ICICI Lombard

CORPORATE INDIA RISK INDEX

2024

Intelligence partner FROST & SULLIVAN

Navigating Risks, Powering India's Growth

SECTOR REPORT 2024

Aerospace & Defence

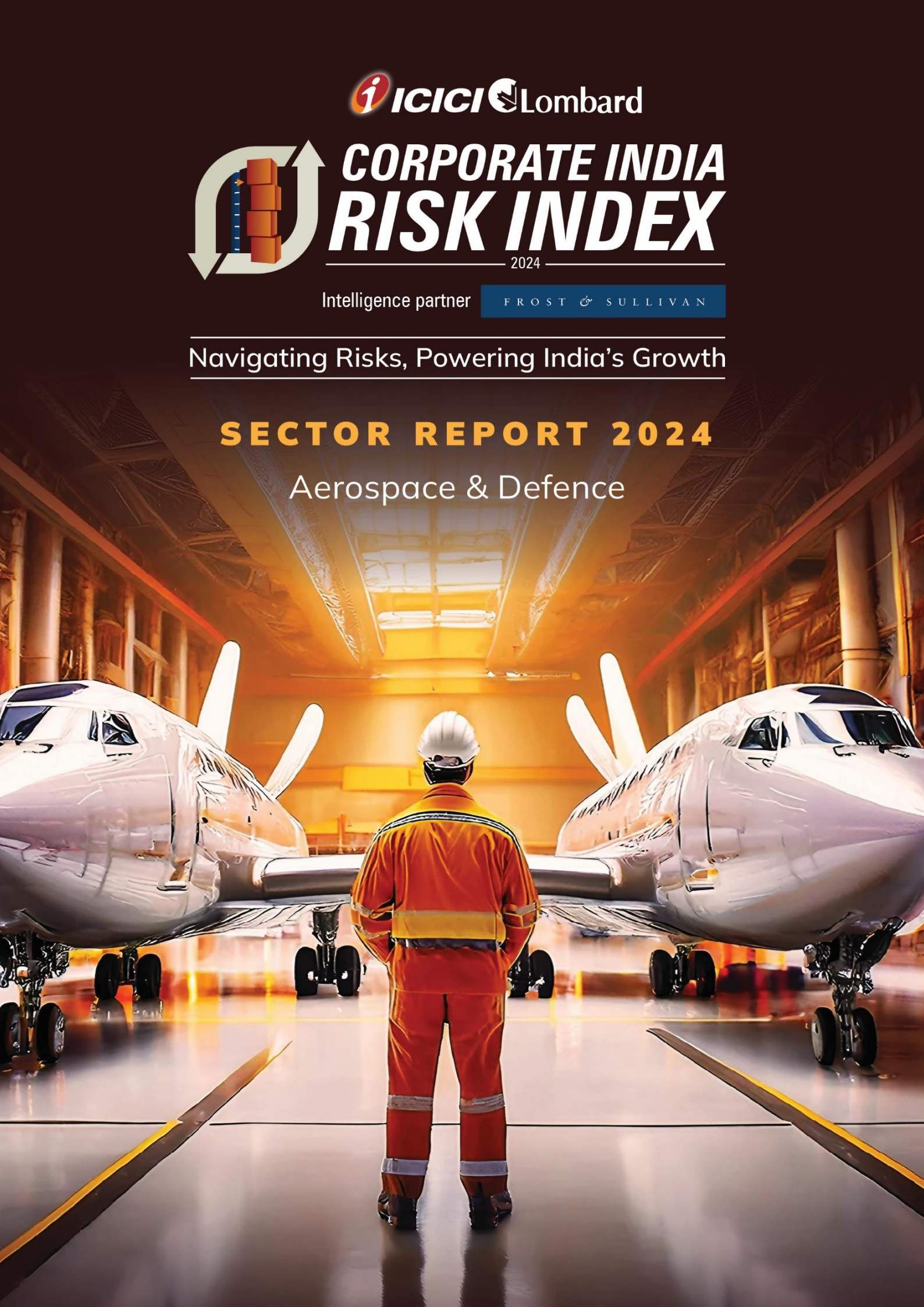


Table of Contents

Preface	3
Executive Summary	4
Introduction	5
Bottom-Up Risk Assessment Approach	10
Defining the Risk Scale	12
India - Resilient Growth and Superior Risk Management	12
India Showcasing an Optimized Risk Handling	17
Aerospace & Defence Sector Insights 2024	20
Aerospace & Defence Sector Risk Index 2024 Vs 2023	22
Key Highlights	23
ICICI LOMBARD: Key Solution Offerings	37
Bibliography	44

Preface

Corporate India Risk Index is primarily an academic exercise to understand the level of risk that companies are facing and also assist in developing a successful risk aversion plan, CIRI is a first-of-its-kind risk measurement tool to gauge the level of a company's risk exposure and preparedness. This Corporate risk comprises of various aspects of the business–spanning customer, competition, regulatory environment, business operations, technology finances, environmental factors etc. The impact of unprecedented events is significantly higher now.

This Index is a comprehensive framework that draws upon global risk management best practices and comprises of 32 risk elements across 6 broad dimensions. The Risk Index is based on the principles of Lean and Six Sigma that qualify business processes by measuring effectiveness and efficiency.

ICICI Lombard's Corporate India Risk Index provides a crucial tool for assessing and addressing risks, fostering resilience and adaptability in the ever-evolving global landscape. In the current climate of increasing macroeconomic uncertainties, it is essential for corporates to prioritize robust risk management. We believe that a proactive approach to risk management not only fortifies individual businesses but also contributes significantly to India's overall economic growth and stability.

Executive Summary

India's Aerospace and Defence sector faced a series of risks in 2024, driven primarily by global supply chain disruptions and geopolitical tensions. The ongoing Russia-Ukraine conflict and instability in the Middle East significantly impacted the availability of critical materials, leading to increased costs and extended lead times for specialized components. Additionally, rising cybersecurity threats targeting sensitive data and intellectual property posed substantial risks to national security and technological advancements, compelling companies to implement strong protective measures.

Financial challenges were exacerbated by currency volatility, with the depreciation of the Indian Rupee against the US Dollar squeezing profit margins for import-dependent manufacturers. Complex taxation structures, coupled with talent shortages in specialized engineering fields, particularly in advanced technology areas, further strained the sector. In response, companies adopted strategic risk management initiatives such as enhanced cybersecurity measures, sophisticated financial hedging strategies, and diversified supply chains. Furthermore, the sector accelerated efforts toward indigenization and sustainability, supported by government initiatives like the Defence Industrial Corridors.

Despite these challenges, the sector demonstrated resilience by leveraging opportunities for transformation. Digital technologies were integrated to boost operational efficiency, and sustainability became a key priority with the adoption of environmental standards. Strategic partnerships with international defence manufacturers and government programs like iDEX and the Technology Development Fund played a pivotal role in bridging technology gaps. These collective efforts not only mitigated immediate risks but also positioned the sector for long-term growth, reinforcing its trajectory toward future success.

Introduction

ICICI Lombard Corporate India Risk Index is a one of its kind, unified, credible, standardized corporate Risk Index that spans over the country level, the industry level, and the company level. The index has a comprehensive sector coverage. Aerospace and Defence, Agriculture and Food Processing, Automotive and Ancillary, BFSI, Biotech & Life sciences, Chemicals and Petrochemicals, Education Skill Development, Energy, FMCG, Healthcare Delivery, Infra and Realty, IT/ITES, Manufacturing, Media and Gaming, Metals and Mining, New Age & Startup, Pharmaceuticals, Telecom and Communication Technology, Tourism and Hospitality, Transportation and Logistics.

The impact is identified across key business risk (internal and external) under the following 'Strategic Risk Areas', The ICICI Lombard Corporate India Risk Index Framework comprises of 32 risk elements across 6 broad dimensions.

Market and Economic Risk

Corporate Risks arising due to market and economy related factors, such as internal or external political uncertainty, global slowdown, taxation-regulatory changes etc. Market and economy related risks are also identified as 'Systematic Risks', we have further classified the risks into below mentioned categories.

- **Inflation**: Inflation is the general increase in prices within the economy. The rising prices for businesses could result in bigger production spending and a fall in profitability. The companies should be attentive, acute, and responsive to changes in inflation to efficiently manage the prices of final products.
- **Taxation**: In a large democracy like India, complexity of multiple taxes (multiple taxes like GST, custom duties, central excise duty, etc.) is a major concern. The changing legislations, increased scrutiny by tax authorities and increasing public attention are together resulting in tax risks for organizations. There is, thus an increasing urgency for firms to manage their tax affairs efficiently to minimize tax risks.

- **Regulatory Risks**: Regulatory risk is the risk of changes in regulations and laws that might affect an industry or businesses. The regulatory changes can pertain to tariffs and trade policies, business laws pertaining to employment, minimum wage laws, financial regulation, Foreign Direct Investment etc.
- **Foreign Exchange Risk**: The exchange rate plays an important role for firms who export goods and import raw materials. The fluctuations in foreign exchange will have great impacts on the prices of traded goods. For example, if the currency depreciates (devaluation), the exporting firms will benefit. However, the firms importing raw materials will face higher costs on imports. The firms need to hedge their exposure to foreign exchange risks to insulate themselves from the impact from forex changes.
- **Geo-political Tension**: Geopolitical risk means the political and economic risks that are a potential threat to the financial and operational stability of companies.
- **Competitive risk**: Competitive risk is the risk associated with the fact that there are multiple companies competing in the market, each seeking to obtain the highest position and consumer ratings, to gain maximum benefits for themselves. The companies devise different strategies to garner a higher market share and acquire customers from competitors. Any failure in managing the competitive stand could lead to losses in business, thereby making marketing and competition a major risk in market.

Technology Risk

Technology risks are also identified as information technology related risks which may arise due to failure of any installed hardware or software system, spam, viruses or any malicious attack. Also delay/over/under adoption of trending disruptive technologies can lead to technology related risks. We have classified the risks in below mentioned categories.

- **Innovation Risk / Obsolete Technology**: Innovation is the key to success in all the industries. Risk of redundancy and losing out to competition on account of poor R&D is a major concern.
- **Intellectual Property risk:** Dependence on trade secrets and unpatented proprietary know-how.
- **Disruptive Technologies:** These will fundamentally alter the financial prospects of the industry.
- **Data Compromise:** Hardware failure refers to malfunctions within the electronic circuits or electromechanical components (disks, tapes) of a computer system; Software failure refers to an operating system crash. Such failures lead to stoppage of entire computer or operating systems creating substantial losses to business.

Operational and Physical Risk

Risk of losses caused due to faulty or failed processes, systems or human resource related inefficiencies are classified as operational and physical risks. We have classified Operational & Physical risks in below mentioned categories.

- **Critical Infrastructure Failure / Machine Breakdown:** Industries with a heavy dependence on machinery consider any rise in machinery breakdowns a hindrance to their businesses operations. An untimely equipment breakdown can bring businesses to a standstill or be the root cause for fires and explosions. Mostly, human errors and deferred maintenances are the major reasons for such breakdowns. The companies should actively invest in timely maintenance of all machineries.
- **Business Continuity / Sustainability:** Non adoption of Business Continuity/ Sustainability Plans and Lack of Internal Control tools would result in: Failure of businesses, Brand Equity / Loss of reputation, Financial Loss, Business model Failure, Ineffective engagement/communication with stakeholders, Losses in productivity, Lack of opportunity monitoring.
- **Supply chain risk:** Raw Material unavailability and Heavy Dependence on Global Supply Chains / Supplier concentration risk. Unavailability of raw materials owing to disruption in the supply chain or heavy dependency on one source (company/country) which is unable to supply owing to some geo- political tensions, fires, or any other incidents. Transportation is one of the key activities for companies making it an important risk to mitigate. The loss of goods in transit and spillage is one of the major concerns as it accounts for a sizeable loss of revenue to companies.
- **Commodity Price Risk - Volatility in prices of raw materials:** The fluctuations in raw material prices creating a margin pressure / top-line pressure in the scenario of rising input costs.
- **Portfolio Risk:** Loss of key customers, Customer concentration - Key customers accounting for a larger share of revenue, Over-dependence on suppliers, Business Model Risk: Transformative changes in business model, Tail Risks: Ability to overcome or manage extreme worst-case scenarios.
- **Environmental Hazard Risk:** Any environmental hazard having the potential to affect the surrounding environment.
- **Workplace Accident:** Fire and Explosion Hazards, Containment Incidents, Workplace Injuries
- **Human Resource:** Key person risk: This risk occurs when a business or business unit becomes heavily reliant on a key individual. Talent acquisition and retention - The companies require a highly skilled labor force for R&D as well as continuous production. Accessing skilled resources and expertise on an on-going basis is one of the major challenges; moreover, retention of trained staff is imperative. Labor shortages, Union Strikes & Industrial Actions, Employee

health, safety, and security (SHE/Sustainability risk).

- **Financial Risk:** Financial Reporting Risk: Material misstatement of Financial Statements, whether due to fraud or error. Interest rates and equity prices: Interest rate risk arising out of working capital borrowings at variable rates. Equity price fluctuations affect the Company's income or the value of its holdings of financial instruments. Liquidity Risk (Credit Risk / Receivables).
- **Breaches of law (local/ international):** Voluntary/ involuntary breaches of law can lead to costly lawsuits.

Crime & Security Risk

Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations. These attacks can cause major financial losses, reputational harm, and a loss of client trust. Regarding cybersecurity, the BFSI industry in India has several difficulties, including difficult-to-secure legacy systems, a shortage of qualified cybersecurity personnel, and the requirement for ongoing system and network monitoring. There is a significant investment in cybersecurity tools like network monitoring, endpoint security, access control, and threat intelligence. Many organizations are also implementing cutting-edge technology like artificial intelligence and machine learning to strengthen their security posture.

We have classified Crime & Security risks in below mentioned categories.

- **Cyber Crimes:** Data Theft, Spam, scams and phishing, Hacking, Malwares and Viruses, Piracy, Fraud, Corruption, Malicious attacks
- **Counterfeiting:** Counterfeiting of goods/services leads to loss of revenues, profits and ultimately affects the brand equity
- Threat to Women Security
- **Terrorism:** Un-lawful use of violence and intimidation, especially against civilians, in the pursuit of political aims.

Natural Hazard Risk

A natural hazard is the threat of an event that will likely have a negative impact. A natural disaster is the negative impact following an actual occurrence of natural hazard if it significantly harms a community. Due to India's geographical structure, it is one of the most disaster-prone countries in the world. Natural hazards like floods, earthquakes, landslides, and cyclones are common risks faced by India. The situation has worsened due to rise in GHG emissions, loss of biodiversity, deforestation, and degradation of environment. Natural disasters hamper the day-to-day

operations of corporates, and it is important for them to understand that such risks cannot go unheeded. Over the years, Indian corporates have learnt to mitigate such risks by diversifying their supply chains, having multiple logistics partners, diversified geographical presence and multiple vendors.

- **Pandemic and other global epidemic diseases:** Risk to business owing to disruptions caused by global pandemic scale events like the COVID-19 pandemic

Strategic Risk

Strategic risk is the risk of undesirable outcomes of business decisions which may impact a company. Strategic risk is often a major factor in determining a company's worth, particularly observable if the company experiences a sharp decline in a short period of time. Several factors, such as unethical or unlawful activities, poor customer service, product recalls, data breaches, or unfavorable media coverage, can lead to strategic risk. An organization's reputation can be severely harmed by a single negative incident, such as a high- profile data breach or fraud scandal, resulting in a loss of clients, income, and market share.

- **Resource scarcity / Misutilization / Overall Utilization:** Difficulties in acquisition of land, water, fuel, or other resources for operations of business.
- **Public Sentiment:** Current events playing out in the public scene can change the public sentiment.
- **Delay in execution of projects:** Delays in execution of projects can surge in the capex.
- **Increased number of recalls and quality audits:** Impacts both the brand equity and increased operational expenses.
- **Failed / Hostile Mergers & Acquisitions:** High dependence on inorganic growth.

Bottom-Up Risk Assessment Approach

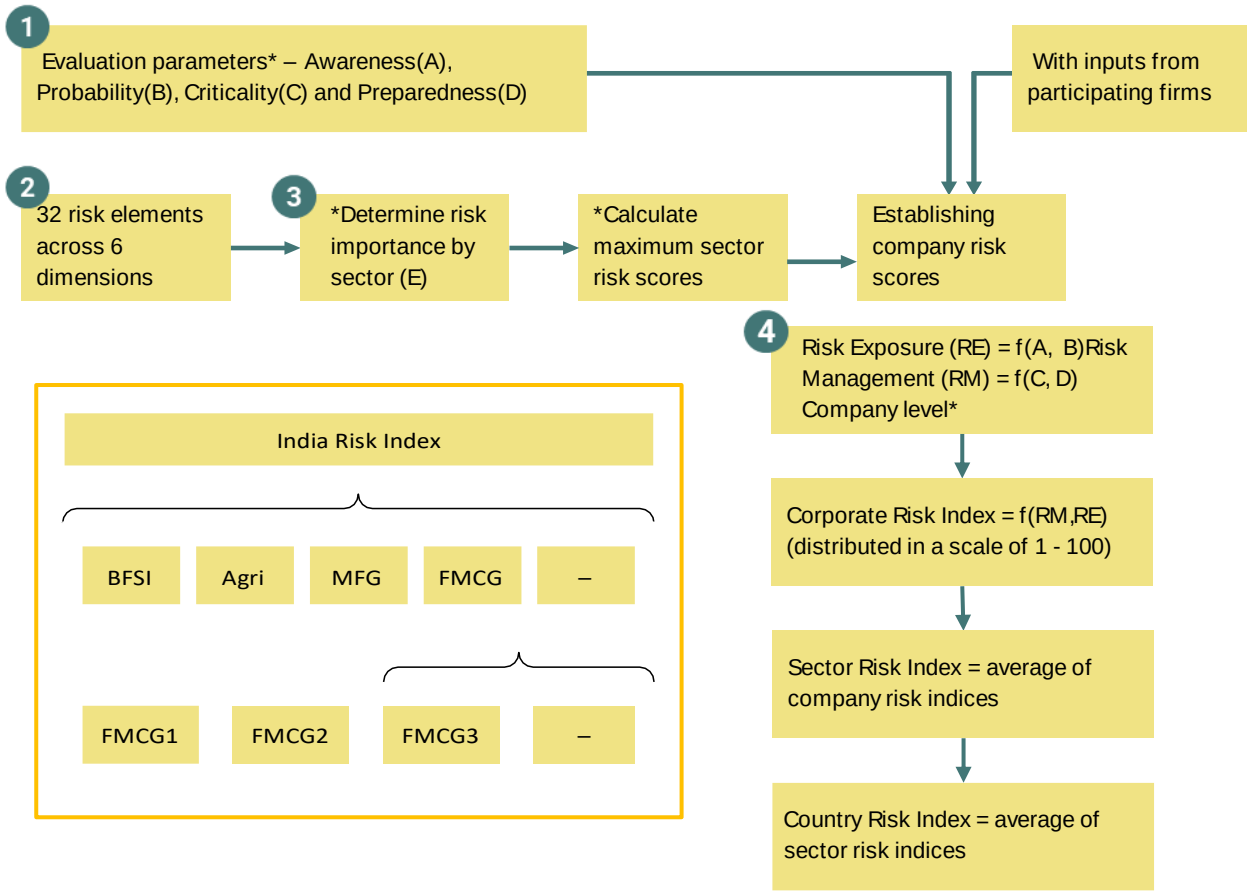


Figure 1: Risk Assessment Approach

1. **Evaluation Parameters*:** The index maps the risks faced by any enterprise basis of Awareness, Probability, Criticality and Preparedness against the defined Risk elements. The evaluation Parameters are defined as:

- Awareness - Level of awareness of potential risk affecting the firm.
- Probability - Likelihood of risk to affect the business goals of the firm adversely.
- Criticality - Level of impact of the identified risk on the success of business goals.
- Preparedness - Risk handling practices/ mechanisms already in place to handle the risk.

2. **Determining Risk Importance*:** Importance/Impact of individual risk element is established against individual sector based on the published corporate risk reports, in depth sector

understanding by F&S team and SMEs.

3. **Calculating Maximum Sector Risk Score**: Weighted Sum of all risk elements based on their importance to the respective sector.

4. **Company Level*:** All the Risk Index scores for companies in a sector are averaged to represent the sector; and sectors average to India. Risk Exposure is defined as the function of corporate's Risk Awareness and Probability of risk occurrence. Risk Management is defined as the function of an enterprise risk preparedness and criticality risk impact assessment.

Defining the Risk Scale

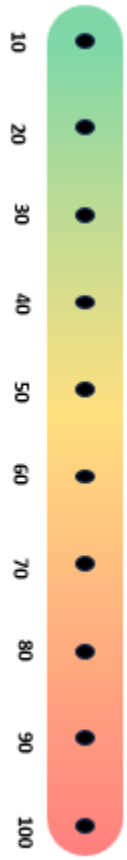
We have selected 20 sectors to understand the current stand of our country today in terms of risk. Risk for various sectors is measured on the risk exposure scale and risk management scale.

A. ICICI Lombard Corporate Risk Exposure – Scale

Risk Exposure: The impact of any internal, external or strategic occurrence on the financial performance of an organization is defined as the corporate risk exposure.

Risk has traditionally been seen as something to be avoided – with the belief that if behavior is risky, it's not something a business should pursue. But the very nature of business is to take risks to attain growth. Risk can be a creator of value and can play a unique role in driving business performance.

Let's look at the risk exposure scale.



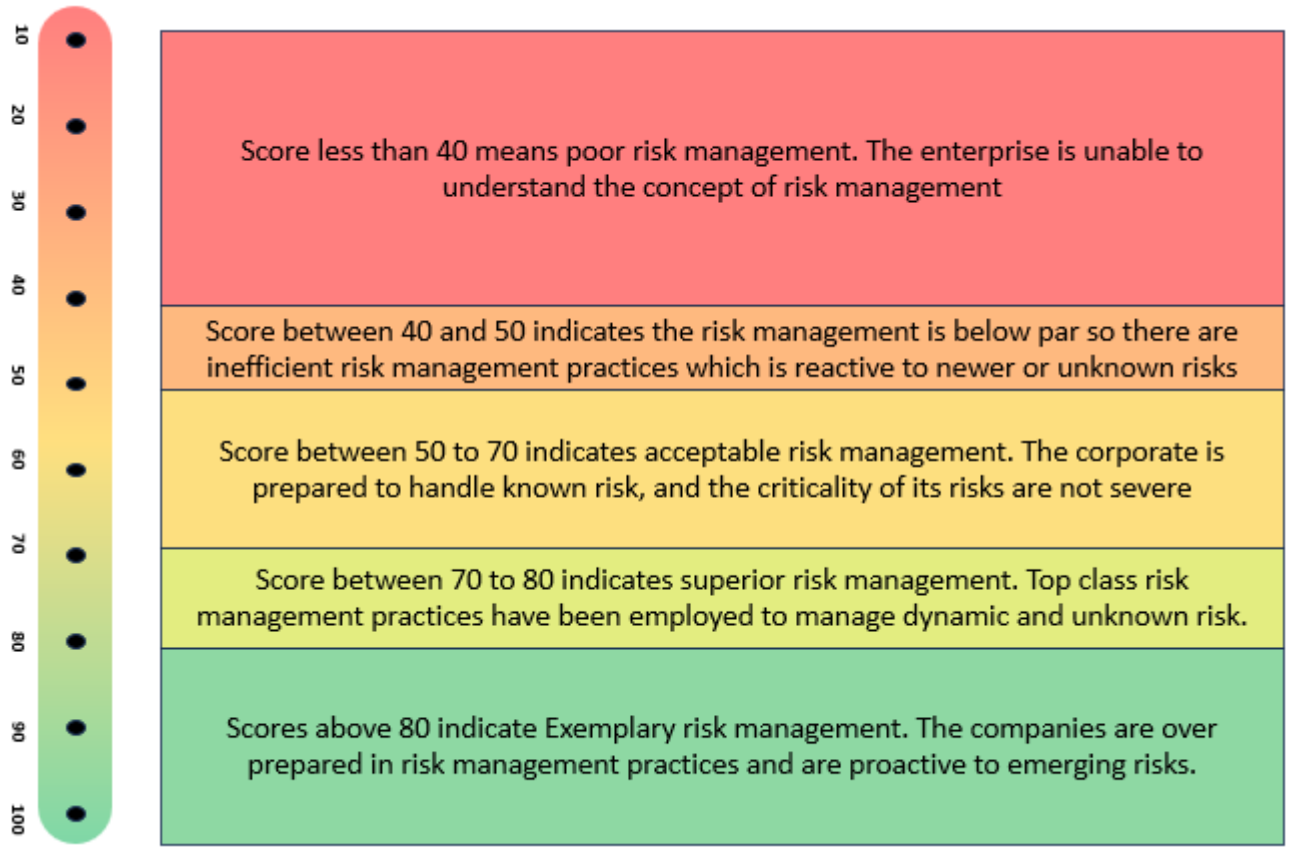
Score: If less than 30 means there is very low risk exposure, and the sector has minimal exposure to overall risk
Score between 30 to 50 indicates low risk exposure and its risk exposure is within acceptable or tolerable limits
Score between 50 to 60 indicates moderate exposure indicating corporate can balance the impact of overall risks up to a certain extent
Score between 60 to 80 indicates high risk exposure and its impact is very high in the industry in which the corporate operates
Score greater than 80 indicates very high-risk exposure. The corporate is unable to foresee risk incidents and probability of occurrence of these incidents may be extremely high

B. ICICI Lombard Corporate Risk Management – Scale

Risk Management: Identification, Evaluation and Prioritization of corporate risks followed by well- coordinated steps to minimize the occurrence of uncertainties in the foreseeable future is defined as the Corporate Risk Management.

The risk management scale works in the opposite to that of the risk exposure scale.

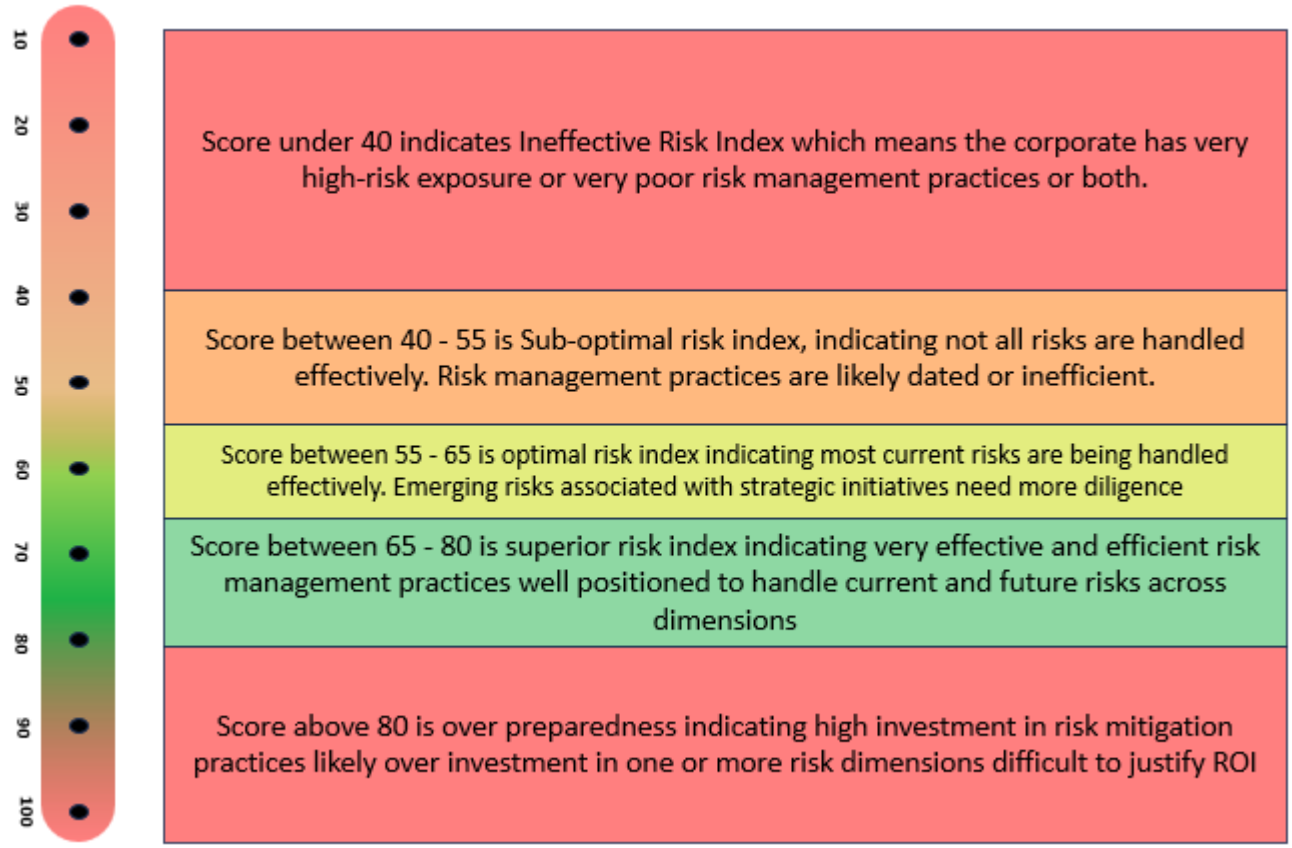
Let's look at the risk management scale.



c. ICICI Lombard Corporate Risk Index – Scale

Risk Index: Risk Index is a measurement tool to gauge the level of Risk Exposure against Risk Preparedness. The score intends to give companies/Sector/Country access to an extensive and quantifiable metrics of risk management.

Let's look at the risk Index scale.



India - Resilient Growth and Superior Risk Management

In 2024, India's diverse sectors demonstrated significant growth and resilience, leveraging technological advancements, strategic reforms, and proactive risk management to navigate an evolving economic landscape. Despite global challenges, industries embraced innovation, digital transformation, and sustainable practices, positioning themselves for long-term success.

In this year, the integration of Artificial Intelligence (AI) across various sectors presented both significant opportunities and risks. While AI-driven innovations enhanced productivity, decision-making, and customer engagement, the adoption also raised concerns around data privacy, cybersecurity, and workforce displacement. India navigated these risks by implementing robust data protection regulations and promoting AI ethics in the development and deployment of technology. Additionally, the government and private sector invested in reskilling programs, ensuring the workforce was equipped to adapt to the evolving digital landscape. AI's strategic implementation across sectors like BFSI, healthcare, and manufacturing helped India enhance operational efficiency while balancing the challenges posed by rapid technological transformation.

The Aerospace & Defence sector saw substantial advancements as India attracted global aerospace companies seeking to strengthen supply chains. Local firms expanded their capabilities, particularly in the growing private space sector, driving both revenue growth and global competitiveness. The Agri & Food Processing sector turned to precision farming and AI-driven analytics to enhance productivity, while renewable energy solutions like solar-powered cold storage reduced post-harvest losses, improving sustainability and efficiency.

In the Automotive sector, the shift toward electric vehicles (EVs) gained momentum, supported by government schemes aimed at promoting EV adoption. Major manufacturers expanded their EV portfolios, addressing both sustainability goals and evolving consumer demands. The BFSI sector continued its digital transformation, with AI integration enhancing fraud detection and compliance, further improving security and efficiency.

The Biotech & Lifesciences sector experienced accelerated growth, particularly in genomics and vaccine development, with India solidifying its role as a global leader in pharmaceutical manufacturing. The sector's innovation, supported by public and private investments, enhanced healthcare technology and medical devices. In Chemicals & Petrochemicals, India attracted significant investments to meet rising demand, driven by growing consumption from its expanding middle class, while the Education sector embraced AI and digital learning platforms, expanding access to quality education and equipping the workforce for future demands in emerging technologies.

The Energy sector made substantial progress towards sustainability, with a focus on renewable

energy, including ultra-mega solar parks and offshore wind projects. These initiatives were supported by favorable government policies and decreasing costs of clean energy technologies. The FMCG sector adapted to inflationary pressures by shifting focus towards premium products and e-commerce platforms, which were increasingly driving sales, particularly in rural markets.

In Healthcare, there was significant growth fueled by digital innovations such as telemedicine and AI-driven diagnostics, which helped improve access and efficiency in healthcare delivery. India also continued to strengthen its position as a global hub for medical tourism, offering competitive treatment options. The Real Estate sector benefitted from increased demand in affordable housing and infrastructure development, with commercial real estate seeing steady growth and an emphasis on sustainable building practices.

The IT sector continued to thrive despite global challenges, driven by demand for cloud services, cybersecurity solutions, and AI technologies. Tier 2 and 3 cities emerged as new tech hubs, with government support enhancing regional tech expansion. The Pharmaceutical sector saw an uptick in exports and domestic manufacturing, with reduced dependence on imports and new product launches in global markets bolstering its growth. In Manufacturing, India focused on boosting production through initiatives like the Production-Linked Incentive schemes, especially in electronics and EV manufacturing, which also contributed to job creation and supply chain resilience. The "China + 1" strategy adopted by global firms has played a pivotal role in shaping India's manufacturing sector. While it has increased risk exposure, it has also driven companies to invest in more sophisticated, globally relevant risk management practices, strengthening the sector's resilience and positioning India as a key player in global supply chains.

Media & Entertainment saw continued growth, with OTT platforms gaining popularity, especially in regional content. The Gaming industry also flourished, becoming a key revenue generator as mobile gaming gained dominance. In Steel and Mining, investments in decarbonization and digitalization allowed the sectors to reduce environmental impact and enhance operational efficiency. Startups saw substantial funding despite global slowdowns, with SaaS, fintech, and D2C brands leading the charge in innovation and market expansion.

The Telecom sector expanded 5G coverage and rural internet penetration, narrowing the digital divide and improving connectivity across the country. The Tourism & Hospitality sector rebounded strongly, attracting both domestic and international visitors, with eco-conscious travelers opting for sustainable tourism options and luxury experiences. Finally, the Logistics sector benefited from advancements in automation and multimodal connectivity, reducing costs and improving efficiency, while the government's National Logistics Policy streamlined operations, cutting transit times and enhancing cross-sector integration.

In summary, 2024 saw India's sectors display resilience and adaptability, addressing emerging risks through innovation, digital adoption, and sustainability initiatives. The country's ongoing focus on risk management, technological advancement, and strategic reforms has positioned its economy for continued growth and transformation, paving the way for India to solidify its place as a global economic leader.

India Showcasing an Optimized Risk Handling

Figure 2: Corporate India Risk Index 2024

A score of 65 on the Corporate Risk Index indicates optimal handling of risk by the Indian companies. In 2024, India faced significant market, economy, and operational risks across various sectors, highlighting areas for improvement in the coming years. The year was further complicated by global events such as the ongoing Israel-Palestine conflict, which led to geopolitical instability and fluctuations in global oil prices. The rise of recession fears in major economies like the United States and Europe disrupted supply chains and created demand uncertainties, impacting Indian exports and manufacturing. Investor sentiment in India remains flat in 2024, reflecting the cautious behavior of Angel and VC investors globally. This persistent challenge, which has carried over from 2023, highlights ongoing risks in the market and underscores the uncertainty that continues to affect investment decisions in the country.

Additionally, India's national elections increased risk exposure, with political uncertainty and policy shifts potentially affecting business operations, investor confidence, and sectoral reforms. These global and domestic challenges underscored the need for stronger risk management

frameworks and adaptive strategies across India's industries to navigate future uncertainties effectively.

In response to the heightened risks in 2024, companies across India have increasingly focused on strengthening their risk management frameworks. With the backdrop of global uncertainties, such as geopolitical conflicts and economic slowdowns, alongside domestic challenges like the national elections, businesses have prioritized proactive risk identification, mitigation strategies, and resilience-building measures. This shift reflects a broader trend of embedding risk management into corporate strategy, with an emphasis on agility, digital transformation, and sustainability.

As a result, sectoral risk indices have remained within the superior and optimal risk index range, demonstrating that most industries in India have effectively managed the challenges they faced. Through a combination of technological innovations, regulatory compliance, and strategic planning, sectors have been able to maintain stability and navigate both internal and external risks. This disciplined approach to risk management has ensured that, despite various pressures, India's sectors remained well-positioned for sustainable growth and continued progress in 2024.

Below is a broader categorization of sectors in terms of risk index:

Figure 3: Corporate India Risk Index 2024 Sector Score

Superior Risk Index

Superior risk handling was found in nine industrial sectors:, Pharmaceuticals, Healthcare Delivery, Automotive & Ancillary, Manufacturing, Metals & Mining, Telecom & Communication, BFSI, Tourism & Hospitality, and Transportation & Logistics.

Optimal Risk Index

Optimal risk handling was found in 11 industrial sectors: Media & Gaming, FMCG, Infra & Realty, Agriculture & Food processing, Biotech & Lifesciences, IT ITES, Energy, New Age & Startup, Aerospace & Defence, Chemicals & Petrochemicals and Education & Skill Development.

Aerospace & Defence Sector Insights 2024

The aerospace and defence industry in India represents a vital strategic sector of the nation's economy. This sector encompasses a diverse range of activities, including aircraft manufacturing, defence equipment production, space exploration, and associated maintenance, repair, and overhaul (MRO) services. With over 45,000 components and subsystems being manufactured domestically, the sector has become increasingly self-reliant while serving as a critical supplier to both civil aviation and military defence needs. India's strategic position in South Asia and its growing technological capabilities have positioned it advantageously in the global aerospace and defence landscape. The sector currently employs more than 200,000 skilled professionals and contributes significantly to India's technological advancement and national security objectives.

The sector witnessed unprecedented investment momentum in 2024, with defence projects worth approximately INR 1.1 Lakh Crores under implementation and future projects valued at nearly INR 4.5 Lakh Crores in various stages of planning and approval. The Ministry of Defence (MoD) and Department of Defence Production are actively pursuing the 'Make in India' initiative for defence manufacturing, creating a conducive environment for both domestic and international investors. The 'Atmanirbhar Bharat' mission in defence has been reinforced through the implementation of the Defence Production and Export Promotion Policy (DPEPP) with sub-schemes focusing on (i) Innovation and R&D in Defence Technologies; (ii) the Defence Testing Infrastructure Scheme; and (iii) the Defence Industrial Corridors in Tamil Nadu and Uttar Pradesh.

The industry faces complex challenges stemming from global supply chain disruptions, technological obsolescence risks, and increasing compliance requirements with international arms control regulations. The fluctuation of the Indian rupee against major currencies has introduced additional cost pressures, particularly affecting imported specialized components and technologies that remain essential for advanced defence systems. Currency volatility has amplified procurement expenses, thereby impacting production costs across the sector. Policy initiatives like the Defence Acquisition Procedure (DAP) 2020 and its subsequent amendments have been implemented to reduce import dependence and strengthen indigenous capabilities in defence manufacturing.

Geopolitical tensions across multiple regions, including the ongoing conflicts in Ukraine and the Middle East, have reverberated throughout India's aerospace and defence sector, leading to accelerated defence modernization programs, increased defence budgets, and shifts in strategic partnerships. These developments highlight the intricate relationship between international

security dynamics and domestic defence industrial priorities.

The Directorate General of Quality Assurance (DGQA) and the Center for Military Airworthiness and Certification (CEMILAC) have intensified quality standards enforcement for aerospace and defence products to ensure operational reliability, combat effectiveness, and personnel safety. In 2024, 18 new Technical Standards Orders (TSOs) have been implemented to regulate product quality and align with global aerospace standards. These regulatory measures aim to enhance safety and reliability while requiring manufacturing enterprises to comply with specified standards and certification processes.

The increasing demand for aerospace and defence products will grow, driven by military modernization programs, expansion of civil aviation, and growing space exploration activities.

In conclusion, despite navigating supply chain vulnerabilities, geopolitical uncertainties, technology transfer restrictions, and currency fluctuations, the aerospace and defence industry in India demonstrates remarkable resilience and growth potential. Supported by governmental policy initiatives and increasing global recognition of Indian manufacturing capabilities, this sector is positioned to achieve sustainable growth while enhancing national security and economic prosperity.

Aerospace & Defence Sector Risk Index 2024 Vs 2023

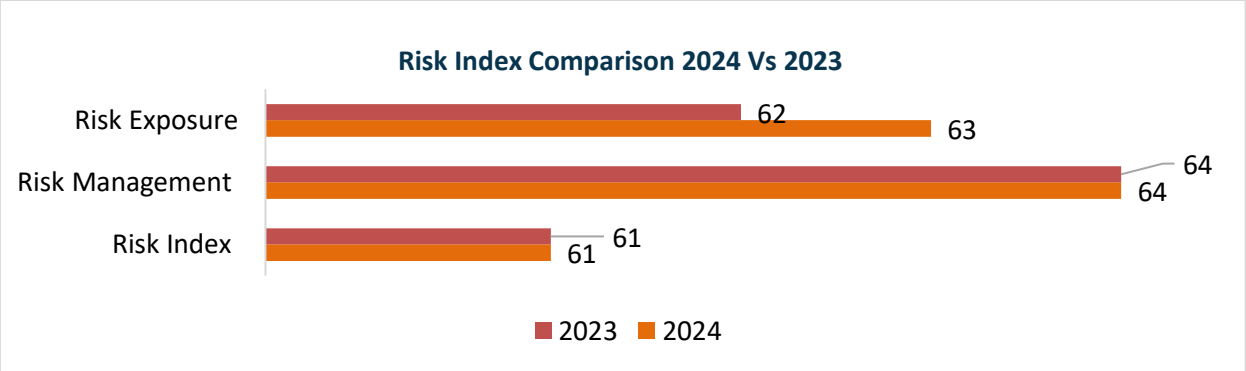


Figure 4: Detailed Comparative Analysis 2024 Vs. 2023

Aerospace & Defence Sector Risk Index 2024 Vs 2023

The overall Risk Index for Aerospace & Defence sector has remained stable at 61 in 2024, owing to an increase in the risk exposure which met by a constant focus on risk management.

Aerospace & Defence Sector Risk Exposure 2024 Vs 2023

In the aerospace and defence sector, the increase in risk exposure in 2024 can be attributed to several key factors. Geopolitical tensions, such as the Russia-Ukraine conflict and ongoing instability in other regions, heightened uncertainties for defence contractors, disrupting global supply chains and increasing the volatility of material costs and lead times for specialized components. Additionally, currency volatility, particularly the depreciation of the Indian Rupee, placed further pressure on import-dependent manufacturers, squeezing profit margins. These external factors, combined with challenges related to regulatory complexities, talent shortages, and cybersecurity threats to sensitive intellectual property, significantly raised the risk exposure for the sector.

Aerospace & Defence Sector Risk Management 2024 Vs 2023

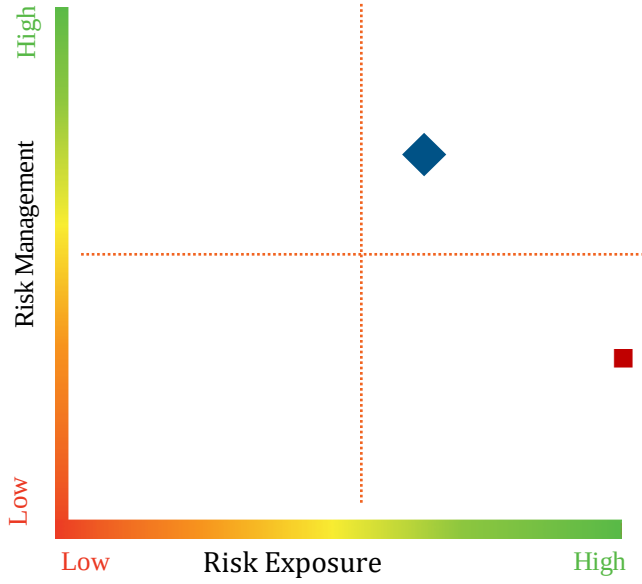
Companies in the aerospace and defence industry continued to implement robust risk mitigation strategies that had been effective in the past, such as strengthening cyber defence protocols through air-gapped networks, zero-trust architectures, and multi-layered security measures. They also maintained hedging strategies to address financial risks arising from currency fluctuations and continued their efforts to diversify supply chains and increase indigenization of critical components, supported by government initiatives. While these measures were essential in managing risks, the increased exposure to external threats and market uncertainties necessitated more proactive and responsive risk management approaches.

Key Highlights

Risk Dimension Analysis: Market and Economy

Risk Exposure Score: 69

Risk Management Score: 66



Inflation

- In 2024, the aerospace and defence industry experienced significant cost pressures due to global inflation in critical raw materials, including titanium, aluminum alloys, and specialty electronics components. The combined effect of supply constraints and demand recovery post-pandemic contributed to price volatility across the manufacturing value chain
- The ongoing conflicts in Ukraine and the Middle East disrupted global supply chains for strategic materials, leading to an increase in component costs for Indian defence manufacturers. Higher energy costs directly translated to increased production expenses for precision manufacturing processes
- Escalating tensions in the Indo-Pacific region could potentially disrupt semiconductor supply chains. A surge in electronic component prices could affect advanced systems development and may lead to extended project timelines and budget overruns
- India is navigating the challenges of establishing domestic manufacturing capabilities for critical defence components, including aero-engines, radar systems, and avionics. New defence manufacturing corridors in Tamil Nadu and Uttar Pradesh are gaining momentum but face price competition from established global suppliers

Taxation Risk

- The aerospace and defence industry in India faces significant tax challenges with GST rates at 18% for most defence-related components and subsystems, while finished platforms attract a higher 28% GST rate, creating financial pressure particularly on smaller suppliers. A complex

tariff structure exists with duties ranging from 5-15% on imported aerospace components, affecting cost competitiveness in the global market.

- Industry stakeholders have advocated for a rationalized import duty structure with incentives for value addition within India. The 2024-25 Union Budget allocated Rs. 6.21 lakh crore (US$ 74.9 billion) to defence, with Rs. 1.72 lakh crore (US$ 20.7 billion) specifically earmarked for defence modernization and domestic procurement, demonstrating substantial financial commitment alongside tax policy adjustments to support sector development.

Geopolitical Risks

- The protracted conflict between Russia and Ukraine has created significant challenges for India's defence modernization programs, particularly for platforms and systems of Russian origin. Supply constraints for critical spares and maintenance support posed operational readiness risks for the Indian armed forces
- These factors, including the United States' CAATSA sanctions implications, led to accelerated diversification of defence procurement sources and intensified efforts toward indigenous development of critical technologies
- Regional tensions along India's northern and western borders contributed to increased defence spending and accelerated procurement timelines
- Higher global defence budgets resulting from geopolitical tensions have intensified competition for limited production capacity among global defence manufacturers, potentially affecting delivery schedules and pricing
- India's aerospace and defence industry is experiencing an annual growth rate of approximately 15%, presenting significant opportunities for both domestic manufacturers and strategic international partnerships. Western nations' growing willingness to share advanced technologies with India and global defence companies establishing manufacturing facilities in India are reshaping the industry landscape, making India an increasingly important hub in global defence supply chain.

Foreign Exchange Risk

- The Indian Rupee experienced moderate fluctuations against the US Dollar, with the Rupee depreciating by 4.2% year-to-date in 2024
- Global defence contractors faced margin pressures throughout 2024 due to foreign currency volatility and increasing offset obligations. The uncertain geopolitical landscape added further complexity to long-term contract pricing, impacting trade dynamics and potentially affecting foreign exchange exposure
- India witnessed a significant increase in aircraft component imports, with avionics systems imports rising by 28% year-on-year and aircraft engine parts increasing by 42%
- Aggressive pricing strategies by international OEMs seeking entry into the Indian market and sluggish execution of major defence programs negatively impacted domestic companies in the

industry

- The implementation of mandatory certification from the Center for Military Airworthiness and Certification (CEMILAC) for aerospace components aimed to ensure quality and safety standards while promoting indigenous development. This regulatory measure could impact foreign exchange outflows by influencing import volumes and promoting domestic value addition
- India's current trade deficit in the aerospace and defence sector is expected to decrease gradually by 2030. While imports will continue for critical technologies, increasing domestic manufacturing capabilities and rising defence exports are projected to improve the trade balance, with the unmanned systems and MRO segments expected to become net exporters by 2030

Regulatory Risk

- India's aerospace and defence sector is navigating through significant regulatory changes with the implementation of the Defence Production and Export Promotion Policy (DPEPP) and simplified industrial licensing processes. Companies must now comply with mandatory AS9100 quality management standards for all aerospace manufacturers supplying to defence and civil aviation sectors, effective September 1, 2024.
- Additional certification requirements from the Center for Military Airworthiness and Certification (CEMILAC) for aerospace components add complexity to the regulatory landscape. The Directorate General of Quality Assurance has intensified enforcement with 18 new Technical Standards Orders in 2024 to align with global aerospace standards.
- India's aerospace and defence industry is experiencing an annual growth rate of approximately 15%, presenting significant opportunities for both domestic manufacturers and strategic international partnerships. Western nations' growing willingness to share advanced technologies with India and global defence companies establishing manufacturing facilities in India are reshaping the industry landscape, making India an increasingly important hub in global defence supply chains

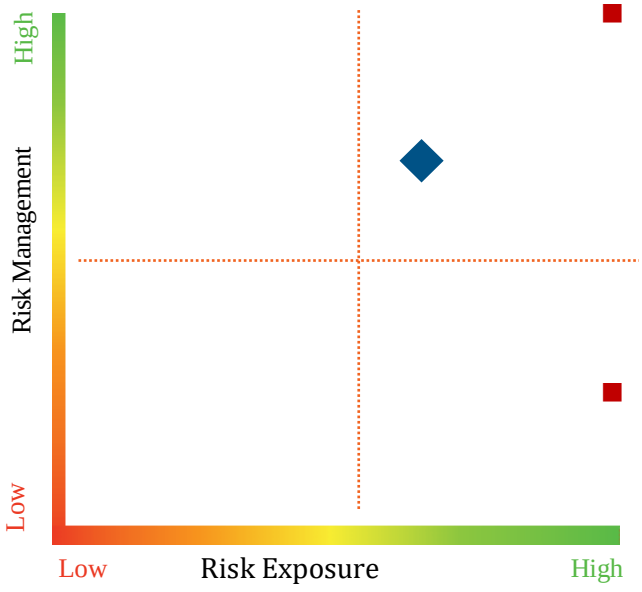
Competitive Risk

- Indian aerospace and defence manufacturers face intense competitive pressure from aggressive pricing strategies by international OEMs seeking entry into the lucrative Indian defence market. Global defence contractors are experiencing margin pressures due to foreign currency volatility and increasing offset obligations, affecting their competitive positioning in the Indian marketplace.
- Higher global defence budgets resulting from geopolitical tensions have intensified competition for limited production capacity among manufacturers. Despite these challenges, the sector continues to grow at approximately 15% annually, with Western nations' growing willingness to share advanced technologies with India reshaping the industry landscape, making India an increasingly important hub in global defence supply chains. f

Risk Dimension Analysis: Technology

Risk Exposure Score: 61

Risk Management Score: 64



Innovation Risk / Obsolete Technology

- The aerospace and defence industry in India is experiencing transformative growth, driven by increasing defence budgets, policy support for indigenous manufacturing, strategic partnerships, and technology transfer arrangements. However, these opportunities are accompanied by innovation risks that require strategic management
- Benchmarking against global aerospace hubs reveals challenges such as limited design and systems integration capabilities, extended certification timelines, and insufficient specialized R&D infrastructure and talent
- International defence companies entering or expanding in India need to strategically evaluate factors such as technology transfer arrangements, industrial offset fulfillment strategies, and navigating complex procurement procedures while addressing structural challenges
- The increasing focus on next-generation technologies like hypersonics, directed energy weapons, and quantum sensing presents both opportunities and risks for the Indian defence industry. Adapting to these technological frontiers requires substantial investment in advanced research capabilities and testing infrastructure
- Investments are accelerating in the sector, with an estimated Rs 3.5 lakh crore expected by 2028. The government's initiatives like the iDEX (Innovations for Defence Excellence) program and Technology Development Fund aim to bridge critical technology gaps through startups and MSMEs in the defence ecosystem

Intellectual Property Risk

- The intellectual property (IP) risks faced by the Indian aerospace and defence industry in 2024 are significant considerations for companies engaged in technology development and manufacturing within this strategic sector
- The evolving framework for protection of defence-related intellectual property in India highlights potential challenges for both domestic and international companies participating in co-development programs
- The industry is challenged by the need to protect sensitive technologies while simultaneously

encouraging knowledge sharing and technology absorption within the domestic ecosystem. This dynamic creates tension between IP protection and technology diffusion goals

- Intellectual property risks in the Indian aerospace and defence industry require sophisticated approaches including compartmentalized IP protection strategies, secure development environments, rigorous cybersecurity protocols, and compliance with defence procurement regulations. By addressing these risks effectively, companies can protect their core technologies while supporting India's defence industrial base development

Disruptive Technology

- The Defence Research and Development Organisation (DRDO) has launched a comprehensive digital transformation initiative, creating an integrated digital platform connecting all its laboratories and research facilities to accelerate technology development and knowledge sharing
- The limited indigenous capabilities in critical technologies such as aero-engines, advanced sensors, and stealth materials due to historical underinvestment in aerospace R&D poses a significant risk for the sector. This challenge constrains the industry's ability to develop next-generation platforms independently, increasing vulnerability to technology denial regimes
- The Indian aerospace and defence sector is undergoing fundamental transformation, with increasing emphasis on investing in deep-tech areas including artificial intelligence, quantum technologies, advanced materials, and autonomous systems. This strategic focus on emerging technologies is essential for maintaining relevance in the rapidly evolving battlefield environment
- Companies with limited access to advanced simulation capabilities and digital engineering tools could fall behind in design efficiency and product development cycles. Additionally, concerns about workforce displacement due to increasing automation in manufacturing processes might create labour relations challenges

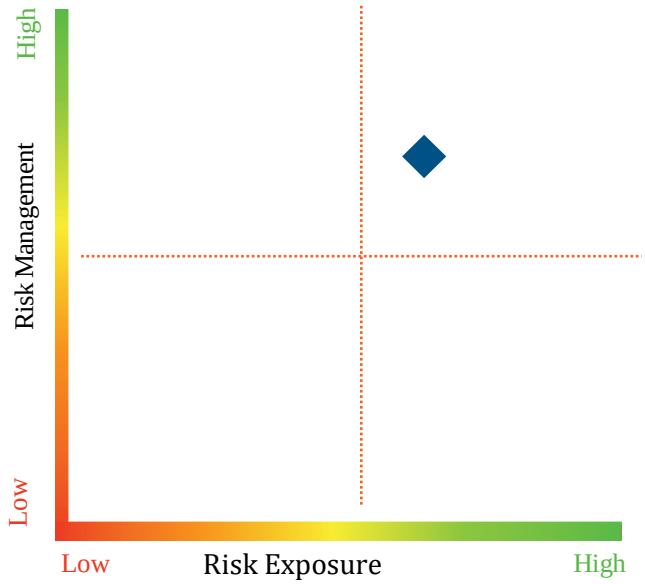
Data Compromises

- The increasing digitalization of defence manufacturing and growing connectivity between design, production, and operational systems has dramatically elevated the risk of cyber-attacks targeting sensitive technical data. The compromise of classified design information or manufacturing techniques could undermine national security and technological advantages, making cybersecurity a critical priority for the sector.
- Companies across the aerospace and defence spectrum have invested heavily in advanced cybersecurity frameworks and technologies to strengthen their defences against sophisticated state-sponsored threats. Implementation of air-gapped networks, advanced persistent threat detection systems, and zero-trust architecture aims to protect against targeted industrial espionage, with collaborative efforts alongside specialized agencies like the Defence Cyber Agency (DCA) and CERT-In to establish industry-specific threat intelligence sharing.

Risk Dimension Analysis: Operational and Physical

Risk Exposure Score: 61

Risk Management Score: 65



Critical Infrastructure Failure / Machine Breakdown

- Operations in India's aerospace and defence manufacturing sector are hampered by continued infrastructure shortages and high risks associated with complex machinery operation. Testing and certification facility constraints create significant bottlenecks in qualification processes for indigenously developed components, affecting production timelines and quality assurance.
- Companies with limited access to advanced simulation capabilities and digital engineering tools are falling behind in design efficiency and product development cycles. The sector suffers from insufficient specialized R&D infrastructure, which limits innovation capabilities and technological advancement, particularly in areas requiring sophisticated testing equipment for next-generation defence technologies.

Business Continuity/Sustainability

- The Indian aerospace and defence industry is increasingly prioritizing sustainable manufacturing practices and environmentally responsible operations. Implementation of standards like the IS/ISO 14001 Environmental Management System and new sustainability reporting requirements demonstrates a growing commitment to reducing environmental impact across manufacturing operations.
- The industry's energy-intensive manufacturing processes, particularly in metal forming, composite curing, and surface treatments, contribute significantly to its carbon footprint. In response, the sector is progressively adopting renewable energy for manufacturing facilities, implementing water recycling systems, and developing sustainable material alternatives, supported by government initiatives like the Green Manufacturing Initiative for Defence PSUs.

Supply Chain Risk

- India's aerospace and defence manufacturing capability is constrained by underdeveloped tier-2 and tier-3 supplier ecosystems, leading to heavy import dependency for precision components and specialized materials. Critical raw materials including titanium and specialized alloys have faced supply constraints, resulting in cost increases and delivery delays as global suppliers prioritize their domestic markets.
- The semiconductor shortage continues to affect advanced avionics systems production, with extended lead times for specialized microelectronics components essential for modern warfare systems. The Russia-Ukraine conflict has disrupted established supply networks for specific aerospace materials and components, particularly affecting programs reliant on Russian-origin systems and creating challenges in maintenance and upgrade pathways for existing platforms.

Commodity Price Risk - Volatility in prices of raw materials

- The aerospace and defence industry experienced significant cost pressures due to global inflation in critical raw materials, including titanium, aluminium alloys, and specialty electronics components in 2024. The combined effect of supply constraints and demand recovery post-pandemic contributed to price volatility across the manufacturing value chain, directly impacting production costs and profit margins.
- The ongoing conflicts in Ukraine and the Middle East disrupted global supply chains for strategic materials, leading to an increase in component costs for Indian defence manufacturers. Higher energy costs directly translated to increased production expenses for precision manufacturing processes, with escalating tensions in the Indo-Pacific region potentially disrupting semiconductor supply chains further, affecting advanced systems development.

Portfolio Risk

- The Indian aerospace and defence sector faces critical challenges in establishing domestic manufacturing capabilities for essential components, including aero-engines, radar systems, and avionics. While new defence manufacturing corridors in Tamil Nadu and Uttar Pradesh are gaining momentum, they face price competition from established global suppliers, requiring strategic portfolio diversification to reduce dependencies.
- Limited indigenous capabilities in critical technologies such as advanced sensors and stealth materials due to historical underinvestment in aerospace R&D constrain the industry's ability to develop next-generation platforms independently. The sector must balance investment between maintaining existing capabilities and developing emerging technologies like hypersonics, directed energy weapons, and quantum sensing to maintain relevance in the rapidly evolving battlefield environment.

Environmental Hazards and Sustainability

- The aerospace and defence industry in India is increasingly focusing on sustainable manufacturing practices and environmentally responsible operations, driving the adoption of greener technologies and manufacturing processes. The introduction of standards like the IS/ISO 14001 Environmental Management System and sustainability reporting requirements demonstrates a growing commitment to reducing the environmental footprint of defence manufacturing
- The industry's energy-intensive manufacturing processes, particularly in metal forming, composite curing, and surface treatments, contribute significantly to its carbon footprint, presenting environmental compliance challenges
- However, the sector is progressively adopting renewable energy for manufacturing facilities, implementing water recycling systems, and developing sustainable material alternatives to improve environmental performance
- Emphasis is being placed on lifecycle assessment of defence platforms to minimize environmental impact from manufacturing through operation to eventual decommissioning
- The government is promoting sustainable aerospace manufacturing through initiatives like the Green Manufacturing Initiative for Defence PSUs and mandatory Environmental Impact Assessments for new defence industrial projects

Workplace Accident

- The aerospace and defence manufacturing sector continues to face high risks of accidents during operation of necessary machinery, as mentioned in the sector report. Natural hazards increase operational risks for facilities handling hazardous materials including specialized chemicals, composite pre-pregs, and volatile substances used in propulsion systems, creating potential for industrial accidents that could compromise worker safety.
- The industry's energy-intensive manufacturing processes, particularly in metal forming, composite curing, and surface treatments, present ongoing workplace safety challenges requiring robust safety protocols. Industrial accidents triggered by natural disasters could impact not only worker safety but also surrounding communities, highlighting the importance of comprehensive safety management systems in these specialized manufacturing environments.

Human Resource

- The aerospace and defence industry in India faces significant shortages of specialized engineering talent despite employing more than 200,000 skilled professionals. This talent gap particularly affects advanced technology areas like systems integration, avionics development, and materials science, constraining growth potential and innovation capabilities in the sector.
- Concerns about workforce displacement due to increasing automation in manufacturing processes might create labour relations challenges in the coming years. The residual effects of

the COVID-19 pandemic continue to influence workforce availability, with international travel restrictions affecting technology transfer activities that rely on face-to-face expert interactions, highlighting the need for comprehensive human resource development strategies.

Financial Risk

- The Indian Rupee experienced moderate fluctuations against the US Dollar, with 4.2% depreciation year-to-date in 2024, creating financial uncertainty for an industry dependent on imported components. Global defence contractors faced margin pressures throughout 2024 due to foreign currency volatility and increasing offset obligations, complicating financial planning and investment decisions.
- The uncertain geopolitical landscape added complexity to long-term contract pricing, impacting trade dynamics and potentially affecting foreign exchange exposure. Sluggish execution of major defence programs negatively impacted domestic companies' financial performance, with higher energy costs and inflation in raw materials creating significant pressures across the manufacturing value chain that affected profitability throughout the sector.

Breaches of law (local/ international)

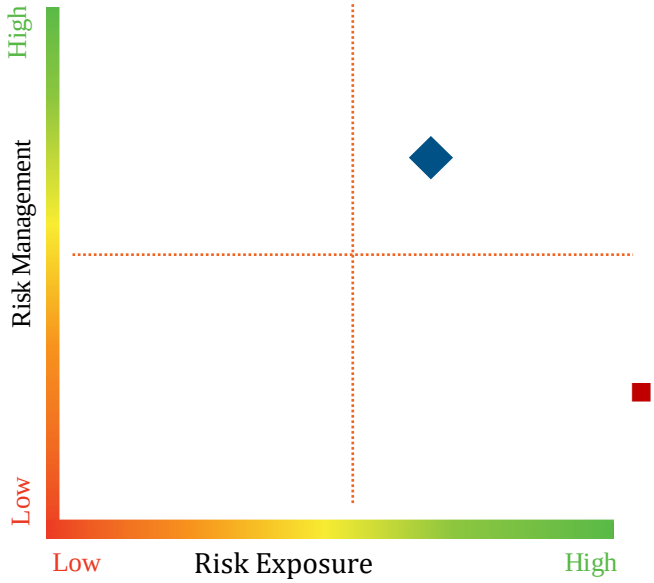
- The aerospace and defence industry faces heightened regulatory scrutiny due to the sensitive nature of defence technologies and their potential dual-use applications. Government agencies have established comprehensive frameworks addressing export controls, technology transfer limitations, and end-use monitoring to ensure responsible development of defence capabilities, creating compliance challenges for manufacturers.
- Companies must navigate complex international arms control regulations, including potential implications of the United States' CAATSA sanctions related to Russian defence procurement. The Directorate General of Aeronautical Quality Assurance's mandatory compliance with quality management standards represents an additional regulatory burden, requiring significant investment in compliance programs to avoid legal breaches.

Risk Dimension Analysis: Crime and Security

Risk Exposure Score: 62

Risk Management Score: 61

Cyber-crimes



- With increasing digitalization of defence manufacturing and the growing connectivity between design, production, and operational systems, the risk of cyber-attacks targeting sensitive technical data has risen dramatically. The compromise of classified design information or manufacturing techniques could undermine national security and technological advantages
- Companies across the aerospace and defence spectrum invested heavily in advanced cybersecurity frameworks and technologies to strengthen their defences against sophisticated state-sponsored threats. This included implementing air-gapped networks, advanced persistent threat detection systems, and zero-trust architecture to protect against targeted industrial espionage
- Collaborative efforts with specialized agencies like the Defence Cyber Agency (DCA) and the Computer Emergency Response Team (CERT-In) were pursued to establish industry-specific threat intelligence sharing and rapid incident response capabilities. These partnerships focused on developing defence-specific security protocols, supply chain integrity verification, and coordinated vulnerability management

Counterfeiting

- Quality control and authenticity verification remain significant challenges in the aerospace and defence supply chain, with counterfeit components posing serious risks to operational safety and performance. The implementation of mandatory certification from the Center for Military Airworthiness and Certification (CEMILAC) for aerospace components aims to ensure quality standards while reducing the risk of counterfeit parts entering critical systems.
- The Directorate General of Quality Assurance has intensified enforcement of quality standards for aerospace and defence products to ensure operational reliability, combat effectiveness, and personnel safety. The 18 new Technical Standards Orders implemented in 2024 create a more

robust framework for authenticating components and identifying potential counterfeits, though the increasingly complex global supply chain continues to present verification challenges.

Threat to Women Security

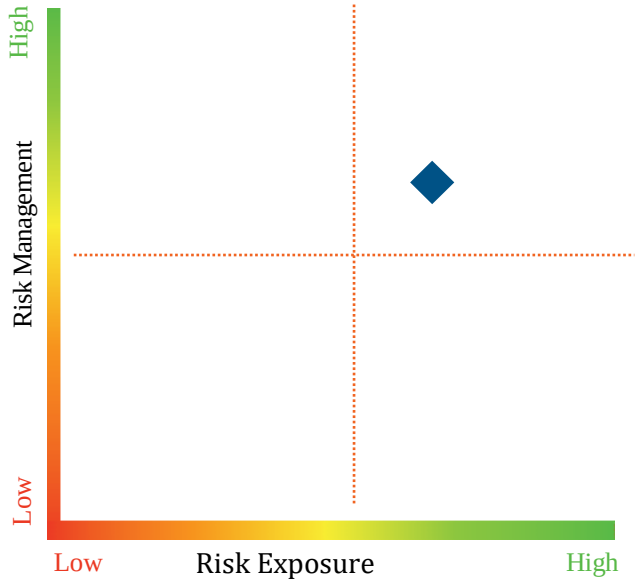
- The aerospace and defence sector, traditionally male-dominated, faces growing pressure to address gender diversity and security concerns for women in the workplace. Creating secure work environments for female engineers, technicians, and administrators is becoming a priority as the industry seeks to expand its talent pool amidst specialized skill shortages.
- Defence manufacturing facilities, often located in industrial corridors or special economic zones, present unique security considerations for women employees, particularly those working in shifts or in remote locations. Effective strategies to address these concerns include enhanced physical security measures, appropriate transportation arrangements, and comprehensive workplace harassment policies tailored to the specific operational environment of defence manufacturing.

Corruption

- The defence sector globally faces heightened corruption risks due to the high-value nature of contracts, complex procurement processes, and national security classifications that may limit transparency. India's defence procurement system continues to evolve with anti-corruption measures including digital procurement platforms, integrity pacts, and enhanced transparency requirements.
- Offset obligations in defence contracts, while designed to ensure technology transfer and domestic industrial development, can create additional corruption vulnerabilities if not properly monitored. The government's emphasis on improving procurement processes through the Defence Acquisition Procedure (DAP) 2020 and its subsequent amendments aims to reduce these risks through standardized procedures and strengthened oversight mechanisms.

Risk Dimension Analysis: Natural Hazard and Event

Risk Exposure Score: 61
Risk Management Score: 66



Natural Hazards like flood, drought, famine, earthquake, landslide etc

- Natural disasters such as cyclones, floods, or earthquakes can cause significant damage to aerospace manufacturing facilities and testing infrastructure, potentially leading to production delays, damage to specialized equipment, and disruption of critical defence programs
- Natural hazards increase operational risks for aerospace manufacturing facilities handling hazardous materials including specialized chemicals, composite pre-pregs, and volatile substances used in propulsion systems. Industrial accidents triggered by natural disasters could compromise worker safety and impact surrounding communities

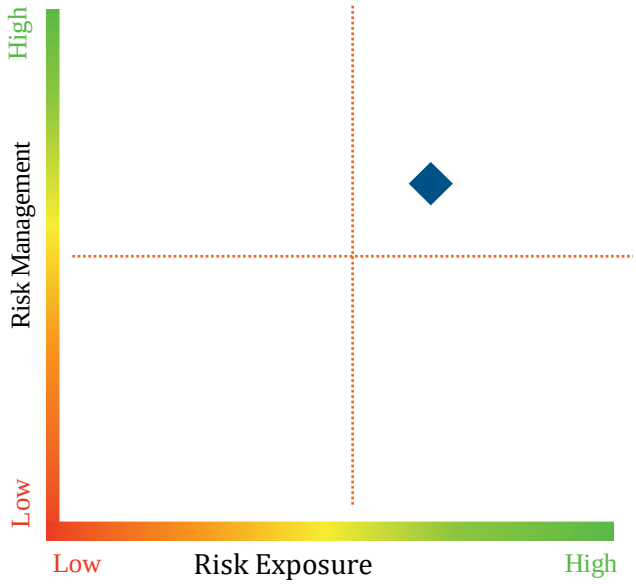
Pandemic and other global epidemic diseases

- The residual effects of the COVID-19 pandemic continued to influence global aerospace supply chains, with lingering impacts on workforce availability, international travel restrictions affecting technology transfer activities, and financial strain on smaller suppliers in the ecosystem
- The pandemic accelerated the adoption of digital manufacturing technologies, remote collaboration tools, and virtual testing methodologies across the aerospace and defence industry. These technological adaptations improved operational resilience while creating new cybersecurity challenges
- Despite the challenges posed by the pandemic, there were opportunities for growth within the aerospace sector. The imperative to develop resilient supply chains less dependent on single-source suppliers presented growth opportunities for the Indian aerospace manufacturing base, driving investments in domestic capabilities
- These consequences highlight the importance of operational flexibility, redundancy in critical supply chains, and digital transformation in enhancing the aerospace and defence industry's resilience against future global disruptions

Risk Dimension Analysis: Strategic Risk

Risk Exposure Score: 62

Risk Management Score: 63



Resource scarcity / Misutilisation / Overall Utilisation

- Specific resource challenges faced by the aerospace and defence industry in India in 2024 include shortages of specialized engineering talent, limited availability of strategic materials, constraints in testing infrastructure, and increasing competition for R&D funding.
- These resource limitations can impact technology development timelines, manufacturing quality, and overall program execution.
- The industry is adapting through initiatives focusing on skill development, material research, shared infrastructure models, and consortium-based funding approaches to mitigate risks associated with resource constraints while maximizing innovation potential.

Increased number of recalls and quality audits

- The aerospace and defence sector has experienced intensified quality standards enforcement by regulatory bodies to ensure operational reliability, combat effectiveness, and personnel safety. The implementation of 18 new Technical Standards Orders in 2024 to regulate product quality and align with global aerospace standards has increased quality compliance requirements across the manufacturing ecosystem.
- Mandatory compliance with AS9100 quality management standards for all aerospace manufacturers supplying to defence and civil aviation sectors, effective from September 1, 2024, has elevated quality assurance requirements. These stricter standards aim to enhance safety and reliability while requiring manufacturing enterprises to upgrade their quality management systems, potentially leading to increased discovery of non-conformities during initial implementation phase.

Delay in execution of projects

- Aerospace and defence programs in India frequently face execution delays due to complex technical requirements, changing specifications, and multi-stakeholder coordination

challenges. The sluggish execution of major defence programs has negatively impacted domestic companies' financial performance and operational credibility, creating a barrier to achieving self-reliance objectives.

- Capacity constraints at testing and certification facilities create bottlenecks in qualification processes for indigenously developed components, further complicating project timelines. Supply chain disruptions, including extended lead times for specialized components and materials, continue to affect project execution schedules, with the semiconductor shortage particularly impacting electronic systems integration timeframes.

Public Sentiment

- The defence industry operates in a domain with significant ethical considerations regarding the ultimate use of its products in conflict situations, creating potential for public relations challenges and stakeholder concerns
- Due to the sensitive nature of defence technologies and their potential dual-use applications, there is heightened regulatory scrutiny and compliance requirements. Concerned stakeholders and government agencies have established comprehensive frameworks addressing export controls, technology transfer limitations, and end-use monitoring to mitigate these risks and ensure responsible development of defence capabilities

Failed / Hostile Mergers & Acquisitions

- The consolidation of the global aerospace and defence industry continues to present both opportunities and challenges for Indian companies seeking strategic partnerships or acquisitions. Failed merger attempts can result in significant financial losses, intellectual property vulnerabilities, and competitive disadvantages in a rapidly evolving market landscape.
- The complex regulatory environment surrounding defence industry ownership, with restrictions on foreign investment percentages and mandatory security clearances, creates additional complications for M&A activities. Companies must carefully navigate these restrictions while pursuing strategic consolidation to achieve scale economies and technology synergies, with unsuccessful attempts potentially exposing them to hostile takeover risks or competitive disadvantages.

ICICI LOMBARD: Key Solution Offerings

Property

Evaluation of various risks to understand areas for improvement, such as fire preparedness, electrical safety, safety & emergency preparedness, maintenance and house-keeping, etc. By evaluating risks, we can identify potential hazards and advise on mitigating risks.

- **Property Loss Prevention:** We believe users should carry out detail risk visit followed by benchmarking of the industry good practices (Industry Risk Profiling). For instance, industries such as chemicals & petrochemicals impose a major challenge in manufacturing due to inherent risk. We recommend solutions for "Low Focus - High Loss Areas. This can help in minimizing severity losses. All the risk recommendations are grouped into four different segments based on cost-impact matrix and the priority is decided accordingly. Key decision makers at user's end can ensure to get recommendations implemented.
- **Comprehensive Risk Assessment (CRA):** A Comprehensive Risk Assessment is a systematic approach to electrical safety specially designed for industries to evaluate potential hazards and recommend improvements, coupled with savings. It is an important tool for identifying risks, severity of hazards and avoid incidents arising out of electrical faults.
- **Electrical Risk Assessment (ERA):** An Electrical Risk Assessment is a basic solutions focused towards electrical safety designed to evaluate potential hazards and recommend improvements. Majority of fires in India are caused due to electrical installations. Ensuring safety of electrical installations of industrial unit or organization is critical to reduce risk and ensure safety compliance with Safety Standards and Regulation. ERA is an important tool which have 6 inbuilt solutions such as Electrical Audit & Thermography, etc.
- **Fire Hydrant IoT:** Fire Hydrant IoT: Fire hydrant IOT (ILGIC Patented Solution) is an automated device for monitoring key parameters such as Hydrant and Sprinkler line pressure, Main and Jockey pump on-off status, Firewater tank level. These can be interpreted to provide intelligence on unauthorized usage of water and leakage, effectively saving water. This information pertaining to breach of above-mentioned parameters is notified through dashboard & email alerts. Monitoring of such system is essential as these fire fighting systems are lifeline during any emergency.
- **Temperature & Humidity IoT:** Provides end-to-end plug & play ambient temperature and humidity monitoring Solution to manage temperature and humidity-controlled environment more efficiently. It generates - Automated reports (historical trends for different locations etc.). Intelligent Alerts - SMS & emails is sent to the concerned (one or multiple) stakeholders in case

any anomaly.

- **Electrical IoT:** Electrical IoT is a patented solution (ILGIC Patented Solution) to avoid any instances of short circuiting due to abnormal voltage & current conditions. These are mainly built for application in warehouses. This solution has been created as these locations are having huge stocks with lesser manpower during emergencies mainly during non-business hours. The device automatically cuts off power in case of abnormality & restarts back when situation is normal.
- **Ultrasound technology for Gas Leak Detection:** Use of ultrasound technology for leak detection in process lines. The methodology recommends a non-destructive way of avoiding losses with no downtime. The main objective is to identify the leakages in all pressurized systems including pipelines by using ultrasound technology and tag them for rectification. It also includes listing leaks with individual CFM losses and cost savings possible.
- **Fire Mitigation Solutions:** Solutions have been designed based on their specific needs, keeping in mind the level of awareness and complexity of the location. These best-in-class solutions which are installed at correct locations.
- **Renewable Solutions:** In line with our philosophy of recommending business solutions, we recommend efficiency measurements for wind and solar power generating assets. Drones are used to provide high accuracy and quick reach which is not possible through any traditional methodology. User get to know about the low performing module and ways to improve the same within the entire solar plant with latlong identification. We recommend advanced drone-based technology for inspection of wind turbines and solar PV modules.

Marine

In the dynamic realm of marine insurance, cargo faces a myriad of risks, from unpredictable weather conditions to unforeseen accidents, safeguarding against potential challenges at sea and in surface transportation / INLAND movement is paramount.

- **MLCE (Marine loss control engineering):** Frequent occurring losses due to Peril such as accident, wet damage, theft, non-delivery, pilferage, hijack of consignments, mishandling shall be examined with ground inspections, to determine root cause analysis with MIS, claim assessment reports collectively in the form of logistics audit.
- **MWS (Marine warranty surveys):** Our inhouse practices of condition survey prior risk inception & post risk inceptions helps our customers to have an independent risk management of the high value / ODC (over dimensional cargo) movements conducted by the Insured so that reliance over logistics service provider is supervised with Insured's nominated risk assessment team having a worldwide presence with a supervised network. Not only marine cargo, but HULL insurance risk exposures are surveyed for risk assessment and risk management.
- **Technical engagements:** Uncertainty of the risk associated with the transit can be concluded

with marine experts. Assessing vessel's condition for SEA transit as a full chartered load on behalf of the Insured, Risk assessment of cargo from packing, handling, lifting, securing, transit and final delivery methodology shall be discussed with the logistics team. Vessel selection, stowage and securing methods can be jointly discussed with the User's logistics team for a safe transit, dispatch and delivery coverage after assessing the risk on desktop with a virtual or F2F engagement and / or a ground visit.

- **Transit Telematics:** With the government's constant agenda of upgrading to digitalized operations by introducing ULIP and NITI Aayog mode of operations, not having a visibility of transit will hamper your logistics operations. IOT and SAAS (software as a service) based products incorporating the design of a cost efficiency and loss mitigation system can help enhance delivery with safe operation. Additionally, a 24*7 risk control is recommended to effectively monitor and mitigate theft / pilferage prone dispatches to ensure a safe transit delivery. Be it a temperature-controlled cargo, expensive cargo in transit or liquid bulk cargo in lorry tankers, it is essential to mitigate the risk and losses that might occur due to accidents caused by fatigue, unexplained conditions, or theft. We have case studies of successful recovery of stolen goods with our telematics services.

Liability

The growing adoption of technology in organizations has not only led to crucial data being stored and processed on digital platforms but also facilitated the automation of operations, thereby enhancing business efficiency. However, this shift also amplifies cyber risk, exposing sensitive information to potential threats and rendering organizations vulnerable to financial losses, reputational damage, and legal liabilities. As organizations delve deeper into the digital realm, fortifying cybersecurity measures becomes imperative to safeguard operational integrity and protect critical data from unauthorized access or breaches.

- **Phishing Simulation:** Experience cutting-edge phishing simulation tests to fortify your organization's defenses against cyber threats. You can enable phishing attack simulations to educate your employees on identifying and handling potential risks. Through engaging and interactive scenarios, you can raise awareness and equip your team with the necessary skills to detect and thwart phishing attempts.
- **Awareness Campaigns:** With Cyber Awareness Campaigns, you can go beyond just educating organizations about cybersecurity. The campaigns are meticulously designed to empower your team with essential best practices, insights into global incident trends and a comprehensive understanding of potential risks. Interactive designs help you captivate and engage your employees, fostering a cyber-aware culture within your organization. Customized campaigns can perfectly align with your unique needs and requirements and stay informed and vigilant.
- **Incident Response and Readiness:** A bespoke service that fortifies organizations with robust processes and clear communication channels for proficient cyber-incident management. This

recommendation not only trims down the incident response time but also facilitates prompt, accurate action within the crucial initial hours. By meticulously assessing your organization's incident response policies and sculpting response systems in alignment with global industry benchmarks, this ensures you are thoroughly prepared to tackle the evolving digital threat landscape.

- **CXO's Session:** CXO's Session service provides immersive training sessions, personalized coaching & interactive discussions to empower your CXOs with cybersecurity knowledge that aligns with your business objectives. The subject matter experts recommend strategic guidance and in-depth insights into the ever-evolving threat landscape, translating technical jargon into practical language. Regular cybersecurity forums facilitate peer-to-peer learning and benchmarking against industry standards. CXO- focused approach ensures a cyber-aware leadership team that drives your organization's success securely into the future.
- **Weekly Threat Intelligence Bulletin:** Stay ahead of cyber threats with the Weekly Threat Intelligence Bulletin. We meticulously curate this comprehensive bulletin, providing timely insights on emerging threats, vulnerabilities, and attack trends. Delivered directly to your inbox, it recommends proactive advantage by promptly identifying potential risks. With continuous updates and ongoing support, you can confidently adapt your Defence strategies to combat the most sophisticated threats. It enables you to make informed decisions and protect your organization from emerging threats with Weekly Threat Intelligence Bulletin.
- **Email Security:** Safeguard your organization's communication channels with the Email Security solutions. We recommend robust measures to protect against phishing, malware & other email-borne threats. The advanced email filtering and authentication technologies prevent malicious emails from reaching your users inbox. Implementing encryption protocols to ensure the confidentiality of sensitive data in transit is a good idea. With real-time monitoring and threat intelligence, email security measures provide proactive Defence, detecting and blocking suspicious activities promptly. You can protect your organization's reputation and sensitive information with comprehensive Email Security measures, ensuring a secure and reliable email environment.
- **Agent-less Patching:** Agent-less patching platform for companies and MSMEs who want a rapid solution to distribute critical security updates and vulnerability fixes without causing system downtime. The patching platform not only assists with patch deployment, but it also enables your system administrator in understanding the patches, Adjustments & impact of the patches on the system. Before applying the patch, the software generates a warning if the system requires downtime or a reboot. You can experience a hassle-free patching process with the platform recommending enhanced security for your organization.
- **EDR/MDR Services:** Elevate your organization's cybersecurity capabilities with the Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR) services. These advanced solutions provide continuous monitoring, rapid threat detection & effective incident response, safeguarding your digital assets in real-time. With EDR, proactively detect and

respond to threats at the endpoint level, while MDR service offers 24/7 monitoring and expert support. You can strengthen defenses against the most sophisticated cyber-attacks with EDR/MDR services, ensuring a resilient and secure digital environment.

- **All-in-one Operating System:** All-in-One Operating System is a true game-changing platform that provides a fortified desktop environment to foster secure collaboration and centrally managed cybersecurity resilience. Inbuilt endpoint security serves as a vigilant guard, blocking potential dangers. Effortless IT management provides with a user-friendly interface, leading to significant cost savings in IT infrastructure. It provides in-built end-point security, automated updates and patches along with extensive device reports. Organizations can unlock a secure and prosperous future by embracing the All-in-One Operating System in their IT infrastructure.
- **Cyber Risk Management & Compliance Dashboard:** Gain a clear understanding of your organization's cyber risk exposure with Cyber Risk Management & Compliance Dashboard. This powerful tool assesses your risk posture, quantifies potential financial Impact & evaluates compliance with industry standards and regulations. Armed with this information you can make informed decisions to prioritize cybersecurity investments and ensure compliance with relevant laws and regulations. The intuitive dashboard provides a comprehensive view of your cybersecurity performance enabling data-driven decision-making. This solution enables organizations to stay ahead of threats and ensure a resilient cybersecurity posture.
- **Security Score Card:** Track your organization's cybersecurity performance with a dynamic Security Score Card solution. This comprehensive rating provides a clear overview of your security posture, highlighting areas that require attention and improvement. It empowers data-driven decisions, allowing you to focus on strengthening key areas. Identify potential risks and compliance gaps with industry standards and regulations. With actionable insights, you can prioritize cybersecurity investments effectively, ensuring a robust and resilient Defence against cyber threats. This Security Score Card solution can be your strategic tool to proactively elevate your cybersecurity posture.
- **VAPT:** Enhance your organization's cybersecurity defenses with the Vulnerability Assessment and Penetration Testing (VAPT) service. Skilled professionals conduct rigorous assessments, simulating real-world attacks to identify potential vulnerabilities in your digital infrastructure. With detailed insights, you can fortify your defenses and proactively address weak points before malicious actors exploit them. This service goes beyond identifying vulnerabilities, you also get actionable recommendations to mitigate risks effectively. Organizations can be one step ahead of cyber threats, ensuring the security and resilience of your critical assets with the comprehensive VAPT service.

Engineering

In engineering risk management, it's vital to adopt a holistic approach that extends beyond immediate concerns to proactively tackle potential risks and uncertainties. Drawing upon

considerable expertise in claims handling and risk evaluation, a robust and customized protection strategy can be ensured.

Construction endeavors face a myriad of risks such as floods, cyclones, impact damage, fires, theft, and collapse. However, the adverse effects of these risks can be mitigated through the implementation of extensive loss prevention measures specifically tailored for engineering projects.

- **Engineering Loss Prevention Exercise (ELP):** To effectively manage losses in Engineering Risk, fostering a culture of loss prevention is crucial. It's widely acknowledged that each construction project is distinct, presenting specific challenges related to geography, geology, occupancy, and construction methodology, which in turn result in unique associated risks. To cater this challenge a specific risk management framework which deals about the unique requirement of each project could be created for the loss prevention with reference to some parameters of distinctive research and industries best practices.
- **Drone Solutions for Linear Projects:** In recent years, the construction industry has undergone significant changes due to the introduction of drone-based construction solutions. These cutting-edge technologies are transforming the planning, design, and execution of construction projects. A major benefit of drone technology in construction is its capacity to conduct aerial surveys, providing extensive coverage and detail. Drones, equipped with advanced cameras and sensors, can rapidly capture precise images and data, offering project managers valuable insights into site conditions. This data can facilitate project planning, cost estimation and design optimization by providing a comprehensive understanding of the project's parameters.
- **CPM - Fleet & Fuel Management:** An advanced GPS-equipped sensor is available to precisely measure direct fuel consumption, evaluate engine efficiency, and detect potential tampering of diesel engines in both mobile vehicles and stationary machinery. This solution enables real-time alerts for service reminders and critical health issues, facilitating prompt resolutions and enhanced utilization. Additionally, it offers valuable insights into machinery and equipment performance through comprehensive analyses, resulting in optimized inventory usage and increased efficiency.

Health

We highly recommend exploring proactive and preventive healthcare solutions, which can make a significant difference in maintaining good health. Recognizing that majority of in-patient department (IPD) admissions could be prevented with timely interventions and regular healthcare, it is important to focus on health, not just during illness.

- **Pioneering Digital Platform:** We recommend exploring digital health innovations offered by industry leaders, which provide cutting edge health solutions through the IL TakeCare (ILTC) app. Our platform has transformed the way health services are delivered by introducing a fully digital and cashless Outpatient Department (OPD) and Wellness Program.

- **Health Advisory Services:** We recommend a suite of health advisory services on the IL TakeCare app. Users can access health risk assessments, diet and exercise trackers, health parameter tracking and trends and sleep, meditation & hydration reminders. In addition, the platform recommends a feature to upload health records up to 1GB, and provides informative health blogs.
- **IL TakeCare App:** IL TakeCare app is a One-Stop-Solution for users with insurance needs. This robust user engagement is a testament to the high-value features that the app provides. Unique to the app is the innovative self-health assessment feature, which includes Face scan technology that can measure blood pressure, heart rate, cardiac variance, and SpO2 levels. The platform provides seamless teleconsultations with medical practitioners and specialists, and even recommends access to mental wellness experts to the insured. The facility for cashless OPD services and the efficient claim settlement process further enhance user experience. By encapsulating a wide range of state-of-the-art health services and solutions, the IL TakeCare platform revolutionizes corporate health management and serves as a comprehensive digital health solution.

Bibliography

https://www.spglobal.com/_assets/documents/ratings/research/101591898.pdf

https://www2.deloitte.com/us/en/insights/industry/aerospace-defence/aerospace-and-defence-industry-outlook.html

https://www.pwc.com/us/en/industries/industrial-products/library/aerospace-defence-review-and-forecast.html

https://www.financialexpress.com/business/defence-2024-a-landmark-year-for-indias-defence-sector-3701524/

https://www.marketresearch.com/Netscribes-India-Pvt-Ltd-v3676/Aerospace-defence-India-36482055/

https://www.alliedmarketresearch.com/resource-center/trends-and-outlook/aerospace-and-defence/aerospace-defence-sector-2024-trends-challenges-innovations-opportunities

https://manufacturing.economictimes.indiatimes.com/news/aerospace-defence/why-aerospace-and-defence-should-be-a-priority-for-indian-msmes/114756675

Disclaimer 1: Risk management Solution / Value Added Solution mentioned in the report are as per the assessment observation & experience in that sector. These solutions are suggested or intended to for a better management and mitigation of corporate risks. The content of the solutions is a proprietary of ICICI Lombard cannot be copied and/or distributed without permission of ICICI Lombard. The content provided is for improvement purposes only and ICICI Lombard is not responsible for any issues or liability arising out of the use of the said information. ICICI Lombard does not make representations or warranties, either express or implied, of any kind with respect to the third party, its actions, content, information or data. ICICI Lombard does 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 acknowledges that any reliance upon such opinion, advice, statement, memorandum, or information shall be at his/her sole risk. Any such person or entity should seek advice based on the particular circumstances from the experts of the respective filed arenas.

Disclaimer 2: 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

ICICI Lombard

CORPORATE INDIA RISK INDEX

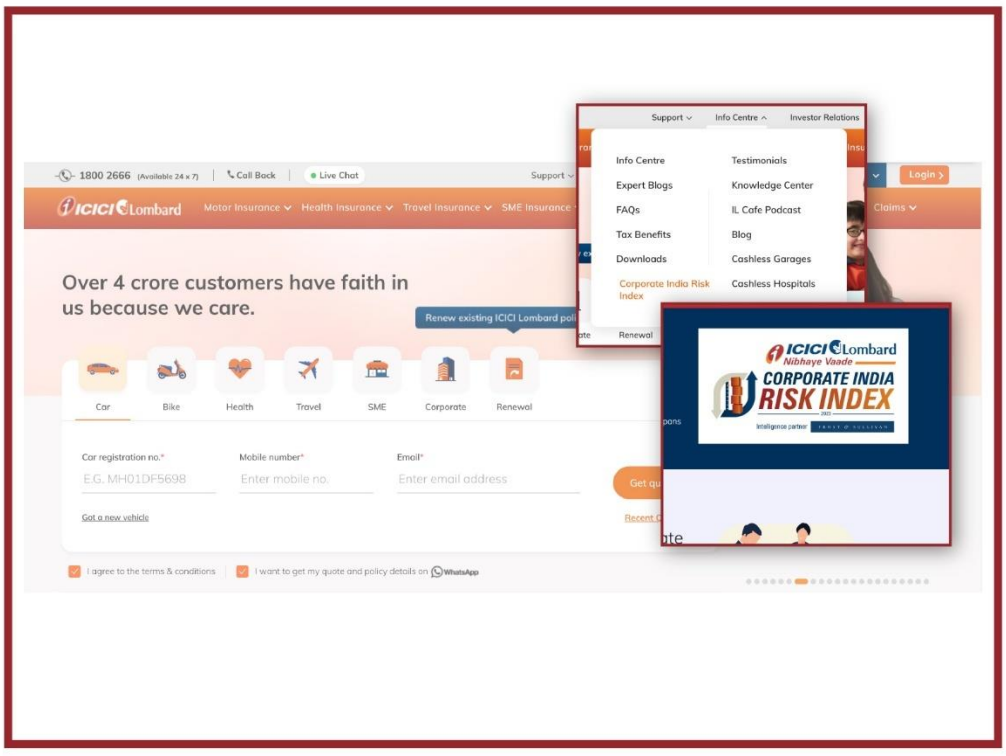
2024

Intelligence partner FROST & SULLIVAN

Navigating Risks, Powering India's Growth

Now accessible at

www.icicilombard.com/corporate-india-risk-index



Please send a mail to ciri@icicilombard.com to get your customized ICICI Lombard Corporate India Risk Index Report

ICICI Lombard

CORPORATE INDIA RISK INDEX

2024

Intelligence partner FROST & SULLIVAN

Navigating Risks, Powering India's Growth