a board can make is to establish a quarterly AI portfolio, risk, and compliance review as a standing full-board item — supplemented by committee deep-dives in Risk and Audit. This is not a procedural change. It signals to management, regulators, and investors that AI is treated as a material strategic matter requiring board-level accountability, not as a technology project delegated entirely downward. The WEF AI Governance Alliance and NIST GOVERN function both emphasise this cadence as the baseline governance expectation for organisations with material AI exposure.

Committee Responsibilities

A functional distribution of AI governance across committees avoids both the oversight gap and the inefficiency of full-board management of technical detail. The Risk Committee owns the AI risk appetite definition, incident taxonomy, and the review of AI initiatives in high-risk categories. The Audit Committee owns AI disclosure controls — the pre-clearance of AI claims in investor materials, the evidentiary pack behind published AI narratives, and the assurance that AI-related disclosures are accurate and substantiated. The ESG or People Committee owns the fairness, non-discrimination, and responsible AI dimensions of the organisation's AI programme, including alignment with India's responsible AI framework and the OECD principles.

Incentive Alignment

One of the most under-examined governance levers is incentive alignment. In most organisations, the performance metrics that govern technology leadership reward deployment pace, feature delivery, and model capability — not safety, fairness, or compliance outcomes. This creates a structural misalignment between what governance requires and what management is incentivised to deliver. Boards should ask whether leaders are rewarded for safe, compliant value creation, or simply for "shipping AI." The answer to that question tells you more about the actual governance culture than any policy document.

Vendor and GPAI Dependency Risk

The concentration of enterprise AI capability in a small number of general-purpose AI and large language model providers represents a vendor dependency risk that deserves explicit board attention. Organisations that have built core customer or operational functions on proprietary third-party models create a strategic dependency that affects their negotiating position, regulatory standing, and resilience. The board's AI portfolio review should include a dependency map — which functions rely on which AI providers, the exit or substitution options, and the obligations those dependencies create under DPDP, DORA, and relevant sectoral guidance.

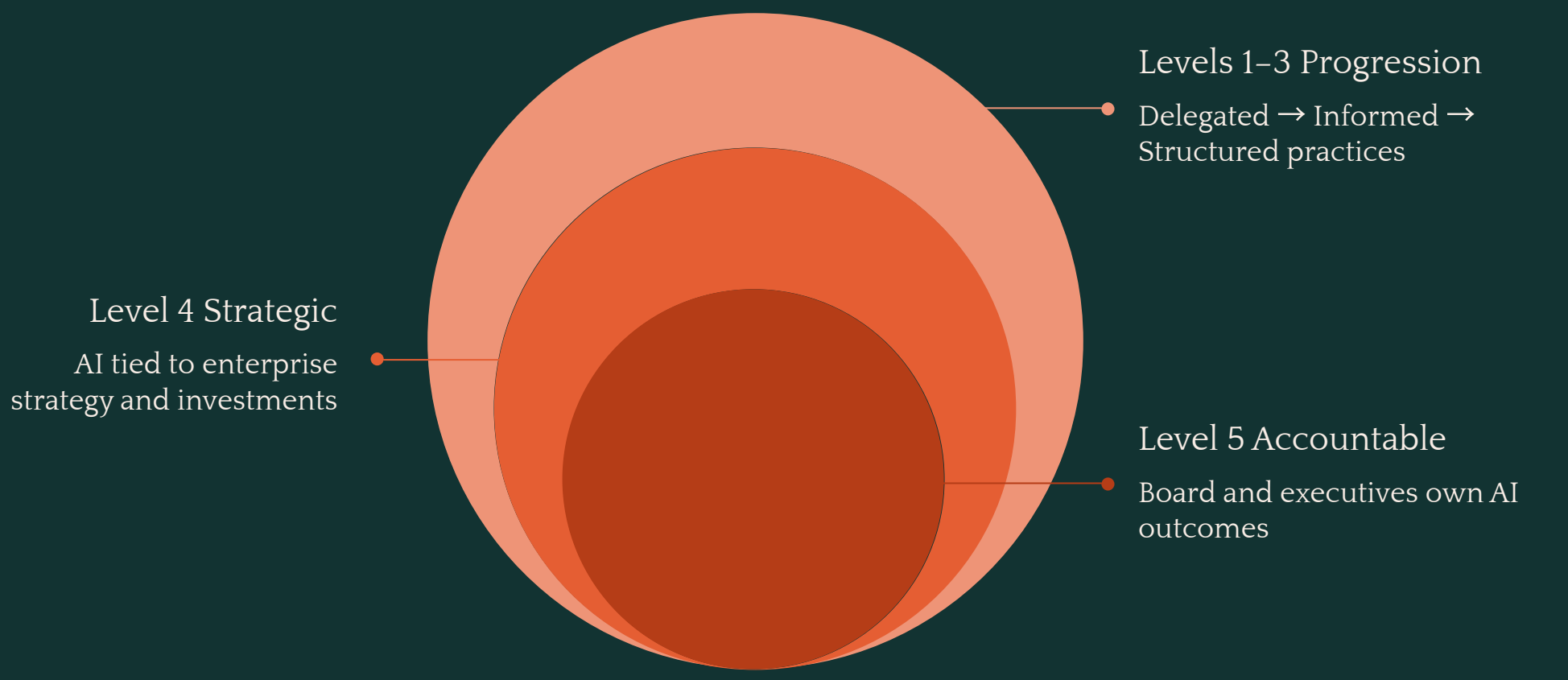
AI Strategy Governance Maturity Framework

The following framework assesses the maturity of an organisation's AI strategy governance — specifically, the extent to which AI decisions are board-driven rather than tech-driven.

Level	Board Governance Characteristics	Accountability Signal
Level 1 Delegated	AI decisions are entirely tech-driven. No board-approved AI strategy, risk appetite, or prohibited-use list. The board receives no regular AI reporting. Success is measured by deployment volume. It manages incidents without board visibility. No rules govern AI claims in investor materials.	Maximum governance gap. Liability is concentrated and unpriced. Regulatory exposure is high.
Level 2 Informed	The board receives occasional AI updates. Some AI initiatives have documented objectives. The risk appetite discussion has begun, but is not formalised. The Audit Committee is aware of AI claims in investor materials, but has no formal review process. No standing AI agenda item.	Governance awareness present, accountability structure absent. Exposure reduced but not managed.
Level 3 Structured	The board has reviewed and approved the AI risk appetite. Portfolio view of AI investment is maintained. Prohibited use cases are defined. Quarterly AI review is a standing agenda item. Committee responsibilities are allocated. KPIs and KRIs are paired for material AI initiatives. AI claims in investor materials require Audit Committee pre-clearance.	Defensible governance posture. The board can demonstrate accountability to regulators and investors.

AI Strategy Governance Maturity Framework (Continued)

Level	Board Governance Characteristics	Accountability Signal
Level 4 Strategic	AI strategy is integrated into the enterprise strategy and capital allocation framework. The AI investment thesis is board-approved with downside scenarios and liability planning. Incentives are aligned to safe, compliant value creation. Vendor dependency is mapped and governed. AI governance maturity is disclosed to investors. Regulatory readiness is benchmarked against NIST, EU AI Act, and DPDP.	AI governance is a competitive and reputational asset. Enables faster regulatory approvals and investor confidence.
Level 5 Accountable	AI strategy governance is inseparable from corporate governance. The board has real-time visibility through AI risk dashboards. Governance is embedded in the AI development lifecycle from inception. The organisation participates in regulatory and industry standard-setting. External reporting on AI governance is a standard component of annual reports and ESG disclosures.	Governance as organisational identity. Regulatory relationships are collaborative. Investor engagement on AI governance is proactive.



Organisations should assess their current maturity level honestly and use this framework to define a clear progression path toward board-driven AI governance.

Board-Level Questions to Ask Management

The questions below are sequenced from portfolio accountability through to accountability structure. They are designed for a standing quarterly AI review or as the basis for an initial AI governance assessment.

1 Portfolio View

Has the board approved a portfolio view of the organisation's AI programme — covering what we are building, buying, and using — including our dependence on general-purpose AI and large language model providers?

2 Prohibited Use Cases

Has the board defined and approved the use cases where AI is explicitly prohibited or requires validated controls before deployment, regardless of commercial opportunity?

3 Paired KPIs and KRIs

For every material AI initiative, can management provide paired KPIs and KRIs — success metrics and risk controls defined before deployment, not retrospectively?

4 Incentive Alignment

Are performance incentives for technology and AI leadership aligned to safe, compliant value creation, or do they primarily reward deployment speed and model capability?

5 Known Hard Problems

How does our AI strategy account for known hard problems — specifically, hallucination persistence in large language models and the risk of training data contamination from synthetic content?

6 Vendor Dependency

What is the organisation's vendor dependency profile for AI — which core functions rely on which providers, and what are our exit or substitution options if a key provider changes its terms, pricing, or availability?

1 AI Claims Process

What is the process by which AI claims in investor communications, annual reports, and marketing materials are reviewed, evidenced, and approved before publication?

2 Standing Review

Is there a standing quarterly AI portfolio, risk, and compliance review at the board level, and are committee responsibilities for AI oversight explicitly allocated and documented?

3 Regulatory Readiness

What is our current regulatory readiness posture for AI-specific obligations — NIST GOVERN function, EU AI Act high-risk system requirements, RBI model risk guidance, and India DPDP constraints on AI training?

4 Independent Review

Has an independent review of the organisation's AI governance been commissioned in the past twelve months, and what were its findings?

5 Ungoverned Deployments

Are there AI systems currently in production that were deployed without a documented risk assessment or board-level awareness? If so, what is the remediation plan?

6 AI Trust Indicators

How does the organisation track "AI trust indicators" — incidents, customer complaints, system overrides, and model performance degradation — and how are these reported to the board?

Case Illustrations

Governance Stability Risk

When AI Governance Becomes Corporate Governance — OpenAI's November 2023

The public leadership transition at OpenAI in November 2023 was not primarily a management event. It was a governance event — one that made visible, in real time, how AI governance structures interact with corporate stability, board confidence, and market perception. The incident demonstrated that the quality of AI governance structures is not a background condition but an active variable in organisational stability, and that board decisions about AI leadership and oversight carry material implications for communication and confidence. For boards outside the AI-native sector, the lesson is that governance of AI organisations and governance by AI-deploying organisations both require explicit structures that can withstand scrutiny under stress.

Strategic Misalignment — Narrative Without Governance

AI Washing and the Cost of an Ungoverned AI Story — SEC Enforcement

The SEC's AI washing enforcement actions confirmed what many governance advisors had argued: the AI narrative an organisation constructs for investors is governance territory, not marketing territory. Organisations that positioned themselves as AI leaders in investor communications, without the underlying governance structures and evidentiary backing to substantiate those claims, faced enforcement action and reputational damage. For boards, the implication is that every investor communication describing AI capabilities is a disclosure decision — and that the process by which those communications are constructed and approved must be subject to the same rigour as any other material disclosure. The Audit Committee's mandate extends to the AI story.

Governance Failure Mode — Incentive Misalignment

The Large Financial Institution That Shipped First and Governed Later

A hypothetical but entirely representative scenario: a financial institution deploys an AI-based product recommendation engine in its retail banking division. A technology leadership team drives deployment, incentivised by deployment timelines. The system has been in production for 11 months before an internal audit flags that the model's training data has systematic demographic biases, leading to differential recommendations for certain customer segments. The remediation cost — model retraining, customer remediation, regulatory engagement — significantly exceeds the original deployment budget. The board learns about the issue through the audit report, not through management escalation. The governance failure is not the bias — it is the absence of the governance structure that would have caught it earlier and managed it at lower cost. A paired KRI for fairness, set at deployment, would have triggered the alert within weeks.

Case Illustrations (Continued)

Governance Success — Board-Approved Strategy Enabling Deployment Confidence

The Insurer That Built the Governance Before the Model

An insurance organisation entering AI-driven underwriting established a board-approved AI investment thesis as a precondition for any deployment above a defined materiality threshold. The thesis included a portfolio view of build, buy, and use decisions; a prohibited-use list covering claims fraud detection without human-in-the-loop review; paired KPIs and KRIs for each initiative; and a quarterly board reporting cadence. When the organisation's AI programme came under regulatory review 18 months later, it was able to produce a complete governance record — from board approval through deployment to performance monitoring. The review concluded in six weeks rather than the twelve-month process faced by peers without equivalent documentation. The governance investment had created a deployment licence that the organisation's competitors did not have.

Tech-Driven: What Goes Wrong

- AI was deployed before the risk assessment was completed
- Investor claims precede governance structures
- Hallucination and bias discovered through customer complaints
- Regulatory review takes 12+ months without a governance record
- Board learns of material AI failures through audit or press

Board-Approved: What Holds

- Deployment preceded by board-approved risk assessment
- AI narrative governed by Audit Committee pre-clearance
- KRIs detect model performance issues before customer harm
- Regulatory review is completed in weeks with a governance record
- Material AI risks escalate to the board through defined thresholds

12–24 Month Action Roadmap

1 Months 0–3 · Foundation — Establish the Governance Mandate

- Commission an AI portfolio inventory: what is the organisation building, buying, and using, at what scale, in what contexts
- Draft a board-level AI risk appetite statement for review and approval
- Define a preliminary prohibited-use list: use cases that require validated controls before any deployment
- Establish a quarterly AI portfolio, risk, and compliance review as a standing full-board agenda item
- Allocate AI oversight responsibilities across Audit, Risk, and ESG committees

2 Months 3–9 · Structure — Build the Investment Thesis and Disclosure Controls

- Require a board-approved AI investment thesis for all material AI spend, including downside scenarios and liability planning
- Mandate paired KPIs and KRIs for every material AI initiative currently in production and all new deployments
- Implement Audit Committee pre-clearance for AI claims in investor materials, earnings communications, and regulatory filings
- Map vendor dependencies for GPAI and LLM providers; assess exit and substitution options
- Review incentive structures for technology leadership: ensure alignment with safe, compliant value delivery

3 Months 9–18 · Integration — Embed Governance in the AI Lifecycle

- Integrate AI risk assessment into the pre-deployment process for all new AI initiatives above the materiality threshold
- Implement AI trust indicator dashboard: incidents, complaints, overrides, model performance degradation — reported quarterly to Risk Committee
- Conduct regulatory readiness assessment against NIST GOVERN, EU AI Act, DPDP, and sector-specific guidance
- Commission first independent review of AI governance framework and publish findings to the board
- Develop an AI governance literacy programme for the board and Non-Executive Directors

4 Months 18–24 · Leadership — Governance as Strategic Positioning

- Disclose AI governance maturity in annual report and ESG reporting; benchmark against peers
- Establish AI governance performance as a board-level KPI linked to executive accountability
- Engage proactively with sector regulators on AI governance practices; participate in consultations
- Achieve Level 4 maturity ("Strategic") across all five framework dimensions

Metrics Boards Should Track

Portfolio Discipline

Share of AI spend mapped to board-approved use cases with defined success criteria

Initiative Coverage

% of AI initiatives with paired KPIs and KRIs defined at deployment

Value Realisation

Time-to-value and adoption rate across material AI initiatives

Trust Indicators

Incidents, customer complaints, model overrides — trend and resolution time

Strategic Conclusion

The question of whether an organisation's AI strategy is board-approved or tech-driven is, at its core, about where accountability lies. Technology leadership can build and deploy AI systems of considerable sophistication. What it cannot do — because it is not constituted to do so — is define the organisation's risk tolerance, set the ethical boundaries of AI use, approve the investment thesis, or hold the organisation accountable to its own values when commercial pressure runs in the other direction. Those are board responsibilities. They have always been board responsibilities. AI has not changed what boards are for. It has made the exercise of those responsibilities more consequential and more urgent.

The organisations that will navigate the AI era with their governance credibility intact are not those that deployed AI earliest or most extensively. They are those that deployed with a board mandate, a documented risk appetite, a defined set of prohibitions, and the accountability structures to detect and respond when things go wrong. Governance does not slow AI down. It makes AI defensible — to regulators, investors, customers, and the public — in a regulatory environment moving decisively toward accountability.

> The board's role is not to become a technology committee. It is to ensure that technology decisions are made within a governance framework approved by the board and that the board can defend.

The question every board should leave its next session having answered is not **"what AI are we building?"** It is **"Have we approved the governance framework within which AI is being built?"** If the answer is yes, the organisation is positioned to lead. If the answer is no, that is the most important AI decision the board has yet to make.

About the Author



Aparna Kumar

Founder, Nexora Tech

sales@nexoratechsolutions.com

www.nexoratechsolutions.com

WhatsApp: +91-8799918172

Apaarna S Kummar is a business and technology leader with deep experience in enterprise transformation, digital strategy, and building high-performance organisations. She writes on the intersection of technology, leadership, and business impact, with over three decades of experience in the banking and multinational IT consulting sectors. She has held pivotal roles before Founding Nexora Tech, including Chief Information Officer at SBI and HSBC, and senior leadership roles at HDFC Bank, Capgemini, Oracle, and Citi, leading transformative digital initiatives with cutting-edge technologies such as AI, cloud computing, and generative AI.

She, alongside her team of seasoned IT professionals, cybersecurity experts, and next-generation technology leaders, actively advises and supports over 25 clients through strategic engagements. She serves as a trusted Digital Transformation and Advanced Technology Advisor to leading organisations, bringing her strategic acumen and deep expertise across the BFSI, Healthcare, Agriculture, Automotive, Retail/FMCG, and Telecom industries. She mentors senior leaders, advises boards, fosters inclusive workplace cultures, and drives enterprise-wide innovation, guiding organisations in shaping forward-looking, resilient, and future-ready business strategies.

Apaarna is a management graduate, an alumna of the Indian School of Business (ISB), Hyderabad, a Master's in Computer Applications and a Graduate in Electronics, and a recognised thought leader and technology strategist.