Risk outlook: A compass to India's risk landscape

FICCI-EY Risk Survey 2026

February 2026

The better the question.
The better the answer.
The better the world works.

Shape the future
with confidence

Foreword EY

The resilience blueprint: Steering Indian enterprises through new age risks

In an era defined by rapid transformation and uncertainty, Indian enterprises are increasingly being called upon to redefine their approach to risk and resilience. I am pleased to present the "FICCI-EY Risk Survey 2026: Risk outlook – A compass to India's risk landscape" for Indian businesses. This year's insights come at a defining point in India's economic trajectory. With the economy projected to grow at 7.4% in 2025–26, supported by strong domestic consumption and continued capital investment, India stands out as one of the world's most dynamic and robust markets.

This momentum is, however, unfolding against a risk environment that is more complex and interconnected than ever. Organizations are navigating an environment shaped by persistent disruption, rapid technological shifts and geopolitical uncertainty. Boundaries between strategic, operational, financial and technology risks have blurred. External shocks and internal vulnerabilities now interact at speed, altering enterprise exposure in ways that demand sharper visibility and faster decisions. In this dynamic environment, the ability to foresee and swiftly adapt to emerging threats has become not just a competitive advantage, but a necessity for survival.

India's position within global supply networks introduces further layers of vulnerability. Heavy dependence on imported capital goods, technology components and energy inputs increases sensitivity to supply bottlenecks, price volatility and trade policy shifts. These dynamics require businesses to strengthen ecosystem intelligence and build adaptability across their value chains.

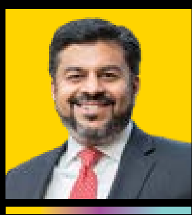
At the same time, the global geopolitical backdrop remains fluid. Changing tariff regimes, energy realignments and shifts in global alliances are influencing trade flows and cost structures, compressing planning cycles and increasing operational uncertainty. Organizations must move from periodic risk assessments to continuous sensing, analytical foresight and scenario driven action. Collaboration across industries and with policymakers will be central to developing agile risk oversight strategies and sustaining long-term growth.

New age risks are also reshaping enterprise priorities. Cyber threats continue to escalate in sophistication, while the rapid infusion of AI across operations introduces new governance, ethical and security considerations. Climate related disruptions, which were once considered as long horizon concerns, are now influencing strategic choices, capital allocation and regulatory expectations. Collectively, these risks cut across digital infrastructure, data environments, third party relationships and board level decision making, underscoring the need for integrated, technology enabled safeguards. Proactive adaptation and investment in technology-driven solutions will empower organisations to not only withstand but also thrive amidst uncertainty.

The 2026 survey sends a clear signal. Indian businesses are confident in the nation's growth trajectory, but they also recognize that their success will depend on their capacity to anticipate and respond to future challenges. Those that do so will lead India's next decade of growth with clarity and conviction. Together, let us embrace this journey of transformation, fostering a culture where resilience and foresight form the bedrock of our shared success.

Rohan Sachdev

India Consulting Leader and Partner, EY India



Sudhakar Rajendran

Risk Consulting Leader and Partner, EY India

Foreword FICCI

Strengthening India's risk preparedness for sustainable growth

Businesses today operate in an environment marked by persistent uncertainty and rapid change. Against the backdrop of economic volatility, climate-related risks, increasing cyber vulnerabilities, accelerated technological disruption and evolving geopolitical realignments, effective risk anticipation and management have become critical to long-term sustainability. Recognizing this, FICCI, in partnership with EY, has continued its efforts of capturing industry perceptions on emerging and evolving risks, consolidating these insights into a comprehensive and analytical risk ranking through the FICCI-EY Risk Survey.

In recent years, businesses have had to navigate overlapping crises like public health disruptions, supply-chain fragilities, energy and food security concerns, financial pressures and shifting workforce dynamics. Even as economic activity is gaining momentum, the global operating environment remains fragile, with uncertainty increasingly becoming a structural feature rather than a temporary phase.

On the domestic front, policy interventions aimed at strengthening economic resilience, improving governance, and positioning India as a globally competitive economy have played a vital role in cushioning external shocks. Through focused policy reforms, institutional strengthening, infrastructure development and greater use of technology, the focus has been on anticipating risks, reducing vulnerabilities and improving preparedness and response capabilities.

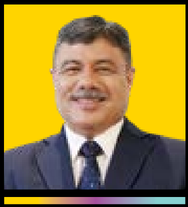
The vision of Atmanirbhar Bharat is steadily translating into tangible outcomes across sectors such as defense, renewable energy, healthcare, digital infrastructure and advanced manufacturing. While continued efforts to rationalize regulations and ease compliance have enhanced India's attractiveness as an investment destination, the evolving regulatory landscape also requires businesses to adapt to higher compliance expectations in certain areas.

As India progresses towards its US$5 trillion-economy aspiration, the ability of businesses to manage risks proactively will be central to sustaining growth, competitiveness, and investor confidence.

At the same time, the risk landscape is undergoing a fundamental shift. Climate-related risks, environmental compliance, resource constraints and sustainability expectations are rising sharply on boardroom agendas. Parallelly, the rapid adoption of digital technologies, while enabling growth and efficiency has amplified exposure to cyber threats, data breaches, and the misuse of emerging technologies such as drones and AI.

Addressing these risks requires not only robust regulation but also active collaboration between government, industry, start-ups and academia. Scientific capability and frontier technologies are increasingly at the core of India's transformation, driving mission-mode initiatives and fostering innovation, intellectual property creation, and global competitiveness.

In this context, understanding risk as a dynamic, interconnected spectrum rather than as isolated challenges is essential for informed decision-making. The FICCI-EY Risk Survey seeks to support organisations in this endeavor by offering a structured view of the evolving risk environment. We hope this report serves as a valuable guide for businesses to assess their risk exposure, strengthen preparedness, and build adaptive strategies in an increasingly complex world.



Rajeev Sharma

Chair, FICCI Committee on Corporate Security & DRR and Cluster
Managing Director, India, Nepal & Bangladesh, G4S Corporate Services (India) Pvt Ltd

Introduction

Business environments worldwide are becoming more complex and interconnected, with uncertainty shaping strategic, operational and investment decisions. Risks now emerge simultaneously from multiple risk vectors and often interact to influence stability, growth and governance. In this setting, organizations need a structured and coherent view of risk to support sound judgement and timely action. Within this broader landscape, India is navigating an economic transition shaped by global developments and domestic pressures. Geopolitical tensions, evolving trade patterns, regulatory changes, technology dependence, climate considerations and workforce dynamics are influencing how enterprises plan and operate, affecting supply chains, market access, compliance and cost structures.

The *FICCI-EY Risk Survey 2026: Risk outlook - A compass to India's risk landscape* for Indian businesses, offers a comprehensive view of these challenges. Drawing on insights from business leaders across sectors, the report examines risk perception, prioritization and management juxtaposed with global trends, India-specific risks and sector-level perspectives to support informed decision-making.

Key findings at a glance

Geopolitical pressures and rapid shifts in the operating environment are increasingly influencing organizational priorities, affecting stability, leadership focus and business confidence. Survey insights reflect growing pressure across technology, governance and workforce dimensions, with respondents highlighting several areas of heightened exposure.

- **Concerns around digital risk remain prominent**

  61% of respondents highlight cyber-attacks and data breaches as major financial and reputational threats

  59% point to limited adoption of emerging technologies, including AI, affecting operational effectiveness

- **Workforce challenges persist**

  64% report talent shortages and skill gaps influencing organizational performance and long-term capability planning

- **Governance-related pressures are also increasing**

  45% of respondents indicate that non-compliance with ESG disclosure requirements has a direct impact on their organization

Together, these findings indicate that risks across technology, governance and talent are becoming more interconnected rather than operating in isolation. As these pressures converge, organizations have to take a more integrated approach to risk management, strengthening oversight, capability planning and decision-making to support stability and sustained performance in an evolving operating environment.

> Indian businesses are navigating an increasingly complex risk landscape marked by geopolitical volatility, regulatory activism, supply chain fragility, rapid digitalisation, and heightened stakeholder scrutiny. These risks are converging, amplifying their impact on profitability, business continuity, and reputation. For Indian enterprises, resilience is now a strategic imperative. Leading organisations are strengthening enterprise-wide risk governance, investing in technology-enabled controls, and embedding risk intelligence into capital allocation and growth decisions. Those that proactively anticipate, quantify, and respond to emerging risks will be better positioned to protect value and sustain long-term growth.

Sudhakar Rajendran
Risk Consulting Leader and Partner, EY India

> In sectors like drones, defence manufacturing, logistics, and critical infrastructure, AI is no longer experimental it is operational. With Military AI moving from labs to live missions, alongside precision and speed come heightened security risks cyber intrusion, data compromise, autonomous misuse, IP theft, and supply-chain vulnerabilities. For Indian businesses, trusted AI built on indigenous systems, secure data frameworks, and strong governance will define sustainable competitiveness.

Bodhisattwa Sanghapriya
Co-Chair, FICCI Drone Committee and Founder & CEO, IG Defence

CHAPTER 01

Major risks shaping business outcomes

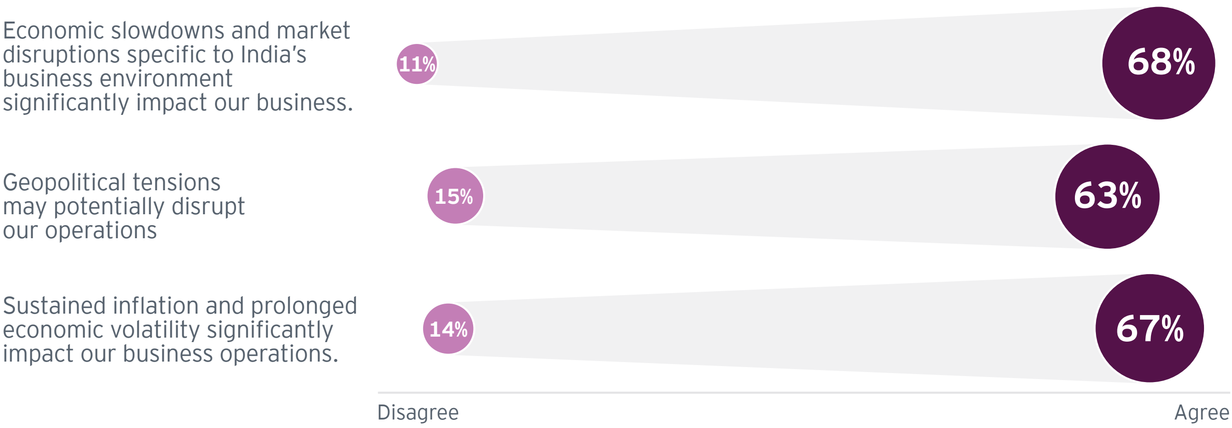
A close look at the changing global conditions influencing investment and sourcing decisions

Geopolitical developments, shaped by evolving trade policies and shifting global priorities, continue to influence the global operating environment. As major economies adjust their policy direction, uncertainty is expected to persist into 2026, affecting trade, investment and supply networks.

These shifts are contributing to a gradual realignment of global trade flows. Many economies are placing greater emphasis on domestic capacity building and supply resilience, particularly across sectors such as semiconductors, clean energy and advanced manufacturing. Changes in trade measures are influencing the availability and pricing of critical inputs used across electronics[1], electric mobility and renewable energy value chains.

Together, these trends reinforce the importance of preparedness. Ongoing geopolitical shifts continue to influence energy markets, supply chains and regulatory environments, with implications across operational, financial and reputational areas. In such an environment, scenario planning and geopolitical awareness are becoming important tools to support informed decision-making and strengthen organizational resilience.

Sentiment gradient on growing concern (left to right)



1. Policy Backgrounder: The Future of the CHIPS and Science Act

> In today's interconnected risk landscape, geopolitical risk is no longer episodic but a new operating reality. Leading organizations are embedding geopolitical intelligence directly into business strategy, not only to build resilience but to sharpen competitive advantage.

Vishal Ruia
Advance Manufacturing, Mobility and Infrastructure (AMI) Risk Leader and Partner, EY India

Resilience and adaptability are no longer optional. Building flexibility and staying attuned to geopolitical shifts can influence how organizations sustain performance in this evolving environment.

The FICCI-EY risk survey data indicates that economic slowdown, market disruptions and sustained inflation remain key areas of attention for Indian businesses, with 68% of respondents reflecting a shared view on their relevance. Economic volatility continues to feature prominently, with 67% of respondents agreeing or strongly agreeing on its impact on business planning and operations. Geopolitical factors also remain relevant, with 64% of respondents acknowledging that geopolitical tensions are having a noticeable impact on their organizations, contributing to uncertainty in decision-making and long-term outlook. These findings reinforce the need for boards to embed geopolitical foresight, prioritize resilience over efficiency and align capital allocation with a fragmented, unpredictable global landscape.

The message for business leaders is clear: Sectoral impacts are real and immediate. Technology, automotive, defense, energy and manufacturing firms should build resilience into their supply chains, diversify sourcing and stay agile in pricing and regional strategy. In this new era, monitoring geopolitical flashpoints is not just prudent but essential for survival and growth.

Organizational key considerations to counter geopolitical risks

- Are we embedding geopolitical foresight into our core governance and decision-making?
- Have we reconfigured our global footprint for resilience rather than pure efficiency?
- Are our capital allocation and growth strategies aligned with geopolitical realities?

> Global shifts are prompting Indian enterprises to rethink how they operate and compete. By strengthening partnerships, embracing smarter planning, and building adaptable networks, businesses can convert uncertainty into opportunity while enhancing confidence across stakeholders.

Monica Malhotra Kandhari
Chair, FICCI Publishing Committee and Managing Director, MBD Group

CHAPTER 02

Cyber risks

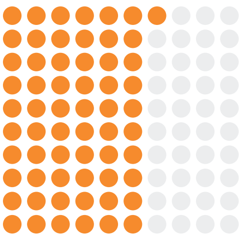
Elevating the conversation from IT threat to boardroom priority

Cyber risk is emerging as a defining challenge for operational stability and infrastructure resilience in today's digital-first business landscape. No longer isolated, these risks now shape the very foundation of enterprise continuity and competitive advantage.

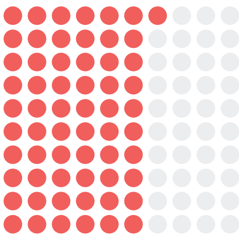
Ransomware and Distributed Denial-of-Service (DDoS) attacks disrupt production, logistics and essential services, resulting in downtime and financial loss. Data breaches expose sensitive customer and business information, leading to lasting reputational damage. As system defenses improve, human error is exploited through phishing and social engineering. In parallel, dependence on third-party vendors expands exposure, where a single security failure can cascade into regulatory, legal and operational consequences across the organization.

Globally, the average cost of a data breach stands at US$4.4 million[2], while ransomware incidents now cost approximately US$5.5 million, up nearly 17% year-on-year[3], reflecting a shift toward data theft and system disruption. Attacks on critical infrastructure are also rising, with manufacturing, healthcare, energy and finance being among the most affected. Ransomware incidents have increased 50% in 2025, largely via phishing and remote access[4].

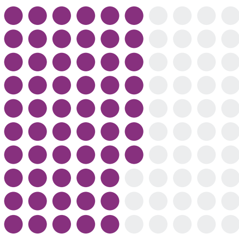
Technology and Cybersecurity risks



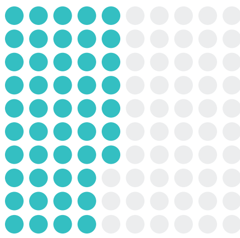
61%
Rapid technological advancements and digital disruption significantly impact our competitive position



61%
Cyber-attacks and data breaches pose significant financial and reputational risks to our organization

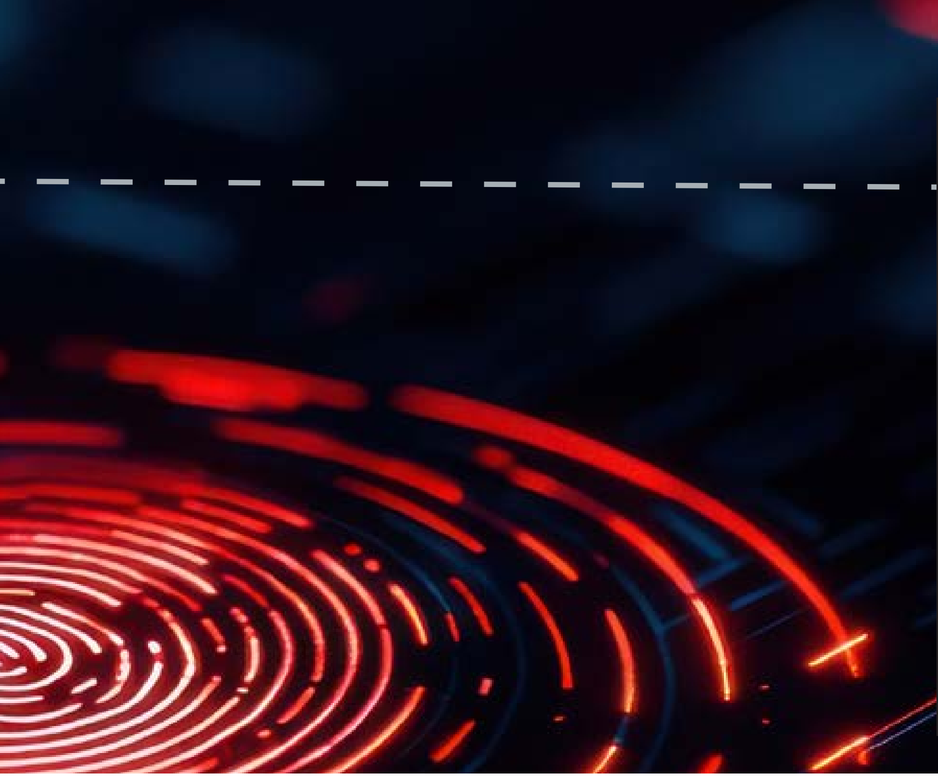


57%
Data theft, insider fraud, and sabotage through business espionage have a significant impact on our organization



47%
Our organization faces substantial challenges in addressing sophisticated cybersecurity threats

2. Cost of a data breach 2025 | IBM
3. HIPAA Journal: Only 23% of Ransomware Victims Pay the Ransom



> The business environment today is dealing with risks that are nuanced due to myriad factors. With the permeation of AI technologies and cyber risks in all walks of life and business, it presents both risks and opportunities. The key for organizations will be to seize the opportunity that technology disruption has to offer while balancing the inherent risks.
>
> **Deepak Bhalla**
> EVP Finance and Chief Risk Officer, Infosys Limited

India faces a sharp rise in cyber intrusions due to AI-based social engineering, cloud gaps (misconfigured or weak cloud security settings that expose systems and data), and vulnerability chaining (attackers linking multiple small security flaws to gain deeper access into networks). Bot activity has increased, with multi-vector campaigns becoming more common. Deepfake voice scams affect the banking sector, leading to losses from fraud and higher complaint volumes on the National Cyber-Crime Reporting Portal (NCRP)[5].

The survey indicates that technology and cybersecurity risks are a growing concern, with 61% of respondents agreeing or strongly agreeing that digital disruption affects competitiveness and cyber attacks pose major threats. Additionally, 57% highlight the impact of data theft and insider fraud, while 47% acknowledge challenges in managing sophisticated cyber threats.

Cyber-attacks and data breaches pose major financial and reputational risks, while rising threat sophistication, insider fraud and business espionage demand stronger internal controls and vigilance. These findings reinforce that the real challenge is not just to defend but to anticipate and adapt.

For organizations, the implication is increasingly evident: Cyber risk poses a direct threat to operations, revenue and trust and cyber readiness is central to business continuity and confidence.

4. Half of 2025 ransomware attacks hit critical sectors as manufacturing, healthcare and energy top global targets - Industrial Cyber
5. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146&utm&reg=3&lang=2

Organizational key considerations for cyber risk management

Do our governance structures provide clear ownership and timely oversight of cyber risk at the enterprise level?

Are we prepared to sustain operations and recover quickly if a cyber incident were to disrupt critical systems?

Do our workforce practices and third-party relationships introduce hidden cyber exposures that are monitored continuously?

> For organizations, particularly those operating critical infrastructure and large-scale, distributed operations, the focus must shift from reactive risk management to building integrated, technology-driven systems that enhance visibility, enable faster decision-making, and strengthen accountability across the enterprise.
>
> **Aditya Khemka**
> Co-Chair, FICCI Committee on Corporate Security & DRR and Managing Director, CP PLUS

CHAPTER 03

Artificial intelligence (AI) risks

Evolving from technical challenge to enterprise imperative

AI is reshaping the business landscape, creating new opportunities as well as risks that require thoughtful oversight from senior leaders. The growing use of AI systems that can complete tasks with very little human involvement makes strong guidance and close coordination across teams more important than ever. AI can introduce inherent risks, including hallucinations that produce confident but incorrect outputs, bias embedded in training data, and weak explainability and poor data quality, all of which can undermine decision accuracy and accountability. These risks are no longer theoretical.

Deepfake incidents have risen sharply, with manipulated content becoming increasingly widespread. In a global survey, around 35% of respondents reported being exposed to manipulated or AI-generated media, including deepfake videos, images or audio encountered through social media, messaging platforms, news feeds or campaign communications. As reliance on AI grows, failures such as model drift, where AI accuracy declines as data patterns change over time and data poisoning, where incorrect or manipulated data affects model outputs, trigger forecasting errors, inventory disruptions and productivity losses, while stricter regulation heightens compliance exposure. Public-facing errors erode trust and unmanaged model extraction risks expose proprietary challenges, creating lasting financial, regulatory and reputational consequences.

Beyond these risks, organizations face emerging AI exposures that directly affect control, liability and talent while incurring additional costs. Shadow AI remains a major concern, as employees use public tools for sensitive work, risking irreversible intellectual property leakage. At the same time, Agentic AI introduces legal ambiguity when autonomous systems execute contracts or financial actions without human approval. New attack vectors, such as prompt injection, allow hidden instructions to bypass traditional security controls.

60%

Surveyed senior executives report an increased concern around potential impact on operational effectiveness due to inadequate adoption of AI

Effective digital and AI governance transforms unmanaged technological risk into managed strategic advantage.

Varun Gupta
President and Chief Financial Officer, Jubilant Ingrevia Limited

Talent dynamics are also shifting, with AI capability gaps driving attrition, while excessive reliance on automation risks weakening critical thinking and judgment across teams. As the focus shifts to AI, it is critical to address AI-related cyber risks through stronger governance, access controls and continuous monitoring to prevent misuse, data leakage and model manipulation. Managing AI risk now requires integrated governance, rigorous model and data management and continuous monitoring to prevent innovation from outpacing organizational control and accountability.

The survey reveals significant operational concerns on both the lack of adoption and the ineffective management of AI. There is a prevailing concern about technological readiness, cost impact and risk management areas associated with the use of AI. About 60% of respondents believe that inadequate adoption of emerging technologies, including AI, can adversely impact operational effectiveness, while more than 54% feel that AI risks, including ethical concerns, are not effectively managed within their organization.

These findings highlight that the true imperative is to proactively embrace and manage AI risks, promoting operational resilience, adaptability and risk governance in a rapidly evolving landscape.

From a leadership standpoint, the priority is to understand that AI risk is now a core business risk and not merely a technology issue. As AI and Agentic systems scale, failures can directly affect decisions, compliance and trust. Strong governance, clear accountability and disciplined controls are essential to protect value and sustain confidence.

Organizational key considerations to counter AI risk

Are accountability and oversight for AI decisions, approvals and outcomes across business functions clearly defined?

Have controls around performance and explainability of data and models been designed and implemented?

Is there robust oversight for AI use, data access and system dependencies to manage emerging risks responsibly.

As AI becomes more deeply embedded in enterprise environments, striking the right balance between autonomy and control is essential. The future belongs to leaders who see governance and resilience not just as safeguards, but as strategic enablers for the next era of autonomous intelligence.

Nitin Mehta
Digital Risk Leader and Partner, EY India

6. Climate change is costing the world $16 million per hour | World Economic Forum

CHAPTER 04

Environmental, social and governance (ESG) risks

Driving cascading global and domestic disruptions

Risks from climate and environmental pressures continue to rise as global warming intensifies, extreme weather events become more frequent and damage to land, forests and natural ecosystems worsens. These risks now disrupt economies, supply chains, food systems and livelihoods in real time. Slower progress on decarbonization, persistently high fossil fuel use and rising greenhouse gas concentrations are leading to severe weather conditions, biodiversity loss, pollution and resource stress, while rapid urban expansion in coastal and dry regions increases exposure for millions of people.

The economic cost of climate change is escalating, with global damages projected to reach US$38 trillion annually by 2050 under current conditions. Storms, floods and heatwaves already cost about US$16 million every hour[6]. Repeated extreme events have damaged infrastructure and agriculture, pushing cumulative losses since 2000 into the trillions. Water mismanagement alone could cut average GDP by 8% and up to 15% in low-income countries, threatening over 50% of global food production[7]. Yield volatility has pushed food prices up by 4% to 6%, disrupted rural demand and raised the risk of a 16% output decline by 2030[8]. Heat stress is increasingly shaping financial and operational risk.

Flooding
Urban flooding across India disrupted transport, power, and essential services'.

Heatwaves
South Asia experienced record heatwaves, leading to deaths.

Desertification
Desertification is impacting agricultural output, causing poverty and economic instability.

Climate shocks in 2025

7. Mismanagement of water resources could lead to 8% GDP loss by 2050 - Sustainability Online
8. ey.com/content/dam/ey-unified-site/ey-com/en-in/insights/tax/economy-watch/documents/2025/11/ey-economy-watch-monitoring-india-s-macro-fiscal-performance-november-2025.pdf

> Effective sustainability risk management goes beyond disclosure and is about proving resilient performance across the enterprise value chain.
>
> **Nitesh Mehrotra**
> Partner, EY India

The survey shows that 45% of respondents agree or strongly agree that non compliance with ESG disclosure requirements affects their organization. Additionally, 44% of respondents feel that climate related financial impacts pose risks, while 41% indicate that limited board oversight increases their exposure to ESG related issues.

45%
Respondents have stated financial impact due to climate change as a critical risk to their operations in India

44%
Respondents stated that non-compliance with ESG disclosure mandates and reporting requirements may significantly impact them

42%
Executives expressed concerns around effectiveness of Board oversight on ESG-related issues

From India's perspective, water scarcity is a growing business risk, with per capita availability estimated at 1,341 cubic meters, below the stress threshold[9]. Severe groundwater extraction in Punjab, Haryana, Rajasthan and Karnataka threatens water-intensive sectors such as agriculture, food processing, textiles, chemicals, power and electronics.

Record temperatures and rising extreme events mean productivity losses of 20% to 30% in construction, logistics and mining, while higher cooling demand has lifted power costs by about 15%[10]. For companies, this raises risks of production disruptions, higher compliance costs, location constraints and supply chain instability. This increases credit risk in agriculture, MSMEs and climate-exposed regions, while insurers face rising crop, health and property claims.

Organizational key considerations to counter climate and environmental risk

- Are climate risks shaping our capital allocation, asset strategy and growth decisions?
- Do we assess climate impacts as a driver of operational, supply chain and financial performance risk?
- Are leadership teams aligned to protect long-term enterprise value and resilience?

9. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2002726&utm&reg=3&lang=2
10. https://internal.imd.gov.in/press_release/20250612_pr_4053.pdf

CHAPTER 05

Workforce risks

Creating structural constraints on business performance

As organizations evolve through shifting market realities and new ways of working, the strength of their talent and culture is emerging as a defining force for long-term success. Growing skill shortages, leadership gaps and rising expectations around workplace safety and conduct are reshaping how businesses attract, develop and retain their people. Hybrid work models continue to test connection and belonging, particularly when culture is left to develop organically. This places greater responsibility on leaders to actively shape engagement and shared identity. As emerging technologies such as AI become deeply embedded across functions, talent strategies should be designed with an openness to continuous learning and future skills so that the workforce grows in step with the enterprise's ambitions.

Talent and culture dynamics are undergoing a profound reset, shaped by changing workforce expectations, evolving skill requirements with the advent of AI and the rising complexity of leadership roles. Organizations are experiencing widening shortages not only in digital and analytics capabilities but also in adaptive, cross-functional skills that are essential for modern work. The EY Work Reimagined 2025 survey finds that while 88% of employees now use AI in their daily roles, only 28% of organizations have the talent systems needed to unlock its transformative value, suppressing potential productivity gains by up to 40% when learning culture, rewards and role design are misaligned[11]. This makes re-skilling and up-skilling a continuous rather than an episodic capability-building mandate that will influence future competitiveness.

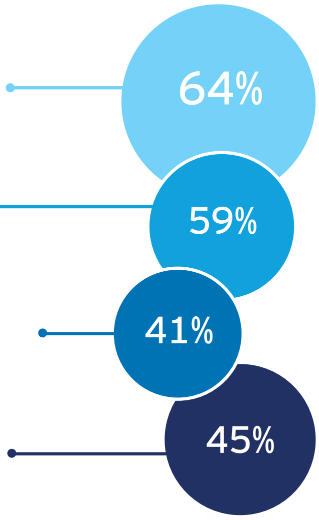
Talent and culture risks

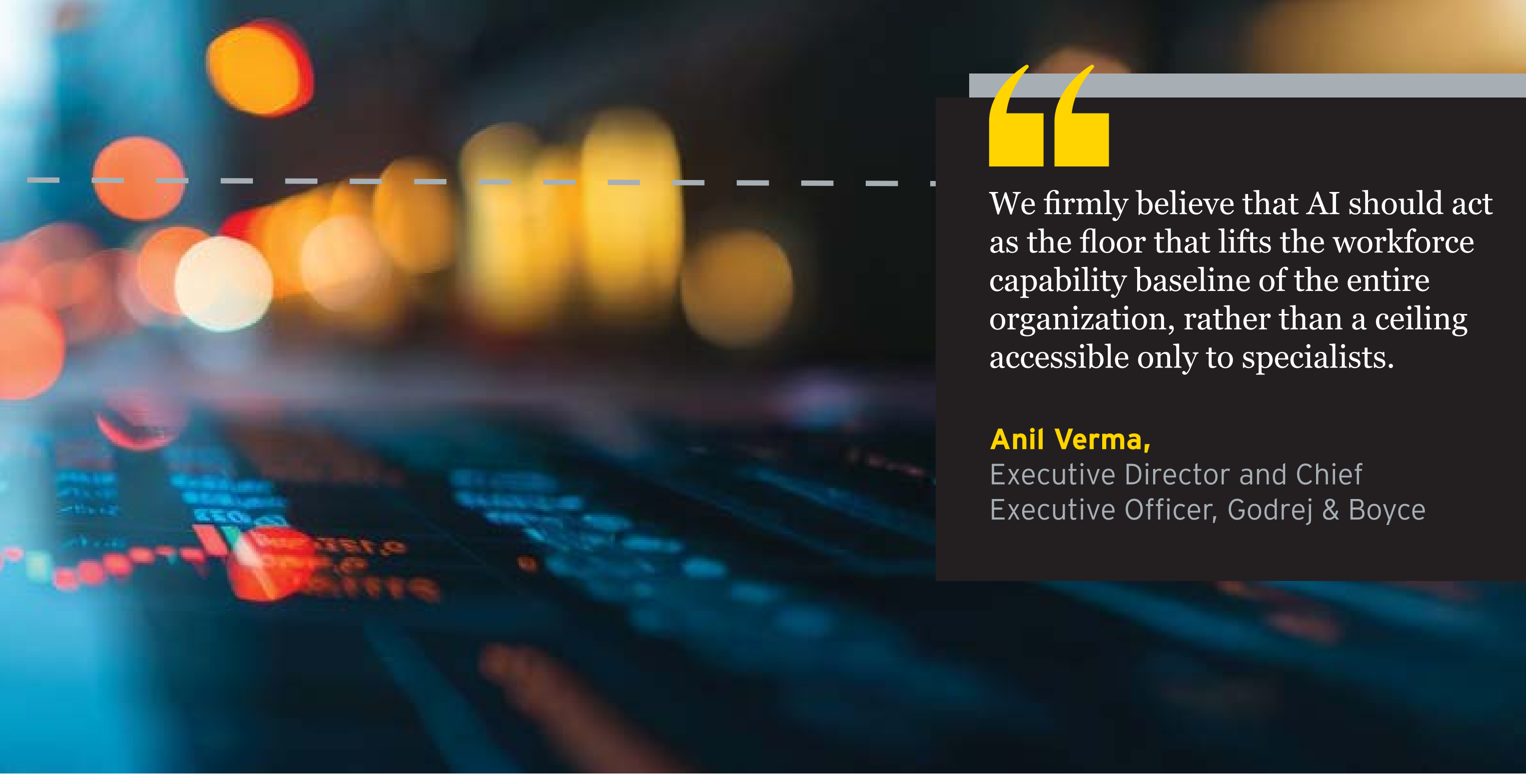
Talent shortages and critical skills gaps prevalent in the Indian market adversely impact our organization's performance.

Inadequate succession planning and leadership development adversely impact organizational stability.

Remote/Hybrid working poses significant risks to our corporate culture, employee engagement, and ethical conduct.

Absence of clear policies that address harassment at the workplace, employee safety issues and women safety).





> We firmly believe that AI should act as the floor that lifts the workforce capability baseline of the entire organization, rather than a ceiling accessible only to specialists.

Anil Verma,
Executive Director and Chief Executive Officer, Godrej & Boyce

Leadership pipelines are also weakening as roles expand in complexity and expectations for empathy, integrity and change readiness increase. The Global 2026 HR trend research indicates an urgent need to rethink succession models, with organizations placing greater emphasis on adaptable leaders capable of guiding hybrid teams and sustaining rapid transformation[12].

Leaders can strengthen organizational resilience by placing people and culture at the heart of strategy. This means building future skills, investing in practical leadership development and shaping workplaces where trust, clarity and connection guide everyday behavior. Organizations that do so can expect to stay relevant and move forward with confidence.

> In India's shifting market, workforce risks from talent gaps to burnout are no longer just HR issues; they are critical business disruptors. Only by supporting and engaging our people can we turn these risks into a sustainable competitive advantage.

Ashish Kansal
Co-Chair, FICCI Defence & Homeland Security Committee and Executive Director, SMPP Pvt Ltd

Organizational key considerations to manage workforce risks

How well are our talent and culture priorities aligned to the organization's long-term strategy and what shifts should the management consider strengthening that alignment?

Do our leadership and succession models equip us for a more digital, hybrid and trust driven future of work?

How effectively are we reinforcing the cultural signals, controls and role modelling needed to sustain trust and cohesion as work becomes more digital and distributed?

What is the impact of AI and related technology on the workforce of the future?

11. Can AI advance toward value if workforce tensions linger? | EY - Global
12. 2026 HR Trends: Planning for Business Impact (https://www.shrm.org/in/topics-tools/news/hr-trends)

CHAPTER 06

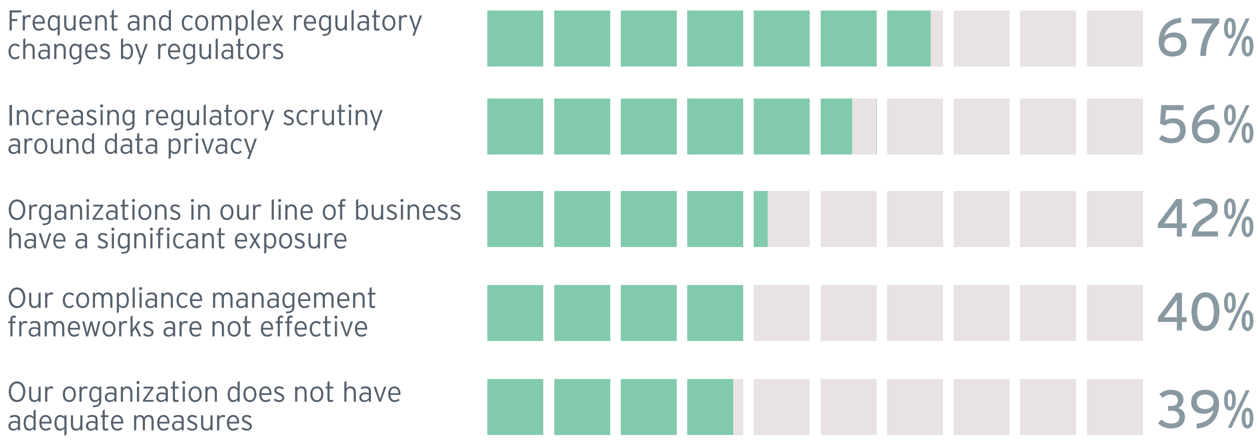
Regulatory and compliance risks

Reshaping business and governance requirements

Regulatory reform, expanding compliance scope and stronger enforcement across sectors are shaping the regulatory and governance risks in India. With changes in data protection rules, New Labour Codes, ESG disclosure requirements, tax administration, competition law and sector-specific regulations, operational frameworks and governance expectations are evolving. Regulators are relying more on digital reporting, automated scrutiny and real-time monitoring to reduce interpretations or delayed compliance. At the same time, compliance and monitoring expectations on senior management are increasing, with greater accountability for risk oversight, disclosures, third-party conduct and internal controls.

Indian organizations are navigating system upgrades, documentation requirements, audits and specialist legal and risk resources. Planning cycles, decision-making and execution effectiveness have to keep pace, particularly for firms operating across multiple states or regulated sectors. Weak governance structures, limited board engagement, or poor visibility over vendors and contractors heighten exposure to regulatory action and reputational damage. For listed companies, specifically in regulated sectors, governance lapses can affect investor confidence and access to capital. As enforcement becomes faster and more data-driven, regulatory and governance risks are increasingly influencing business continuity, growth priorities and long-term credibility in the Indian market.

Regulatory and compliance risks



Percentage of respondents agreeing to the above mentioned concern with respect to regulatory compliance risk themes

> Compliance and regulation risks worry CEOs and Boards for good reason: overlooked, they trigger steep fines, operational disruptions, and lasting damage to investor confidence. Strong governance turns these pitfalls into managed routines, safeguarding the business and preventing escalations.
>
> **Maya Ramachandran**
> Partner, EY India

Views on internal readiness remain mixed, with organizations continuing to evolve compliance frameworks to keep pace with regulatory change. Strengthening data privacy requirements such as India's Digital Personal Data Protection (DPDP) Act and global standards like the General Data Protection Regulation (GDPR) are elevating expectations around responsible data use and helping build a more transparent ecosystem. As technology, budget and resource capabilities gradually improve, it is vital that compliance and regulatory measures are viewed not as constraints but as enablers of transparency, resilience and sustainable growth.

The New Labour Codes standardize wages, introduce a national digital license, expand social security and strengthen online enforcement across establishments. These steps could lead to a rise in overall payroll costs and closer oversight on hiring temporary or contract workers. Organizations may require changes to internal control processes and stronger compliance reporting. There is also a growing need for regular monitoring, workplace safety checks and health assessments to meet regulatory requirements.

The survey shows that 67% of respondents agree or strongly agree regulatory changes need to be addressed. In addition, 56% highlight increased scrutiny around data privacy as a substantial risk. A further 42% point to exposure to improper conduct or unethical behavior, while 40% indicate that their compliance frameworks struggle to keep pace with regulatory shifts. Lastly, 39% note that gaps in technology, budget or resources limit their ability to manage compliance demands.

Business leaders should acknowledge that regulatory and compliance risk is a core business challenge and not a formality. Strong board oversight, disciplined controls and proactive compliance planning are essential to protect profitability, trust and long-term credibility.

Business imperative

New Labour Codes
Compliance and cost impact
New Labour Codes from November 2025 standardize wages, expand social security, and tighten digital enforcement. Businesses may see a change in payroll costs along with stricter compliance and workforce oversight.

Data privacy and protection
Expanding data privacy rules, including India's DPDP Act and global standards are pivotal, and demand for compliance and cost. With changes in data handling, need for security investment and high penalties, data protection is a board-level focus area as it affects trust and long-term viability.

Organizational key considerations for regulatory, compliance and governance risks

- Are regulatory ownership, escalation and accountability clearly defined with active board oversight?
- Are regulatory changes identified and monitored proactively to assess their impact across businesses, locations and functions?
- Are our controls, documentation and third-party oversight strong enough to withstand faster, data-driven enforcement?

CHAPTER 07

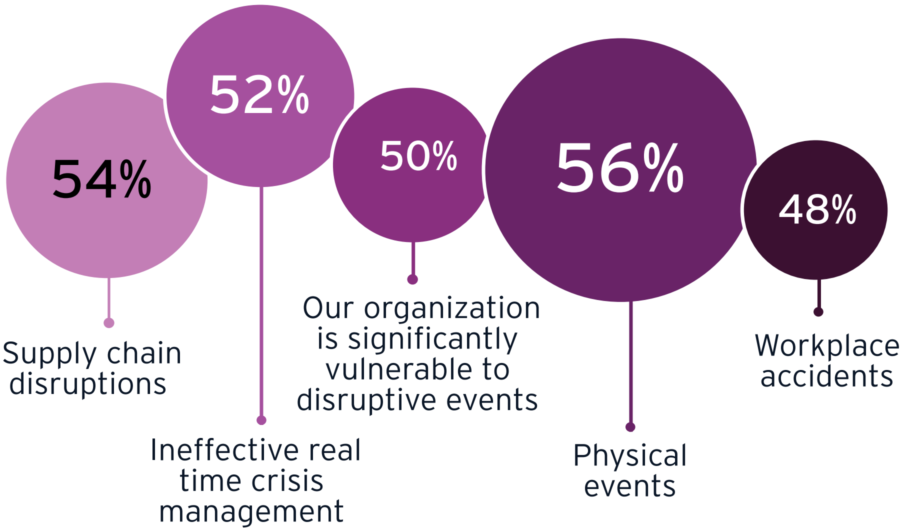
Operational and business continuity risks

Increasing pressure on continuity and resilience

In today's environment of constant disruption, operational resilience and business continuity have become fundamental to how organizations protect performance and earn stakeholder confidence. Businesses now face a wider and faster-moving set of risks, from physical events and supply chain shocks to technology outages and communication breakdowns, that can interrupt operations without warning. As leaders work to steer their organizations through this uncertainty, resilience is emerging as a defining capability to enable preparedness, respond with clarity and maintain momentum even when the unexpected strikes. It is now a strategic necessity over a defensive discipline.

The last few years have shown, with uncomfortable clarity, how quickly a single failure can cascade into widespread disruption. When the 2024 global IT outage, triggered by a faulty security update, brought many airlines, hospitals, ports and retailers to a standstill within hours, it exposed the deep interconnectedness and fragility of modern operations. Many organizations

Operational and business continuity risks



Percentage of respondents agreeing on growing concern of operational and business continuity risks

> In today's rapidly evolving and interconnected risk landscape, ERM enables organizations to take proactive measures; however, those with robust business continuity plans and strong crisis response mechanisms will maintain a distinct competitive edge.

Anil Mathew
President, Public Policy Advocacy and Chief Risk Officer, Hindalco Industries Limited

that had invested early in backup systems and isolation protocols, particularly in aviation and financial services, were able to restore services within the day. Several others took days to recover, facing mounting losses, customer grievances and, in some cases, regulatory scrutiny. Similarly, the Suez Canal blockage in 2021 and successive climate-induced floods in Asia disrupted supply chains worldwide, hitting sectors like electronics, pharmaceuticals and auto manufacturing the most. Companies with diversified supplier bases and flexible logistics models recovered faster, while those relying on single-source dependencies struggled for months.

Around the world, governments and regulators have responded decisively. Acts such as the EU's Digital Operational Resilience Act (DORA), the UK's stringent operational resilience requirements and Australia's CPS 230 have mandated impact tolerance thresholds, rigorous scenario testing and stronger third-party oversight, signaling to businesses worldwide that resilience is no longer optional. In India, a similar regulatory direction is evident through the Reserve Bank of India's Guidance Note on Operational Risk Management in 2024 , which aligns with Basel principles and requires regulated entities to define robust resilience practices[13].

Such developments indicate a clearly evolving strategic priority for business leaders: organizations that endure are those that anticipate strain, build capacity before it is tested and treat resilience as a core business capability. Ultimately, preparedness becomes the quiet advantage that separates businesses that merely cope from those that continue to lead.

13. Press Releases - Reserve Bank of India: https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=57818

Key considerations for board and management

- Which disruptions have the potential to materially affect long-term enterprise value and how clearly are strategic dependencies identified and managed?
- What level of organizational shock is acceptable in pursuit of strategic objectives and is this reflected in current governance and oversight arrangements?
- Are organizations strengthening resilience to address emerging risks, or do operating models remain oriented toward historical disruption patterns?

> Continuity risks arising from cyber threats, climate volatility, supply chains, and workforce challenges demand proactive leadership. Enterprises that anticipate disruption and invest in resilient systems and processes will not only protect value, but also strengthen trust and long-term growth.

Rituraj Mehta
Co-Chair, FICCI Committee on Corporate Security & DRR and Group Safety Head, Adani Group

Converging risks and performance

A shifting business outlook

Organizations are operating in a period of sustained disruption where multiple forces are reshaping how risk is experienced, managed and prioritized. Rather than emerging in isolation, today's risks are converging across technology, markets, regulation, geopolitics and the workforce, creating a more complex and tightly connected operating environment. As a result, shocks in one area increasingly spill over into others, amplifying business impact.

Digital dependence has pushed cyber risk to the forefront, turning security incidents into immediate threats to operations, customer trust and enterprise value. At the same time, rapidly shifting customer expectations are redefining competitiveness, forcing organizations to adapt products, services and delivery models at speed. Geopolitical uncertainty continues to influence trade dynamics and supply chains, while frequent regulatory change is increasing compliance intensity and execution risk.

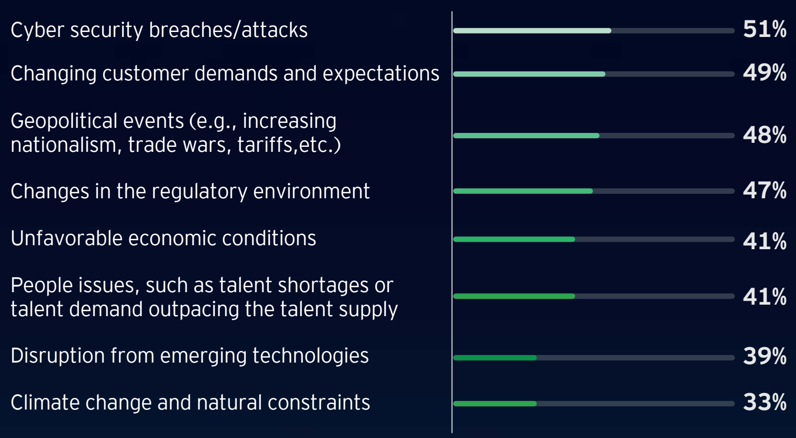
Economic conditions and workforce pressures add further strain. Skills shortages, reskilling challenges and talent availability are affecting productivity and growth plans, particularly as new technologies reshape roles and operating models. Emerging technologies themselves introduce disruption, requiring organizations to balance innovation with control and governance. Climate and resource constraints, once seen as longer-term concerns, are increasingly shaping resilience planning and strategic decisions.

Together, these dynamics signal a fundamental shift in the risk landscape. Managing risk now requires integrated, enterprise-wide approaches that connect strategy, operations and governance. Organizations that strengthen resilience, improve visibility across risks and align decision-making accordingly will be better positioned to navigate uncertainty and sustain performance.

The survey highlights a risk landscape dominated by cyber threats, shifting customer expectations and geopolitical uncertainty, closely followed by regulatory change. Economic pressure, workforce challenges and technology disruption continue to affect execution capability, while climate risk is emerging as a longer-term concern. Together, these risks demand integrated decision-making and stronger enterprise resilience.

The message for business leaders is that today's risk landscape is no longer dominated by a single threat. Cyber, regulatory, geopolitical, workforce and customer-related risks are converging to shape performance and resilience. Managing these interconnected risks requires integrated oversight, faster decision-making and stronger coordination across the enterprise to protect value, trust and long-term growth.

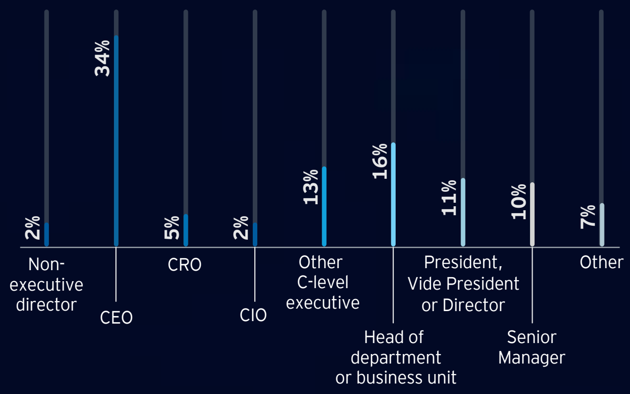
Top risks shaping organizational performance



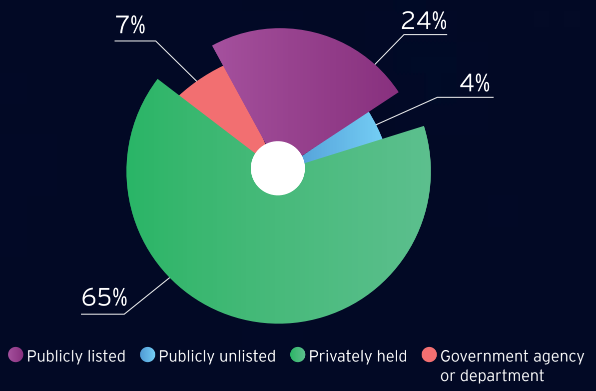
Methodology

This survey was conducted as a structured, web-based research exercise designed to capture perspectives on emerging risks and organizational readiness. Responses from 137 people were gathered from senior decision-makers across leadership, risk, finance and operational roles, representing a broad mix of industries and organizational sizes. Participants shared insights on their risk priorities, preparedness, governance practices and business decision-making. The survey covered a wide range of risk themes, including strategic, operational, regulatory, technology and people-related risks. Responses were compiled and analyzed centrally to maintain consistency and comparability. Findings reflect aggregated perceptions and experiences, providing directional insights into the evolving risk landscape rather than precise measurements.

Respondents by business area and function



Respondents by type of company



Respondents by industry

- 7%- Health
- 1%- Hospitality
- 2%- Insurance
- 1%- Life sciences
- 2%- Mining & metals
- 2%- Oil & gas
- 1%- Power & utilities
- 11%- Professional firms & services
- 2%- Retail
- 21%- Technology
- 1%- Telecommunications
- 6%- Government & public sector
- 2%- Consumer products
- 4%- Construction & engineering
- 2%- Banking & capital markets
- 3%- Automotive & transportation
- 6%- Agribusiness
- 7%- Advanced manufacturing
- 2%- Combining aerospace, chemicals and industrials
- 17%- Other

Acknowledgements

FICCI

Sumeet Gupta
Deputy Secretary General,
FICCI

Akhil Gupta
Director,
FICCI

Mainak Majumdar
Joint Director,
FICCI

Anjali Choudhary
Sr. Asst. Director,
FICCI

EY

Core team
Maya Ramchandran
Srikanth Potturi
Tushar V Shah
Aditya Iyer
Arun K Puppala

Brand, marketing & Communications
Jerin Verghese
Amrutha Anil

Editorial
Prosenjit Datta
Kartik Verma
Radhika KTP

Design
Sneha Arora

Our offices

Ahmedabad
22nd Floor, B Wing, Privilon
Ambli BRT Road, Behind Iskcon Temple
Off SG Highway
Ahmedabad - 380 059
Tel: + 91 79 6608 3800

Bengaluru
12th & 13th Floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground & 1st Floor
11, 'A' wing
Divyasree Chambers
Langford Town
Bengaluru - 560 025
Tel: + 91 80 6727 5000

3rd & 4th Floor
MARKSQUARE
#61, St. Mark's Road
Shantala Nagar
Bengaluru - 560 001
Tel: + 91 80 6727 5000

1st & 8th Floor, Tower A
Prestige Shantiniketan
Mahadevapura Post
Whitefield, Bengaluru - 560 048
Tel: + 91 80 6727 5000

Bhubaneswar
8th Floor, O-Hub, Tower A
Chandaka SEZ, Bhubaneswar
Odisha - 751024
Tel: + 91 674 274 4490

Chandigarh
Elante offices, Unit No. B-613 & 614
6th Floor, Plot No- 178-178A
Industrial & Business Park, Phase-I
Chandigarh - 160 002
Tel: + 91 172 6717800

Chennai
6th & 7th Floor, A Block,
Tidel Park, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100

Delhi NCR
Aikyam
Ground Floor
67, Institutional Area
Sector 44, Gurugram - 122 003
Haryana
Tel:+91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Gautam Budh Nagar, U.P.
Noida - 201 304
Tel: + 91 120 671 7000

Hyderabad
THE SKYVIEW 10
18th Floor, "SOUTH LOBBY"
Survey No 83/1, Raidurgam
Hyderabad - 500 032
Tel: + 91 40 6736 2000

Jaipur
9th floor, Jewel of India
Horizon Tower, JLN Marg
Opp Jaipur Stock Exchange
Jaipur, Rajasthan - 302018

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 433 4000

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

3rd Floor, Unit No 301
Building No. 1
Mindspace Airoli West (Gigaplex)
Located at Plot No. IT-5
MIDC Knowledge Corridor
Airoli (West)
Navi Mumbai - 400708
Tel: + 91 22 6192 0003

Altimus, 18th Floor Pandurang
Budhkar Marg Worli,
Mumbai - 400 018
Tel:+91 22 6192 0503

Pune
C-401, 4th Floor
Panchshil Tech Park, Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

10th Floor, Smartworks
M-Agile, Pan Card Club Road
Baner, Taluka Haveli
Pune - 411 045
Tel: + 91 20 4912 6800

Notes

Ernst & Young LLP

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at Ground Floor, Plot No. 67, Institutional Area, Sector - 44, Gurugram - 122 003, Haryana, India.

EYIN2602-005
ED None

SA1

ey.com/en_in

@EY_India   EY   EY India

EY Careers India   @ey_india

About FICCI

Established in 1927, FICCI is the largest and oldest apex business organisation in India. Its history is closely interwoven with India's struggle for independence, its industrialization, and its emergence as one of the most rapidly growing global economies. A non-government, not-for-profit organisation, FICCI is the voice of India's business and industry. From influencing policy to encouraging debate, engaging with policy makers and civil society, FICCI articulates the views and concerns of industry. It serves its members from the Indian private and public corporate sectors and multinational companies, drawing its strength from diverse regional chambers of commerce and industry across states, reaching out to over 2,50,000 companies. FICCI provides a platform for networking and consensus building within and across sectors and is the first port of call for Indian industry, policy makers and the international business community.

www.ficci.in

ficci_india   ficci   blog.ficci.com

ficciindia   ficci_india