On the risk agenda 2026

Board Leadership Center (India)

April 2026

kpmg.com/in

KPMG. Make the Difference.

Governing risk in an era of structural uncertainty

Risk is no longer a periodic discussion in the boardroom. It has become a permanent strategic condition.

The risk environment confronting boards today is structurally different from the one that shaped governance frameworks a decade ago.

Digital infrastructure now underpins essential business services. Artificial intelligence is increasingly embedded in operational and strategic decision making. Cyber incidents can disrupt entire enterprise ecosystems. Supply chains are being reshaped by geopolitical pressures, while climate transition expectations are influencing capital allocation and disclosure credibility. Regulatory scrutiny continues to expand across technology governance, sustainability and data protection.

These forces rarely operate independently. They interact and reinforce each other, increasing both the speed at which risks emerge and the scale at which they affect organisations.

In response, risk governance is moving closer to the centre of strategic decision making. Over the past decade the role of enterprise risk leadership has expanded significantly, with many large organisations establishing a chief risk officer or equivalent executive role with direct engagement at board level. Risk committees are evolving in parallel. Their role increasingly extends beyond oversight of control frameworks to providing forward looking risk insight, advising on risk appetite and ensuring alignment between strategy, resilience and governance.

For boards, the question is no longer whether risks exist. The question is whether the organisation has the **visibility, capability and leadership discipline required to operate effectively when risks interact and accelerate.**

The themes that follow highlight issues likely to shape risk committee discussions in the year ahead and support board level reflection on how oversight may continue to evolve in an environment that is more interconnected, more digital and more uncertain than ever before.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

01 Agility under uncertainty:
Macro, market, liquidity, and innovation risk

Macroeconomic conditions remain non-linear, with inflation persistence, policy and rate shifts, uneven growth, and episodes of abrupt liquidity tightening often occurring simultaneously. These dynamics reinforce that agility—rather than precise forecasting—must guide decision-making, particularly in an environment where India continues to outperform global peers even as tariff actions and trade tensions create market-level pressures on Micro, Small and Medium Enterprises (MSME)-heavy sectors such as textiles and autos. Fiscal uncertainty, shifting policy signals, and domestic liquidity operations further influence market pricing, interest-rate dynamics, and investment flows.

Liquidity risk has re-emerged as a defining vulnerability, with stress episodes pushing up funding costs and driving outflows similar to earlier tightening cycles across Asia and digital-asset markets. Sector-specific liquidity gaps and climate-transition exposures remain insufficiently embedded in risk frameworks, while evolving market structures and product complexity are amplifying model, conduct, and market-liquidity risks faster than governance processes typically adapt.

Innovation-driven risk is rising in parallel. The rapid expansion of data-intensive models, cross-border digital products, and AI-generated content requires disciplined governance of intellectual property and data ownership. Protection, valuation, and monetisation of IP are increasingly central to competitive strategy, and disputes are becoming more complex across jurisdictions.

Against this backdrop, boards may prioritise trigger-based playbooks, diversified funding structures, valuation discipline, and clear decision rights enabling rapid adjustments to pricing, costs, capex, and portfolio actions under stress. Equally, they must strengthen IP strategy, digital-risk governance, and dispute readiness across key markets to ensure agility amid macro, market, liquidity, and innovation-driven uncertainty.

Board consideration

- What are our trigger points for rapid financial and portfolio actions?
- How resilient is our funding plan to tighter liquidity and margin calls?
- Where do we have hidden concentrations (customers, sectors, lenders, currencies)?
- Are valuation, model, and collateral controls robust for stress conditions?
- Do we have a coherent IP strategy covering creation, protection, licensing, and enforcement across jurisdictions?

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

02 Competing through credibility:
Governing regulatory complexity

Regulatory change is increasingly reshaping market structure and competitive advantage, making compliance a strategic capability tied to trust, market access, and operational speed. Yet many organisations still struggle to align with evolving frameworks, resulting in fragmented controls and rising exposure to oversight gaps. New mandates across sustainability, governance, and data protection are expanding accountability expectations and raising the stakes for credible reporting, integrated risk management, and consistent evidence trails. As global rules extend deeper into supply chains, Indian enterprises must strengthen compliance architecture to remain competitive and resilient.

Boards are increasingly evaluated on their ability to implement regulatory change smoothly and without operational strain. Yet many organisations still lack the tools, culture, and incentives needed for proactive compliance, resulting in slow detection and inconsistent governance. As expectations tighten, firms must embed compliance into their risk appetite, strengthen evidence and assurance mechanisms, and align leadership incentives with regulatory outcomes.
A unified, technology-enabled Governance, Risk and Compliance (GRC) approach turns compliance from a reactive obligation into a driver of resilience and competitive advantage.

Board consideration

- Where does compliance slow growth—and where can it enable growth?
- Do we have clear ownership and evidence for our major obligations?
- What is our maturity in executing regulatory change at scale?
- Which compliance risks are actually data and evidence risks?
- How aligned are incentives and culture with our conduct expectations?
- Are the risk mitigation and management plans articulated in our Enterprise Risk Management (ERM) framework genuinely actionable, with clear ownership, adequate resourcing, defined timelines, and the capability to be executed under real-world constraints?

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

03

From global efficiency to regional resilience:
Navigating geopolitics

The era of seamless global integration is giving way to a more fragmented operating environment. Geopolitical tensions, strategic competition and economic-security priorities are pushing governments to emphasise resilience, domestic capability and regional blocs over globally optimised systems.

This shift is reshaping international business. Supply chains, trade routes and logistics networks are more exposed to disruption, leading to higher transportation costs, energy volatility and unpredictable inventory cycles. Regulatory complexity is also increasing as export controls, industrial policies and investment-screening regimes alter market access and the flow of strategic goods.

Operating models designed for efficiency are now more vulnerable to geopolitical shocks and regulatory divergence. Organisations are reassessing concentrated dependencies across suppliers, trade corridors, energy inputs and critical materials, driving a rebalancing toward resilience, redundancy and regional diversification.

At the same time, competitive dynamics are being reshaped by national industrial strategies that favour localised production, technology self-sufficiency and on-shoring in strategic sectors. These shifts are influencing capital allocation decisions, access to incentives and the long-term viability of globally distributed footprints. Companies with heavy exposure to single-country manufacturing models or tightly coupled cross-border production systems face increasing operational and strategic pressure.

For boards, the strategic challenge is evaluating geopolitical exposure and concentration risks across global operations, and ensuring operating models remain robust as trade fragmentation and shifting policy environments reshape long-term business conditions.

Board consideration

- How exposed is our supply chain to geopolitical, trade policy, or sanctions-related shocks, and where are our single-point-of-failure risks?
- Which three dependencies (suppliers, geographies, logistics routes, or technologies) would hurt us most if restricted or disrupted?
- What would ‘regional resilience’ require in our operating and sourcing model?
- How quickly can we reconfigure suppliers, routes, or market focus if conditions change?
- Do we have governance to monitor policy shifts as leading indicators, not lagging events?
- Where could contested contexts trigger reputational or stakeholder backlash?
- Given that large organisations now engage full-time economists, do we have sufficient economic and geopolitical advisory capability to inform timely board decisions?

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

04

Beyond recovery:
Governing continuity in a digitally-dependent enterprise

Operational resilience is being defined by the ability to sustain critical services during disruption rather than simply restore them afterwards. Core business activities now depend on digital platforms, automation and interconnected technology systems. Customer onboarding, payments processing, supply chain coordination and internal decision making often rely on continuous availability of digital infrastructure. As enterprises adopt digital first operating models, disruptions affecting technology environments can quickly interrupt essential services.

Recent incidents across industries demonstrate how outages in cloud environments, enterprise software platforms or technology service providers can affect operations for extended periods. Ransomware has become a major operational-resilience threat, capable of crippling critical systems and extending recovery timelines. Recovery timelines following major technology disruptions are increasingly measured in days rather than hours when critical systems are affected.

These events highlight governance challenges as much as technical ones. Decision authority during major disruptions may be unclear, escalation protocols may not function effectively under pressure, and many organisations have not defined minimum viable operating levels for critical services.

Regulatory expectations are evolving accordingly. Supervisory frameworks increasingly expect organisations to identify critical business services, map technology dependencies supporting those services and test severe but plausible disruption scenarios.

For boards, effective oversight requires understanding which services must continue during disruption, how digital dependencies support those services and whether the organisation can sustain operations when critical technology infrastructure becomes unavailable.

Board consideration

- Are crisis decision rights and escalation protocols clearly defined and regularly tested?
- How dependent are essential services on external technology providers or cloud platforms?
- Which critical dependencies sit outside our control, and what are credible fallbacks?
- How do we define continuity when reputation and stakeholder confidence are impaired?
- Has management defined a Maximum Tolerable Period of Disruption (MTPD) for the organisation's most critical digital services?
- When was the last time the board or risk committee participated in a tabletop crisis simulation, such as a severe ransomware attack or major cloud outage?

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

05

Trust by design:
Cyber resilience and data stewardship

Digital trust is increasingly shaped by how effectively organisations protect and govern data. As enterprises expand their reliance on cloud infrastructure, third-party ecosystems and API-driven architectures, the digital attack surface continues "to widen across sector. **India recorded more than 265 million cyberattack attempts between october 2024 and september 2025**[1].Globally, organisations experienced an average of **1,968 cyberattacks per week in 2025**, representing a **70% increase since 2023**, as attackers increasingly leverage automation and AI to move faster, scale more efficiently, and operate simultaneously across multiple attack surfaces[2].

Organisations are also confronting emerging risks such as AI generated deepfakes, synthetic identities and executive impersonation attacks that can bypass traditional authentication mechanisms and enable sophisticated social engineering.At the same time, persistent structural vulnerabilities continue to drive large scale breaches. Cloud misconfigurations, insecure APIs and weaknesses in third party integrations remain among the most common pathways through which sensitive data is compromised.

Regulatory expectations are evolving alongside these technological shifts. India's Digital Personal Data Protection (DPDP) framework introduces new obligations around consent management, data protection assessments and accountability for organisations that process significant volumes of personal data. Sector regulators are also strengthening expectations related to encryption standards, cyber resilience testing, incident simulations and board level oversight of technology risk

Cybersecurity is no longer solely an operational-technology concern; it has become a matter of **data stewardship and enterprise-wide risk governance.**

Boards are therefore expected to develop clearer visibility into how sensitive data is collected, classified, protected and restored during disruptions. Leading organisations are mapping critical data assets, conducting multi-party cyber-incident simulations and monitoring resilience indicators such as system integrity, recovery time and data-restoration capability. Effective oversight now depends on tighter alignment between cybersecurity leadership, privacy governance and enterprise-risk management.

Board consideration

- What are our crown-jewel data assets, and what scenarios could compromise them?
- How quickly can we detect, contain and recover from a cyber incident affecting business-critical services?
- Are privacy and data-protection obligations embedded by design across products, processes and third-party arrangements?
- What would credible internal and external communications — including regulatory engagement — look like in the first 72 hours of an incident?
- What indicators does the board currently receive on detection capability, vulnerability management and emerging threats?
- How prepared is the organisation to comply with evolving data-protection and cyber-resilience regulations?
- Are cyber-incident simulations conducted regularly, and do they involve senior management and key decision-makers?

1. India records 265 million cyber attacks; Seqrite releases the India cyber threat report 2026, The Economics Times, December 2025
2. Global cyber attacks at all-time high as AI spreads, MSN, January 2026

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

06

Assuring automated decisions:
Responsible and ethical AI

Artificial intelligence is rapidly shifting from experimental deployments to becoming an embedded decision engine across organisations. Algorithms now influence credit assessments, recruitment screening, fraud detection and customer engagement. As these systems integrate into core processes, they introduce structural risks related to model opacity, data dependency, rapid error amplification and the potential for embedded bias.

Board oversight is beginning to adapt, but governance maturity remains inconsistent. While more boards now acknowledge AI-related risks, many organisations still lack formal frameworks for model accountability, validation and lifecycle monitoring. In the absence of these mechanisms, automated systems can shape operational outcomes without sufficient visibility into how decisions are produced or how failures may propagate.

High-impact use cases demand heightened scrutiny. AI models used in lending, hiring or behavioural monitoring can generate discriminatory outcomes when trained on incomplete, historically biased or unrepresentative datasets. When automated decisions affect customers, employees or access to essential services, algorithmic "bias and limited explainability become material governance concerns.

Regulatory regimes are starting to respond. The EU Artificial Intelligence Act introduces a risk-based framework with stringent obligations for high-risk systems, including documentation, oversight and continuous monitoring. In India, the DPDP Act, 2023 reinforces organisational accountability for responsible data processing and underscores the importance of robust data governance in automated decision environments.

Limited model explainability can hinder internal audits and weaken the defensibility of automated decisions. Reliance on third-party AI solutions can also create dependencies that operate outside direct organisational oversight. As adoption accelerates, responsible governance will increasingly require structured model oversight, independent validation and continuous monitoring to detect bias, model drift and unintended outcomes.

For boards, the central challenge is to ensure innovation advances within governance guardrails that uphold fairness, accountability and transparency—while maintaining clear visibility into how automated systems influence critical operational decisions.

Board consideration

- Does the board have visibility into where AI systems are used across the organisation?
- Are high impact AI applications subject to independent validation and oversight?
- How does the organisation ensure automated decisions remain explainable and fair?
- Are responsibilities for AI governance clearly defined across risk, technology and compliance teams?
- How frequently does the board review developments in AI related regulation?
- How is the committee balancing the risks of AI adoption against the strategic risk of falling behind competitors due to AI inaction?
- What controls are in place to prevent the leakage of proprietary corporate intellectual property when employees utilise public generative AI tools?

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

07 Transition with evidence:
ESG oversight and disclosure credibility

Climate transition and sustainability risks now span physical, regulatory and reputational dimensions. Increasingly, the credibility of corporate disclosures has become the central focus of scrutiny. Investors, regulators and civil society are demanding verifiable evidence of progress rather than broad sustainability narratives.

Regulatory frameworks are tightening in response. Emerging global standards require more rigorous emissions reporting, clearer transition planning and greater transparency across value chains. These developments are exposing gaps in organisational readiness, particularly where climate commitments are not supported by measurable targets, operational plans or clear governance oversight.

At the same time, physical climate impacts are already affecting operations in several sectors through supply disruptions, exposure to extreme weather events and rising insurance costs. Transition risks associated with evolving carbon pricing regimes and tightening regulatory expectations are adding further financial and strategic pressures. Together, these dynamics are making credible climate strategies and transparent disclosures central to long term resilience.

In India, the Business Responsibility and Sustainability Reporting framework requires listed companies to provide structured disclosure on environmental, social and governance metrics, with increasing emphasis on data integrity and independent assurance.

Assurance credibility is therefore becoming a central governance concern. While investor expectations for verified sustainability disclosures continue to rise, many organisations still rely on limited or unaudited reporting. Reviews by oversight bodies have highlighted weaknesses in unsupported or inconsistent claims, increasing exposure to regulatory scrutiny and reputational damage.

For boards, the challenge is ensuring that climate commitments are supported by measurable progress. Integrating transition metrics into strategy, strengthening disclosure controls and linking executive incentives to climate accountability are increasingly viewed as essential steps in closing the gap between stated ambitions and demonstrable outcomes.

Board consideration

- Are sustainability risks embedded in strategy or treated primarily as reporting?
- Can we defend our claims with consistent evidence and audit-ready data?
- Which assets and suppliers are most exposed to physical disruption?
- How do transition scenarios change capex, sourcing, insurance, and product choices?
- Who owns disclosure integrity and external assurance readiness?

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

08

People as control infrastructure:
Workforce, talent, and culture

People and organisational culture are increasingly recognised as decisive determinants of risk outcomes. In many situations they determine whether controls hold under pressure or fail when systems are stressed. Human behaviour continues to contribute to a significant share of cyber incidents, while many organisations face persistent shortages in specialised capabilities related to AI governance, cybersecurity and regulatory compliance.

At the same time, many organisations still lack behavioural indicators capable of signalling emerging risks early. As enterprises become more digital, distributed and platform based, culture, role clarity and incentives increasingly function as the internal control infrastructure that determines whether policies are followed, concerns are escalated, and governance frameworks operate as intended.

Cultural misalignment remains a recurring driver of governance failures. Several high-profile organisational breakdowns have been linked not to the absence of formal policies, but to weak escalation mechanisms, ineffective challenge processes and incentive structures that prioritised growth or performance without sufficient regard to risk discipline. Despite this pattern, relatively few boards systematically link executive compensation or leadership evaluation to measurable indicators of risk accountability.

Regulators are also examining cultural drivers more closely following major incidents. Supervisory reviews frequently identify weak escalation channels, inadequate whistleblower protections and misaligned incentive structures as contributing factors in governance failures.

As organisations deploy increasingly complex technologies including artificial intelligence and automated decision systems, workforce capability and organisational culture will play a critical role in determining whether emerging risks are identified early or allowed to escalate. For boards, strengthening risk culture is therefore becoming a central governance priority. Embedding risk accountability into leadership objectives, incentive frameworks and everyday decision-making helps ensure that governance structures operate effectively not only in policy but in practice.

Board consideration

- Do incentive structures reinforce prudent risk behaviour across the organisation?
- Are employees encouraged and protected when raising concerns about misconduct?
- How does management measure and monitor risk culture?
- Do leaders visibly reinforce expectations around ethical conduct and risk awareness?
- Are investments in risk related skills sufficient to support evolving regulatory and technology risks?
- What indicators does the board receive regarding whistleblower activity and issue escalation?

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

09

Ecosystems under stress:
Third-party concentration and exit readiness

Enterprises now operate within dense, interdependent ecosystems where operational risk extends far beyond individual vendor failures. Concentration, lock-in, and deep fourth-party dependencies mean that disruptions can cascade rapidly across platforms and services. Yet many organisations remain underprepared: visibility into extended supply-chain pathways is limited, stress testing is infrequent, and few have a clear view of how vulnerabilities propagate across their digital ecosystems. As reliance on a small number of critical suppliers intensifies, boards increasingly recognise ecosystem fragility as a strategic risk—one that demands stronger resilience measures, improved oversight, and credible exit options.

Across the financial sector, regulatory expectations are rising. Firms are now required to identify critical service providers, conduct independent audits, maintain comprehensive maps of vendor dependencies, and establish workable exit and substitution strategies. Stress-testing continues to expose significant concentration risks, highlighting how quickly disruption can spread when a major provider falters. The encouraging insight, however, is that effective mitigation is achievable. Diversified ecosystem design, enhanced contractual resilience requirements, and real-time monitoring of critical services have consistently proven effective in reducing cascade risks and accelerating recovery when incidents occur.

Board consideration

- Which third parties are effectively 'too critical to fail' for us?
- Do we have tested exits and portability for essential providers?
- Where does vendor concentration create industry-wide exposure?
- Are service level agreements and remedies aligned to real-world disruption scenarios?
- How much visibility do we have into fourth-party dependencies?

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Illustrative 12-month risk committee agenda (for consideration)

Oversight priorities	Key topics	Expected outcomes
Risk baseline and resilience posture	Enterprise risk profile; risk appetite alignment; operational resilience of critical services; cyber readiness; liquidity and macro stress indicators	Risk appetite confirmation; resilience priorities defined; cyber testing schedule
Technology, data and ecosystem risk	Artificial intelligence governance; cyber maturity review; data protection readiness; vendor concentration; digital transformation risk; emerging cryptographic risks including post quantum encryption readiness	AI oversight framework confirmed; cyber resilience improvement priorities; vendor concentration mitigation actions; initial roadmap for long term cryptographic resilience
Strategic risk and external environment	Geopolitical developments; supply chain exposure; macroeconomic volatility; climate transition risk; sustainability disclosures	Strategic risk insights integrated into planning; supply chain resilience actions; ESG disclosure assurance roadmap
Assurance and governance effectiveness	Internal control effectiveness; internal audit findings; liquidity stress testing; risk governance evaluation; committee self-assessment	Assurance over key controls; remediation priorities confirmed; next-year agenda defined

Signals and metrics the board may wish to see quarterly

- **Strategic integration:** Risk discussions are linked directly to strategy and capital allocation decisions.
- **Early warning indicators:** Management provides forward-looking risk signals rather than only historical reporting.
- **Scenario-based oversight:** The committee regularly reviews scenarios that test resilience under severe but plausible disruptions.
- **Integrated risk information:** Cyber, operational, financial and regulatory risks are reported through a unified enterprise view.
- **Continuous learning:** Boards maintain regular education sessions on emerging risks such as AI, digital ecosystems and climate transition.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG in India contacts:

Ritesh Tiwari
Partner
Board Leadership Center
E: riteshtiwari@kpmg.com

Vikash Somani
Partner
Governance, Risk and Compliance Services
E: vsomani@kpmg.com

kpmg.com/in

Access our latest insights on KPMG Insights Edge

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai-400 011
Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

This document is for e-communication only. (TL_0426_AC)