irm
Developing risk professionals
www.theirmindia.org

ICICI Lombard

INDIA IN THE AGE OF
CONVERGENCE

Decoding Interconnected Risks.
Building Resilient Growth.



INDIA RISK REPORT 4.0 | 2026



TABLE OF CONTENTS

SR. NO.	CHAPTER	PAGE NO.
1	Introduction	1
2	Foreword	3
3	Executive Summary	8
4	Global Risk Landscape	13
5	India Risk Landscape	20
6	Risk Perceptions of India Inc	26
7	Enterprise Resilience	41
8	Risk Management and Insurance	48
9	Convergence of Forces and Emerging Risks	53
10	Midsize Enterprises in Focus	60
11	Parametric Insurance	70
A1	Appendix: Survey Methodology & Respondent Demographics	77
A2	Appendix: References	79
A3	Key Contributors	81

INTRODUCTION

ABOUT ICICI LOMBARD

ICICI Lombard is one of the leading private general insurance companies in the country. The Company offers a comprehensive and well-diversified range of products through multiple distribution channels, including motor, health, crop, fire, personal accident, marine, engineering, and liability insurance.

With a legacy of over 25 years, ICICI Lombard is committed to customer centricity with its brand philosophy of 'Nibhaye Vaade'. The company has issued over 39.2 million policies, processed over 3.4 million claims, and has a Gross Written Premium (GWP) of ₹ 306.18 billion for the year ended March 31, 2026. As of March 31, 2026, ICICI Lombard has 341 branches and 15,008 employees.

ABOUT IRM INDIA AFFILIATE

The Institute of Risk Management (IRM), headquartered in the UK and established in 1986, is the world's leading professional body for Enterprise Risk Management (ERM) across 140+ countries and the only body to grant Fellowship in ERM.

IRM India Affiliate is building the largest community of risk-intelligent leaders and organisations. Its vibrant ERM ecosystem comprises the Global Centres of Enterprise Risk Management, industry immersions, research collaborations, thought leadership initiatives, exclusive member networking opportunities and flagship platforms such as the India Chief Risk Officers' Meeting and What's The Risk?® show. With access to global knowledge, industry leaders and a growing professional network, IRM membership opens doors to meaningful connections, continuous learning and opportunities to contribute to the evolving world of risk management.



ABOUT THE REPORT

India Risk Report 4.0 is the fourth edition of our annual assessment of the enterprise risk landscape and risk preparedness, jointly published by IRM India and ICICI Lombard.

Last year's report highlighted accelerating uncertainties arising from Technology/AI, Geopolitics and Trade. These forces have now intensified and begun to act on one another. This year's report examines how Technology/AI, Geopolitics and Trade, and Climate Change are converging, and how they interact with one another and with Governance, the one force within the enterprise's own control. The convergence and interaction are giving rise to a new set of emerging risks. The result is a risk environment that is more dynamic, more interconnected, and less amenable to traditional, siloed approaches to risk management.

The report's analysis is grounded in the Enterprise Risk Perception Survey (ERPS-2026) conducted jointly by ICICI Lombard and IRM India to capture how India Inc perceives and prepares for risks. The survey gathered the views of senior business and risk leaders across a broad range of sectors and enterprise sizes. Its findings form the evidence base for the report as a whole: they identify the risks enterprises consider most significant, gauge the maturity of their risk management practices and use of insurance, and reveal how strongly they believe the converging forces are shaping their risk profiles.

Against this backdrop, the report sets out what enterprises should do to strengthen their resilience. It also highlights innovative insurance products that enterprises can deploy to transfer and manage exposures that conventional cover does not adequately address.

The report consists of the following chapters:

- Global and India Risk Landscapes: Sets the overall context and background for the discussion of enterprise risk.
- Risk Perceptions of India Inc: Analyses top risks facing India Inc, as identified in ERPS-2026, and how enterprises view the risks and opportunities presented by AI.
- Enterprise Resilience: Assesses the maturity of risk management practices in the industry, based on responses to ERPS-2026.
- Risks and Insurance: Examines the insurance practices of the industry, as reported in ERPS-2026, and highlights innovative insurance products that enterprises can deploy.
- Convergence of Forces and Emerging Risks: Explores the core theme of this report: how the four forces are interacting, what the resulting emerging risks are and the practices that enterprises need to follow to thrive in the environment. The chapter also presents industry perceptions of how strongly these forces influence their risks.
- Special Focus, Midsize Enterprises: This chapter focuses on the analysis of ERPS-2026 for the midsize industry segment – defined for the purpose of this report as enterprises with annual revenue of up to ₹2000 Cr.

The insights have been further enriched by views from experts in the industry and insurance domain. We thank them for their contributions, which have helped make this report a valuable industry resource.

FOREWORD



Sanjeev Mantri
MD & CEO
ICICI Lombard

We are living through a period in which volatility is no longer an interruption to business, but part of the environment in which businesses must operate. In such a world, the ability to anticipate risk, understand its interconnections and respond with agility is becoming a defining marker of leadership.

This fourth edition of the **India Risk Report**, developed with IRM India, examines that reality through the theme, ***"India in the Age of Convergence"***. The premise is simple but important: risks today are interconnected and myriad, but they amplify one another with far greater speed. A geopolitical event can become an energy and supply-chain shock; climate disruption can affect operations, costs and credit; advances in AI can create opportunity while simultaneously reshaping cyber, governance and operational risk.

India confronts this changing landscape from a position of strength. The economy grew 7.7% in FY 26, supported by resilient consumption and investment. Yet resilience at the macro level does not make enterprises immune to increasingly interconnected shocks.

Our Enterprise Risk Perception Survey reflects this changing reality. Cyber risk remains a pressing near-term concern, while Technology and AI are rising rapidly in both immediacy and impact. ***To quote Robert S. Muller - "There are only two types of companies: those that have been hacked and those that will be"***

Additionally, Climate Change has emerged among the significant long-term risks, reinforcing the need to look beyond individual threats towards the connections between them. As per our findings in this report, the annual insured losses from extreme weather consistently exceed $100 billion, while extreme weather events remain the No.1 global risk over the 2026-2036 horizon.

This is also why governance sits at the heart of this report. Technology, geopolitics and climate may largely be external forces, but how an organisation anticipates, governs and responds to them remains within its control. Risk, therefore, cannot reside in silos. It must be understood in the boardroom and embedded across the enterprise.

At ICICI Lombard, **25 years of keeping our promises have reinforced one enduring belief: resilience is what makes growth durable**. I hope this report helps leaders strengthen that resilience and approach an increasingly complex world with greater foresight, preparedness and confidence.



Hersh Shah

CEO,
IRM India Affiliate

The greatest risk facing organisations today may be the assumption that risks can still be understood, managed and contained independently.

We are witnessing a fundamental reordering of the world. Trade is increasingly shaped by national security, technology is amplifying economic power, and climate change is influencing everything from agriculture to financial stability. A localised conflict can disrupt supply chains across continents. An AI breakthrough can create extraordinary opportunities while simultaneously challenging established models of governance, employment and trust. The boundaries that once separated risks are rapidly disappearing.

As one of the world's fastest-growing major economies, India finds itself at the intersection of unprecedented opportunity and uncertainty. Our journey towards Viksit Bharat 2047 will depend not only on how quickly we grow, but also how we navigate the forces capable of shaping, accelerating or derailing that growth. **Resilience must therefore enable India's economic ambition, rather than merely defend against disruption.**

The Fourth Edition of the ICICI Lombard–IRM India Risk Report arrives at a pivotal moment. Drawing on the perspectives of 253 industry respondents, it reveals a compelling contrast between risk awareness and organisational preparedness. While structural and long-term challenges are increasingly being recognised, some of the most significant preparedness gaps lie precisely where risks are evolving fastest. This raises an uncomfortable question: are organisations becoming more risk-aware without necessarily becoming more risk-intelligent?

In my view, the next evolution of Enterprise Risk Management (ERM) must enable organisations to recognise interconnected exposures, challenge assumptions, anticipate cascading consequences and make informed decisions even when the future cannot be reliably predicted. This demands stronger governance, a pervasive risk culture, and an understanding that every strategic decision carries both risk and opportunity. It also calls for closer integration of risk management, financial protection, and organisational resilience.

We also have a greater responsibility. India's next generation of entrepreneurs, professionals, policymakers and business leaders will inherit an environment where uncertainty is not an occasional interruption but a permanent feature of decision-making. Building universal enterprise risk intelligence is therefore as important as building technological, financial or physical infrastructure. **A risk-intelligent India can become a global benchmark for responsible and sustainable growth.**

I congratulate the teams at ICICI Lombard and IRM India behind this collaborative thought-leadership initiative for continuing to advance a conversation of national importance. My hope is that this report encourages boards, executives, and risk professionals to move beyond preparing for the next crisis and make better decisions in a world where multiple crises, transformations, and opportunities may unfold together.

The future will not be defined solely by the risks we encounter, but by the quality of the decisions we make in their presence.



Anand Singhi

Chief – Corporate, International, Bancassurance (KRG) & Govt Business
ICICI Lombard

India's risk landscape is undergoing a profound transition. As digital ecosystems deepen, AI becomes embedded across business processes, climate volatility intensifies and global events transmit rapidly through supply chains, risks that once appeared distinct are increasingly interacting with one another.

India Risk Report 4.0 examines this shift through the theme, India in the Age of Convergence: Understanding Interconnected Risks, Building Resilient Growth. Its central message is particularly relevant for businesses: resilience can no longer be built risk by risk. Enterprises must understand not only individual exposures, but also how disruption in one area can cascade across operations, finances, people and markets. This builds on the report's evolution from risk culture and preparedness towards emerging risks and organisational resilience.

Climate illustrates this interconnectedness particularly well. An extreme weather event can disrupt production and logistics, raise input costs, affect employees and communities, interrupt cash flows and create new liability exposures. Technology and AI bring a similar duality, creating extraordinary possibilities while introducing new dimensions of cyber, operational and governance risk.

This changing environment also calls for greater innovation in the way risk is financed and transferred. Parametric solutions, for instance, can complement traditional indemnity insurance by linking payouts to predefined, objectively measured triggers, potentially providing faster access to liquidity after a qualifying event. It requires a robust data infrastructure that integrates historical climate patterns with real-time weather and satellite data. Aligning these insights with product design and measurable triggers is essential to developing effective solutions.

For enterprises, particularly MSMEs with limited ability to absorb prolonged disruption, solutions such as these can become part of a broader resilience architecture combining prevention, mitigation, risk retention and insurance.

At ICICI Lombard, we see our role extending beyond responding when a loss occurs. It is about helping businesses understand risk better, reduce vulnerabilities and build the confidence to keep moving forward.

I thank IRM India, the business and risk leaders who shared their perspectives, and everyone who contributed to this report. I hope its insights encourage enterprises to view resilience not simply as protection against disruption, but as an enabler of sustained growth.



Dinesh Kanabar

Chairman & CEO,
Dhruva Advisors India Private Limited

In business, we take risks every day. We commit capital, enter new markets, hire people and invest in technology, knowing that things may not work out quite as we expect. The quality of those decisions depends largely on whether we have asked the right questions—and whether we are willing to revisit our assumptions when circumstances change.

That, to my mind, is what makes this edition of the ICICI Lombard–IRM India Risk Report particularly relevant. Geopolitics, artificial intelligence and climate change are all familiar subjects in boardroom discussions. The difficulty is that they increasingly affect one another. A decision taken to address one concern can create an exposure elsewhere, sometimes in ways that are not immediately apparent.

What struck me in the report is the gap between recognising a risk and being prepared to deal with it. Businesses seem more comfortable managing risks they have encountered before. That is understandable. But some of the risks they are less prepared for could significantly affect their future. This finding should give boards and management teams reason to pause.

Take geopolitics. Its growing importance as a short-term concern, without a similar position among the leading long-term risks, raises an interesting question. Are we assuming that the present difficulties will eventually settle down and business will return to familiar conditions? Perhaps some will. But when we are making investments intended to last for years, we need to consider what happens if they do not.

The findings on AI also deserve reflection. Most businesses understandably see efficiency as the immediate opportunity. There is, however, a larger question: how might AI change what our customers expect from us, the services we offer, and the people we need? We should think about that even as we work through concerns about data, reliability, and confidentiality. And we need to be clear about who takes responsibility when an AI-assisted decision goes wrong.

Climate change presents a similar challenge in moving from awareness to action. Its place among the leading long-term risks is significant. The next step is to bring that concern into practical decisions about where we invest, how we operate and how we prepare for disruption.

For me, much of this comes back to the quality of governance. A board cannot anticipate every development. It can, however, insist that important assumptions are examined, that information moves across functions and that people feel able to raise a concern early. A well-documented risk process offers little comfort if it has no bearing on the decisions being taken.

Indian business has much to look forward to. As our enterprises grow and pursue opportunities across the world, their ability to understand and manage risk must grow with them.

I congratulate ICICI Lombard and IRM India on this initiative. I hope the report leads to candid discussions within organisations about where they stand, what they may be overlooking and what they need to do next. Those conversations would be a valuable outcome.



Fiona Davidge

LLB(Hons), Chartered Fellow of the
Institute of Risk Management
Chair of the International Standards Organization
Technical Committee 262 - Risk Management

In my role as Chair of ISO Technical Committee 262, which focuses on creating standards in risk management, I have the privilege of working with many experienced risk professionals from around the world. There is no doubt, listening and interacting with them, mixed with my own varied risk manager background across public, private and charitable sectors, that the world has become a much more complex and fast-paced place in the last few years.

Risks that span the globe still impact us locally in unique ways, determined by our locations, sector-specific factors, financial and non-financial impacts and human factors. Without detailed reports like this one, it can be easy to miss some of the complexity and interpretation in these large-scale risks. This fourth edition of the report provides vital identification and analysis of the latest risks we face and helps the organisation respond in advance to potential impacts, whether positive or negative. Only by being informed can organisations avoid major pitfalls and maximise any advantages.

The leading global risk management standard, 'ISO 31000:2018 – Risk Management Guidelines', places the creation and protection of value; however, that concept is realised in any individual organisation, at the heart of why we carry out risk management.

The risk management process that the standard recommends expects risk managers to use the full range of tools available to them to identify and understand the range and scale of uncertainty that may prevent their organisations from achieving their objectives. All risk and business managers should be striving to ensure their organisations are successful and deliver on their objectives.

Therefore, understanding the range of volatility of global risks and how they may impact the world in which your organisation operates is ever more important and relevant.

3. EXECUTIVE SUMMARY

The enterprise risk landscape has become markedly more complex over the last two years. The ICICI Lombard–IRM India Risk Report 3.0 (2025) highlighted the rapid evolution of AI and Geopolitical Risks. During 2026, these two forces, together with climate change, intensified and began to converge and reinforce each other.

India stands at the centre of this convergence. To accelerate growth, expand its export markets, and progress towards the goal of Viksit Bharat, Indian industry must capture the vast opportunities these forces present while controlling and managing the significant risks that accompany them.

- How Indian industry perceives its key risks, including the opportunities and risks presented by AI
- How the converging forces interact and give rise to emerging risks
- How organisations assess their own risk management processes and preparedness
- Evolution of insurance solutions to address the emerging risk environment.

The findings are based on the analysis of ICICI Lombard - IRM Enterprise Risk Perception Survey 2026 (ERPS-2026), conducted during August-Sep 2026. The survey received 253 responses from a broad cross-section of industry sectors. The analysis is discussed in the contextual background of global and India risk landscapes, drawn from a selection of reputed reports.



3.1 TOP RISKS OVER FOUR YEARS

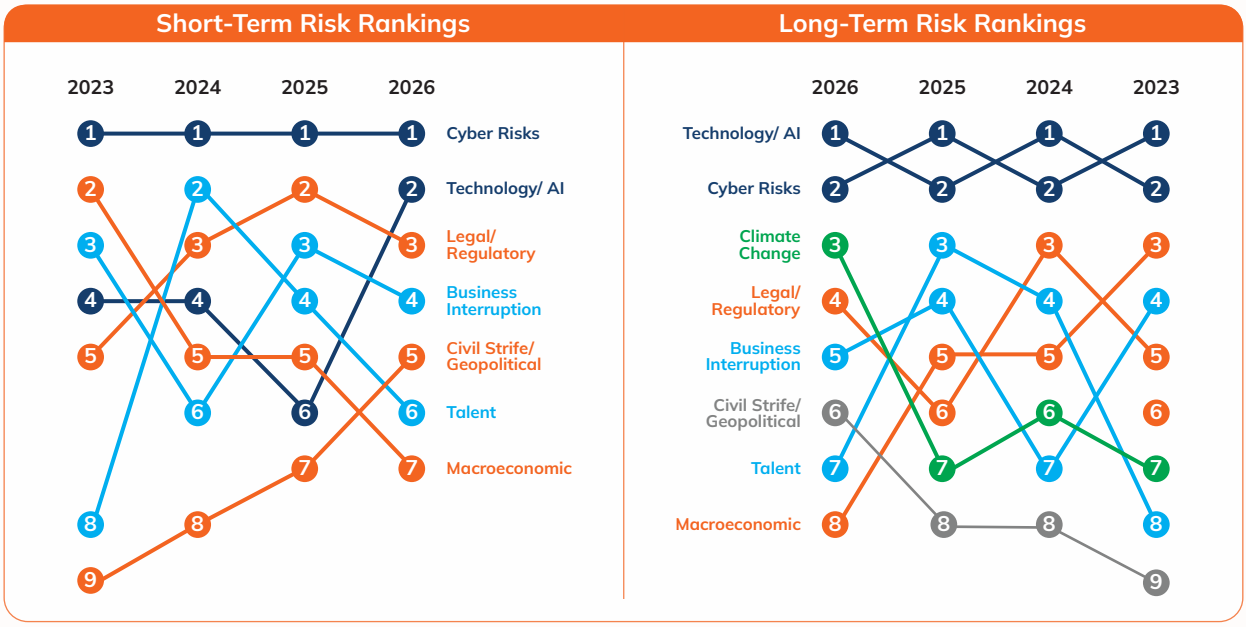


Figure 3.1 Highlights the top short- and long-term risks across 2023-2026.

KEY INSIGHTS

Cyber Risk has remained the top concern of the industry. It has ranked first among short-term risks and in the top two long-term risks in all four years.

Technology/AI risk has ranked in the top 2 long-term risks in all four years, but rose to #2 in short-term rankings only in 2026. Much of the digital investment expected after the pandemic was deferred as geopolitical pressures weighed on budgets. The rapid advance of AI since 2025 has now created near-term expectations of AI-led transformation.

Civil strife and Geopolitical risk has risen steadily in the short-term rankings, reaching fifth place in 2026. However, it has not appeared in the top 5 long-term risks in any year. This suggests that the industry has viewed geopolitical tension as a temporary disruption, an assumption that has not held true.

Legal/Regulatory and Business Interruptions have mostly stayed in the top 5 for the entire period for both short- and long-term, with some exceptions.

Climate Change risk has been ranked in the top 5 in the long term for the first time, at third place. This could indicate that the industry accepts climate change risk as a structural issue.

3.2 PREPAREDNESS TO FACE RISKS

Risk Exposure Gap

HIGH EXPOSURE — Readiness lags risk rank

- Civil Strife / Geopolitical Issues
- Technology / AI
- Trade War / Global Trade Realignment
- Climate Change

MEDIUM EXPOSURE — Little or no gap

- Macroeconomic Risks
- Cyber Risks
- Talent Risk (Attract / Grow / Retain)
- Business Interruption (incl. Supply Chain Disruption)

LOW EXPOSURE — Readiness ahead of risk rank

- Legal / Regulatory Risks
- Natural Catastrophes
- Fire / Explosions



Figure 3.2 Industry exposure to risk: short-term risk rank minus relative preparedness rank

ERPS-2026 asked respondents to assess how well they were prepared to address individual risks – whether they had a strategy, the capability, both or none. The relative exposure of an organisation to a risk has been calculated as the difference between the short-term rank of a risk, as rated in ERPS-2026, and the organisation's readiness for that risk – derived from the ERPS-2026 responses to the preparedness questions. Figure 3.2 maps the risks against industry exposure.

The chart shows that industry is well prepared for familiar risks, but lags in preparedness for risks that are now rising in importance. To some extent, this also highlights the evolving nature of these risks and uncertainty about how they will develop. However, Civil Strife / Geopolitical risks and Trade War/ Global Trade Realignment have received lower ranks, and yet they appear in the high exposure zone. Industries need to pay close attention to these risks.

The types of measures organisations use to manage each risk offer further insight.

ERPS-2026 asked respondents to identify measures they have deployed to manage each risk: Insurance, Non-insurance, Both or None.

The responses showed that more than 85% of respondents actively manage established risks such as cyber, fire, legal, business interruption and natural catastrophes. By contrast, over 20% have no measures for trade war / global trade realignment, macroeconomic risk, talent risk or climate change, even though climate change now ranks third among long-term risks. These are the areas where building resilience is most urgent.

3.3 AI OPPORTUNITIES AND RISKS

With AI evolving rapidly, the survey sought industry views on the top opportunities and risks it presents.

Rank	AI Opportunities	AI Risks
1	Operational Efficiency	Information Risk
2	Improved Decision Quality	Technology Risk
3	Innovation	People Risk
4	Customer Value – Experience Quality	Legal / Regulatory Risk
5	Revenue Growth	Operational Risk

Table 3.3 AI-related opportunities and risks.

Table 3.3 shows the top 5 AI opportunities and AI risks as perceived by the industry. Operational efficiency is seen as the largest opportunity by far, indicating that organisations are prioritising AI investments for efficiency improvements and cost reduction. Growth-oriented opportunities, such as innovation, revenue growth and faster technology adoption, rank lower in current priorities.

Information Risk, chiefly concerns around data, leads AI-related risks. Technology risk follows, with concerns around technology implementation, AI biases and potentially inaccurate outputs.

The opportunities and risks indicate immediate investment directions – both in AI implementations and in risk management capability.



3.4 THE ERA OF CONVERGING FORCES

Risks have always interacted with one another. However, the rise of **AI, intensifying Geopolitical tensions** and more frequent **Climate Change events** have created an environment fundamentally different from the relatively stable, globalised era of the past 25 years. These forces do not act alone; they reinforce each other and continuously reshape the enterprise risk landscape.

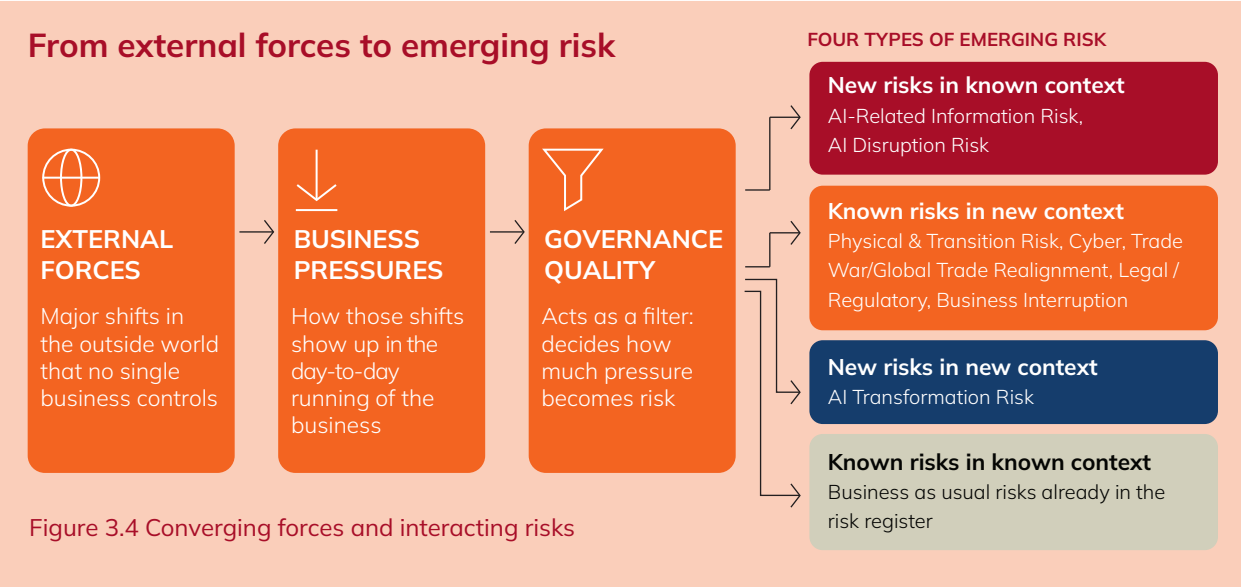


Figure 3.4 Converging forces and interacting risks

Figure 3.4 shows how external forces create business pressures which ultimately result in business risks. The quality of an organisation's governance is the critical factor that determines the severity of resulting business risks.

The forces do not operate in isolation – they interact with each other, and the resulting business pressures may be interconnected. These dynamics create a complex environment of compounding, interconnected risks. For example, AI adoption would create great demand for electricity and technology infrastructure, while climate events or geopolitical issues can restrict access to energy or technology, resulting in heightened supply chain risks. The business risks shown here are the emerging risks of the new era. They include new risks as well as existing risks which will intensify as the forces evolve and interact.

The conventional approach, often limited to identifying, assessing and mitigating risks, will no longer be sufficient. Organisations will need to understand how the risks are likely to develop and how they may affect the businesses. Because many existing risks are evolving due to changing contexts, managing emerging risks must become a formal part of the Enterprise Risk Management (ERM) framework.

In practice, this means:

- Continuously monitoring the external environment for early signs of change;
- Developing scenarios that consider several risks together;
- Strengthening governance across functions; and
- Building the ability to adapt quickly.

Equal attention should go to the opportunities these forces create. These practices are not new, but they have largely been confined to the most mature organisations. The era of converging forces now requires them to become standard practice across Indian industry.

4. GLOBAL RISK LANDSCAPE



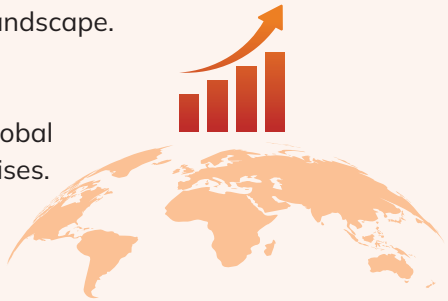
This chapter presents a comprehensive view of the evolving global risk landscape, providing the context for the analysis and discussions that follow in this report.

The global risk perspective draws on assessments from five leading international institutions, combining societal, environmental, economic, technological, and geopolitical developments with expert insight to identify key short- and long-term strategic risks:

- The Global Risks Report 2026 published by the World Economic Forum [WEF-2026]
- International Monetary Fund's Global Financial Stability Report 2026 [GFSR-2026]
- Protiviti–NC State University's Executive Perspectives on Top Risks and Opportunities [EP-2026]
- Risks in Focus by Internal Audit Foundation of The Institute of Internal Auditors [IIA-2026]
- Risk Trends 2026 published by Institute of Risk Management, UK [IRM-2026]

Each selected report offers a distinct perspective and area of focus:

- WEF-2026 report provides the broadest view of the risk landscape, including societal and environmental risks.
- GFSR-2026 concentrates on the economic and financial risk landscape.
- EP-2026, IIA-2026 and IRM-2026 focus on enterprise risks.



Collectively, these reports provide a comprehensive view of the global risk landscape and insights essential for building resilient enterprises.

Additional insights are drawn from:

- Eurasia Group's Top Risks 2026 Report
- Oxford - GlobeScan Global Corporate Affairs Survey: 2026 Survey Report

4.1 A WORLD UNDER COMPOUNDING PRESSURE

This section examines the top five short- and long-term risks curated from the reference reports.

Heightened geopolitical uncertainty, financial strain, and rapid technological progress are contributing to the risk landscape for 2026 and are common themes across all reference reports.

4.1.1 TOP FIVE SHORT-TERM RISKS

WEF-2026	GFSR-2026	IIA-2026	EP-2026	IRM-2026
Geoeconomic Confrontation	Sovereign Debt, Rising Yields and Rollover Risk	Cybersecurity	Cyber Threats	AI & Digital Disruption
Misinformation and Disinformation	Emerging-Market Capital Outflows and Currency Pressures	Digital Disruption (Including AI)	Third-Party Risks	Cyber & Data Resilience
Societal Polarization	Forced Selling and Liquidity Stress by Leveraged NBFIs	Business Resilience	Emerging Technologies / Upskilling-Reskilling	Geopolitical Fragmentation
Extreme Weather Events	Private-Credit and Corporate-Credit Deterioration	Human Capital	Operations And Legacy IT Infrastructure	Climate & Transition Risk
State-based Armed Conflict	AI-related Market Correction and Equity–Bond Selloffs	Regulatory Change	Economic Conditions, Inflationary Pressures	Third-Party & Supply-Chain Interdependence

Table 4.1.1 Depicts a comparative ranking of the top five global risks in the short term (0-2 years), based on insights from various industry reports.

The reports differ primarily in their analytical lens and assessment priorities, reflecting their distinct institutional mandates. The enterprise-oriented reports have effectively translated many of the broad concerns raised by WEF-2026 and GFSR-2026 into enterprise-specific terms. For example, Geoeconomic Confrontation in WEF-2026 appears as Regulatory Change or Third-Party risks in enterprise-oriented reports.

4.1.2 TOP FIVE LONG-TERM RISKS

WEF-2026	EP- 2026	IRM-2026
Extreme weather events	Customers and Competition	AI & Digital Disruption
Biodiversity loss and Ecosystem Collapse	Security and Privacy	Cyber & Data Resilience
Critical change to Earth Systems	AI Deployments	Geopolitical Fragmentation
Misinformation and Disinformation	Markets and Economies	Climate & Transition Risk
Adverse outcomes of AI technologies	Talent Challenges	Third-Party & Supply-Chain Interdependence

Table 4.1.2 Depicts a comparative ranking of the top five global risks in the long term (2-10 years), based on insights from various industry reports.

It may be noted that only three of the five reports considered have explicitly addressed long-term risks, which limits direct comparison across all the reference reports.

WEF-2026 takes a broader view of long-term risks, led by environmental and societal threats, whereas the long-term lens in EP-2026 and IRM-2026 centres on competitiveness and security risks arising out of AI and other enterprise risks.

EP-2026 highlights Talent risks, which have risen from 9th rank in the short-term to 5th rank in the long-term. Talent challenges relate to the evolution of talent requirements as enterprises embark on transformational journeys using AI and other disruptive technologies.

4.2 GLOBAL RISK SUMMARY

While the previous section compared long- and short-term global risks depicted in a selection of reports, this section summarises the most significant five risk domains covered by these reports, namely:

- Cybersecurity
- Technology and AI, including misinformation and disinformation.
- Geopolitics, encompassing supply-chain disruption and third-party exposure.
- Macroeconomic pressures.
- Climate change and extreme weather events.

Beyond these risks, we will also examine Governance Risk, which features prominently across all the reference reports and often determines how successfully enterprises manage the top risks they face.

Together, these domains highlight major operational, strategic, economic, and organisational risks to which institutions and economies are exposed in the evolving global risk environment.

4.2.1 CYBERSECURITY

Cybersecurity continues to be a major risk theme in the 2026 Global Risks Landscape, with implications extending beyond information systems to operational continuity, data security, financial stability, and institutional resilience. For example, the April 2026 breach of the Canvas Learning Management System resulted in widespread examination disruptions and payment of a ransom to avoid further disruption.

As AI adoption deepens and reliance on complex digital supply chains grows, the potential impact of cyber incidents grows exponentially, further connecting technology with heightened financial and operational vulnerabilities. This is illustrated by a cyber-attack on Boston Scientific's global information systems and applications, detected in August 2026. As a result, the company is unlikely to meet its net sales growth and adjusted EPS guidance ranges for Q3 and full-year 2026.

Enterprise-oriented risk reports have ranked it among the top risks in short- and long-term enterprise-oriented reports. IIA-2026 identifies cyber risk as the biggest concern for organisations, as cited by 73% of respondents. EP-2026 ranks Security and Privacy 2nd in the long term, driven by broader AI and technology implementations.

WEF-2026 gives it a 6th rank in short-term and 8th in the long-term.

GFSR-2026 highlights that the global financial system is increasingly vulnerable to cyber-driven shocks and disasters due to growing interdependence in the digital world. Cyber risk has become a fundamental operational, financial, and strategic business risk.

Overall, the evidence positions cybersecurity as a core enterprise risk, with its potential to disrupt operations, finances, and strategic priorities making resilience a central business imperative.

4.2.2 ARTIFICIAL INTELLIGENCE AND DIGITAL DISRUPTION

Artificial intelligence and digital disruption risks are rising to a strategic level, with rapid adoption creating challenges around governance, data integrity, workforce readiness, and the responsible integration of emerging technologies. Rapid progress in the capabilities of GenAI is continuously changing the impact scenarios – both in opportunities and in risks.



WEF-2026 highlights AI as both a strategic opportunity and an emerging source of systemic risk. Most respondents to EP-2026 show strong confidence in the growth opportunities created by AI.

On the other hand, "Adverse outcomes of AI technologies" moved from 30th in short-term risk rankings to 5th in the long term, representing one of the largest leaps by a risk this year. A recent survey by MIT Sloan Management Review listed AI risks ranging from weapons to income inequality. Some of the key risks emerging out of AI are:

WEF-2026 estimates that by 2030, labour-market shifts could create 170 million jobs and displace 92 million.

As per the AI and Future of Entry-Level Work report published by WEF, around 37% of young workers have medium to high exposure to AI-driven task changes. This has far-reaching implications for talent pipeline management and the availability of entry-level jobs.

GFSR-2026 underscores financial vulnerabilities arising from elevated valuations and concentration in AI-related firms.

IIA-2026 observes that digital disruption is intensifying business risk, requiring stronger capabilities, governance, and workforce readiness.

IRM-2026 considers AI reshaping enterprise risk management, making strategic adaptation and forward-looking risk oversight increasingly essential.

Technological disruption—especially the rapid rise of AI—is becoming a major force shaping future strategy and business models, as enterprises navigate new opportunities and risks.

4.2.3 GEOPOLITICAL FRAGMENTATION AND TRADE PROTECTION

Geopolitical factors are increasingly shaping financial markets, investment decisions, corporate strategy, and operational resilience.

Assessments from the WEF and IMF show that rising geopolitical tensions can transmit rapidly through trade flows, energy markets, financial conditions, and sovereign risk, increasing exposure across sectors.

IIA-2026, IRM-2026, and EP-2026 emphasise integrating geopolitical intelligence into strategic planning, supply-chain resilience, and enterprise risk management amid persistent geopolitical tensions and a rapidly changing global order.

GFSR-2026 highlights that conflicts, particularly in the Middle East, can transmit swiftly through financial markets, amplifying the potential for broader economic instability.

WTO forecasts 2026 global merchandise trade growth at 1.9%, a sharp deceleration from 4.6% in 2025. If oil prices remain high, growth could be shaved further to 1.4%.

Eurasia Group's Top Risks 2026 frames 2026 as a geopolitical tipping point, shaped by heightened political uncertainty, conflicts, de-globalisation pressures, AI related geopolitical dynamics and resource competition. It also flags water scarcity as an emerging strategic security concern with significant implications for economic resilience and national stability.

Geopolitical and Trade fragmentation is a structural and systemic risk driver, with implications that extend across markets, supply chains, and institutional stability.

4.2.4 MACROECONOMIC AND FINANCIAL INSTABILITY

Financial and macroeconomic vulnerabilities form another major component of the 2026 risk landscape. GFSR-2026 provides the strongest evidence to support this, linking high public debt, financial conditions, sovereign financial vulnerabilities, nonbank leverage, and market concentration to broadened financial risks.



WEF-2026 connects economic pressures with broader global fragmentation, while other reports demonstrate that economic uncertainty continues to influence organisational risk perceptions and strategic decision-making.

Global gross government debt rose to nearly 94% of GDP in 2025, and on current trajectories, it will reach 100% by 2029, a level previously reached only in the aftermath of World War II.

WEF-2026 records a notable deterioration in economic risk perceptions, with economic downturn rising from 19th to 11th place and inflation moving from 29th to 21st place in its two-year risk ranking.

GFSR-2026 highlights rising external financial exposure in emerging markets, with cumulative cross-border portfolio flows reaching about US$4 trillion and portfolio debt liabilities increasing to 15% of GDP.

GFSR-2026 observes that energy prices have raised two-year inflation expectations by 0.3–0.8 percentage points, with tariffs and debt monetisation posing further inflation risks.

4.2.5 CLIMATE, ENERGY AND ORGANISATIONAL RESILIENCE

Business continuity, infrastructure, energy security, and supply chain resilience are increasingly impacted by climate and environmental pressures.

Climate change is being felt across the world with ever-increasing impact. The first half of 2026 brought unusually hot summers around the world, accompanied by massive wildfires in Europe and Canada. The Canadian wildfires also affected weather in the United States. A record El Niño event has caused erratic and uneven rains, bringing floods and landslides in India, Nepal, and eastern Africa and drought in the Caribbean.

Beyond sustainability, climate and energy shocks can amplify economic, geopolitical, and operational risks and vulnerabilities.

- Annual insured losses from extreme weather consistently exceed $100 billion, while extreme weather events remain the No. 1 global risk over the 2026–2036 horizon.
- GFSR-2026 quantifies the financial transmission of the Middle East conflict through the energy market: global equity prices declined by 8% from February 2026. Brent oil futures rose from around $61 per barrel in early 2026 to $118 per barrel by the end of March 2026.
- IIA-2026 reports business resilience remains a significantly larger organisational priority at 47%, indicating that climate-related disruptions increasingly need to be considered through the broader lens of continuity, adaptability, and recovery.
- EP-2026 reinforces the sectoral materiality of climate risk, ranking climate change, environmental, and sustainability requirements as the #1 near-term risk in Energy and Utilities, while catastrophic natural disasters and weather phenomena rank among the sector's top three risks.
- IRM-2026 recognises climate volatility as a risk that exists alongside the other two risks: geopolitical fragmentation and technological transformation.



4.2.6 GOVERNANCE RISK

While Governance may not appear as a top risk in the reference reports listed earlier, it is discussed consistently in the context of top risks in virtually all the reference reports:

- In identifying Adverse outcomes of AI Technologies as the most consequential long-term risk, WEF-2026 notes that slow development of governance frameworks could accelerate AI risks. It further observes that recursive self-improvement may erode governance systems as organisations lose understanding of how AI actually works.
- IIA-2026 ranks Regulatory Change as the #5 short-term risk and Governance/Reporting risk at #9 – over and above the importance of Governance implied within other top risks such as AI and Regulatory Change.
- When asked about significant priorities for AI deployment, 24% of EP-2026 respondents voted for Lack of Governance as a significant factor.
- AI and Digital Disruption is the top risk identified in IRM-2026. The report discusses Governance issues as one of the key factors underlying this risk.

The Global Corporate Affairs survey 2026, published by the University of Oxford and GlobeScan, highlights the rising prominence of Governance risk. Among the top Environmental, Social and Governance (ESG) issues, Governance ranks second, immediately behind Climate Change. Notably, when respondents were asked to rank Environment, Social, and Governance factors in terms of reputational risks to business, 45% selected Governance, with the remainder divided almost equally between the other two options.

In the emerging risk landscape, Governance stands out as a significant risk, influencing how organisations leverage AI, manage the risks it introduces, respond to changing regulations, and build and safeguard their reputations.

KEY TAKEAWAYS

The 2026 Global Risks Landscape reflects an increasingly complex interplay of geopolitical, economic, financial, technological and environmental pressures.

- The short-term risk landscape is dominated by Geopolitical tensions, high public debt, financial fragility, AI and technology disruptions, cybersecurity and third-party risks.
- The long-term risk landscape: extreme weather, Biodiversity loss and AI deployment risks are rising in prominence. Rapid AI adoption brings new opportunities and challenges across talent management, productivity, financial stability, data security, and cyber resilience.

The central concern for 2026 is not only in the severity of individual risks but also their ability to reinforce one another and trigger wider disruptions across economies, financial systems, and societies. The convergence of climate volatility, geopolitical fragmentation, and technological transformation is creating interconnected exposures that cascade rapidly across energy security, financial stability, supply chains, and organisational resilience.

5. INDIA RISK LANDSCAPE

5.1 INTRODUCTION

Building on the global risk landscape examined in the preceding chapter, we now focus on the risks facing India and its organisations. In 2026–27, geopolitical conflict, trade barriers, volatile energy prices, climate disruptions and cyber threats are shaping India's risk environment. These risks are affecting energy markets, supply chains, access to technology, data security, and infrastructure, with growing implications for organisational decision-making.

At the same time, India continues to demonstrate considerable domestic resilience. Economic activity remains comparatively strong, with GDP growth of 7.7% in 2025–26. Private-sector output continues to expand, with the PMI above the threshold value of 50 for over five consecutive years, and the financial system remains well-capitalised. These strengths provide an important buffer, even as organisations operate in a more complex and interconnected external risk environment.

A review of relevant reports and evidence identified five significant risk areas for organisations operating in India: macroeconomic, cybersecurity and technology, operational, climate change and natural disasters, and geopolitical. Consistent with previous editions, this chapter evaluates each risk's current severity and change from the previous year. Key sources include:

- The RBI's Financial Stability Reports (December 2025 and June 2026)
- The IMF's World Economic Outlook update (July 2026)
- The World Bank's Global Economic Prospects
- S&P Global PMI releases
- Government of India releases on cybersecurity and extreme weather
- Cisco and IBM industry reports, and
- The Climate Risk Index 2026.

Risk	Risk in 2023	Risk in 2024	Risk in 2025	Risk in 2026	Change from 2025
Domestic Macroeconomic Risk	Medium	Medium	Medium	Medium	↑ Higher
Cybersecurity and Technology Risk	High	High	High	High	↑ Higher
Operational Risk	Low	Low	Low	Low	↓ Lower
Climate Change and Natural Disasters Risk	High	High	High	High	↑ Higher
Geopolitical Risk	High	High	Very High	Very High	↑ Higher



Overall, the 2026 risk landscape points to a broad upward movement in risk, with four of the five categories assessed as higher than in 2025, while operational risk is the only category showing an improvement.

5.2 MACROECONOMIC RISK

Macroeconomic risk for India is assessed as moderate, with a slight increase in risk compared with the previous year.

Growth and Inflation Outlook

India's domestic macroeconomic fundamentals remain comparatively strong. The economy grew by 7.7% in 2025 - 26, supported by private consumption and fixed investment. However, growth is expected to moderate in 2026 - 27 as elevated energy and commodity prices, along with weaker global growth, weigh on activity. The RBI and World Bank both project 6.6% growth in FY2026 - 27, while the IMF's July 2026 update projects 6.4%, with a recovery expected thereafter. Inflation also remains a source of uncertainty, particularly through the energy channel (International Monetary Fund, 2026) (Reserve Bank of India, 2026) (World Bank, 2026).

External Vulnerabilities

India's principal macroeconomic vulnerabilities arise from external shocks. The economy remains dependent on imported oil and other key commodities, increasing its exposure to geopolitical disruptions and global price volatility. Although the current account deficit remained manageable in 2025 - 26, the overall balance of payments remained in deficit for a second consecutive year because of weak capital inflows. Geopolitical tensions also contributed to depreciation pressure on the rupee and higher longer-term government bond yields, although these pressures have since eased (Reserve Bank of India, 2026).

Climate-Related Macroeconomic Vulnerability

El Niño has added a climate-related dimension to India's macroeconomic risk in 2026. As of 9 September, 53.2% of India's landmass was experiencing some degree of drought, while southwest monsoon rainfall remained below normal. The resulting stress on kharif crops and lower soil moisture ahead of winter sowing could affect agricultural output, rural incomes and food prices, potentially adding to inflationary pressures and moderating growth.

Risk Implication

Strong domestic demand, moderate inflation, healthy corporate and financial-sector balance sheets and policy buffers continue to contain macroeconomic risk. Nevertheless, slower expected growth, higher energy prices, weaker capital flows, continuing geopolitical uncertainty, and worsening climate-related risks indicate a modest increase in macroeconomic risk compared with the previous year.

5.3 CYBERSECURITY AND TECHNOLOGY RISK

Cybersecurity and technology risk remains high, with the level of risk increasing compared with the previous year.

Incident volumes are rising sharply. CERT-In tracked 15.93 lakh incidents in 2023, 20.41 lakh in 2024 and 29.44 lakh in 2025, representing an increase of about 44% in the last year alone.

The financial impact is also increasing. IBM estimates that the average cost of a data breach in India rose from USD 2.51 million in 2025 to USD 2.79 million in 2026 (IBM Corporation, 2025) (IBM Corporation, 2026).

AI is amplifying both attack capability and exposure – IBM reports that more than one in four organisations experiencing a malicious attack faced an AI-driven attack - a 56% year-on-year increase - with deepfake impersonation and AI-enabled malware among the leading vectors. AI-driven attacks also added around USD 1 million to average malicious breach costs (IBM Corporation, 2026).

Preparedness remains uneven – Cisco's 2025 Cybersecurity Readiness Index found that only 4% of organisations globally were classified as Mature, while 70% remained in the Formative or Beginner stages; 60% also lacked confidence in their ability to identify unapproved AI tools (Cisco, 2025).

RBI evidence points to rising systemic exposure – Nearly one-third of surveyed banks and NBFCs perceived a moderate or significant increase in cyber risk. AI-enabled cyber threats were identified by 95% of respondents as a leading risk over the next 12 months, while third-party and supply-chain risks were cited by 70% (Reserve Bank of India, 2026). The RBI also finds substantial dependence on external technology providers, creating concentration and contagion risks if critical providers are compromised (Reserve Bank of India, 2026).

Risk Implication

Overall, the combination of rising incident frequency, higher breach costs, AI-enabled attacks, and third-party dependencies indicates that cybersecurity and technology risk remains high and has increased compared with the previous year.

5.4 OPERATIONAL RISK

Operational risk in India is assessed as low, although the pace of improvement has moderated compared with the previous year.

The Purchasing Managers' Index (PMI) provides a useful forward-looking indicator of operating conditions across India's manufacturing and services sectors. A reading above 50 indicates expansion relative to the previous month.

The Manufacturing PMI stood at 53.5 in July 2026, down from 54.2 in June and its lowest level since August 2021, indicating a moderation in momentum compared to earlier years.

The services sector growth softened during the middle of the year. The Services PMI declined from 57.4 in June to 54.5 in August. The Composite Output Index rose from 54.3 in July to 54.6 in August, while private-sector employment strengthened, led by services.

Some pressures remain, particularly rising input costs, weaker manufacturing hiring, and slower purchasing activity. Geopolitical tensions continue to create uncertainty around supply-chain conditions. However, continued expansion in output and new orders, improving supplier delivery times, and positive employment trends indicate that operational risk remains low.



Risk Implication

The principal concern is not operational contraction but a moderation in momentum that could make firms more vulnerable to external supply chain or cost shocks.

5.5 CLIMATE CHANGE AND NATURAL DISASTER RISK

Climate change and natural disaster risk for India remains high, with the level of risk increasing compared with the previous year.

Physical and Agricultural Exposure

India remains highly exposed to floods, cyclones, droughts, and heatwaves. The Climate Risk Index 2026 records nearly 430 extreme-weather events between 1995 and 2024, affecting almost 1.3 billion people, causing more than 80,000 fatalities, and generating nearly USD 170 billion in inflation-adjusted economic losses (Germanwatch, 2025).

The 2026 monsoon illustrates how global climate patterns can directly affect India. Rainfall this year has been erratic and, on average, below normal, with a strengthening El Niño being identified as a key factor. This raises risks for summer crops such as cotton, soybeans, maize, and pulses, and reduces the soil moisture required for winter crops. The implications are significant because roughly half of India's farmland remains unirrigated.

Risk Implication

Longer-term increases in temperature, extreme precipitation, drought exposure, and severe cyclonic activity suggest that physical climate risk will remain structurally elevated. These risks can cause business interruption, infrastructure damage, agricultural losses, and supply-chain disruption, with regional events such as the 2026 Nepal - Tibet glacier collapse highlighting potential cross-border impacts.

Although initiatives such as Mission Mausam and the Bharat Forecasting System are strengthening preparedness, firms face rising exposure to business interruption, asset damage, and potential insurance losses.

Overall, climate risk remains high and is increasing, with growing implications for agriculture, infrastructure, supply chains and business continuity.

5.6 GEOPOLITICAL RISK

Geopolitical risk faced by companies in India remains very high, having increased compared with the previous year.

Trade and Energy Risks

The Russia–Ukraine war, hostilities in the Middle East, and disruptions to strategic maritime routes continue to expose India to higher energy prices, shipping costs, trade uncertainty, and financial market volatility. These risks are amplified by growing trade fragmentation and the use of tariffs and sanctions as geopolitical tools. For Indian firms, the principal transmission channels are higher input costs, supply chain disruptions, and uncertainty around export markets and sourcing arrangements.

Technology and Strategic Inputs

Geopolitical competition is increasingly extending to critical technologies and strategic materials. China continues to restrict or license exports of heavy rare earths such as dysprosium, terbium and yttrium, which are important for automobiles, electronics, renewable energy, aerospace, and defence. These restrictions highlight the vulnerability created by concentrated supply chains and have strengthened India's focus on domestic rare-earth processing and permanent-magnet production.

Similar concerns are emerging around advanced AI and computing. The United States has tightened controls on advanced AI technologies, while China is considering restrictions on overseas access to leading AI models. This raises the possibility that access to advanced models, chips, and computing infrastructure may increasingly depend on jurisdiction and strategic alignment.

Risk Implication: India's geopolitical resilience will increasingly depend on diversified trade and energy relationships, stronger domestic capabilities, and secure access to critical minerals, semiconductors, and advanced technologies.

EXPERT PERSPECTIVE



SUJOY MAITRA
Vice President - Corporate Underwriting - Marine
ICICI Lombard

The Long Way Round

How geopolitics is redrawing global trade, and what it means for India?

Trade used to follow the shortest, cheapest route. Today it follows the safest route that geopolitics allows.

Trade ambition and exposure

India's $2 trillion export ambition relies on maritime trade, carrying about 95% by volume and 70% by value. Rising cargo values increase exposure and underinsurance risk.

Geopolitics is redrawing routes

Conflict has turned the Red Sea and Gulf into risk corridors. Closure of the Strait of Hormuz would constrain energy supplies and raise freight and war-risk costs. Circumventing cape acts like a war risk aversion but it also elevate proportions of other risks like long voyages, increasing operational and cargo risks.

Crude prices transmit the shock

Higher crude prices raise transport, manufacturing and distribution costs. Persistent inflation can keep rates elevated, increase working-capital costs and weaken demand. Insurers must reassess sums insured and premium adequacy.

Trade policy creates concentration risk

Tariffs shift shipment timing, origins, values and port flows. India's dependence on China-linked supply chains for critical minerals, electronics, batteries, solar equipment and pharmaceuticals creates strategic exposure amid export controls and political realignment. Businesses need alternative suppliers, deeper mapping and appropriate contingent business interruption protection. Just like crude oil procurement where we are sourcing from 40+ countries. We must adopt the same strategy for other commodities.

Rays of opportunity amid gloomy logistical landscape

India’s expanding FTAs, dedicated freight corridors, improving port connectivity and growing shipbuilding capabilities can strengthen the country’s trade competitiveness. These developments can open new export markets, reduce logistics costs and transit times, and improve supply-chain efficiency. They can also help Indian manufacturers and MSMEs integrate more deeply into global value chains and establish India as a major regional trade and logistics hub

Way forward

Businesses should identify critical routes, ports and suppliers; update cargo values; and test coverage for war, delay, duties and storage accumulation. Insurers need faster pricing, vessel and sanctions screening, accumulation monitoring and clearer wording. Trade will continue through less predictable supply chains. Those prepared for the long way round will still arrive on time.

CONCLUSION

India's 2026–27 risk landscape is increasingly shaped by the interplay among AI, geopolitics, climate change, and governance.

- AI and geopolitics: Strategic controls over AI models, semiconductors, and digital infrastructure are increasing the importance of technological sovereignty for India.
- Climate and business resilience: Extreme weather can disrupt agriculture, infrastructure, power systems, and supply chains, increasing operational and asset-loss exposure.
- Domestic resilience as a buffer: Strong economic fundamentals and a resilient financial system provide support, but do not eliminate exposure to rising external and non-financial risks.

For Indian organisations, resilience will increasingly depend on managing these risks as interconnected rather than standalone exposures.



6. RISK PERCEPTIONS OF INDIA INC



This chapter analyses responses to questions on the top risks identified in the ICICI Lombard – IRM Enterprise Risk Perception Survey 2026 (ERPS-2026). The analysis is framed within the context of the Global and India risk landscapes discussed in the preceding chapters and further examines how respondents prioritised risks across different time horizons.

6.1 TOP RISKS

The respondents to the ERPS-2026 were asked to identify and rank their top five risks for both the short term (0–2 years) and the long term (2–4 years, as defined for this survey). Figure 6.1.1 illustrates these rankings, derived from the weighted scores awarded to each risk based on the ranks they received.

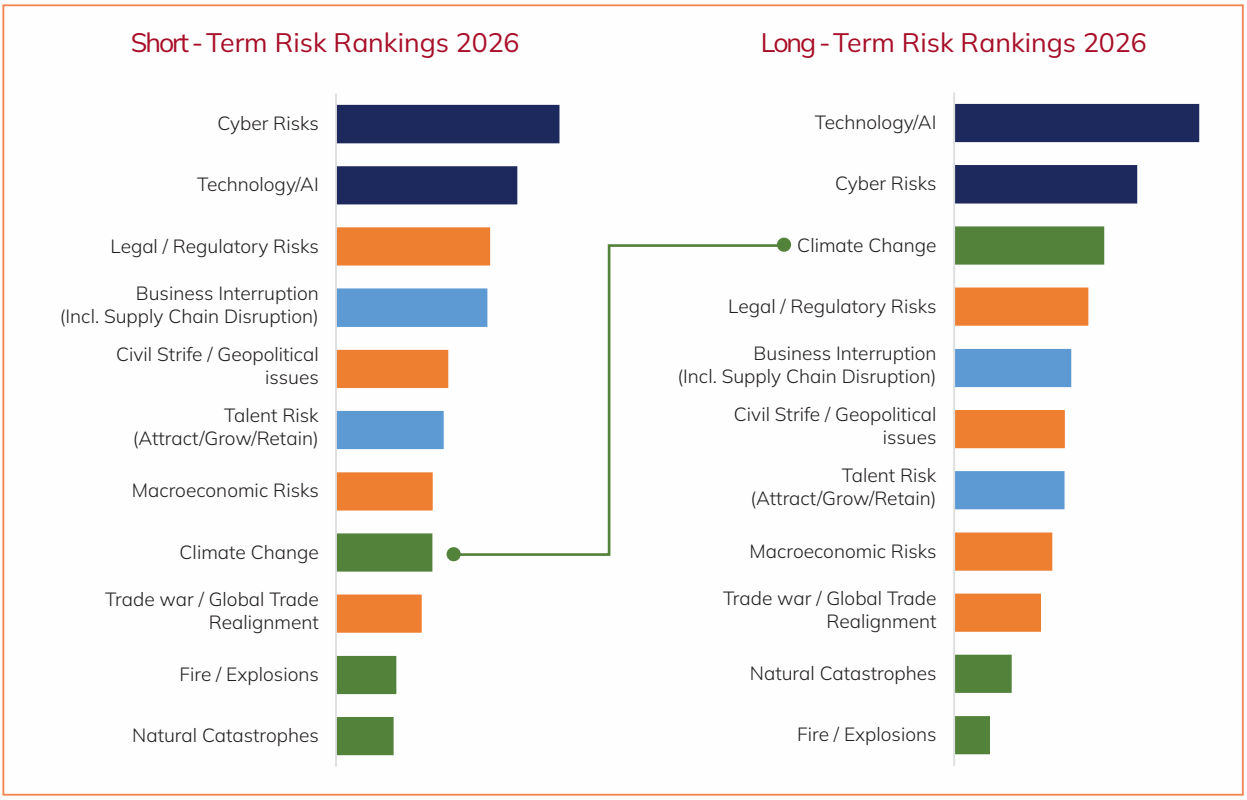


Figure 6.1.1 Depicts comparison of short-term and long-term risk rankings from ERPS-2026.

Figure 6.1.1 shows short- and long-term risk rankings for ERPS-2026. The rankings were derived by weighting the ranks assigned to various risks in the survey responses. The notable points are:

- Among all risks, Climate risk rank has moved up the most from short-term to the long-term. This indicates growing concern that Climate Change will become a structural issue that will shape planning in the next 2-4 years.
- Technology and Cyber take the top two ranks in short- and long-term rankings, with Technology/AI moving to first rank in the long-term. Digital exposure is no longer an IT matter — it now sits at the core of business continuity, data-protection compliance and customer trust, and needs board-level ownership and dedicated budget.
- Legal and Regulatory risks are in the top 5 in the short and long term, reflecting a tightening compliance regime.
- Macroeconomic risks are ranked low in the short and long term, much lower than the previous year's rankings. This is in variance with the India Risks Landscape analysis, which indicates Macroeconomic risks have stayed at a "Medium" level, with a slight increase from the previous year.

Overall, the rankings show enterprises treating Technology/AI, Cyber, Business Interruption, Climate Change and Legal/Regulatory risks as the top concerns.

6.1.2 KEY INSIGHTS FROM RISKS RANKED AT NUMBER 1

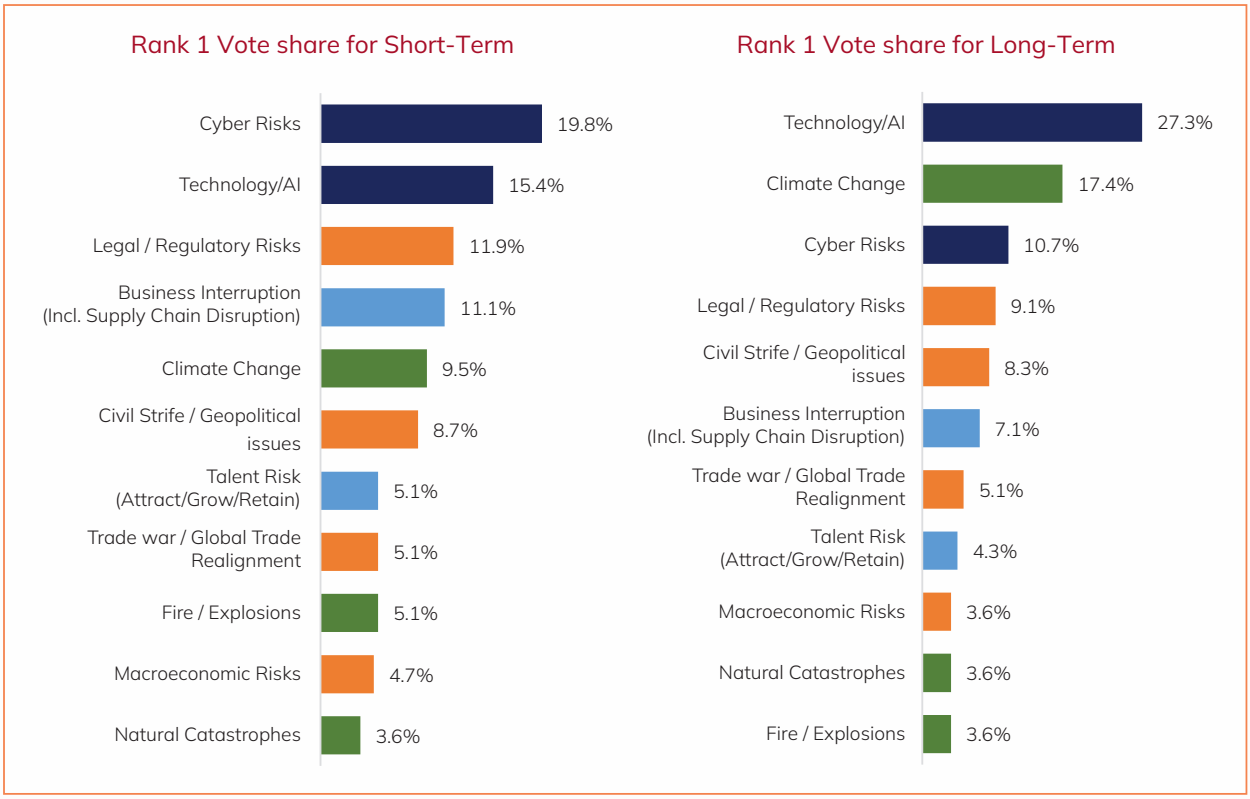


Figure 6.1.2 Depicts % of respondents ranking each risk at the #1 for the short- and long-term horizons in ERPS-2026.

While figure 6.1.1 showed risk rankings based on weighted scores, Figure 6.1.2 presents the percentage of respondents who assigned each risk as Rank 1, across both short- and long-term horizons.

Long-term voting shows Climate Change receiving the 2nd-highest number of votes, a big jump from the short-term vote share, clearly indicating a rise in the importance of Climate Change risk in the long term. This could also indicate that enterprises will invest more in climate risk management over the 2-4 year timeframe. Similarly, Technology/AI is ranked as the top risk by more respondents when viewed in long-term, with its vote share going up by over 77%. This shows the risk is rapidly evolving and may have a significant impact.

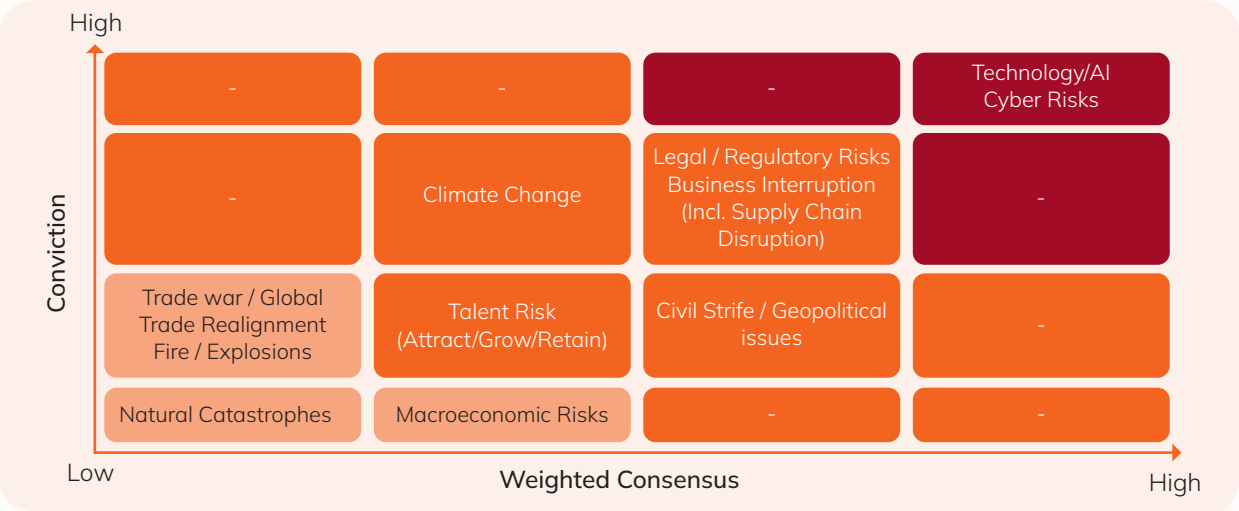


Figure 6.1.2.1 Highlights consensus vs conviction for individual risks in the short-term

Mapping risks on a two-dimensional plane, with weighted risk rankings on one axis and rank 1 vote share on the other, offers an interesting view of consensus v/s conviction.

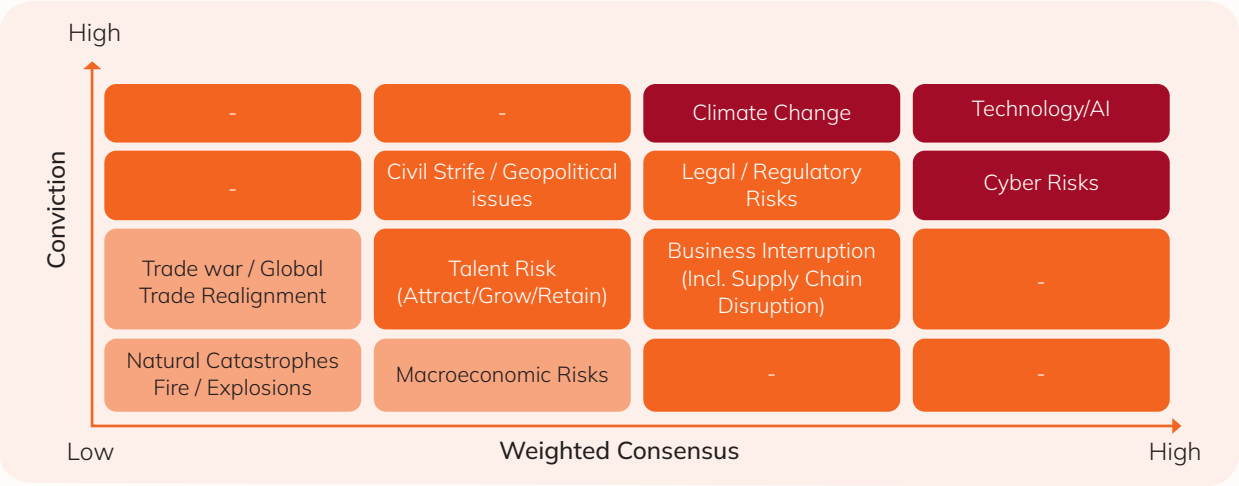


Figure 6.1.2.2 Highlights consensus vs conviction for individual risks in the long-term

Figure 6.1.2.1 depicts Consensus–Conviction mapping, or CC-mapping, for short-term risks; Figure 6.1.2.2 depicts it for long-term risks.

Consensus, measured by the weighted score a risk receives across all respondents, indicates how broadly a risk is felt across respondent sectors. Conviction, measured by the percentage of respondents who consider a risk their top risk, indicates how strongly it is prioritised across sectors. The CC-maps are divided into three zones.

The top-right three boxes, or Zone 1, represent risks considered top by the maximum number of sectors. The short-term CC-map indicates Technology/AI and Cyber risks as the industry's top concerns, with high rankings across multiple sectors. In the long term, Climate Change also joins Technology/AI and Cyber in Zone 1, with Cyber losing some conviction. This indicates the expectation that technology evolution will continue to drive change over the long term as well; Cyber risks will remain important, but Climate impact will increase significantly.

The middle, Zone 2, shows risks that are significant, and possibly at the top for a few sectors. These depend on sector characteristics and vulnerabilities.

Zone 3 – the left lower three boxes – contain risks that are important across sectors and may rank high in a sector. These will not represent new risks, and industry will be well prepared to handle these risks.

6.1.3 SHORT-TERM RISK RANKINGS: FOUR-YEAR ANALYSIS

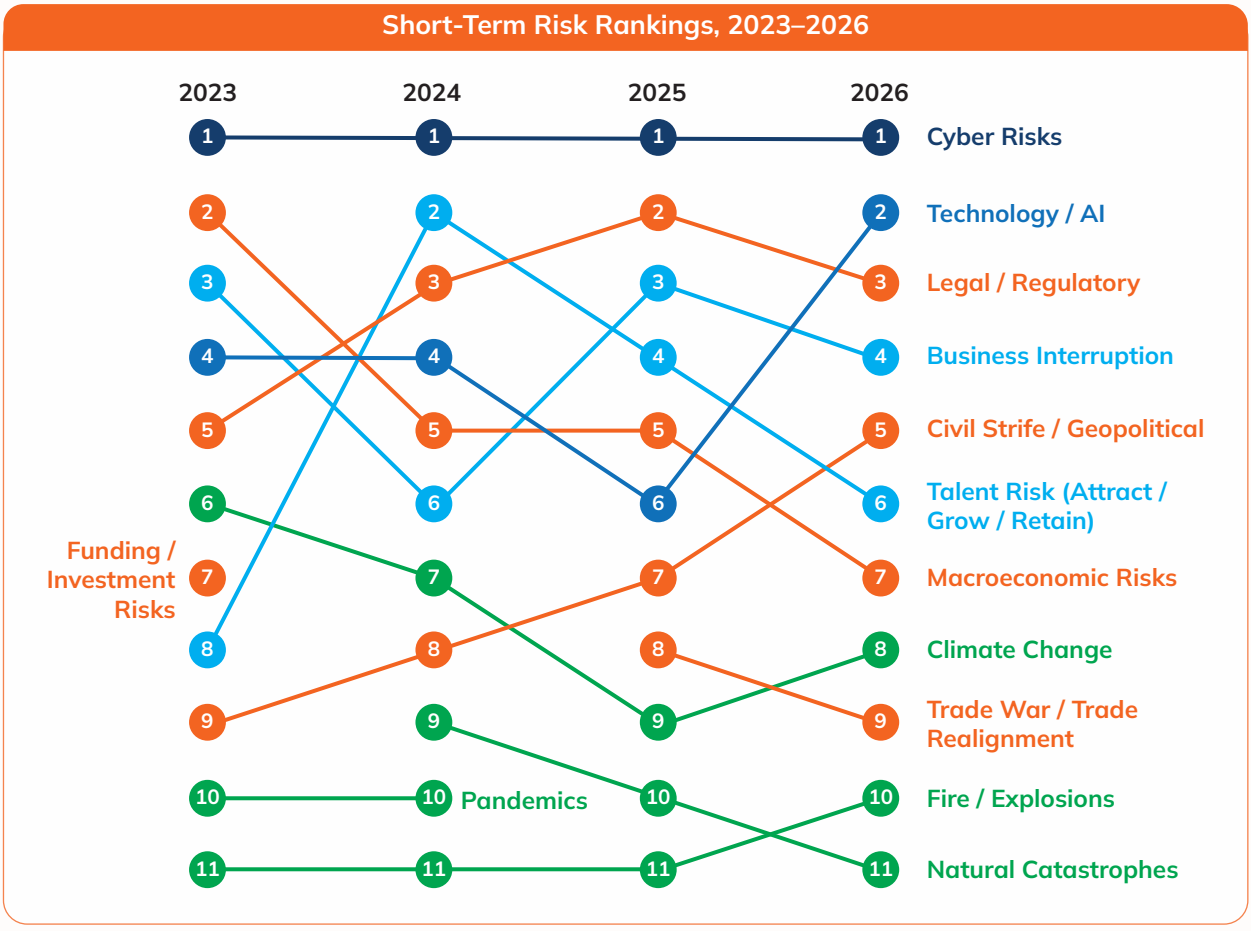


Figure 6.1.3 Depicts how short-term risk rankings have changed over four years (2023-2026)

(Note: Funding/Investment Risk was dropped in 2024 and Natural Catastrophes was added to the survey; Pandemics was dropped in 2025 and Trade War/Global Trade Realignment was added)

A comparison of this year's results with those from the previous three years (2023 - 2025), as depicted in Figure 6.1.3, shows that:

- Technology Risks have moved from 6th rank in short-term rankings of 2025 to 2nd rank this year. This aligns with the rapid evolution of AI capabilities.
- Cyber risks have remained at the top. What the ranking does not show is that risk severity has increased over time, with new technologies playing a dual role as both a risk accelerator and a risk controller.

- Legal/Regulatory risks have stayed in the top 5 in all four years due to tightening compliance regimes.
- Civil Strife/Geopolitical Risk rank in the short term has risen every year in the four-year period, possibly driven by trade fragmentation and armed conflicts.
- Talent risks peaked in 2024, possibly due to increased hiring and acceleration in digitisation efforts in the immediate post-Covid period and reduced thereafter.
- Trade-related concerns continue to be perceived at a lower level than operational risks. However, the sectoral analysis later highlights sectors concerned about the state of global trade.
- Macroeconomic concerns seem to have dropped in ranking significantly from 2023 to 2026.

This indicates a movement from technology and economic risks to technical and structural risks; the economy is perceived to be stable.

6.1.4 LONG-TERM RISK RANKINGS: FOUR-YEAR ANALYSIS

The long-term horizon reflects the challenges that organisations view as enduring and structural in nature. It also shows how concerns are expected to shift over time.

Long-Term Risk Rankings, 2023–2026

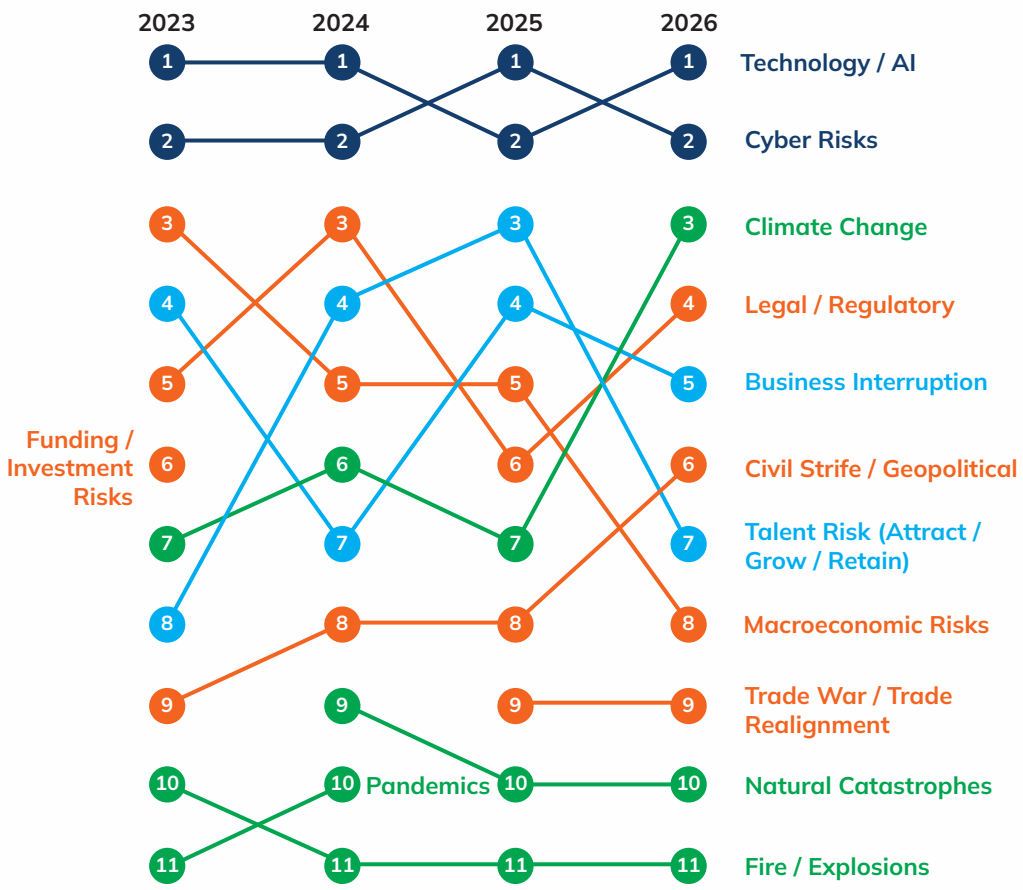


Figure 6.1.4 Depicts how Long-term risk rankings have changed over four years (2023-2026)

(Note: Funding/Investment Risk was dropped in 2024 and Natural Catastrophes was added to the survey; Pandemics was dropped in 2025 and Trade War/Global Trade Realignment was added)

A comparison of long-term risk rankings over the four-year period (2023 – 2026) highlights the following trends:

- Cyber and Technology Risks have consistently occupied the top two positions due to the continued evolution of technology over the years.
- Climate Change has been ranked at a high level for the first time since this survey was started. Its rise is in both consensus and conviction, indicating that enterprises are seeing Climate Change as a structural business risk.
- Civil Strife/Geopolitical risks have risen in rank each year in the four-year period.
- Talent Risk stayed in top 5 long-term risks in 2024 and 2025, but has dropped in 2026 rankings. This implies that concerns about talent may not be uniform across sectors.
- Macroeconomic concern rank has dropped significantly in the long-term ranking as well from 2023 to 2026, with the biggest drop from 2025 to 2026.

Thus, long-term rank changes during the four-year period also indicate a move from economy-technology risks to technology-structural risks.

6.2 TOP RISKS ACROSS REVENUE DEMOGRAPHICS

Emerging **< ₹ 500 cr** **17.4%**	**Medium** **₹ 500 cr to ₹ 1,999 cr** **17.4%**	**Large** **₹ 2000 cr to ₹ 9999 cr** **26.9%**	**Mega** **>= ₹ 10,000 cr** **38.3%**
Cyber Risks	Cyber Risks	Cyber Risks	Cyber Risks
Technology/AI	Business Interruption (Incl. Supply Chain Disruption)	Business Interruption (Incl. Supply Chain Disruption)	Technology/AI
Legal / Regulatory Risks	Technology/AI	Technology/AI	Legal / Regulatory Risks
Business Interruption (Incl. Supply Chain Disruption)	Legal / Regulatory Risks	Legal / Regulatory Risks	Civil Strife / Geopolitical issues
Climate Change	Talent Risk (Attract/Grow/Retain)	Trade war / Global Trade Realignment	Business Interruption (Incl. Supply Chain Disruption)

Table 6.2.1 Depicts comparison of the Top Five Short-Term Risks by Annual Revenue Segment

Table 6.2.1 compares the top five short-term risks across different revenue segments and highlights the following patterns:

- Cyber Risk is at the top for all revenue segments.
- Technology/AI, Business Interruption and Legal/Regulatory risks appear in the top 5 ranks for all segments.
- Climate Change appears in the top 5 only for Emerging enterprises. Typically, smaller firms operate from fewer sites – and thus are more vulnerable to climate impacts on their operations.

Emerging < ₹ 500 cr 17.4%	Medium ₹ 500 cr to ₹ 1,999 cr 17.4%	Large ₹ 2000 cr to ₹ 9999 cr 26.9%	Mega >= ₹ 10,000 cr 38.3%
Technology/AI	Technology/AI	Technology/AI	Technology/AI
Cyber Risks	Cyber Risks	Climate Change	Cyber Risks
Climate Change	Legal / Regulatory Risks	Cyber Risks	Climate Change
Legal / Regulatory Risks	Business Interruption (Incl. Supply Chain Disruption)	Legal / Regulatory Risks	Civil Strife / Geopolitical issues
Talent Risk (Attract/Grow/Retain)	Climate Change	Business Interruption (Incl. Supply Chain Disruption)	Legal / Regulatory Risks

Table 6.2.2 shows a comparison of the top five long-term risks across different revenue segments:

- Technology/AI is the top risk for all revenue segments.
- Cyber Risks, Climate Change, and Legal/Regulatory risks appear in the top 5 for all revenue segments, resulting in a high overall ranking.

6.3 TOP RISKS BY INDUSTRY SECTORS

6.3.1 SHORT-TERM TOP RISKS BY INDUSTRY SECTOR

Physical, technical, people/skill, and ecosystem characteristics determine its top risks.

Industry Sector	Rank 1	Rank 2	Rank 3	Rank 4	Rank 5
BFSI	Cyber Risks	Technology/AI	Legal / Regulatory Risks	Talent Risk (Attract/Grow/ Retain)	Macroeconomic Risks
Construction and Infrastructure	Business Interruption (Incl. Supply Chain Disruption)	Cyber Risks	Climate Change	Legal / Regulatory Risks	Civil Strife / Geopolitical issues
Energy, Oil and Gas	Fire / Explosions	Legal / Regulatory Risks	Climate Change	Civil Strife / Geopolitical issues	Trade war / Global Trade Realignment
Logistics and E-Commerce	Business Interruption (Incl. Supply Chain Disruption)	Climate Change	Macroeconomic Risks	Legal / Regulatory Risks	Cyber Risks
Manufacturing and distribution	Business Interruption (Incl. Supply Chain Disruption)	Cyber Risks	Trade war / Global Trade Realignment	Talent Risk (Attract/Grow/ Retain)	Technology/AI
Pharma, Chemicals and Fertilizers	Cyber Risks	Business Interruption (Incl. Supply Chain Disruption)	Legal / Regulatory Risks	Trade war / Global Trade Realignment	Civil Strife / Geopolitical issues
Services	Cyber Risks	Technology/AI	Talent Risk (Attract/Grow/ Retain)	Civil Strife / Geopolitical issues	Business Interruption (Incl. Supply Chain Disruption)
Other	Technology/AI	Macroeconomic Risks	Cyber Risks	Civil Strife / Geopolitical issues	Talent Risk (Attract/Grow/ Retain)

Table 6.3.1 The Table above depicts the Short-term risk ranking by Industry Sectors

Table 6.3.1 shows top 5 short-term risks for various industry sectors as per responses to ERPS-2026.

- Cyber and Business Interruption risks are the most frequent in the top 2 risks. Technology-intensive sectors have rated it a top risk because a cyber-attack can have a huge impact on operations, financials and reputation.
- Fire/Explosions is the top risk for Energy, Oil and Gas.
- Technology/AI has been prioritised by BFSI, and Services and Manufacturing industries. BFSI and Services rank highly because they are technology- and people-intensive. High ranking by Manufacturing is driven by its technology-intensive nature.
- Trade War / Global Trade realignment appears in the top 5 risks for Manufacturing, Energy, and Pharma – all dependent upon cross-border trade.
- Talent Risk is cited in BFSI, Services due to their people-intensive nature and in the Manufacturing sector due to its dependence on specific skills.
- Climate Change is present in the top 5 risks for Construction, Energy and Logistics and E-commerce – all sectors most impacted by weather events.

6.3.2 LONG-TERM TOP RISKS BY INDUSTRY SECTOR

Industry Sector	Rank 1	Rank 2	Rank 3	Rank 4	Rank 5
BFSI	Technology/AI	Cyber Risks	Legal / Regulatory Risks	Talent Risk (Attract/Grow/ Retain)	Climate Change
Construction and Infrastructure	Climate Change	Technology/AI	Legal / Regulatory Risks	Civil Strife / Geopolitical issues	Business Interruption (Incl. SupplyChain Disruption)
Energy, Oil and Gas	Climate Change	Technology/AI	Business Interruption (Incl. Supply Chain Disruption)	Trade war / Global Trade Realignment	Fire / Explosions
Logistics and E-Commerce	Climate Change	Business Interruption (Incl. Supply Chain Disruption)	Technology/AI	Civil Strife / Geopolitical issues	Macroeconomic Risks
Manufacturing and distribution	Technology/AI	Climate Change	Civil Strife / Geopolitical issues	Cyber Risks	Business Interruption (Incl. Supply Chain Disruption)
Pharma, Chemicals and Fertilizers	Legal / Regulatory Risks	Business Interruption (Incl. Supply Chain Disruption)	Climate Change	Technology/AI	Civil Strife / Geopolitical issues
Services	Technology/AI	Cyber Risks	Talent Risk (Attract/Grow/ Retain)	Civil Strife / Geopolitical issues	Business Interruption (Incl. Supply Chain Disruption)
Other	Technology/AI	Civil Strife / Geopolitical issues	Climate Change	Legal / Regulatory Risks	Macroeconomic Risks

Table 6.3.2 Depicts Top Long-Term risk ranking by Industry Sectors

The long-term risk pattern in Table 6.3.2 reflects industry expectations of transformative impacts from Technology/AI and Climate Change, along with lingering geopolitical and economic issues.

- It is notable that Climate Change is ranked as the top long-term risk by three sectors and is present in the top 5 risks for four more sectors.
- Technology/AI is the top concern in the long term for 3 sectors and is present in the top 5 across all other sectors.
- Legal/Regulatory concerns are expected to persist in the long term in 4 industry sectors.
- Cyber risks are present in the top 5 for only 3 sectors in the long-term risks.

6.4 PERCEPTION OF TOTAL RISK

While risk rankings and their shifts provide insights into how respondents perceive individual risks, the survey also included a question designed to gauge overall exposure: "Considering all the risks relevant to your business, how would you rate your organisation's overall risk level today?"

Respondents were asked to rate total risk on a scale of 0 to 10.

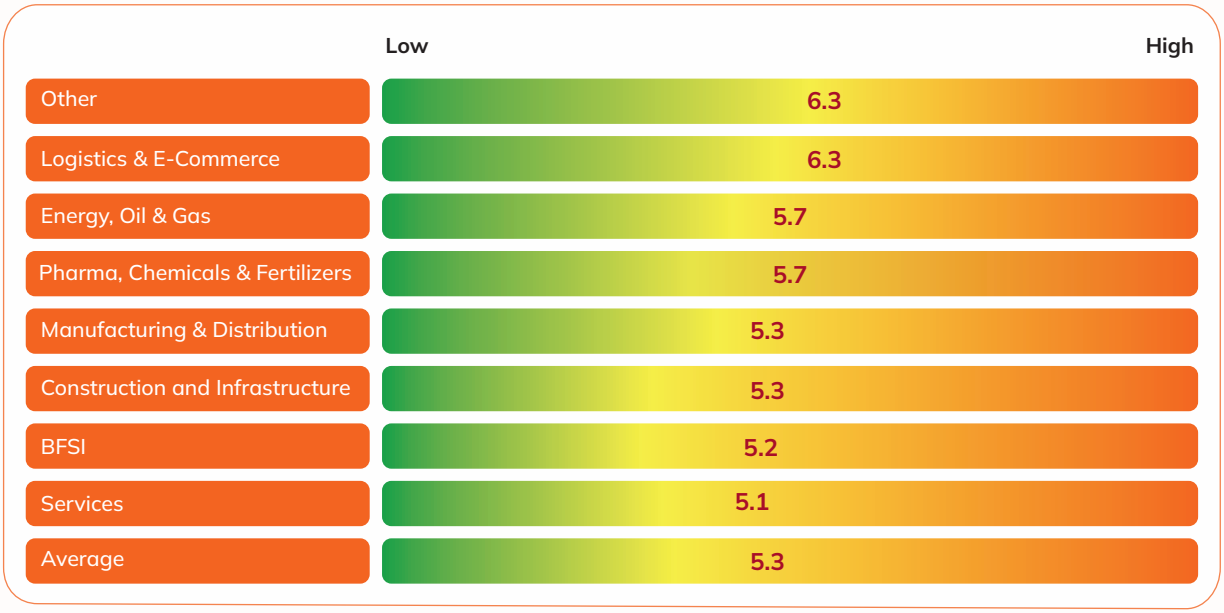


Figure 6.4 The above heat map depicts the Perception of Total Risk on a scale of 0 (low) to 10 (high) by industry sector

Logistics, Energy and Pharma see the overall risk level to be higher than other sectors. On an average, it is not seen to be a high risk environment.

Table 6.4.1 provides a comparison of how the total risk perception has moved across four years.

Industry Sector	2023	2024	2025	2026	Trend 2023–26
Logistics and E-Commerce	4.8	5.2	5.2	6.3	Strong rise, highest score in 2026
Energy, Oil and Gas	6.3	4.4	7.0	5.7	Mild fall, sharp swings, peak 2025
Pharma, Chemicals and Fertilizers	5.8	5.3	6.2	5.7	Broadly flat, peaked 2025, then eased
Manufacturing and distribution	5.0	5.1	5.5	5.3	Mild rise, peaked 2025, then eased
Construction and Infrastructure	6.2	-	5.9	5.3	Mild fall, down from 2023 high
BFSI	5.3	6.0	5.2	5.2	Broadly flat, peaked 2024, then eased
Services	5.0	6.0	5.6	5.14	Broadly flat, peaked 2024, then eased
Other	6.0	5.2	6.7	6.3	Mild rise, sharp swings, peak 2025
Overall Average	5.3	5.6	5.6	5.33	

Table 6.4.1 Depicts evolution of Total Risk Level perception over four years. Note: in 2024, Construction and Infrastructure sector was not considered separately.

It is notable that the total risk level is at its lowest level compared to the previous two years, despite global escalation in geopolitical and Tech/AI risks during the year. This could indicate that enterprises have higher confidence in their controls now than in earlier years.

EXPERT PERSPECTIVE



DEEPAK ARORA
Vice President - Corporate Solutions Group
ICICI Lombard

Q With the rapid expansion of renewable energy infrastructure, what evolving risks could threaten its long-term sustainability, and how can insurance provide a financial safeguard against unforeseen disruptions?

India's renewable energy sector has reached a significant milestone, with installed renewable energy capacity of approximately 300 GW, bringing the country closer to its ambitious target of 500 GW of non-fossil fuel-based capacity by 2030. The sector is also undergoing a structural transformation, with players increasingly pursuing backward integration into manufacturing of solar modules, cells and other critical components, while expanding downstream into emerging businesses such as green hydrogen, green ammonia and energy storage. This expanding value chain is reshaping the industry's risk landscape.

Larger solar and wind installations, growing adoption of Battery Energy Storage Systems (BESS) and increasing dependence on interconnected digital infrastructure are creating new risk exposures. While conventional physical and climate-related risks continue to remain significant, cyber threats targeting SCADA systems, operational technology and remote monitoring platforms could disrupt generation, compromise operational controls and affect grid connectivity. Combined with dependence on specialised equipment, such as transformers, and their long replacement lead times, these exposures can significantly amplify business interruption losses.

The challenge is no longer limited to protecting physical assets; it is equally about safeguarding digital infrastructure, ensuring operational continuity and protecting project economics. This calls for a more forward-looking approach to risk assessment, with resilience embedded in project design, operations and cybersecurity frameworks.

As the renewable energy industry evolves, so will its risk protection requirements. The insurance industry must keep pace with these changing demands by developing innovative, relevant and integrated solutions that address emerging physical, operational and cyber exposures. Specific solutions such as parametric insurance can provide protection against generation losses arising from defined weather-related triggers, while warranty insurance can help address risks associated with the performance and reliability of critical equipment and components. Beyond financial compensation, insurers have an opportunity to become strategic risk partners, bringing technical expertise, proactive risk management and tailored protection to strengthen resilience and investor confidence.

As India accelerates its energy transition, the ability to anticipate, absorb and recover from disruptions will be as important as the capacity we add.



6.5 AI RISKS AND OPPORTUNITIES

While risks and opportunities are the two sides of the same coin, AI presents as many opportunities as risks. It has the potential to immensely transform the business landscape over the next few years.

ERPS-2026 asked enterprises to rank the top 5 opportunities and risks presented by AI. The results are depicted in Figure 6.5.



Figure 6.5.a Depicts ranks of AI Opportunities based on weighted ranking and rank 1 vote share in ERPS-2026.

Operational Efficiency is voted as the top AI opportunity. Its weighted score is almost double that of the next opportunity, Improved Decision Quality. Operational Efficiency also gets almost half of all Rank 1 votes, with Revenue Growth getting the second-highest vote share, though trailing by a huge margin.

This indicates that the industry plans to use AI more as a tool to improve process efficiency and reduce costs, rather than to grow or innovate. The sector-wise analysis later provides a more nuanced view of industry approach.

AI as a tool to better manage Risks has got the lowest scores.

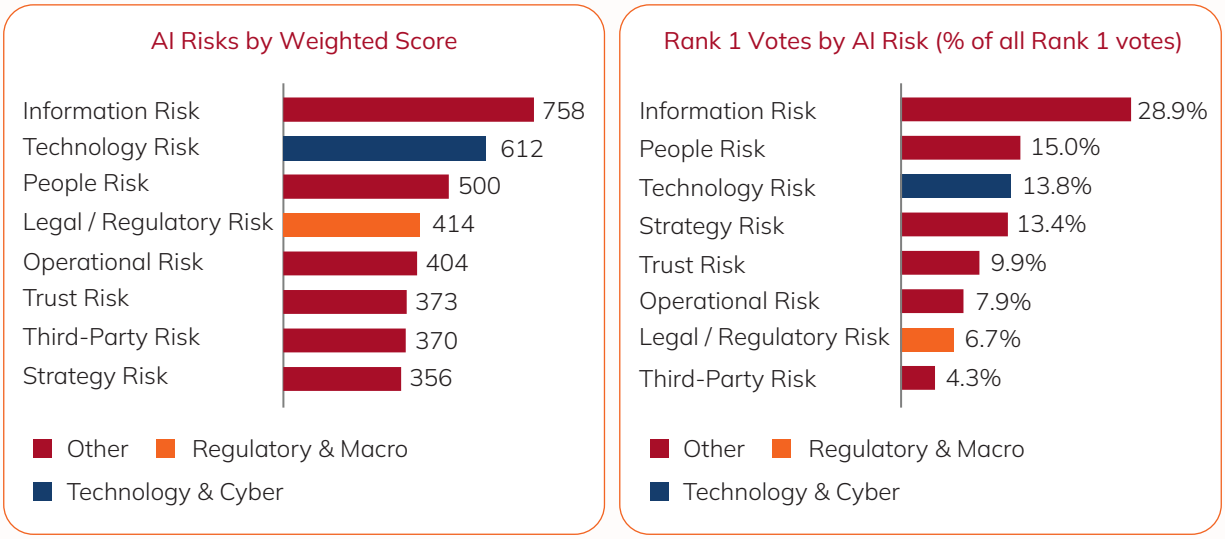


Figure 6.5.b Depicts ranks of AI Risks based on weighted ranking and rank 1 vote share in ERPS-2026.

As depicted in Figure 6.5.b, Information Risk is the top AI concern, followed by Technology Risk in second place. However, the vote shares for People Risk and Technology Risk for rank 1 are in the same range, implying that several sectors consider people risk as the top risk, whereas other sectors give it a much lower risk.

While Operational Efficiency is the top opportunity, Operational Risk ranks 5th.

6.5.1 AI OPPORTUNITIES AND RISKS BY INDUSTRY SECTOR

While risks and opportunities are the two sides of the same coin, AI presents as many opportunities as risks. It has the potential to immensely transform the business landscape over the next few years.

ERPS-2026 asked enterprises to rank the top 5 opportunities and risks presented by AI. The results are depicted in Figure 6.5.

Industry Sector	AI Opportunities		AI Risks	
	Rank 1	Rank 2	Rank 1	Rank 2
BFSI	Operational Efficiency	Customer Value - Experience/Quality	Information Risk	Technology Risk
Construction and Infrastructure	Operational Efficiency	Improved Decision Quality	Information Risk	Technology Risk
Energy, Oil and Gas	Operational Efficiency	Innovation	Information Risk	Technology Risk
Logistics and E-Commerce	Operational Efficiency	Improved Decision Quality	Operational Risk	Information Risk
Manufacturing and Distribution	Operational Efficiency	Improved Decision Quality	Information Risk	Technology Risk
Pharma, Chemicals and Fertilizers	Operational Efficiency	Improved Decision Quality	Information Risk	Trust Risk
Services	Operational Efficiency	Revenue Growth	Information Risk	Technology Risk
Other	Operational Efficiency	Revenue Growth	Information Risk	Strategy Risk

Table 6.5.1 AI Opportunities and Risks by Industry Sector

Every sector has ranked Operational Efficiency as the top opportunity. Sectors vary in their 2nd ranks, with only the Services sector voting Revenue Growth in second place and only BFSI ranking Customer Value – Experience/Quality in second place.

On risks, Information Risk is most consistently seen as the top risk. Technology Risk ranked at 2nd place by five sectors.

Looking at opportunities and risks together, we can conclude that as of now, respondents see AI mainly as an operational efficiency lever, and the data it depends on is seen as the top risk. As AI technology and its adoption evolve, we can expect changes in the rankings, as well as new opportunities and risks.

EXPERT PERSPECTIVE



RISHI GARG
Chief Risk Officer
Nippon Life India - Asset Management Company Limited

AI Opportunities and Risks

Operational efficiency is currently the leading AI opportunity across sectors. Enterprises expect AI to make them more efficient by speeding up processing and reducing errors. AI also offers cost savings by cutting the effort needed for many tasks and processes.

AI is also expected to improve decision-making. It can handle far more data, and in far more depth, than traditional IT systems. This lets it find correlations and insights that people using those systems could not.

On the risk side, Information Risk is the top concern for enterprises. Weak controls over how AI is used could leave enterprise data exposed on the public internet. Unauthorised or malicious use of that data could then create liability and reputational risks.

Technology Risk is the second most important AI concern. It covers the liability, damages and remediation costs that can arise from errors made by AI agents. Because these agents act on their own and at high speed, the impact of such errors could be greater.

The same AI capabilities that drive operational efficiency, better decision-making and innovation also help malicious actors find and exploit cyber vulnerabilities in enterprise systems. Cyber Risk is the top short-term concern in the survey, and enterprises report a high level of readiness for it. However, as AI-enabled attacks grow more sophisticated, enterprises may well be overestimating how prepared they are.



6.5.2 PREPAREDNESS FOR AI

To understand enterprise views more deeply, ERPS-2026 also asked questions on how organisations perceived the importance of AI and how prepared they were to leverage the opportunities and manage AI risks.

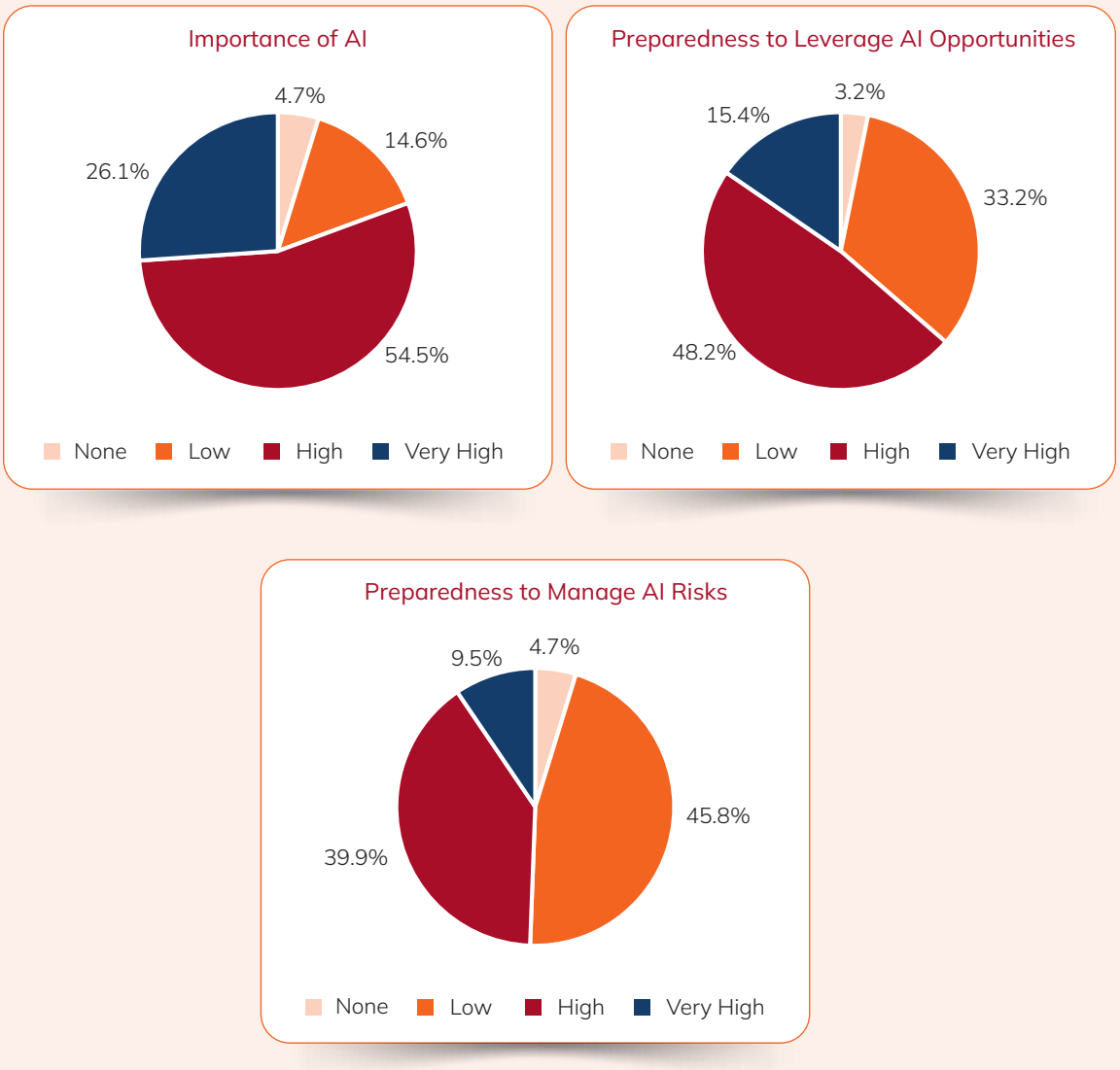


Figure 6.5.2 depicts the importance of AI as perceived by organisations and their preparedness to leverage opportunities and manage risks as per ERPS-2026

Around 51% of respondents indicate none or low preparedness to manage AI Risks. This indicates that risk readiness is not keeping pace with the speed of evolution of AI capabilities.

Around 37% of respondents indicate none or low preparedness to leverage AI opportunities, while 15.9% show very high preparedness. While these scores show better preparedness for opportunities than for risks, preparedness lags behind the importance attached to AI. Around 54.5% respondents rate the importance as High and 26.1% as very high.

The analysis indicates that enterprises rate AI as important, but their readiness lags.

7. ENTERPRISE RESILIENCE

Organisational resilience depends on more than recognising the risks an organisation faces. It requires strategies and capabilities to respond when those risks materialise, processes that bring risk considerations into decisions, and a culture in which responsibility extends beyond the specialist risk team. As risks become more interconnected, organisations must also assess whether their readiness keeps pace with the exposures they consider most likely.



In this chapter, we examine organisations' preparedness to manage risks and their exposure to those risks. This is followed by a discussion of risk management maturity and the components that contribute to it. The analysis is based on findings from the Enterprise Risk Perceptions Survey-2026 (ERPS-2026) and, where available, comparison with earlier editions of the India Risk Report.

7.1 PREPAREDNESS TO FACE RISKS

In the ICICI Lombard - IRM India Enterprise Risk Perceptions Survey – 2026, respondents rated their preparedness to face various risks. The question provided four possible options. The responses are tabulated in Figure 7.1.1, with the four options as column headings.

Risk	Not Prepared	Have Strategy	Have Capability	Have Strategy and Capability
Technology / AI	8%	23%	27%	42%
Cyber Risks	7%	13%	22%	58%
Business Interruption (incl. Supply Chain Disruption)	9%	14%	23%	54%
Talent Risk (Attract / Grow / Retain)	10%	24%	24%	42%
Legal / Regulatory Risks	4%	14%	20%	62%
Civil Strife / Geopolitical Issues	18%	21%	32%	29%
Macroeconomic Risks	16%	25%	25%	34%
Trade War / Global Trade Realignment	22%	24%	23%	31%
Fire / Explosions	8%	15%	21%	56%
Natural Catastrophes	17%	18%	26%	39%
Climate Change	21%	25%	21%	33%

Technology/Cyber Business Interruption/Talent Regulatory & Macro Hazards

Figure 7.1.1 Depicts analysis of preparedness for managing risks

Key Takeaways

Preparedness is strongest for Legal/Regulatory and established operational risks: Legal/Regulatory Risks record the highest proportion of respondents with both strategy and capability (62%), followed by Cyber Risks (58%), Fire/Explosions (56%) and Business Interruption/Supply Chain Disruption (54%). The highest preparedness score for Legal/Regulatory indicates a focus on compliance.

Technology/AI preparedness is still developing: 42% of the respondents report having both strategy and capability, while only 8% are not prepared. However, a further 50% possess either strategy or capability, but not both, indicating scope to translate emerging AI initiatives into more integrated preparedness.

Climate-related preparedness remains comparatively uneven: Only 33% report both strategy and capability for Climate Change, while 39% do so for Natural Catastrophes. Given the increasing frequency and interconnected impact of climate-related disruptions, these areas offer important opportunities to strengthen organisational resilience.

External and systemic risks show the largest preparedness gaps: Only 29% of respondents have both strategy and capability for Civil Strife/Geopolitical Issues, 34% for Macroeconomic Risks and 31% for Trade War/Global Trade Realignment. Trade-related risk also records the highest proportion of respondents who are not prepared (22%).

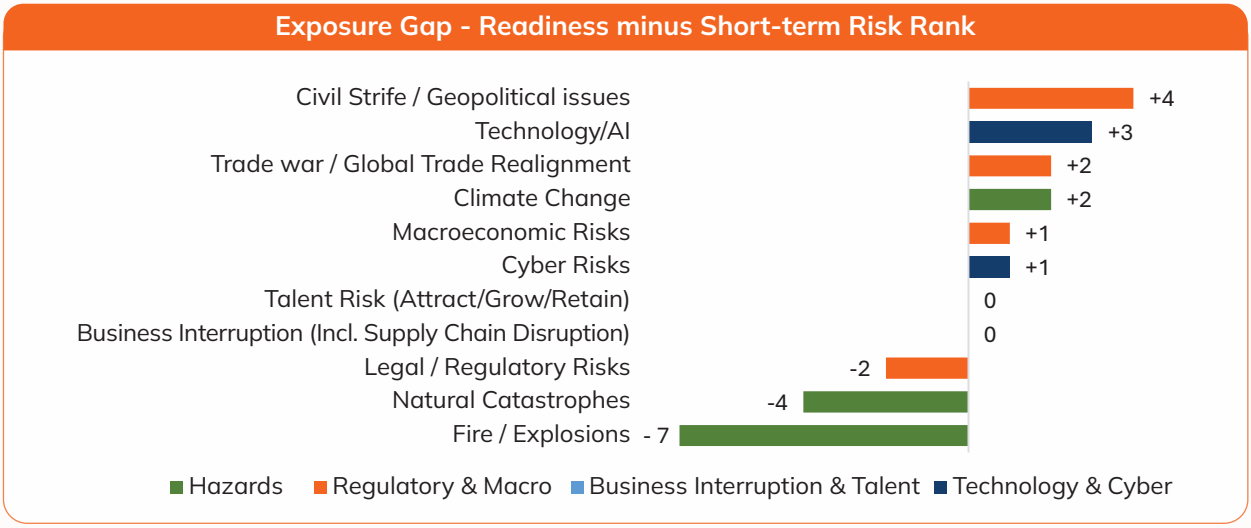


Figure 7.1.2 Depicts enterprise exposure gap levels to risks

Note: The gaps compare relative rankings; they do not measure the absolute size of exposure or readiness.

The preparedness results become more revealing when viewed alongside short-term risk ranks, revealing respondents' likely exposure gap for individual risks.

The exposure gap, depicted in Figure 7.1.2, is calculated as the difference between the readiness rank and the short-term risk rank of a risk. The readiness rank is derived from the table in Figure 7.1.1 by assigning 0-3 marks for the four options and calculating the average readiness index for each risk. The short-term risk ranks are discussed in Chapter 6, Risk perceptions of India Inc.

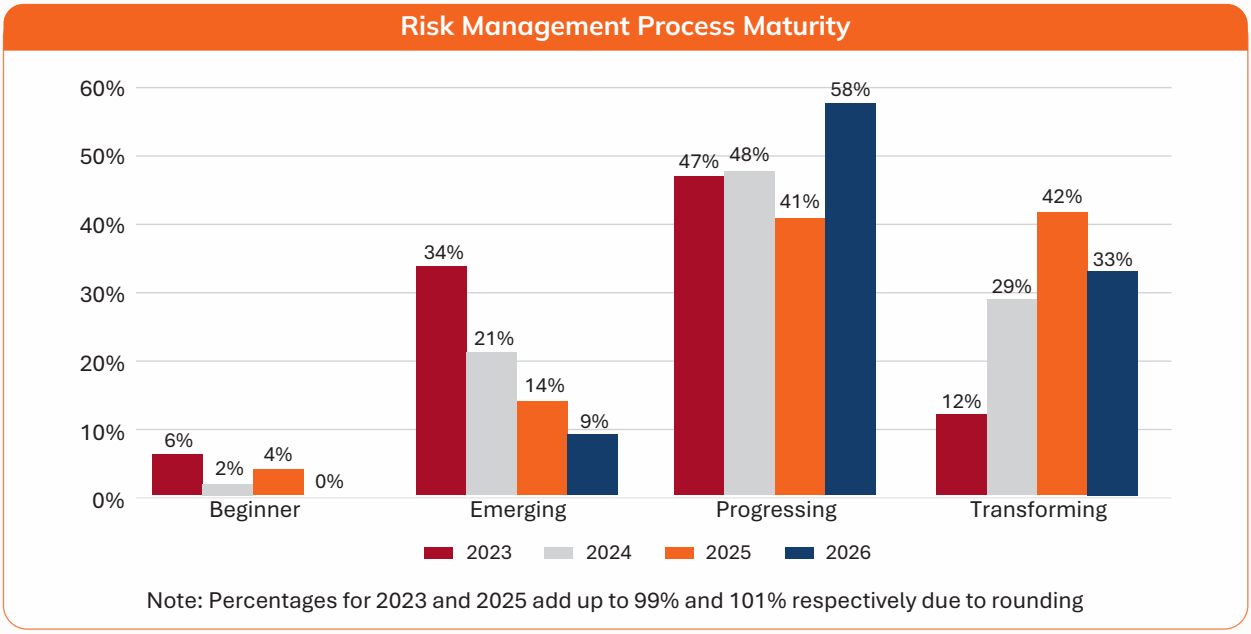
Risks with positive exposure gaps, at the top of Figure 7.1.2, are the enterprises' priorities for strengthening preparedness, both in terms of having a clear strategy and investments in the capability to manage the risks.

A negative gap tends to point to well-understood risks with clear ownership and processes in the organisation. These risks tend to receive a relatively lower ranking and a higher preparedness score, resulting in a "negative" gap, as depicted in Figure 7.1.2.

7.2 RISK MANAGEMENT PROCESS MATURITY

In ERPS-2026, respondents assessed the maturity of their organisations' enterprise risk management (ERM) processes. These ratings reflect respondents' own assessment of how consistently risk management practices are implemented, rather than an independent evaluation. The four maturity levels are:

- Level 1 - Beginner: Organisations whose ERM practices are at an initial stage.
- Level 2 - Emerging: Inconsistent implementation of certain risk management practices.
- Level 3 - Progressing: High level of maturity across multiple areas of ERM.
- Level 4 - Transforming: High levels of maturity across all areas.



Note: Percentages for 2023 and 2025 add up to 99% and 101% respectively due to rounding

Figure 7.2 Depicts enterprise Risk Management maturity of respondents over four years

- The maturity profile remains concentrated in the upper-middle band: In 2026, the largest share of respondents (58%) falls in the Progressing category, indicating established risk-management practices. The share of Transforming organisations has moderated from 42% in 2025 to 33% in 2026. However, the total of Progressing plus Transforming organisations, growing year on year, now represents 91%, which is an encouraging development.
- Lower maturity levels remain limited, but not negligible: None of the respondents are in the Beginner category in 2026, while 9% remain Emerging.

7.3 FACTORS DRIVING RISK MANAGEMENT MATURITY

The risk management process maturity scores discussed in the previous section are based on respondents' self-assessment of the following factors:

- Responsibility for risk identification in the organisation
- Risk management process ownership in the organisation
- Risk management framework used
- Who drives risk management in the organisation?
- Organisation's attitude towards risk

These factors were assessed over five questions in ERPS-2026.

7.3.1 RESPONSIBILITY FOR RISK IDENTIFICATION IN THE ORGANISATION

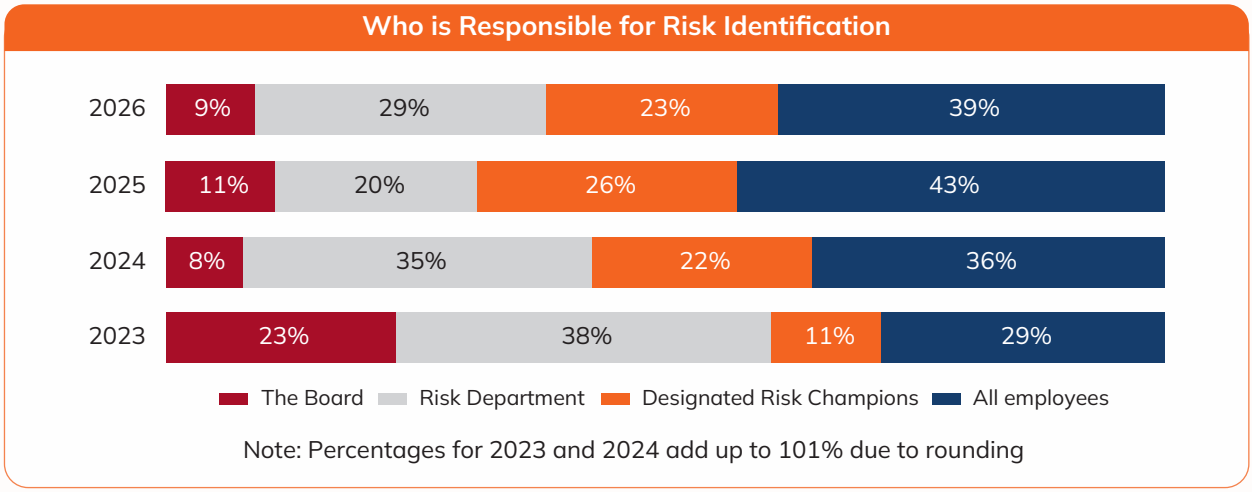


Figure 7.3.1 Depicts risk identification practices of respondent companies over four years

Respondents were asked who identifies risk in their organisations. In a mature organisation, every employee is responsible for Risk Identification. The survey response shows a slight drop in the percentages for the most mature options (All employees and Designated Risk Champions), from 69% in 2025 to 62% in 2026. Enterprises need to improve risk identification capabilities across the organisation.

EXPERT PERSPECTIVE



SUNIL KUMAR SINGH

Chief - Insurance
Reliance Industries Limited

Organisations must move towards a decision-making culture where risk intelligence is embedded in every strategic priority, rather than viewed as a separate control mechanism. Whether pursuing growth, entering new markets or transforming operations, understanding uncertainty is essential to making informed choices.

This requires leadership ownership, clear accountability and a forward looking view of emerging exposures. The true measure of risk maturity is the ability to balance opportunity with preparedness and translate uncertainty into sustainable business value.

7.3.2 RISK MANAGEMENT PROCESS OWNERSHIP IN THE ORGANISATION

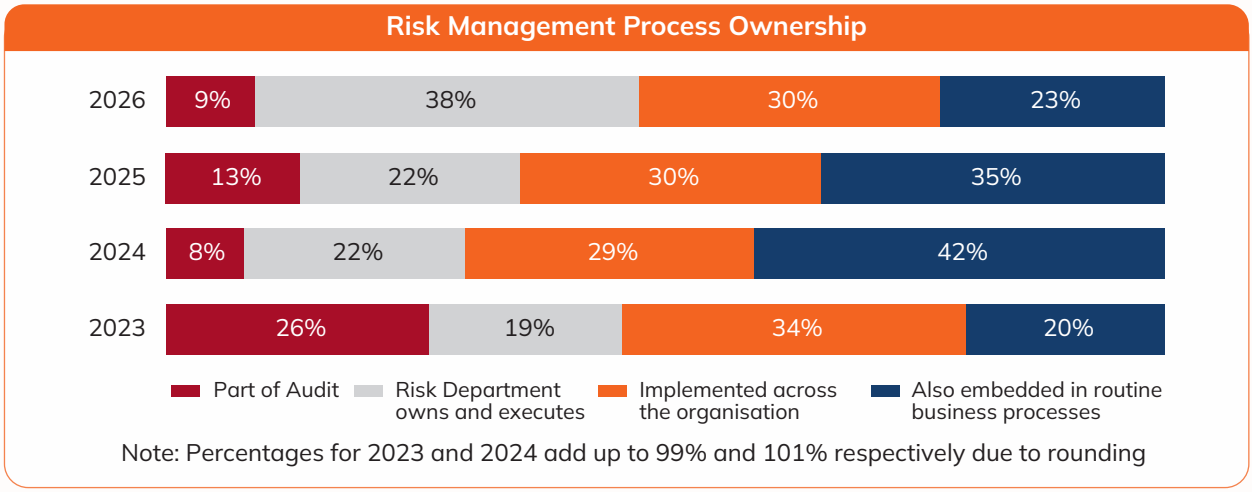


Figure 7.3.2 Depicts risk management process ownership adopted by respondent companies

Respondents were asked to identify who owns the risk management process in their organisations. The goal was to find out whether the process ownership is siloed in Audit / Risk Management departments or whether it is embedded in all the routine processes of the organisation. The analysis shows the percentage of the two most mature options – namely Embedded in routine business processes and Implemented across the organisation - drops from 65% to 53%.

Enterprises need to connect the risk function's oversight with decisions across the organisation so process ownership translates into day-to-day practice.

7.3.3 RISK MANAGEMENT FRAMEWORK USED

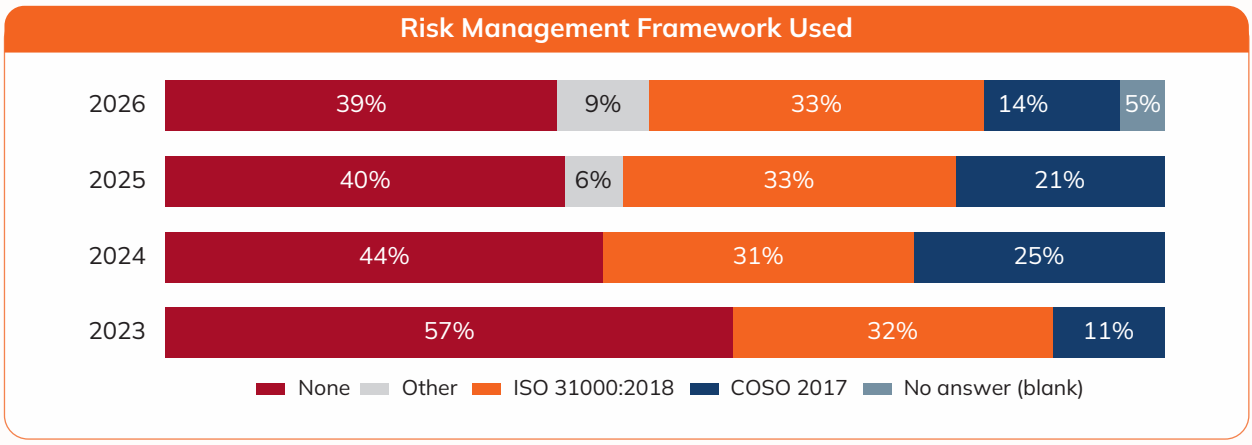


Figure 7.3.3 Depicts risk management framework adopted by respondent companies for developing risk management processes

Respondents were asked to identify standards on which their risk management processes were based.

The number of respondents identifying COSO framework fell from 21% in 2025 to 14% in 2026, while the share reporting no framework declined slightly from 40% in 2025 to 39% in 2026.

Nevertheless, the substantial share reporting no framework points to a continuing need to strengthen formal risk management practices.

7.3.4 WHO DRIVES RISK MANAGEMENT IN YOUR ORGANISATION?

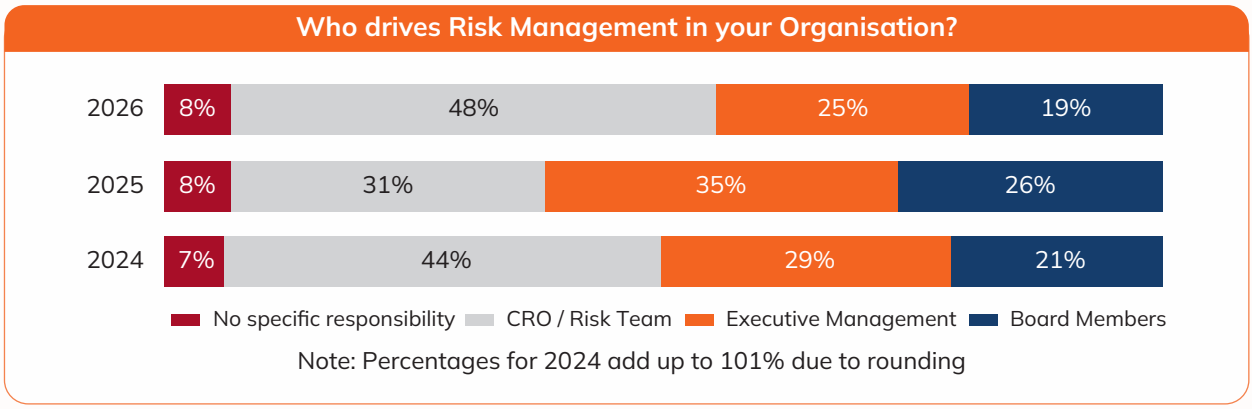


Figure 7.3.4 Depicts respondents identifying who drives risk management in their organisation

The respondents were asked to identify the ultimate driver of risk management in their organisations. The CRO/Risk Team is the most frequently identified driver of risk management in 2026 (48%), up from 31% in 2025. The share identifying Board Members fell from 26% to 19%. Mature organisations tend to have their boards drive the risk management program, providing a clear tone from the top.

7.3.5 ORGANISATION'S ATTITUDE TOWARDS RISK

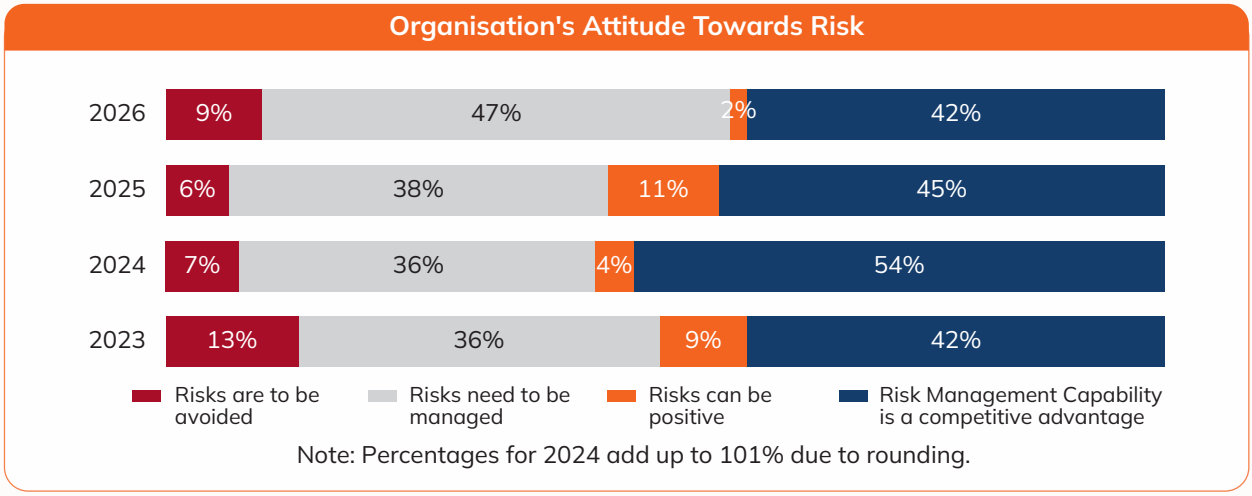


Figure 7.3.5 Depicts organisations' attitude towards risk

Respondents were asked to assess their organisation's attitude towards risk.

Mature organisations view Risk Management as a competitive advantage. In 2026, respondents most often described their organisations' attitude as Risks need to be managed (47%), followed by recognition of risk management capability as a competitive advantage (42%). Only 2% of organisations selected Risks can be Positive.

The responses suggest an opportunity to develop risk culture beyond controlling threats, helping organisations assess which risks are worth taking to pursue their objectives. This is especially relevant in the current environment, where factors like technology and AI offer significant opportunities for organisations.

EXPERT PERSPECTIVE



NIKHIL KUDALKAR
Chief Risk Officer
UTI Pension Fund Limited

While the higher maturity scores for individual risk management practices are encouraging, there remains clear scope for improvement.

Many organisations continue to view risk management as a compliance function or an impediment to decision-making. This perception must change so that:

- Risk processes are embedded across all business processes, and
- Every employee takes ownership of identifying risks.

Artificial intelligence presents a range of transformative opportunities, and organisations that treat risk management as a source of competitive advantage will be better positioned to capitalise on them.

To this end, enterprises should take deliberate steps to:

- Deepen the understanding of risk across departments, including its value in pursuing opportunities, and
- Raise the visibility of the risk management function and its activities.

CONCLUSION

The ERPS-2026 findings present a mixed picture of organisational resilience.

Enterprise exposure figures – defined as the difference between Readiness rank and short-term risk rank for Geopolitical disruptions, Technology/AI, Trade realignment and Climate Change highlight relatively high priorities for strengthening preparedness.

Most respondents assess their organisations' risk management processes as relatively mature, with 58% in the Progressing category and 33% in Transforming. The lower share in the highest maturity band compared with 2025 points to scope for more consistent implementation of all five maturity practices discussed in this chapter. Use of international standards in developing risk management processes will also help improve maturity. Around 39% respondents do not use any standards for their processes.

Strengthening resilience therefore requires organisations to sustain established controls, develop strategies and capabilities for less well-addressed risks, and integrate risk considerations into everyday decisions. A more developed risk culture should support informed risk-taking in pursuit of objectives as well as protection against losses. These findings reflect respondents' assessments; comparisons across editions indicate changes in survey responses rather than verified changes within the same organisations.

8. RISK MANAGEMENT AND INSURANCE

In its simplest form, the risk management process involves identifying, assessing and managing risks. Once a risk is identified and evaluated, an organisation can manage it in multiple ways:

REDUCE THE RISK THROUGH CONTROLS:

Controls are safeguards that reduce the likelihood and/or impact of a risk. They bring the risk down to a lower, more manageable level, known as residual risk. Several controls can work together to reduce the risk further and more reliably. Designing them well requires a clear understanding of the risk itself: what causes it, what harm it does directly, and how that harm can spread to other parts of the business.

INSURE THE RISK:

Residual risks can be transferred to an insurer by buying a suitable cover. The right insurance policy will fit an organisation's needs. Insurance costs are part of the total cost of insuring risks.

ERPS-2026 asked a set of questions to understand how organisations procure and manage insurance for their risks. This chapter provides an analysis of the responses.

8.1 RISK SOLUTIONS DEPLOYED

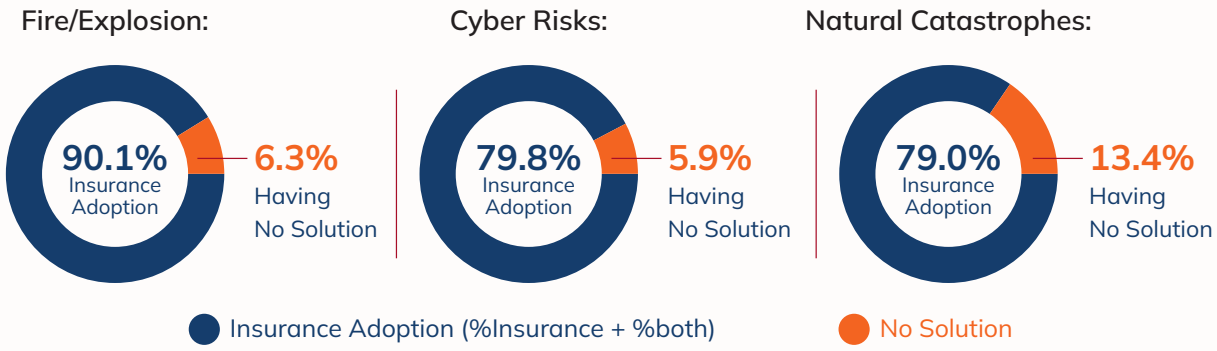
Respondents were asked to indicate the type of risk management solutions they use across different risk categories, selecting from four options: Insurance, Non-insurance, Both, or None. Table 8.1 summarises the results.

Risk	% Insurance	% Non-Insurance	% Both: Insurance and Non-insurance	% None
Fire / Explosions	39.5%	3.6%	50.6%	6.3%
Cyber Risks	33.6%	14.2%	46.2%	5.9%
Natural Catastrophes	33.2%	7.5%	45.8%	13.4%
Legal / Regulatory Risks	21.7%	28.1%	42.3%	7.9%
Climate Change	21.7%	21.7%	34.8%	21.7%
Business Interruption (Incl. Supply Chain Disruption)	21.3%	21.7%	43.5%	13.4%
Technology/AI	17.4%	35.6%	28.9%	18.2%
Civil Strife / Geopolitical issues	15.8%	34.4%	30.4%	19.4%
Macroeconomic Risks	10.3%	45.8%	20.2%	23.7%
Trade war / Global Trade Realignment	9.1%	44.7%	20.9%	25.3%
Talent Risk (Attract/Grow/Retain)	8.7%	53.0%	16.6%	21.7%
Total	21.1%	28.2%	34.6%	16.1%

Technology/Cyber Business Interruption/Talent Regulatory & Macro Hazards

Table 8.1 The table depicts the risk management solutions deployed to manage the risks

THE TOP THREE INSURED RISKS ARE:



Business Interruption and Legal/Regulatory risks have just over 64% of respondents with insurance solutions, while 13.4% of respondents have no solutions for Business Interruption. Just over 56% of respondents insure for Climate Change risks.

Other five risks are the least insured for. These risks, along with Climate Change, are the six risks respondents are least prepared for, with 18%-25% choosing no solution for each.

Some of these risks can be insured with products firms may not know about: political risk and trade credit cover for geopolitical and trade risks, key-person cover for talent, parametric cover for climate. Many enterprises are substantially exposed and need to take urgent action to establish controls and procure insurance. This has become even more relevant and urgent in the current environment of converging and interconnected risks, as exposures can arise due to unforeseen interactions between various influencing forces.

In order to effectively plan and deploy insurance solutions, enterprises need to monitor and control the cost-effectiveness of insuring a risk in an end-to-end manner.

EXPERT PERSPECTIVE



RAJEEV ROSHAN
Channel Partner
ICICI Lombard

In the general insurance industry, it is important to understand whether a disruption is temporary or a structural change, as it directly impacts underwriting, pricing and long term business strategy. A temporary disruption, like a sudden increase in claims due to floods or a short term supply chain issue, may have an impact for a limited period.

However, structural changes such as increasing frequency of natural calamities, rising reinsurance cost, changes in customer expectations and technology advancement can have a long term impact on the industry. One way to identify this difference is by looking at the trend over a period of time rather than taking decisions based on one particular year or event. If the same pattern continues across multiple years and starts impacting loss ratios, pricing and availability of insurance, it may indicate a structural change.

Insurers need to regularly review their portfolio, claims experience and underwriting approach to identify these changes early. In my view, the biggest challenge is that sometimes we continue to assess future risks based on past data, whereas the risk environment is changing much faster.

8.2 MEASURING TOTAL COST OF INSURING RISK

The Total Cost of Insuring Risk (TCOIR) includes both internal and external costs of risk management, covering the expenses of retaining as well as transferring risk. Respondents were asked whether they measure these costs, and which specific components they track. Figure 8.2 shows the response analysis.

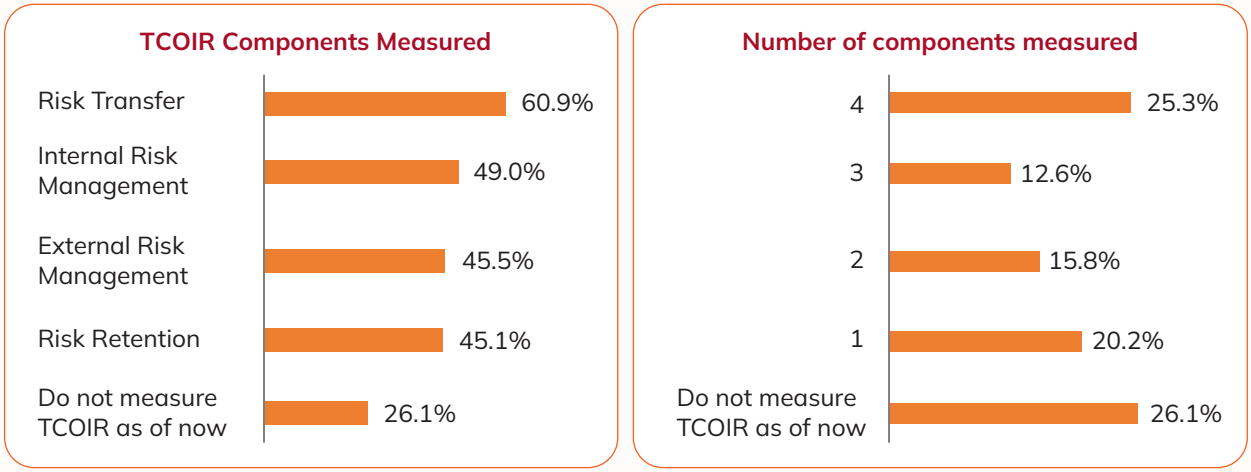


Figure 8.2 Depicts TCOIR measurement responses: Which components measured and how many components measured

Risk transfer cost – relating to direct insurance purchase costs – is the component measured by most respondents. Around 26% of respondents do not measure the cost of insurance, and an almost equal number measure all four components.

8.3 FACTORS INFLUENCING CHOICE OF INSURANCE PRODUCTS

Respondents were asked to choose the top four factors influencing their choice of insurance solution provider. The results are shown in Figure 8.3.

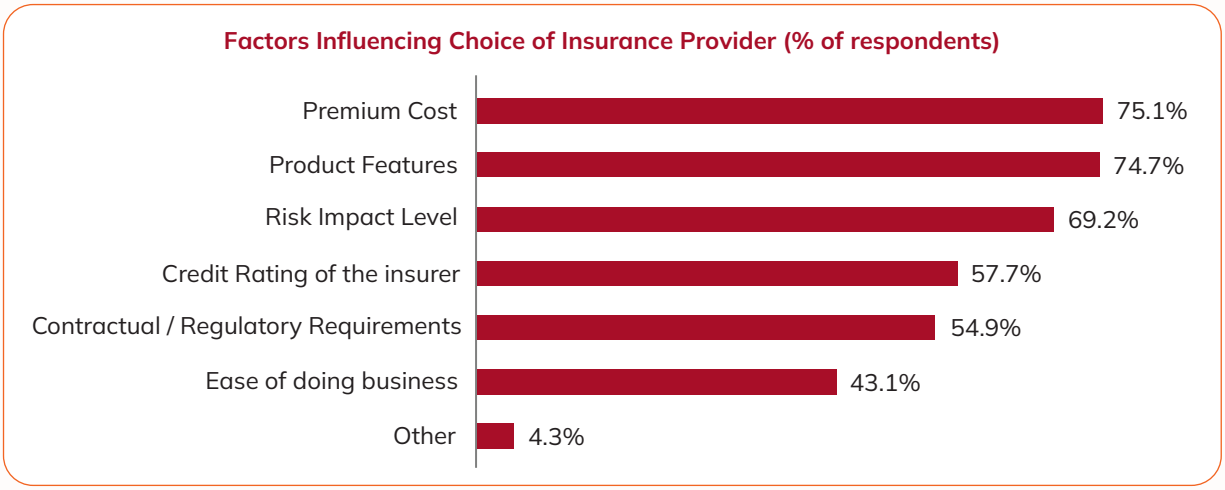


Figure 8.3 Factors Influencing the Selection of Insurance as a Solution

The survey reveals that organisations prioritise functional insurance solutions that deliver value through comprehensive coverage at reasonable costs.

Additional factors cited by those choosing “Other” include Exclusions and deductions, claims settlement, and understanding of business needs.

EXPERT PERSPECTIVE



RITESH SACHANAND ROCHWANI
Channel Partner
ICICI Lombard

Indian market has long been a price sensitive market & discussions mostly with customers while discussing risk perspective has been more on price rather than a comprehensive risk cover. This is true more so for the SME/MSME segment who are either un-insured, under-insured or wrongly insured, in terms of risk solutions vs actual risks faced by them. Majority customers in the segment have taken insurance only to the extent of their bank funding & never realised the implications of being under-insured unless a claim hit them.

Hence very important that SME'S/MSME's are counselled properly & hand held into getting their asset valuation & risk inspections done & recommendations implemented, to ensure that they can use insurance as a tool to not only protect their assets incase of eventual adversities, but also as a tool to grow/sustain & withstand the same.

8.4 ADDITIONAL SERVICES

Survey respondents' preferences for value-added services from insurance providers are shown in Figure 8.4

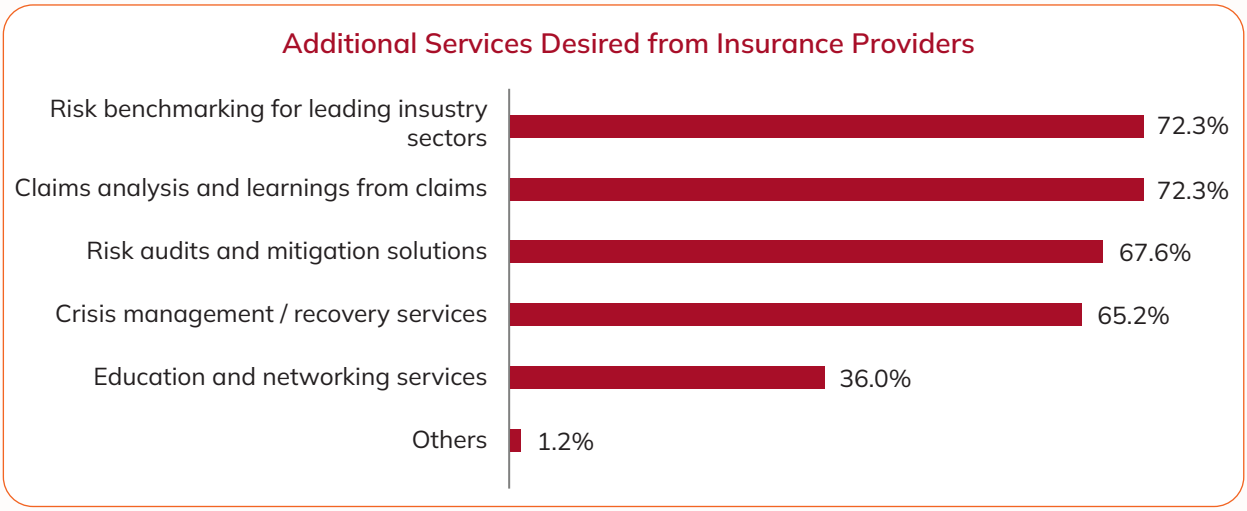


Figure 8.4 Depicts the top additional services expected from Insurance providers by the survey respondents.

Risk benchmarking and Claims analysis services together get the maximum votes, closely followed by audits and crisis/recovery services.

EXPERT PERSPECTIVE



HARSH SEWANI
Channel Partner
ICICI Lombard

"From Risk Protection to Risk Anticipation"

In an increasingly uncertain business environment, organisations must shift from reacting to losses, to proactively anticipating and mitigating risks. This requires continuous risk assessment, early identification of emerging threats, and regular reviews of insurance adequacy and business continuity plans.

The role of an insurance professional must evolve beyond policy placement and claim settlement to that of a strategic risk partner, helping businesses identify vulnerabilities, address protection gaps, and build long-term resilience. Ultimately, the true value of insurance lies not merely in compensating for losses, but in enabling organisations to anticipate uncertainty, minimise financial impact, and remain resilient when disruption occurs.

SUMMARY

Similar to last year's results, six risks are least prepared for, and five of these are least insured for. Organisations need to understand and invest in Geopolitics, Trade and Climate Change related risks, as they are likely to accelerate in the current era of converging forces and interacting risks, as discussed in Chapter 9, Convergence of Forces and Emerging Risks. Given the era of converging and interacting risks, organisations need formal preparations for all risks regardless of their past history.

Number of respondents not measuring cost of insuring risks has come down from 36% last year to 26% this year, which is a positive change.

Premium costs and Product Features are the top two drivers of insurance product selection. The two most desired additional services are Risk Benchmarking and Claims Analysis.

9. CONVERGENCE OF FORCES AND EMERGING RISKS



The rise of AI, intensifying Geopolitical tensions, and accelerated Climate change events have created an environment fundamentally different from the relatively stable, globalised era of the past 25 years. These forces do not act alone; they reinforce each other. This chapter examines their impact on enterprises, the risks they create and how enterprises can respond.

9.1 THE ERA OF CONVERGING FORCES

Every era develops its own language of risk. The 2000s introduced us to Black Swans; the 2010s popularised VUCA, for a world that was volatile, uncertain, complex and ambiguous. Then came BANI, capturing a reality that was brittle, anxious, nonlinear and often incomprehensible.

The mid-2020s confront us with an even greater challenge. Various formidable forces are evolving and intensifying simultaneously, reinforcing one another and amplifying existing risks, creating a landscape in which the consequences of one disruption can quickly trigger another.

Risks have always influenced one another. What has changed is the speed, scale and number of pathways through which a disruption can spread across an enterprise.

Technology/AI, Geopolitics, and Climate Change do not just create risks independently. As individual forces, they create business pressures and produce multiple, interconnected risk outcomes. The forces interact with each other, increasing the complexity. The ultimate severity of the risk outcome is determined by the **Governance Quality**, the fourth force within an enterprise's own control.

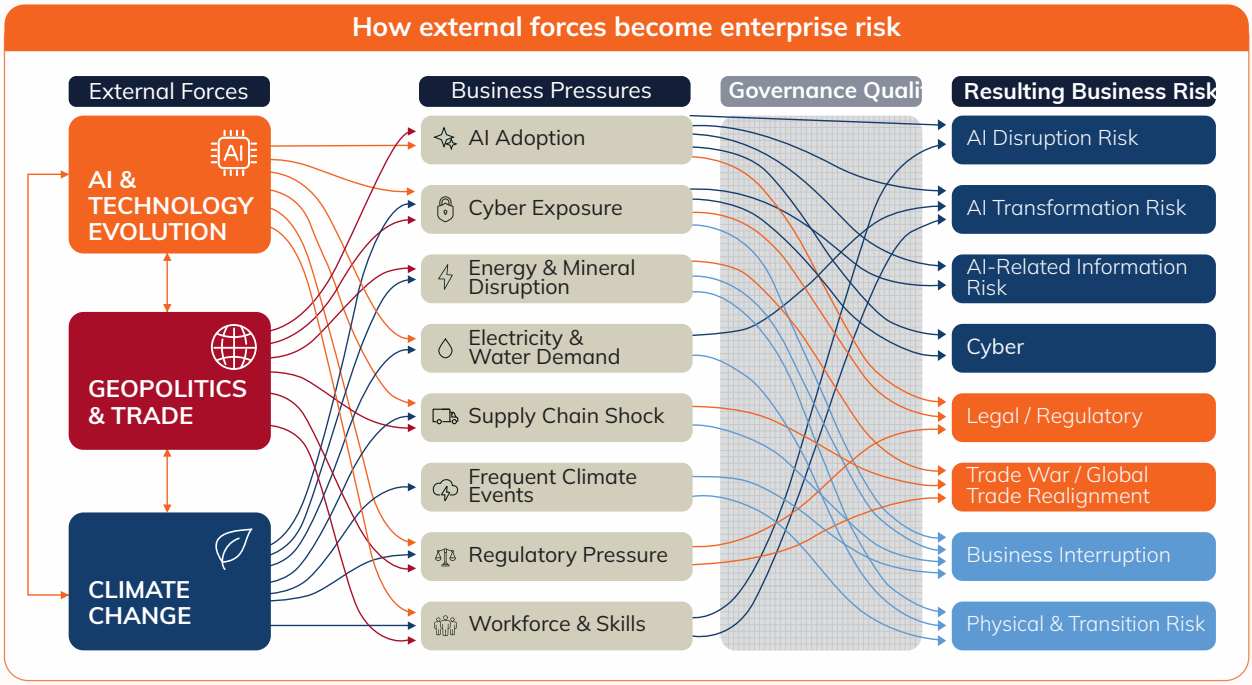


Figure 9.1 Depicts how external forces create business pressures that translate into risks, with Governance Quality determining the severity of the resulting risks. The pathways shown are illustrative.

Each individual force can create multiple pressures, and each business pressure can create multiple risks. While the environment creates emerging risks for enterprises worldwide, India stands at the centre of this convergence. As the world's fastest-growing large economy, it faces huge risks and opportunities from these forces in the journey towards Viksit Bharat (Developed India) 2047 goal:

AI & TECHNOLOGY EVOLUTION:

- Rapid evolution of GenAI is creating risks at a speed and scale never seen before. Increasing AI adoption or transformation can increase cyber exposure, electricity and water demand, climate issues, regulatory pressure and workforce risk. A data breach involving an AI system may therefore become more than a technology problem: it can cause a cyber-incident, attract regulatory action, interrupt operations and damage customer trust.
- AI also creates two distinct risks of its own: disruption risk, where AI-enabled competitors or substitutes erode an existing business model, and AI transformation risks, where a transformation fails to deliver business value or faces risks of model error, bias, opacity or over-reliance.
- AI is an opportunity for all enterprises. As the world's 5th most digitalised country, India can use AI to extend the reach of digital services and accelerate growth.
- Access to AI models may depend upon evolving geopolitical and trade environments. This exposes Indian enterprises to additional, critical supply chain risks.

GEOPOLITICS AND TRADE:

- Geopolitical tension, policy uncertainty and protectionism have reached new levels, exposing Indian supply chains and exports to significant disruption. Geopolitical conflict can disrupt energy supplies, critical minerals, shipping routes and access to technology. A disruption in the Red Sea or the Strait of Hormuz may increase freight and energy costs, delay imported components and interrupt manufacturing. What begins as a geopolitical event may ultimately appear as a financial or Business Interruption risk. These risks have an amplified impact on the Indian economy and enterprises.
- Geopolitics and trade realignment can create regulatory pressures, restrict access to markets, technologies and materials. This aspect is specifically relevant for Indian enterprises, dependent upon global supply chains.
- As global companies diversify their sourcing, India can attract investment, scale up manufacturing and deepen its role in global value chains. (World Bank, 2024, pp. 27–34).

CLIMATE CHANGE:

- Frequent climate events such as extreme heat, floods or water scarcity can damage infrastructure, reduce workforce productivity, interrupt suppliers and increase insurance and compliance costs. Climate risk therefore extends beyond sustainability; it can become an immediate operational, financial and strategic concern. Record temperatures, erratic monsoons and rising sea levels are pushing India's climate exposure to levels it has never faced, making it one of the most climate-vulnerable major economies.
- Record investments in AI infrastructure and its energy demands have created concerns that the data centre could lead to environmental and climate impacts. According to the Chief Economist Outlook poll published in Sep 2026, nearly 80% of respondents felt that data centre expansion will face significant pushback from communities.
- Due to varied reasons, Climate Change impacts India in multiple ways, impacting the growth and profitability of Indian enterprises.
- The low-carbon transition creates room for leadership in renewables, green manufacturing and climate finance.

GOVERNANCE QUALITY:

- Governance Quality represents a crucial internal capability that determines how an enterprise handles the external forces and resulting business pressures.
- With risks evolving faster than ever, weak oversight and risk management that has not kept pace can turn external shocks into enterprise-level crises. Weak governance can allow a manageable disruption to spread across functions and develop into a larger crisis.
- Enterprises with strong governance can identify connections early, assign clear ownership, coordinate enterprise-wide response and turn resilience into a competitive advantage.
- As Indian enterprises scale up in domestic and export markets, Governance Quality will enable mature risk cultures, reducing risk impacts and improving opportunity conversion.

AI, geopolitics and climate change do not just create business pressures on their own; each one amplifies the others. AI's appetite for power, water and critical minerals ties it to both climate and geopolitical competition. Climate shocks and the race for clean-energy resources sharpen trade tensions, while rising geopolitical rivalry slows the global response to climate change. The business pressures interact with each other as well.

The central argument is simple: although risks may be listed separately, they rarely materialise separately. The real emerging risk lies in the connections between forces, the business pressures and risks.

EXPERT PERSPECTIVE



SUDHARSAN NARASIMHAN
Head - Corporate Insurance
Larsen & Toubro

The pace at which external developments translate into business disruptions is accelerating. Geopolitical uncertainty, regulatory shifts, and climate-related events can rapidly affect operations, cost and market access.

Businesses must move beyond historical assessments towards forward-looking intelligence and scenario-based planning. Competitive resilience will depend on recognizing emerging threats early and translating insights into timely, informed decisions.

9.2 INFLUENCE OF CONVERGING FORCES: THE INDIAN ENTERPRISE VIEW

The Enterprise Risk Perception Survey 2026 (ERPS-2026), conducted jointly by IRM and ICICI Lombard, asked respondents to assess four major forces shaping organisational risk: one internal force, governance quality, and three external forces, namely AI and technology, geopolitical developments, and climate change. For each force, the respondents could choose from None / Weak / Moderate / Strong / Not Sure.

Figure 9.2 shows the mean scores received by each force.

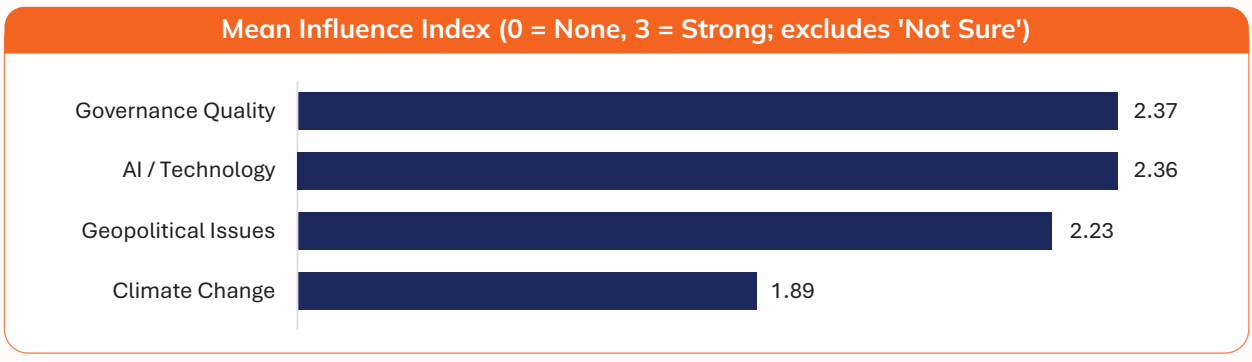


Figure 9.2 Responses to level of influence of the forces: Mean value per force

GOVERNANCE QUALITY, almost at the same level as AI/Technology, emerges as the top overall influence. While it has emerged as the strongest influence only in Energy, Oil and Gas and Pharma – jointly with Geopolitics, it has consistently high scores across all the sectors. This may be interpreted to indicate the importance of the central role of boards and senior management in setting accountability, strengthening controls and responding to rapidly changing risks. It may be noted that Governance Quality also has 12 respondents out of 253 who chose "Not Sure" as the answer.

AI/TECHNOLOGY follows closely and has received the highest scores in the BFSI and Services sectors. The short-term risk ranking derived from ERPS-2026 ranks Cyber Risk and Technology/AI as the top two short-term priorities. As per ERPS-2026, Information Risk is also the most significant AI-related risk. For example, adopting AI may improve efficiency but also create exposure to data leakage, biased decisions, deepfake fraud, technology failure, and regulatory scrutiny. Transforming the business with AI may result in additional risks such as the transformation itself failing to deliver, or model error/biases/opacity etc. It may be noted that only 4 respondents chose "Not Sure" for AI/Technology.

GEOPOLITICS AND TRADE follow closely behind AI/Technology. It influences sourcing, energy costs, shipping routes, currencies, export markets and access to critical technology. A conflict affecting a maritime chokepoint could delay imported components, increase freight and energy costs, interrupt manufacturing and place additional pressure on working capital. Only 5 respondents chose "Not Sure".

CLIMATE CHANGE has scored much lower than the other three factors. It has the highest mean score for Logistics and e-Commerce and also strong scores for Construction and Infrastructure and Energy, Oil and Gas. An extreme-weather event may damage physical assets, interrupt transport networks, reduce labour productivity, disrupt suppliers and increase insurance costs. The survey also indicates that climate readiness remains weaker than preparedness for familiar physical hazards such as fire and natural catastrophes. It may be noted that 17 respondents have selected Not Sure as the option for Climate Change.

Sector differences reinforce the need for a contextual approach. BFSI and services are more exposed to technology, cyber and information risks. Construction and infrastructure face project delays, material shortages and climate-related disruption. Manufacturing depends on access to raw materials, components and reliable logistics. Energy businesses are affected by commodity volatility, geopolitical developments and the physical effects of climate change.

Apart from Cyber Risk and Technology/AI, ERPS-2026 ranks Legal and Regulatory Risk, Business Interruption and Civil Strife/Geopolitical risks in the top 5 short-term ranks. These are not unrelated concerns. They represent different stages of the same possible risk chain:

AI or technology dependence ➡ cyber or information failure ➡ regulatory consequences ➡ operational interruption ➡ financial and reputational loss.

A similar chain can begin with a geopolitical or climate event:

Conflict or extreme weather ➡ disrupted transport and energy supplies ➡ shortages and higher costs ➡ production delays ➡ weaker financial performance.

Governance connects all these pathways. Effective governance can ensure that opportunities are pursued with appropriate controls and risks do not escalate into an enterprise-wide crisis.

The survey assesses each force separately and therefore does not, by itself, establish causal interaction. Nevertheless, it shows that organisations are simultaneously exposed to several powerful forces. Their convergence should be examined through scenario planning, interdependency mapping, stress testing and cross-functional discussion—not inferred from risk rankings alone.

EXPERT PERSPECTIVE



SOUMITRA KANSABANIK
AGM, Risk and Control Management Lead and Internal Audit Head
Blue Star Limited

Converging Forces and Emerging Risks for the Manufacturing Sector

- **Geopolitics:** Geopolitical risk ranks highest for manufacturers because it directly disrupts the supply chain. It is also the top underlying cause of several other risks, creating a snowball effect across the broader risk landscape.
- **Macro:** Businesses face economic and financial stress, driven by persistent inflation and uneven growth across markets.
- **Concentration:** Production landscapes are concentrating in fewer locations and suppliers. Tighter regulation is driving smaller players out of the market.
- **Scarcity:** Critical minerals are increasingly hard to secure. Even silicon for PCB's is scarce: data-centre companies are absorbing much of the supply and pre-booking production capacity through capacity reservation agreements.
- **Blue Collar Talent Crunch:** Shortage of blue-collar workers is creating a large impact on the manufacturers and project site execution.

Technology and AI

- AI is not yet regulated, and adoption has only just started. Most organisations use it as an intelligent search tool. Data security is a growing concern as AI use expands.
- Agentic AI will create a high level of dependence as it makes business easier. This dependence is itself a risk, as major suppliers of GenAI models are outside India. India lags in original research and development, which limits its ability to reduce dependence on foreign technology.
- Data centres are both an opportunity and a risk. They create new demand, but they compete for components and add to climate pressure.

Emerging risks and continuity

- Business Continuity planning must cover the continuity of the whole business and not be limited to IT / Disaster Recovery. Continuity planning must also cover sudden legal change, as it could impact markets or supplies.
- Current preparedness for emerging risks is low. Because technologies are evolving so quickly, we are currently in a dark room. Organisations are striving to build strong internal risk management and resilience.

9.3 MANAGING EMERGING RISKS IN THE AGE OF CONVERGENCE

An emerging risk is a new or changing risk whose likelihood, severity or interaction with other risks is poorly understood but expected to grow materially. Emerging risks can be categorized as:

- **New risks in a known context:** New risks that have emerged in the external environment but are associated with the organisation's existing context consisting of strategy, business model, processes and operations.
- **Known risks in a new context:** risks the organisation already recognises, whose nature or scale has significantly changed because of change in the internal or external context.
- **New risks in a new context:** risks the organisation has not faced before, arising from changes to its own context – such as new business models or core processes.

The distinction matters because different categories create different challenges for risk management, both in recognising new risks and in reassessing existing risks.



Figure 9.3 Depicts emerging risks and their categories

The emerging risks in Figure 9.3, also shown in Figure 9.1, need to be viewed not as single, siloed risks, but as outcomes of several interacting forces. This renders a single-risk approach to risk management inadequate.

Emerging risks require a formal place within the ERM architecture. An effective emerging-risk management process serves as an early-warning mechanism, identifying both new risks on the horizon and material changes in existing risks before they become costly surprises. This requires organisations to look beyond individual risk categories and examine the broader forces and underlying shifts reshaping their operating environment.

Conventional risk management techniques can miss weak signals, nonlinear change, common dependencies and the pathways through which one risk activates another. The enterprise response must therefore become more continuous, forward-looking and connected.

The responses to ERPS-2026 indicate why this change is necessary. As highlighted in Chapter 7 on Enterprise Resilience, organisations are strongest where risks are familiar and ownership is clear, but weaker on geopolitical disruption, trade realignment, climate change, and rapidly changing technology.

Enterprises need to:

- Scan continuously - combine external horizon scanning with internal risk sensing to identify new threats and material changes in existing exposures.
- Build integrated scenarios - test plausible combinations, such as an AI-enabled cyberattack during geopolitical disruption or a climate event affecting a critical supplier.
- Map critical dependencies - identify concentrated suppliers, platforms, data, utilities, skills and permissions that can transmit disruption across the enterprise.
- Define indicators and escalation - assign owners, warning signals, thresholds and pre-agreed actions for risks under observation.
- Strengthen cross-functional governance - connect the board, strategy, risk, technology, finance, sustainability, legal, HR, operations and internal audit. (COSO, 2017)

- Build adaptive capacity - diversify suppliers, maintain financial buffers, test recovery plans and exercise decision-making under incomplete information. (ISO, 2023; OECD, 2024a)
- Layer the response - combine insurance with prevention, continuity planning, scenario analysis and a complete view of the cost of risk.
- Assess opportunity with risk - ask what new demand, capability or advantage may arise from the same change and define safeguards before scaling it.

These techniques, while not new, have become essential for most enterprises in the modern environment. The practical objective is not to predict the future correctly, but to recognise plausible changes early, understand how they could combine, prepare options, and make better decisions as evidence develops. In an age of convergence, resilience comes less from confidence in a single forecast and more from the capacity to detect, interpret, adapt and act.

EXPERT PERSPECTIVE



PALLAV KAPOOR
Chief Risk Officer
IREDA

Resilience in an Age of Converging and Dynamic Risks requires

a. Moving From Tail Events to Baseline Conditions

Climate stress, concentration, correlated risk drivers rarely arrive alone. What were once treated as tail events are progressively becoming baseline operating conditions. The residual vulnerability is no longer the individual risk.

b. Capital Resilience

A more useful view is the flow of capital adequacy across scenarios that combine direction and surprise; Adverse & Anticipated, Positive & Unanticipated, Adverse and Unanticipated. Institutions may usefully ask which of these three trajectories they actually test

c. Moving From Periodic Stress Testing to Continuous Residual Risk Management

Stress tests and scenario analysis remain necessary, however, Resilience now requires the continuous management of residual risk.

CONCLUSION

The current risk environment is characterised by convergence of forces that create business pressures resulting in business risks. Emerging risks arising from this interplay of converged forces include new risks in existing and new contexts as well as existing risks being transformed by new contexts.

The heightened interconnectedness of risks means they cannot be managed effectively in silos. Organisations need continuous horizon scanning, scenario-based analysis, clear ownership, disciplined management of opportunities and regular reassessment using agreed indicators. India stands at the intersection of powerful risks and historic opportunities; enterprises that understand the system as a whole will be better placed to navigate the volatility and capture the upside.

10. MIDSIZE ENTERPRISES IN FOCUS



Midsize enterprises, organisations with annual revenues up to ₹2,000 crore, occupy an increasingly important position in India's evolving business landscape. They represent businesses that have moved, or are moving, beyond the traditional small-enterprise scale and are developing their capabilities to compete in larger domestic and international markets.

MSMEs form an important subset of the Midsize segment considered in this chapter. Ministry of Micro, Small and Medium Enterprises defines MSME as enterprises with revenues up to ₹500 Cr. The Economic Survey 2025-26 reports that MSMEs account for approximately 31.1% of India's GDP, 35.4% of manufacturing output, and 48.58% of exports. The sector comprises more than 7.47 crore enterprises and employs over 32.82 crore people, making it the country's second-largest source of employment after agriculture.

Against this backdrop, this chapter examines the responses to the Enterprise Risk Perception Survey-2026 (ERPS-2026) and presents how India's midsize enterprises perceive and respond to the evolving risk landscape. The Midsize segment is represented by 88 respondents out of a total of 253.

10.1 RISK PERCEPTIONS

Rank	Midsize Enterprises	Aggregate Sample
1	Cyber Risks	Cyber Risks
2	Technology/AI	Technology/AI
3	Business Interruption (Incl. Supply Chain Disruption)	Legal / Regulatory Risks
4	Legal / Regulatory Risks	Business Interruption (Incl. Supply Chain Disruption)
5	Talent Risk (Attract/Grow/Retain)	Civil Strife / Geopolitical issues

Figure 10.1.1 depicts top 5 short-term risks for the Midsize segment in comparison with the aggregate sample.

Midsize enterprises rated Talent Risk higher than the overall sample, likely because the segment faces greater challenges in attracting and retaining critical skills.

Rank	Midsize Enterprises	Aggregate Sample
1	Technology/AI	Technology/AI
2	Cyber Risks	Cyber Risks
3	Legal / Regulatory Risks	Climate Change
4	Climate Change	Legal / Regulatory Risks
5	Business Interruption (Incl. Supply Chain Disruption)	Business Interruption (Incl. Supply Chain Disruption)

Figure 10.1.2 Depicts top 5 long-term risks for the Midsize segment and overall sample.

EXPERT PERSPECTIVE



FAIZ AHMAD
Vice President - SME Agency
ICICI Lombard

Q As MSMEs scale their operations, even minor disruptions can affect business continuity and financial stability. How can MSME businesses transition from reactive problem solving to proactive risk management, and what practical, cost effective measures can help them mitigate risks, navigate disruptions, and achieve sustainable growth?

India's MSME sector contributes approximately 31.1% of GDP and nearly half of the country's exports, making its resilience critical to economic growth. Businesses across manufacturing, services and trade face a wide range of exposures—from supply-chain disruptions , consequential loss, and price volatility to cyber incidents, employee-related risks and natural catastrophes.

For enterprises operating with limited financial reserves, even a short interruption can create significant pressure and hence it is more appropriate to move from reactive response to risk preparedness.

A key concern is the gap between these evolving risks and the financial preparedness of MSMEs, that are proportionate to the business's size and resources. Even a temporary disruption can delay deliveries, affect customer commitments, strain cash flows and threaten business continuity, particularly for MSME's.

Proactive risk management begins with identifying critical vulnerabilities. Pragmatic and prudent risk measures include diversifying suppliers, maintaining essential backup inventory, strengthening cybersecurity and data recovery, monitoring receivables, creating contingency funds and periodically testing business-continuity plans.

Insurance should complement these preventive measures, not replace them. MSMEs should review their protection against property damage due to fire or other allied perils, business interruption, cyber incidents, liability exposures, trade-credit losses and supply chain exposure's etc ensuring that coverage remains aligned with their operations and evolving risk profile. This should be regularly reviewed to remain synchronised with the organisation's growth and evolving risk profile.

While enterprise's have resource constraints, limited awareness and competing priorities, this often hinder structured risk management. The insurers and risk advisors can help MSMEs understand their exposures, strengthen preventive controls and select appropriate protection.

Ultimately, sound financial planning, preventive risk mitigation and appropriately structured insurance solutions can enable MSMEs to manage disruptions, safeguard business continuity and pursue sustainable growth with greater confidence.

Figure 10.1.2 depicts top 5 long-term risks for the Midsize segment in comparison with the aggregate sample. The long-term ranking includes the same five risks for both, but in different orders.

Midsize enterprises recognised the structural importance of Climate Change in the long term and included it in the top 5, with Talent Risk moving out.

10.2 COMPARING RISK PERCEPTION ACROSS SECTORS

About 86% of the Midsize respondents to ERPS-2026 are from BFSI, Manufacturing and Distribution, Services, and Construction and Infrastructure sectors. The sectoral analysis focuses on these four sectors.

Rank	BFSI (27.3%)	Manufacturing and distribution (23.9%)	Services (27.3%)	Construction and Infrastructure (8.0%)
1	Cyber Risks	Business Interruption (Incl. Supply Chain Disruption)	Cyber Risks	Business Interruption (Incl. Supply Chain Disruption)
2	Technology/AI	Cyber Risks	Technology/AI	Climate Change
3	Legal / Regulatory Risks	Climate Change	Business Interruption (Incl. Supply Chain Disruption)	Legal / Regulatory Risks
4	Talent Risk (Attract/Grow/Retain)	Talent Risk (Attract/Grow/Retain)	Talent Risk (Attract/Grow/Retain)	Fire / Explosions
5	Macroeconomic Risks	Technology/AI	Legal / Regulatory Risks	Natural Catastrophes

Figure 10.2.1 Top 5 short-term risks for industry sectors

Figures 10.2.1 and 10.2.2 depict the top 5 short- and long-term risks for the four selected sectors.

- BFSI: Cyber, Technology/AI and Legal/Regulatory are the top 3. They reflect the sector's high exposure through digital channels and a heavy regulatory load.
- Manufacturing and Distribution: Business Interruption (incl Supply Chain Disruption) is the top concern, reflecting the sector's dependence on supply chains.
- Services: Cyber and Technology/AI are the top 2 concerns, followed by Business Interruption. It is a people-intensive sector, which explains why Talent appears at #4.
- Construction and Infrastructure: Business Interruption, Climate Change and Legal/Regulatory are the top 3 sectoral concerns. With relatively few respondents, this column is only a rough indication.

Rank	BFSI (27.3%)	Manufacturing and distribution (23.9%)	Services (27.3%)	Construction and Infrastructure (8.0%)
1	Technology/AI	Business Interruption (Incl. Supply Chain Disruption)	Technology/AI	Climate Change
2	Cyber Risks	Technology/AI	Cyber Risks	Legal / Regulatory Risks
3	Legal / Regulatory Risks	Climate Change	Climate Change	Technology/AI
4	Talent Risk (Attract/Grow/Retain)	Cyber Risks	Civil Strife / Geopolitical issues	Business Interruption (Incl. Supply Chain Disruption)
5	Macroeconomic Risks	Legal / Regulatory Risks	Talent Risk (Attract/Grow/Retain)	Talent Risk (Attract/Grow/Retain)

Figure 10.2.2 Top 5 long-term risks for the industry sector.

In the long-term rankings:

- Technology/AI rises with the longer horizon. It overtakes Cyber for #1 in BFSI and Services and climbs from #5 to #2 in Manufacturing. Respondents see AI as a longer-term disruption, cyber as a constant concern.
- Manufacturing and distribution: Business Interruption, Technology/AI and Climate Change occupy three top ranks with scores very close to each other. Technology/AI replaces Cyber Risks at #2, reflecting the sectors' dependence on innovation and efficiency.
- Climate Change gains ground: It is present in top 5 risks for three sectors.
- Talent Risk: Appears in the top 5 for three sectors, indicating that Talent could be a longer-term concern for multiple sectors, specifically in the Midsize segment.

10.3 ARTIFICIAL INTELLIGENCE: PREPAREDNESS, OPPORTUNITY & RISKS

10.3.1 AI Opportunities

Table 10.3.1 lists top 2 opportunities voted by the top four sectors in Midsize segment.

Sector	Rank 1	Rank 2
BFSI	Operational Efficiency	Innovation
Manufacturing and Distribution	Operational Efficiency	Improved Decision Quality
Services	Operational Efficiency	Revenue Growth
Construction and Infrastructure	Operational Efficiency	Improved Decision Quality

Table 10.3.1 Top two AI opportunities by sector, midsize enterprises

Midsize enterprises prioritise artificial intelligence primarily to enhance operational performance rather than drive top-line revenue expansion.

- Operational Efficiency emerges as the primary focus, voted to the top by all sectors.
- Improved Decision Quality has been voted by two sectors for the second position, while BFSI ranks Innovation and Services ranks Revenue Growth at the second position.

Why the ranking matters

Operational Efficiency leads across every sector without exception, reflecting a preference for AI applications that lower cost and effort in existing operations over AI aimed at new revenue, which demands a transformational approach, capital, and risk appetite to pursue.

Improved Decision Quality takes the second spot for both Manufacturing and Distribution and Construction and Infrastructure, pointing to AI's growing role in sharpening judgment for sectors managing complex, asset-heavy operations.

Innovation breaks into the top two only for BFSI, while Revenue Growth does so only for Services, showing midsize companies are only beginning to extend AI beyond operational efficiency into growth-oriented or innovation-led territory.

While not shown in the table, Risk Management is voted the lowest, indicating that risk leaders are yet to incorporate AI in risk processes.

10.3.2 AI Risks

Table 10.3.2 lists the top 2 risks voted by the top four sectors in the Midsize segment.

Sector	Rank 1	Rank 2
BFSI	Information Risk & Technology Risk (tied)	Legal / Regulatory Risk
Manufacturing and Distribution	Information Risk	People Risk
Services	Information Risk	Technology Risk
Construction and Infrastructure	Technology Risk	Information Risk

Table 10.3.2 Top 2 AI risks for top Midsize sectors

Information Risk and Technology Risk are the most prominent top AI risks for midsize companies, with Information Risk leading by a clear margin. Legal / Regulatory Risk and People Risk have also been ranked in 2nd position by one sector each.

Similar to the overall response, Midsize enterprises' main concern with AI adoption is data leakage, privacy, misinformation and deepfakes, and data poisoning, leading to Information Risk. Technology risk is the second most prominent concern related to model biases, possible issues due to Agentic AI and cyber-attacks.

People risk relates to the ability to attract and retain talent, train people to use AI or to function with revised processes and responsibilities.

10.3.3 AI Importance and Preparedness

ERPS-2026 asked respondents to gauge the importance of AI to their organisations and their organisations' preparedness to leverage AI opportunities and manage AI risks. The options presented were None, Low, High and Very High. The analysis for the Midsize segment, depicted in Figures 10.3.3.1 and 10.3.3.2, is derived by scoring these options on a scale of 1-4. The indices in these figures are the mean scores for Importance, Preparedness to Leverage Opportunity, and Preparedness to Manage Risks.

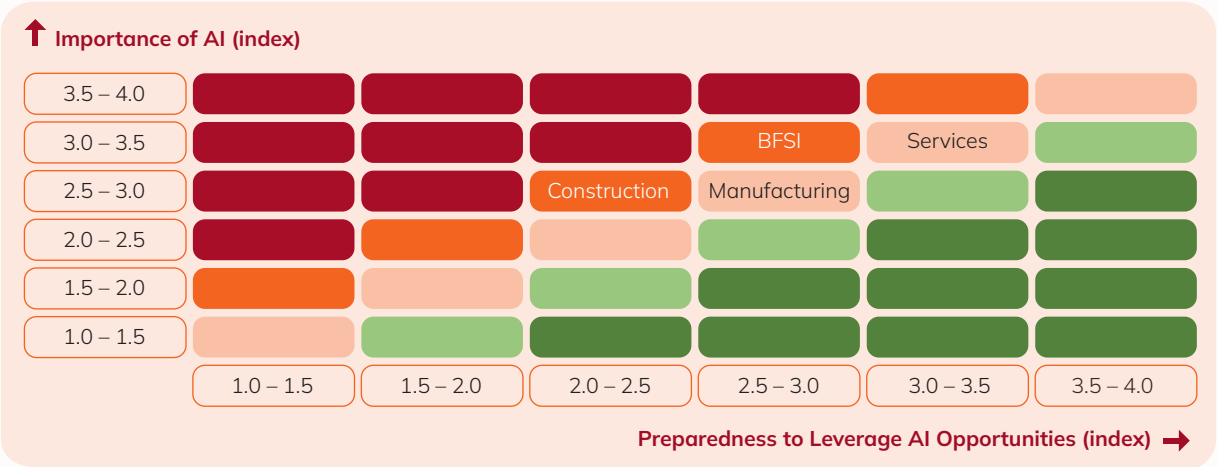


Figure 10.3.3.1 Importance of AI and Preparedness to Leverage AI Opportunities by sector

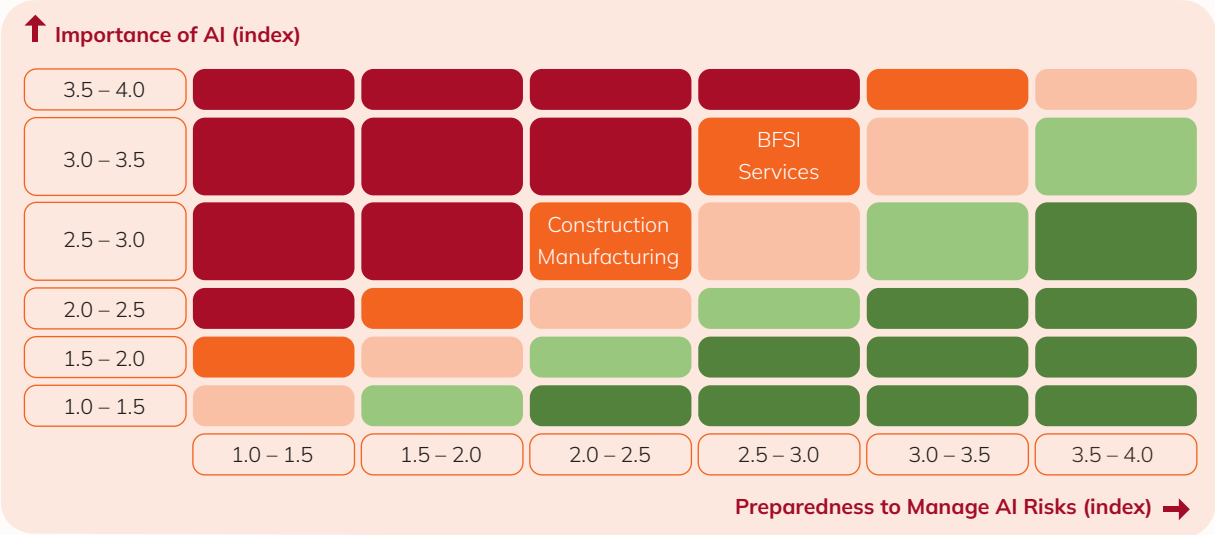


Figure 10.3.3.2 Importance of AI and Preparedness to Manage AI Risks by sector

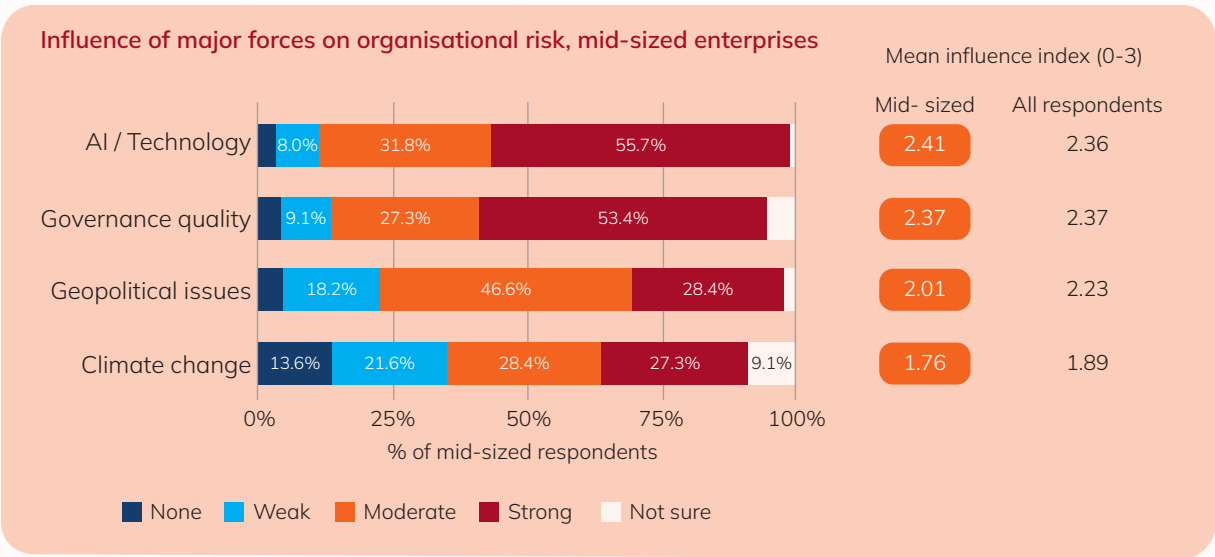
BFSI and Services give the highest scores to the importance of AI. BFSI opportunity and risk preparedness indices seem to be lagging slightly behind their importance index for both opportunities and risks. This indicates that the sectors are yet to make the investments necessary to capture Operational Efficiency and Innovation opportunities and to manage information, technology and legal risks.

Construction/Manufacturing seem to have their importance and opportunity preparedness indices aligned but are lagging slightly behind in risk preparedness indices. This indicates that the sectors' investments to capture the operational efficiency and revenue growth opportunities are on track. However, they have yet to invest in managing information, people, and technology risks.

10.4 FORCES SHAPING RISK

Figure 10.4 depicts Midsize companies' responses to the question on the influence of forces in ERPS-2026. The question examines the level of influence of four major forces on organisational risk: one internal force, governance quality, and three external forces, namely AI and technology, geopolitical developments, and climate change. Respondents were required to choose from None, Weak, Moderate, Strong and Not Sure. Figure 10.4 gives a breakdown of responses for individual forces as well as mean influence per force, based on scoring None as 0 to Strong as 3, and excluding Not Sure in the mean influence index. Figure 10.4 also gives the mean index for the total sample.

Figure 10.4 Influence of forces on organisational risk



Midsize companies feel the strongest influence from AI/Technology and Governance Quality:

- AI / Technology stands out as the most strongly felt force, narrowly ahead of Governance Quality, which in turn comfortably outweighs Geopolitical Issues and Climate Change, the two forces felt least.
- Midsize companies weigh AI / Technology slightly more than the overall sample, while rating Geopolitical Issues and Climate Change lower. Governance Quality is the one force where the two groups score the same.

Overall, the mean influence index for midsize companies tracks the all-respondent average fairly closely across all four forces, suggesting these forces are felt in broadly similar measures regardless of company size.

10.5 PREPAREDNESS: MATURITY, READINESS & RISK SOLUTIONS

10.5.1 Risk-Management Maturity

Risk-management maturity is scored across five components:

- Who drives risk management
- Who is responsible for risk identification
- Process ownership
- Attitude towards risk, and
- Compliance with international risk management standards.

Figure 10.5.1.1 shows the risk management maturity profile of Midsize companies in comparison with the overall sample.

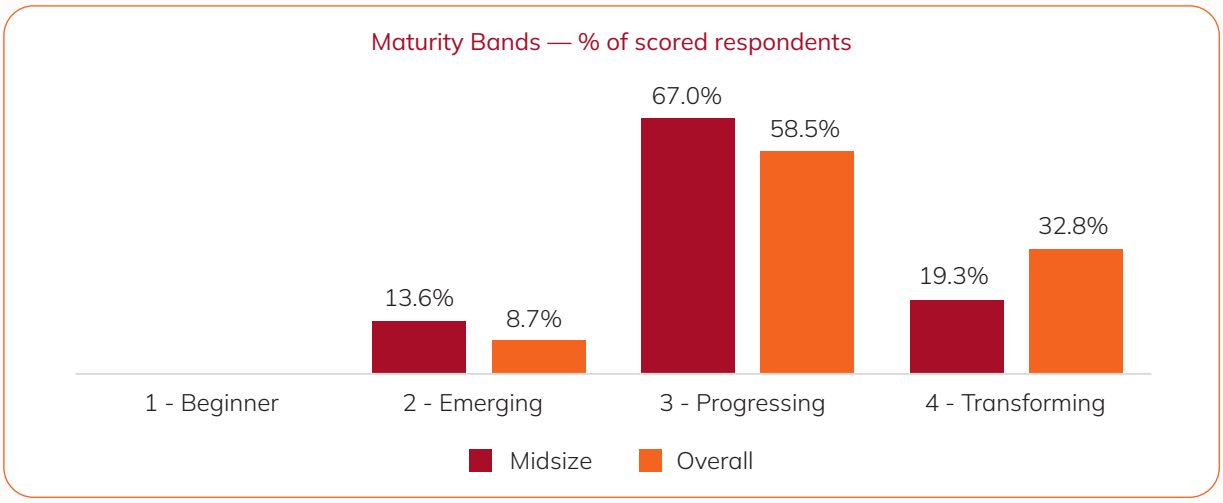


Figure 10.5.1.1 Risk Management maturity profile: Midsize vs aggregate sample

As can be noticed, midsize companies tend to display lower levels of maturity compared to their larger counterparts. The current scenario of converging forces and emerging risks, as described in Chapter 9, indicates that Midsize companies will need to increase their investments in Risk Management functions in the immediate future to build resilience and grow in the AI age.

Figure 10.5.1.2 shows comparison of mean scores for individual questions for Midsize and Aggregate sample.

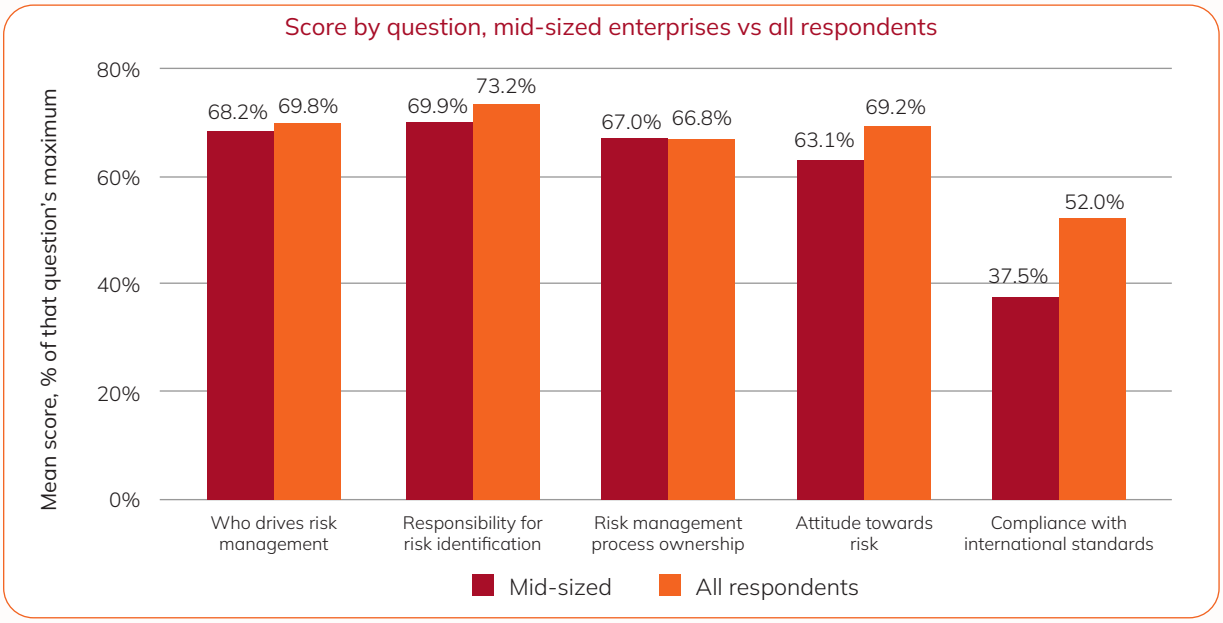


Figure 10.5.1.2 Score by question (% of that question's maximum): midsize enterprises vs all respondents

Compliance with International Standards shows the maximum gap from the overall sample. Midsize enterprises need to base their risk management processes and practices on well-accepted international standards to ensure comprehensive and continuously improving processes.

Attitude towards risk is the next largest gap. The current risk environment cannot be leveraged without considering risk management as a competitive advantage – providing capability to pursue new opportunities provided by AI.

Responsibility for risk identification is the third highest gap. In a mature environment, all employees are empowered and made responsible for identifying risks.

10.5.2 Readiness to Manage Priority Risks

Respondents' readiness to manage priority risks is assessed as having 'have strategy and capabilities', 'have a strategy', 'have capabilities', or 'having no readiness at all'. Table 10.5.2.1 summarises Midsize responses to the question by individual risk.

- Legal / Regulatory Risks and Cyber Risks are the risks midsize companies are best prepared for, with over half reporting both a strategy and capabilities in place.
- Fire / Explosions, Business Interruption, and Talent Risk are partially prepared for, with close to half having both a strategy and capabilities.
- Climate Change, Trade war / Global Trade Realignment, and Civil Strife / Geopolitical issues show the lowest readiness, with roughly three in ten midsize companies having no preparation at all.

Risk	None	Strategy only	Capabilities only	Both	Readiness Rank
Legal / Regulatory Risks	5.7%	12.5%	23.9%	58.0%	1
Cyber Risks	10.2%	10.2%	27.3%	52.3%	2
Fire / Explosions	12.5%	11.4%	29.5%	46.6%	3

Risk	None	Strategy only	Capabilities only	Both	Readiness Rank
Business Interruption (including Supply Chain interruption)	12.5%	12.5%	28.4%	46.6%	4
Talent Risk	9.1%	22.7%	22.7%	45.5%	5
Technology/AI	10.2%	19.3%	36.4%	34.1%	6
Macroeconomic Risks	18.2%	23.9%	27.3%	30.7%	7
Natural Catastrophes	27.3%	11.4%	33.0%	28.4%	8
Civil Strife / Geopolitical issues	28.4%	20.5%	25.0%	26.1%	9
Trade war / Global Trade Realignment	29.5%	20.5%	22.7%	27.3%	10
Climate Change	33.0%	19.3%	22.7%	25.0%	11

Table 10.5.2.1 Readiness distribution by risk, midsize enterprises (ordered by readiness rank)

The exposure gap, as depicted in Figure 10.5.2.2, measures the distance between a risk's readiness rank and its short-term priority rank. The higher the gap, the greater the exposure.

- Climate Change and Technology/AI show the widest exposure gaps, with readiness lagging furthest behind their priority.
- Fire / Explosions, Legal / Regulatory Risks, Natural Catastrophes and Macroeconomic risks show their preparedness rank to be much higher than the risk rank, probably indicating historical preparedness for these risks.

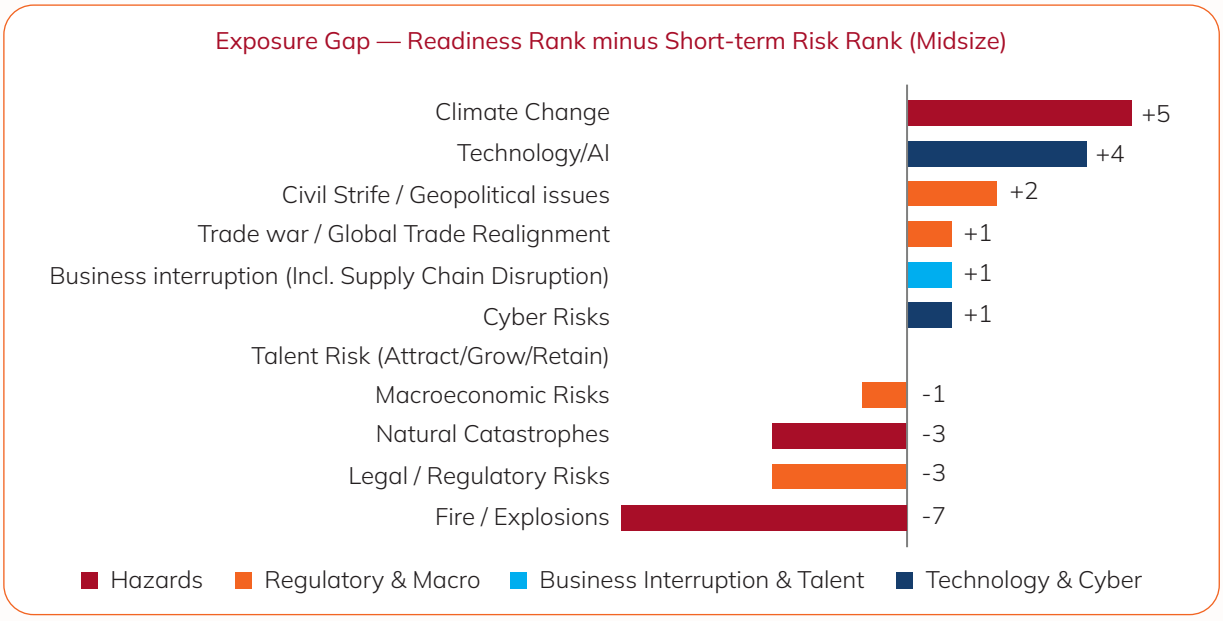


Figure 10.5.2.2 Exposure gap by risk: midsize enterprises vs all respondents

10.5.3 Risk Management Solution

A Risk Management solution consists of measures to reduce the risk and to transfer the residual risk, possibly to an insurer. In the age of converging forces and interconnected risks, organisations need holistic risk control to ensure risks are reduced effectively.

While Cyber Risk ranks as the top short-term risk and 2nd long-term risk, only 55.7% of Midsize organisations indicate having non-insurance solutions for Cyber Risk, far lower than 77.3% having Insurance. These organisations could face amplified cyber risks as AI solutions come into their organisations, either through enterprise implementations or individual employee use.

Risk	Insurance	Non-Insurance	No Solution
Fire / Explosions	84.1%	52.3%	9.1%
Cyber Risks	77.3%	55.7%	8.0%
Natural Catastrophes	72.7%	50.0%	18.2%
Legal / Regulatory Risks	60.2%	65.9%	11.4%
Business Interruption (including supply chain interruption)	60.2%	61.4%	20.5%
Climate Change	51.1%	39.8%	31.8%
Civil Strife / Geopolitical issues	43.2%	51.1%	28.4%
Technology/AI	42.0%	55.7%	28.4%
Trade war / Global Trade Realignment	30.7%	55.7%	33.0%
Talent Risk	28.4%	63.6%	23.9%
Macroeconomic Risks	26.1%	58.0%	30.7%

Figure 10.5.3 Risk-management solution by risk

For Fire/Explosions and Natural Catastrophes as well, enterprises having non-insurance solutions are far fewer than those having insurance.

About a third of Midsize organisations claim to have no solutions for Trade War/Global Trade Realignment, Macroeconomic, and Climate Change Risks. Technology/AI and Civil Strife/Geopolitical issues follow closely, with around 28% of organisations indicating no solutions. These numbers again indicate a need to reinforce risk management across all Midsize organisations.

CONCLUSION

Midsize enterprises' responses to ERPS-2026 are broadly aligned to the overall responses in most important areas such as risk rankings and influence of forces. The differences from the overall sample indicate either Midsize segment or specific industry sector characteristics:

- Unlike the overall sample, Talent Risk is in the top 5 for short-term ranks and also in the top 5 for three sectors in long-term ranks. This indicates that Midsize enterprises face greater difficulty attracting and retaining talent.
- BFSI risk priorities are based on technology dependence and regulatory load, Services on technology and people dependence and Manufacturing on supply chain dependence.

Like the overall sample, Midsize enterprises see Operational Efficiency as the top opportunity from AI and Information Risk as the top risk. Their preparedness to manage AI-specific risks lags the importance they attach to AI.

In terms of risk management, they are best prepared for Legal/Regulatory, Cyber and Fire risks. Technology/AI and Climate Change risks require further investment from the segment.

Their risk management maturity is lower than the overall sample. Given the age of convergence and the expected impact of AI, Midsize enterprises need to improve their attitude toward risk, invest more in risk management, base their processes on international standards, spread responsibility for risk identification and implement controls alongside insurance solutions. This will help them play an even stronger role in the Indian economy and a bigger role in growing exports from India.

11. PARAMETRIC INSURANCE

Over the past decades, India has seen a sharp rise in climate-related disruptions, with 1,036 weather-related loss events between 1980 and 2019 causing USD 158 billion in economic damage, of which less than 6% was insured.

India also recorded the third-highest number of natural disaster events globally between 2000 and 2019, after China (577 events) and the United States (467 events), with 321 events recorded, ranging from extreme rainfall and floods to cyclones, droughts and severe heatwaves. These increasingly frequent shocks highlight the limitations of traditional insurance, which relies on lengthy assessments and detailed documentation. As the country ranks sixth in global climate vulnerability, several states have begun adopting faster, data triggered mechanisms such as parametric insurance to deliver timely and predictable financial relief.

Parametric insurance provides a pre agreed payout based on a clearly defined and measurable trigger such as rainfall, temperature, or wind speed. When the chosen parameter crosses the specified threshold, the benefit is automatically activated without requiring proof of actual loss.

This eliminates the need for surveys, damage assessments, or documentation, making the process simple and transparent. As a result, settlements are significantly faster, more objective, and hassle free for the insured.

Before the cover begins, five elements are agreed upon.

What is being measured:
For example, rainfall, temperature, wind speed or any other number that can be tracked.

Where it is measured:
the specific geographic area such as a village, district, block or mapped grid that determines payout eligibility.

When it is being measured:
the time window during which the parameter will be tracked.

Trigger level:

Start level:
Where the payout begins

Exit level:
Where the payout reaches its maximum

As the parameter moves from start to exit, the payout increases automatically.

SOURCE OF MEASUREMENT:

A certified, independent data provider, with a designated backup source, supplies the recorded measurement.

Parametric insurance does not insure “new risks.” It is simply a new way to pay for existing risks, using objective data instead of loss assessment. Its growth has been driven by:

- **Rising frequency of extreme weather events**
- **Cheaper and continuous independent data sources**
- **Regulatory acceptance of index-linked products, including in India**

11.1 HOW PARAMETRIC INSURANCE DIFFERS FROM TRADITIONAL INSURANCE

Dimension	Traditional Indemnity Cover	Parametric Cover
Basis of payment	Actual loss sustained, assessed and proved	Value of an agreed index against an agreed threshold
Physical damage	Required (including for BI)	Not required; insured event itself is the contingency
Claims process	Notification --> survey --> assessment --> negotiation	Automatic calculation on certified data; no survey
Settlement time	Weeks to months	Days to a few weeks, based on certified data
Use of proceeds	Typically tied to reinstating damaged assets	Unrestricted payroll, relief, logistics, debt service
Underwriting inputs	Asset schedules, valuations, risk survey	Long historical index series, exposure location, hazard model
Residual risk	Underinsurance, exclusions, deductibles	Basis risk: index and loss may diverge
Moral hazard	Present	Very low, insured cannot influence rainfall/windspeed
Administration cost	High (survey, documentation, litigation)	Low (data license + calculation agent)



11.2 EMERGING SEGMENTS IN PARAMETRIC INSURANCE

THE EMERGING SEGMENTS ARE:



AGRICULTURE:

Agriculture sustains over half of India's population and contributes around 18% to national GVA, making index based parametric protection crucial for managing high weather driven risk exposure. It has historically been the most mature and consistently measured vertical within parametric insurance. In India, it is anchored by RWBCIS, and the premium volumes under RWBCIS have increased year on year, as reflected in the annual data published on the official PMFBY portal dashboards.



FINANCIAL INSTITUTIONS:

Banks and other lenders serve borrowers whose incomes depend on the weather. Parametric covers pay on an agreed index without a loss survey, and the proceeds are unrestricted, including for debt service, which helps protect liquidity when a weather event occurs.



ENERGY AND CONSTRUCTION:

Energy is becoming a rapidly expanding parametric segment as increasing weather variability affects wind, solar and hydro generation, while construction is also growing, supported by the rising need for weather triggered protection during project execution.



RENEWABLES:

Renewables sit within Energy, which has emerged as the fastest-growing vertical in the parametric insurance market for the 2026–31 period. Renewable generators face weather-driven output and revenue risk, such as wind speed, that an objective index can cover with fast payouts.



AGRI - VALUE CHAIN:

Businesses between farm and market, such as aggregators, processors and traders, depend on weather-linked crop supply. Parametric covers can protect their revenue and procurement continuity when an agreed index is breached, building on India's operational experience with weather-index schemes and weather stations.



LABOURERS AND INFORMAL WORKERS:

Outdoor and informal workers are an emerging segment, as extreme heat typically costs self-employed women in India 40 to 50% of their income on exceptionally hot days. SEWA's heat cover grew from 21,000 women in 2023 to 50,000 women across 22 districts in 2024–25. Insurance payouts were made in 17 of the 22 districts, reaching about 92% of the 50,000 insured women.

11.3 GLOBAL MARKET SIZE

Estimates for the overall parametric market vary with definition.

Market estimates become much larger when different studies use wider definitions and different ways of measuring the parametric insurance sector.

For example, Global Market Insights puts the market size at USD 22.6 billion in 2026.

Research & Markets estimates USD 21.09 billion in 2025 and USD 23.85 billion in 2026, and expects it to grow to USD 38.68 billion by 2030 at about 12.8% CAGR.



The wide range between USD 4.02 billion and USD 23.85 billion shows how differently various studies define the parametric market.

Some estimates include more types of parametric products, distribution channels, industry uses and related risk-transfer activities, while others focus only on premium-based calculations.

Even with these differences, all forecasts indicate the same global trend.

Parametric solutions are becoming increasingly important across agriculture, energy, infrastructure, corporate resilience and climate-risk financing.

This growth is happening because businesses, governments and communities want faster, clearer and trigger-based financial protection.

11.4 THE INDIA LANDSCAPE



Where India Stands Today

India operates one of the largest index based insurance programmes, distinguished by its nationwide coverage, the scale of farmer participation, and substantial premium volumes.

RWBCIS, the Restructured Weather Based Crop Insurance Scheme, is a government-run weather-index crop insurance programme that remains one of India's most significant parametric initiatives, with its premium volumes continuing to rise, as per the annual PMFBY reports.

The scope of work with Financial Institutions is increasing, as banks, NBFCs and other lenders with exposure to weather-sensitive borrowers look to parametric covers to protect portfolios and preserve liquidity. The Renewables Industry also offers growing opportunities, as renewable energy developers face weather-driven generation and revenue risk that index-based triggers are well suited to address.

11.5 PARAMETRIC RECORD IN INDIA

Pilot Phase (2023)

A parametric heat stress protection pilot was developed through a multi stakeholder collaboration focused on climate resilience for informal women workers. The Atlantic Council's Climate Resilience Centre (Adrienne Arsht–Rockefeller Foundation) funded the initiative, which was co designed with community institutions such as SEWA and technical partners including Blue Marble.

The index used NASA POWER satellite derived daily maximum temperature data to create an objective, trigger based payout mechanism. The pilot covered approximately 21,000 women across five districts in Gujarat.

Scale Up Phase (2024–25)

Following the initial pilot, the programme was scaled through collaboration among SEWA, HERA, and Climate Resilience for All, with international risk design partners providing technical support and capacity. The scaled product used gridded daily maximum temperature data to define clear heat stress thresholds for payout eligibility.

Coverage expanded to nearly 50,000 women across 22 districts. Trigger levels ranged from 41.6°C to 46.1°C measured over two consecutive days, and the design was subsequently adapted to allow year-round protection reflecting increasing climate variability.

Core Elements of Parametric Protection

Globally, parametric solution offerings are structured around clearly defined, measurable triggers that pay out based on event intensity rather than assessed losses. Leading carriers offer solutions across weather-related perils, geophysical hazards and crop yield deviations, providing coverage for both corporate and public sector clients. These solutions are designed to deliver rapid liquidity following measurable events such as cyclone wind speeds, excess or deficit rainfall, heat stress thresholds, river level surges, or seismic magnitude readings, enabling organisations to resume operations faster.

Modern parametric products also incorporate advanced data sources including satellite observations, remote-sensing platforms and automated weather-station networks, to ensure independent verification and transparent payouts. Standard exclusions apply to events that cannot be objectively measured or validated, ensuring payouts.



11.6 CHALLENGES AND BASIS RISK

Basis risk is the risk faced by the insured person or entity when the parametric trigger does not perfectly match their actual loss. In simple terms, it is the chance that the index shows one result while the customer experiences something different on the ground.



Types of Basis Risk & Mitigation

Type	Description	Mitigation
Mismatch in Location	Event happens in one place, but measurements come from another	More weather stations, satellite data, coverage of smaller map areas
Index Doesn't Reflect Real Loss	Index trigger doesn't mirror actual impact	Multi variable indices, back testing with real client data
Issues with Data Source	Data source fails or is updated later	Backup source, clear publication rules, independent verification
Customer Feels Payout Doesn't Match Loss	Customer thinks trigger doesn't reflect true experience	Showing historical back tests where triggers paid or didn't pay

EXPERT PERSPECTIVE



GIRIJESH SHARMA
Vice President - Health & Analytics - Agri. & Mass Underwriting
ICICI Lombard

India's businesses are increasingly vulnerable to extreme rainfall, floods, cyclones and heatwaves, leading not only to physical damage but also to operational disruptions, supply chain delays and liquidity pressures. In 2026, the ElNiño caused one of the weakest monsoons in over a decade resulting in a national deficit of 13-15%. These shocks affected the availability of raw materials, raised input costs and slowed the movement of goods, making it more difficult for industries to maintain consistent production, logistics and delivery.

Recent instances show that climate shocks are increasingly disrupting business operations through production stoppages, worker availability issues, loss of inventory and damages to assets. Many businesses have limited access to emergency funds or specialized climate risk solutions, leaving them more exposed to repeated climate driven disruptions.

Rather than depending only on conventional insurance or reactive measures, businesses can

strengthen their continuity planning by incorporating parametric solutions that trigger payouts, the moment predefined weather thresholds are breached. When these objective, data driven triggers are embedded into operational systems, companies gain a clear sense of when financial support will be activated. This allows decision makers to respond with greater confidence, maintain liquidity during volatile periods and reduce downtime when climate related disruptions occur.

Businesses can therefore enhance their resilience by adopting a layered strategy that combines risk mitigation, risk retention, traditional insurance and parametric solutions to address protection gaps and liquidity needs.

Ultimately, parametric insurance helps shift risk management from merely compensating losses to prearranging funds for recovery, improving financial readiness and enabling businesses to resume operations more quickly after climate induced disruptions.

CONCLUSION

Parametric insurance should be viewed as a financial resilience tool that converts measurable events into timely liquidity. It complements traditional indemnity covers, especially where climate or catastrophe events disrupt revenues, operations or livelihoods.

India's extensive weather-index ecosystem positions it to expand parametric solutions into commercial risks. Successful adoption will depend on reliable data, clear hazard-index-loss alignment, transparent triggers, robust back-testing, appropriate portfolio limits and reinsurance support.



Parametric insurance can significantly strengthen India's climate-risk financing ecosystem, bridging the gap between a measurable event and the liquidity required for business continuity and recovery.

APPENDIX 1

SURVEY METHODOLOGY AND RESPONDENT DEMOGRAPHICS

A1.1 METHODOLOGY

ICICI Lombard and IRM India conducted the Enterprise Risk Perception Survey [ERPS-2026] in August-September 2026. The comprehensive online survey comprised 24 questions spread across 4 distinct sections:

- Section 1 Demographics: Covering organisational profile and respondent background - 7 questions
- Section 2 Risk Perceptions: Examining enterprise risk perceptions including specific questions on AI and interacting risks – 7 questions
- Section 3 Enterprise Risk Management Practices: Assessing risk management maturity - 6 questions
- Section 4 Risk Management and Insurance: Evaluating risk mitigation strategies and insurance practices - 4 questions

For risk perceptions, the risk list used last year was maintained. New questions were introduced in Section 2 for assessing AI preparedness, AI opportunities and AI risks and influence of forces on risks.

Survey responses were analysed to assess:



- Top risks and their perceived significance
- AI opportunities, risks and preparedness
- Interconnected nature of risks
- Organisational preparedness levels
- Maturity of risk management processes
- Insurance practices

A1.2 PARTICIPANT DEMOGRAPHICS

ERPS-2026 received a total of 253 responses, compared with 227 for ERPS-2025.

A1.2.1. INDUSTRY REPRESENTATION

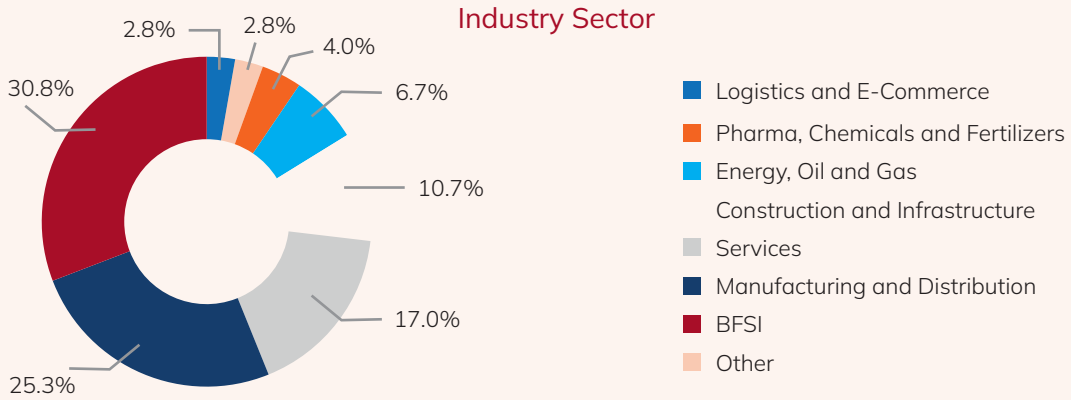


Figure A1.2.1: The pie chart depicts the Industry Sectors represented by respondents to ERPS-2026

The respondents represented a balanced mix of industry sectors. Largest three sectors represented by respondents are BFSI, Manufacturing and Distribution, and Services.

A1.2.2 REVENUE MIX

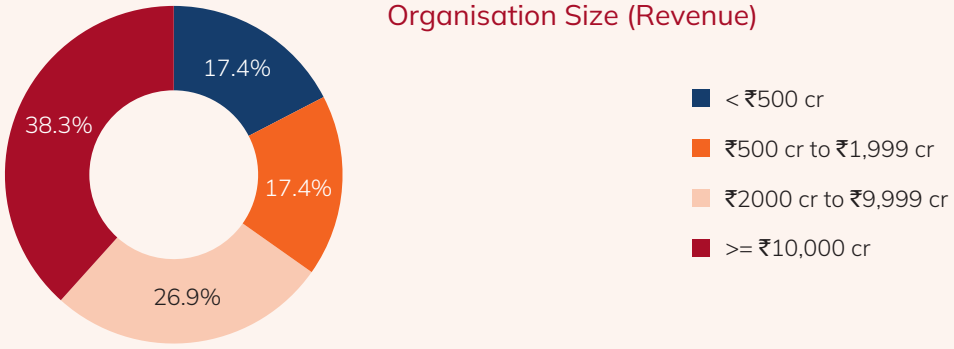


Figure A1.2.2 The pie chart depicts Respondent organisation sizes in terms of annual revenue.

The respondents represented a balanced mix of organisation sizes, from revenue less than ₹500 Cr per annum to above ₹10,000 cr per annum. The largest number of respondents were from mega corporations with revenues above ₹10,000 Cr.

A1.2.3 AGE OF ORGANISATION

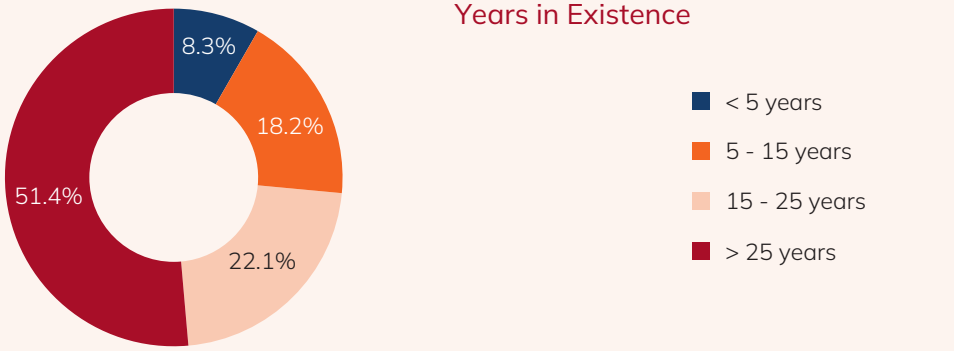


Figure A1.2.3 The pie chart depicts the age of Responding organisations (in years).

More than half of the respondents represented organisations that have operated for over 25 years. On the other hand, organisations with less than 5 years in existence contributed 8.3% of

A1.2.4 RESPONDENTS PROFILE

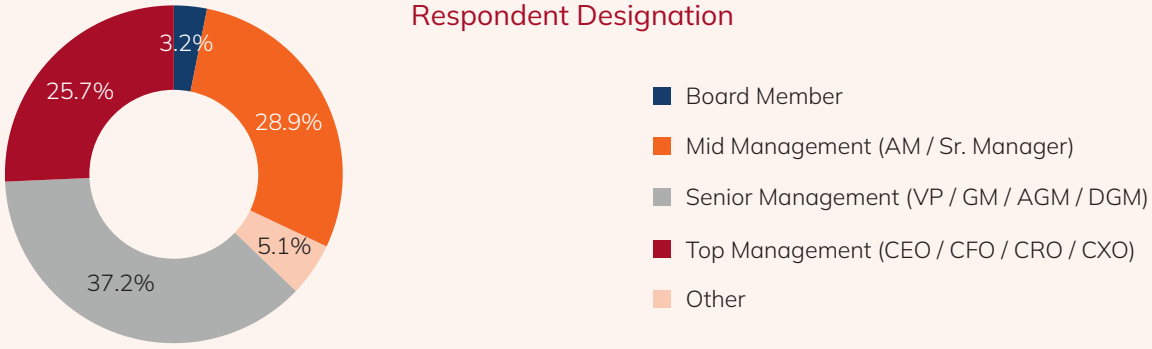


Figure A1.2.4 The pie chart depicts the Respondent designations.

Respondents represented a broad range of designations from managers, Vice Presidents, CXO to board members. Board and Top Management together made up 28.9% (3.2% + 25.7%).

APPENDIX 2

REFERENCES

a) The Global Risks Report 2026 published by the World Economic Forum, [WEF-2026]
b) IMF's Global Financial Stability Report 2026, [GFSR-2026]
c) Protiviti–NC State University's Executive Perspectives on Top Risks and Opportunities [EP-2026]
d) Risks in Focus by Internal Audit Foundation of The Institute of Internal Auditors [IIA-2026]
e) Risk Trends 2026 published by Institute of Risk Management, UK [IRM-2026]
f) Eurasia Group's Top Risks 2026 report
g) Oxford - GlobeScan Global Corporate Affairs Survey: 2026 Survey Report
h) Cisco. (2025). 2025 Cisco Cybersecurity Readiness Index.
i) Germanwatch. (2025). Climate Risk Index 2026. Germanwatch e.V.
j) IBM Corporation. (2025). Cost of a Data Breach Report 2025 - The AI Oversight Gap.
k) IBM Corporation. (2026). Cost of a Data Breach Report 2026 - The AI tipping point.
l) International Monetary Fund. (2026). World Economic Outlook Update: Global Economy in Crosscurrents of War and Technology. Washington, DC: International Monetary Fund, Publication Services.
m) International Monetary Fund. (2026). World Economic Outlook: Global Economy in the Shadow of War. Washington, DC: International Monetary Fund, Publication Services.
n) Reserve Bank of India. (2025). Financial Stability Report - December 2025. Mumbai: Financial Stability Department, Reserve Bank of India.
o) Reserve Bank of India. (2026). Financial Stability Report - June 2026. Mumbai: Financial Stability Department, Reserve Bank of India.
p) World Bank. (2026). Global Economic Prospects, June 2026. Washington, DC: World Bank.
q) Websites/Links referred:
    1. Canvas Learning Management System Data Breach
    https://www.reedsmith.com/articles/canvasinstructure-cyberattack-key-developments-and-action-items-for-higher-education-institutions/
    2. Boston Scientific Cyber Attack
    https://www.hipaajournal.com/boston-scientific-cyberattack/
    3. AI Risks – MIT Sloan Management Review
    https://mitsloan.mit.edu/ideas-made-to-matter/these-are-most-urgent-ai-risks-according-to-272-experts
    4. Artificial Intelligence and the future of Entry Level work: An Insight report published by WEF in June 2026.
    5. WTO Growth Rate:
    https://www.wto.org/english/news_e/news26_e/stat_19mar26_329_e.htm
    6. Greenpeace article on climate events

    https://www.greenpeace.org/international/story/85518/natural-disasters-2026-heat-fires-oil-gas-climate-renewables/
    7. What the Global Risks Report really says about the urgency of environmental threats: article
    https://www.weforum.org/stories/global-risks/2026-global-risks-report-environmental-risks-remain-urgent/
    8. IMF's Fiscal Monitor April 2026 – Executive Summary
    https://www.imf.org/en/publications/fm/issues/2026/04/15/fiscal-monitor-april-2026
    Access Executive Summary tab on the above page:
    9. Oxford - GlobeScan Global Corporate Affairs Survey: 2026 Survey Report
    10. Brent oil futures prices from Jan 2026 to March 2026: US Energy Information Administration – Oil price analysis dated April 7, 2026
    https://www.eia.gov/todayinenergy/detail.php?id=67424
    11.

    https://economictimes.indiatimes.com/news/economy/agriculture/el-nio-effect-kharif-crops-winter-sowing-face-stress-as-

14. https://www.pmi.spglobal.com/Public/Home/PressRelease/1c6afb992feb4eeebfe1221e16fc0109
15. https://www.pmi.spglobal.com/Public/Home/PressRelease/d0e480346d37482c85ac08e670f0109a
16. https://www.reuters.com/business/environment/india-expects-below-average-september-rains-after-weak-august-2026-08-31/
17. https://www.reuters.com/business/environment/what-triggered-catastrophic-flood-nepal-tibet-border-2026-08-26/
18. https://www.reuters.com/world/asia-pacific/nepal-hydropower-sites-centre-flood-rescue-efforts-2026-08-31/
19. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2238774&reg=48&lang=2
20. https://www.reuters.com/business/aerospace-defense/trump-xi-weigh-rareearth-truce-extension-chinas-curbs-still-bite-2026-05-13/
21. https://www.reuters.com/world/india/india-targets-rareearth-permanent-magnet-production-by-yearend-minister-says-2026-02-19/
22. https://www.reuters.com/world/beijing-is-looking-curbing-overseas-access-chinas-top-ai-models-sources-say-2026-07-07/
23. https://www.reuters.com/world/china/us-china-hold-ai-talks-september-sources-say-2026-07-21/
24. Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management: Integrating with strategy and performance. https://www.coso.org/guidance-erm
25. International Organization for Standardization. (2023). ISO/TS 31050:2023 risk management—Guidelines for managing an emerging risk to enhance resilience. https://www.iso.org/standard/54224.html
26. OECD-2024a: Organisation for Economic Co-operation and Development. (2024). Framework on management of emerging critical risks (OECD Public Governance Policy Papers No. 49). https://doi.org/10.1787/2f2eddd8-en
27. World Bank. (2024). India development update: India's trade opportunities in a changing global context. https://documents1.worldbank.org/curated/en/099513209032434771/pdf/IDU113d06cd810fec1465e1a7e318a711ea131b8.pdfdocuments1.worldbank.org
28. India is the 5th most digitalised country: https://icrier.org/pdf/State_of_India_Digital_Economy_Report_2026.pdf
29. Data centre pushback expected to increase: https://www.weforum.org/stories/economic-growth/ai-data-centre-pushback-will-linger-chief-economists-say
30. https://www.indiabudget.gov.in/economicsurvey/
31. https://power.industry-report.net/2026/10/08/india-renewable-capacity-299-gw-september-2026-biomass-nil-addition/
32. https://static.pib.gov.in/WriteReadData/specificdocs/documents/2026/may/doc2026514869801.pdf
33. https://my.msme.gov.in/files/MSME-Collab.html
34. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2182563&reg=48&lang=2
35. https://www.thehansindia.com/hans/opinion/news-analysis/salaried-households-middle-class-and-rural-poor-bearing-the-super-el-nio-brunt- 1136521

APPENDIX 3

KEY CONTRIBUTORS

Content and Execution Team



Uday Gharpure
Research Chair
IRM India Affiliate



Rupesh Malpani
Deputy Vice President
Commercial Lines Product & Strategy
ICICI Lombard



Dr. Keerti Pendyal
Associate Professor &
IRM India Coach at
Mahindra University



Gaurav Abhishek
AVP - Commercial Lines
Product & Strategy
ICICI Lombard



Sahil Kale
Senior Product Manager,
Business Strategy &
Solutions Team
ICICI Lombard

Academics Team



Dr Parimala Veluvali
Director, MA, FCS. Ph D,
Symbiosis School for
Online and Digital
Learning, Symbiosis
International (Deemed
University), Pune



Dr. Mrutyunjay Dash
Director
Global Centre for
Enterprise
Risk Management
Sri Sri University



Jashandeep Singh
PhD, Professor,
Chitkara Business School,
Chitkara University,
Punjab, IN



Kosha Parekh
IRMCert, Director -
Academics and
Trainings,
IRM India Affiliate

Legal Team



Dinal Morjaria
AVP - Legal
Corporate Legal
and Compliance
ICICI Lombard



Amrita Dandwani
Senior Manager
Corporate Legal
and Compliance
ICICI Lombard

Marketing, Designing and Support Team



Ishita Shah
Director - Marketing &
Communications,
IRM India Affiliate



Priya Rajani
Associate
Vice President,
Marketing
ICICI Lombard



Grishma Gori
Associate Director -
Institutional Partnerships
and Affiliations,
IRM India Affiliate



Bhairavi Naganath
Asst. Manager
Level II - Marketing:
Research & Operations,
IRM India Affiliate



Smriti Upadhyay
Asst. Manager
Level II – Academics:
Research and Analysis,
IRM India Affiliate

We extend our sincere gratitude to the senior leadership, members of the Advisory Council and experts from the Institute of Risk Management (IRM), ICICI Lombard and other distinguished industry leaders for their invaluable guidance, support and contributions to the India Risk Report 2026-2027.

We also express our appreciation to the industry respondents who generously shared their insights and perspectives through our survey, providing an understanding of risk preparedness.

Furthermore, we are thankful for the valuable suggestions and contributions from our colleagues, whose collaboration and commitment were instrumental in the successful completion of this report. Their collective efforts have enriched our understanding of risk management in India.

DISCLAIMER

This report contains forward-looking statements regarding risk trends and the convergence of emerging forces. Such statements reflect current analysis and assumptions and are subject to change; neither ICICI Lombard nor IRM India Affiliate undertakes any obligation to update these statements in light of future events.

Views attributed to named experts in this report are the personal views of those individuals and do not necessarily represent the views of their employers, ICICI Lombard, or IRM India Affiliate. Such contributions have been included with the consent of the individuals concerned.

Survey responses contributing to the Enterprise Risk Perception Survey 2026 (ERPS-2026) were collected and processed in accordance with the data-protection practices of ICICI Lombard and IRM India Affiliate. Individual respondent identities and organisation-level responses are not disclosed in this report; only aggregate findings are presented.

We are not responsible for any errors or omissions or for the results obtained from the use of such information. We do not make representations or warranties, either express or implied, of any kind with respect to any third party, its actions, content, information or data. We do not represent or endorse the accuracy or reliability of any advice, opinion, statement or other information provided for the purpose of rendering services hereunder. Users acknowledge that any reliance upon such opinions, advice, statements, memoranda or information shall be at their sole risk. Any such person or entity should seek advice from experts in the relevant field, based on their particular circumstances. The content of this report is proprietary to ICICI Lombard and IRM India Affiliate. The content may not be copied, distributed or communicated to any third party without the prior permission of ICICI Lombard and IRM India Affiliate.

ICICI trade logo displayed above belongs to ICICI Bank and is used by ICICI Lombard GIC Ltd. under license and Lombard logo belongs to ICICI Lombard GIC Ltd. ICICI Lombard General Insurance Company Limited, ICICI Lombard House, 414, P. Balu Marg, Off Veer Savarkar Road, Near Siddhi Vinayak Temple, Prabhadevi, Mumbai 400025. Toll Free: 1800 2666 Fax No: 022 61961323 IRDA Reg. No. 115 CIN: L67200MH2000PLC129408. Customer Support Email ID: **customersupport@icicilombard.com** Website Address: **www.icicilombard.com.**

The IRM logo displayed above belongs to the Institute of Risk Management (IRM) and is used by IRM India Affiliate under authorisation. IRM India Affiliate is the official trade name for Gleco International Private Limited (as per GST registration). IRM India Affiliate, 102, Lodha Supremus, New Cuffe Parade, Opp. New GST Bhavan, Wadala, Mumbai 400037, CIN U74140MH2019PTC333967. Email ID: **communications@theirmindia.org,** Website Address: **www.theirmindia.org.**

NOTES

Scan the QR code to instantly access the soft copy of the India Risk Report 4.0.

ICICI Lombard

irm
Developing risk professionals
www.theirmindia.org

25 Years ONE IL Team
CELEBRATING A LEGACY OF TRUST

ICICI Lombard General Insurance Company Ltd.

ICICI Lombard House. 414, P. Balu Marg,
Off Veer Sawarkar Marg, Near Siddhivinayak Temple,
Prabhadevi. Mumbai- 400025.

https://www.icicilombard.com

IRM India Affiliate

101-102, 108, 1st Floor Lodha Supremus,
New Cuffe Parade, Wadala East, Mumbai,
Maharashtra - 400037

https://www.theirmindia.org/

https://www.theirmindia.org/thought-leadership

General Insurance Online: ICICI Lombard is one of the leading private general insurance companies in the country. The company offers a well-diversified range of products across multiple distribution channels, including motor, health, crop, fire, personal accident, marine, engineering and liability insurance.