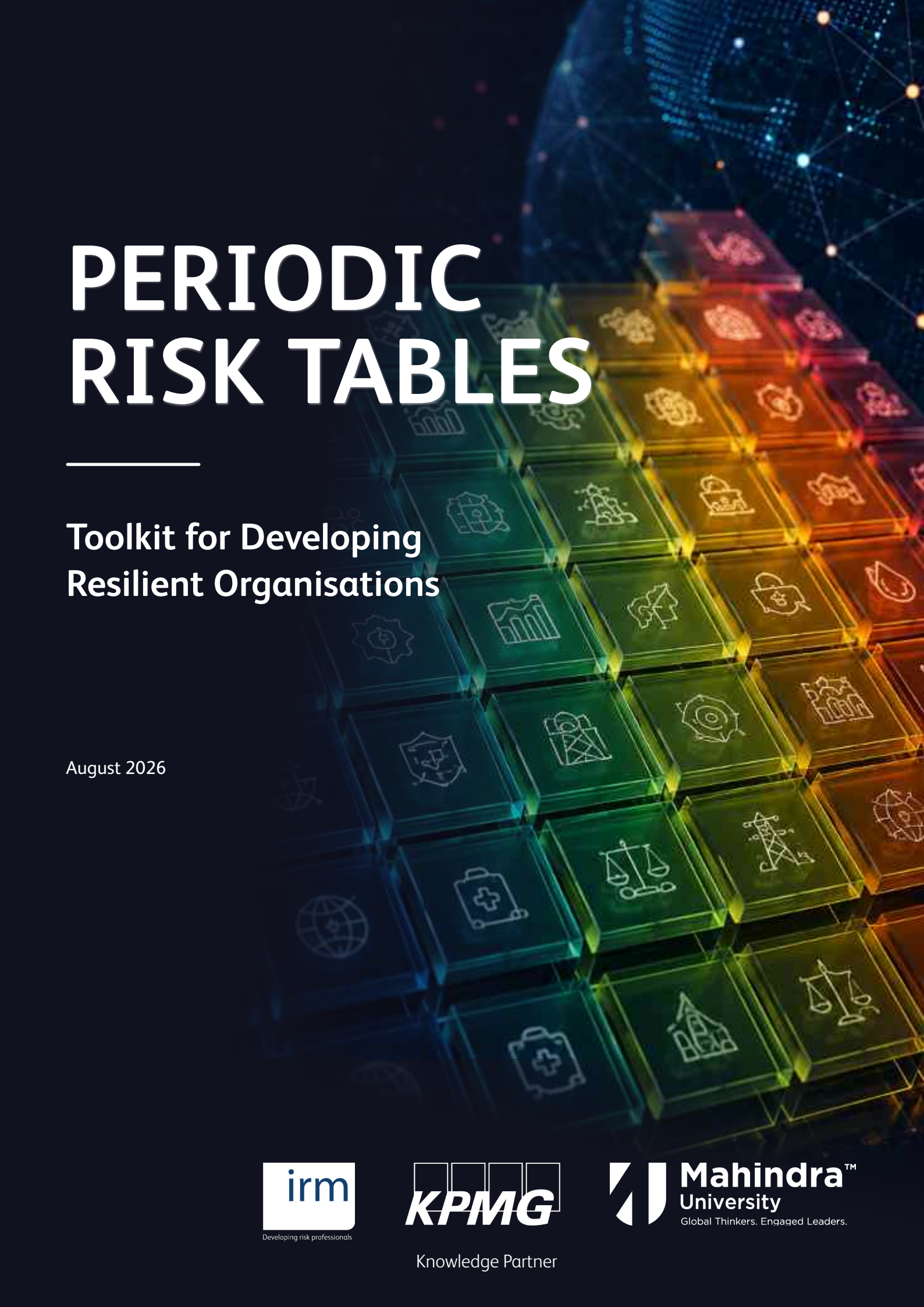


PERIODIC RISK TABLES

Toolkit for Developing Resilient Organisations

August 2026

irm
Developing risk professionals

KPMG
Knowledge Partner

Mahindra™ University
Global Thinkers. Engaged Leaders.

Foreword

In the evolution of any discipline, a moment arrives when complexity demands structure, requiring dispersed knowledge to be organised into a system that not only explains the present but anticipates the future. Enterprise Risk Management stands at precisely such a juncture today.

For many years, organisations approached risk in silos - financial risk here, operational risk there, and compliance somewhere in between often reacting to events rather than truly understanding the interconnected nature of uncertainties. While frameworks, standards, and governance mechanisms have significantly matured, the pace, scale, and velocity of change in today's environment have rendered static approaches increasingly inadequate. Enterprises now operate in a world where risks do not emerge in isolation. They interact, amplify, and evolve in real time. A cyber incident is no longer just a technology risk; it is a reputational, regulatory, operational, and even geopolitical risk. Climate change is not merely an environmental concern; it affects supply chains, capital allocation, insurance viability, and long-term strategy. Artificial intelligence introduces unprecedented efficiencies, but also ethical dilemmas, model risks, and systemic vulnerabilities.

In such a landscape, the question is no longer whether organisations have a risk framework, but whether they truly understand the underlying "elements" of risk and how these elements combine, react, and transform. In this context, the concept of "Periodic Risk Tables" becomes both relevant and necessary. Much like the periodic table revolutionised chemistry by organising elements based on their properties and relationships, a structured taxonomy of risks can fundamentally transform how organisations perceive and manage uncertainty. It enables boards, leadership teams, and practitioners to move beyond fragmented thinking toward a more integrated, dynamic, and intuitive understanding of risk.

A periodic view of risks does not merely categorise; it reveals patterns. It highlights correlations that may otherwise go unnoticed. It allows institutions to see how certain risks tend to co-exist, how some act as catalysts for others, and how emerging risks often evolve from the recombination of known ones. Most importantly, it shifts the conversation from reactive risk management to proactive risk intelligence. Importantly, this is not about creating another static model or checklist.

The true value lies in adopting a dynamic approach that continuously evolves with changing business models, technological advancements, regulatory landscapes, and societal expectations. A modern risk taxonomy must be fluid and adaptable, capable of incorporating

Hersh Shah

CEO, IRM India Affiliate and India's Youngest Enterprise Risk Expert

new "elements" as they emerge, while reclassifying existing ones as their nature and impact evolve. For boards and senior leadership, such an approach enhances clarity and decision-making. It provides a common language to discuss risks across functions, business units, and geographies. It strengthens risk culture by making risk more accessible, relatable, and actionable. For practitioners, it offers a structured yet flexible tool to design more comprehensive risk assessments, scenario analyses, and response strategies.

At IRM India, KPMG in India and Mahindra University, there has been a consistent focus on advancing a holistic and forward-looking approach to risk management - one embedded in strategy, culture, and performance. The idea of a periodic table of risks aligns closely with this vision. It represents not just a tool, but a mindset shift: from viewing risk as a compliance requirement to recognising it as a strategic enabler. As organisations navigate increasing uncertainty, resilience will be built not through control alone, but through understanding. Understanding, in turn, builds on clarity - clarity about existing risks, how they relate, and how they evolve over time.

The journey ahead requires a re-examination of how risks are defined, categorised, and communicated. It calls for innovation in frameworks, creativity in thinking, and discipline in execution. If this work helps organisations take even a small step toward that clarity, toward seeing risk not as a set of isolated events but as an interconnected system; it will have served its purpose. The future of risk management is not static. It is dynamic, interconnected, and continuously evolving. The approaches adopted by enterprises must be no different.

Table of Contents

Executive Summary

Why a Periodic Risk Tables Approach to ERM

Organisations today operate in an environment characterised by increasing uncertainty, complexity, and interdependence. While risk management frameworks, governance structures, and reporting mechanisms have become more mature, many organisations continue to face challenges in developing a coherent view of enterprise-wide risk. Risks are often assessed and managed within functional silos, making it difficult to identify relationships, dependencies, and cascading effects across the organisation.

The Periodic Risk Tables (PRT) framework has been developed to address this challenge by providing a structured approach to organising and understanding enterprise risks. Drawing inspiration from the logic of the periodic table in chemistry, the framework classifies risks into distinct elements and broader risk families based on their characteristics, sources, and potential impact pathways. This enables risks to be viewed not as isolated events but as components of a broader and interconnected system.

This study catalogues 1,492 risk elements across nineteen sectors of the Indian economy, organised into nineteen sector-specific Periodic Risk Tables and one consolidated cross-sector table of 45 universal risks — twenty tables in total. Each element is classified by risk category, scored on a 5×5 likelihood–impact scale, and assigned to one of three bands: low, moderate, or critical. The tables draw on faculty-led sectoral analysis, structured secondary research, and 38 practitioner responses from chief risk officers and senior risk professionals at leading organisations in each sector.

The framework recognises that risks differ in their severity, velocity, and level of interdependency. Some risks are foundational in nature, such as governance and culture, while others are rapidly evolving, including cybersecurity, artificial intelligence, and data-related risks. Other risks, such as climate change, demographic shifts, and geopolitical developments, emerge gradually but can have systemic consequences over longer time horizons. Organising risks within a structured taxonomy improves visibility into these differences and supports more consistent risk assessment and prioritisation.

A key premise underpinning the framework is that organisational resilience requires an enterprise-wide understanding of risk relationships. Institutions that adopt common risk taxonomies and integrated approaches to risk management are generally better positioned to identify emerging threats, coordinate responses, and support informed decision-making. By providing a common reference structure, the Periodic Risk Tables framework supports communication between boards, senior management, business functions, and risk practitioners.

For Indian organisations, this approach is particularly relevant given rapid digitalisation, regulatory evolution, growing global interconnectedness, climate-related pressures, and technological disruption. The framework is designed to provide sufficient standardisation to support comparability and governance requirements while remaining flexible enough to accommodate sector-specific risk characteristics.

Cross-Sectoral Risk Patterns and Emerging Themes

Analysis across the sectors covered in this study indicates that many of the most significant risks are common across industries, although their manifestations and implications vary by sector. Risks related to cybersecurity, data governance, artificial intelligence, climate change, supply chain disruption, geopolitical uncertainty, and workforce capability recur across the sector risk registers compiled for this study, and were also prominent in the practitioner responses received. Given the size of the response base, these should be read as directional themes rather than as statistically representative findings.

While these risks recur across sectors, their interaction depends on industry-specific operating environments. In financial services, technology-related risks frequently intersect with regulatory, conduct, and model risks. In sectors such as manufacturing and infrastructure, supply chain vulnerabilities interact closely with safety, climate, and operational risks. In technology-driven and consumer-facing industries, cyber resilience, platform reliability, reputation, and data ethics are often closely linked.

The cross-sector analysis reveals several recurring themes.

First, a relatively small number of risks act as catalysts for broader disruption. Cyber incidents, climate-related events, infrastructure failures, and reputation-driven crises frequently trigger secondary impacts across multiple risk categories and business functions.

Second, governance, leadership, and organisational culture consistently emerge as factors that influence the severity and propagation of risk events. Strong governance structures and risk-aware cultures enhance resilience, while weaknesses in these areas can amplify the effects of disruptions.

Third, the distinction between strategic, operational, and technological risks is becoming increasingly blurred. Digitalisation, interconnected infrastructure, and platform-based business models have created an environment in which disruptions frequently cross traditional organisational boundaries.

Finally, the analysis highlights the growing importance of systemic and interconnected risks. Risks no longer emerge solely within individual organisations or sectors; they increasingly arise through networks of suppliers, technology providers, infrastructure systems, regulators, and broader economic ecosystems. As a result, understanding interdependencies has become a critical component of effective enterprise risk management.

The Periodic Risk Tables framework is intended to support this understanding by providing a structured mechanism for identifying, classifying, and monitoring risks across sectors. By making risk relationships more visible, the framework supports prioritisation, scenario analysis, risk communication, and resilience planning.

Overall, the findings of this report indicate that the risk environment faced by organisations is increasingly shared, interconnected, and dynamic. The Periodic Risk Tables approach provides a practical framework for understanding these relationships and strengthening enterprise-wide risk management, while supporting a more resilient and forward-looking approach to organisational decision-making.

Chapter 1

Introduction

1.1 The Evolution of Enterprise Risk Management (ERM) in India

Enterprise Risk Management (ERM) in India has undergone a significant transformation over the past two decades, evolving from a traditionally fragmented, compliance-driven function into a more integrated, strategic discipline. Historically, risk management within Indian organisations was largely confined to financial risk controls, insurance, and regulatory compliance, with limited emphasis on enterprise-wide risk integration or strategic risk considerations. This approach has been primarily reactive, focusing on mitigating risks after their occurrence rather than anticipating and managing them proactively.

The liberalisation of the Indian economy in the 1990s marked a critical turning point in the evolution of risk management practices. Increased exposure to global markets, foreign investment, and international competition introduced new dimensions of risk, including market volatility, currency fluctuations, supply chain dependencies, and geopolitical uncertainties. As Indian organisations expanded both domestically and globally, the need for more structured and comprehensive risk management frameworks became increasingly evident.

Regulatory developments played a pivotal role in accelerating ERM adoption. Authorities such as the RBI, SEBI, and the MCA strengthened governance expectations, while frameworks such as Clause 49 and the SEBI Listing Regulations enhanced board accountability. These changes encouraged organisations to formalise risk governance and reporting structures.

In parallel, global frameworks such as the COSO Enterprise Risk Management framework and ISO 31000 began influencing Indian risk management practices, particularly among large corporates and multinational organisations. This led to the gradual adoption of enterprise-wide approaches to risk management, integrating risk considerations across functions such as operations, finance, technology, and compliance. However, in many cases, ERM implementation remained largely compliance-oriented, with periodic assessments and limited integration into strategic decision-making.

In recent years, the risk landscape in India has grown increasingly complex and dynamic, driven by rapid digitalisation, the proliferation of cybersecurity threats, evolving regulatory expectations, and heightened focus on environmental, social, and governance (ESG) factors. The COVID-19 pandemic further underscored the limitations of traditional risk management approaches, exposing vulnerabilities in supply chains, workforce preparedness, and business continuity planning. Organisations were compelled to reassess their risk frameworks and adopt more agile and resilient approaches to managing uncertainty.

Today, ERM in India is gradually shifting toward a forward-looking, resilience-oriented model that aligns risk management with organisational strategy and value creation. Leading organisations are increasingly embedding risk considerations into strategic planning, leveraging data analytics for real-time risk monitoring, and fostering a risk-aware culture across the enterprise. There is also a growing recognition of the need to manage interconnected and systemic risks, particularly in areas such as technology, climate, and global supply chains.

Despite this progress, several challenges remain. Many organisations continue to face issues related to siloed risk ownership, inconsistent risk assessment methodologies, and limited integration of risk management into business decision-making processes. Variations in maturity levels across sectors further highlight the uneven adoption of ERM practices within the Indian context.

Against this backdrop, there is a clear need for structured, standardised, and dynamic tools that can support organisations in navigating an increasingly complex risk environment. Frameworks such as Periodic Risk Tables offer a practical approach to enhancing risk visibility, enabling continuous monitoring, and supporting data-driven decision-making, thereby strengthening organisational resilience in the Indian context.

1.2 Context: Changing Risk Environment

Organisations today operate in a highly dynamic environment characterised by Volatility, Uncertainty, Complexity, and Ambiguity (VUCA). A combination of structural forces is reshaping the external risk landscape and increasing the frequency and intensity of disruptions. This era of deep, continuous disruptions has been further articulated in models such as BANI (Brittle, Anxious, Non-linear, Incomprehensible), RUPT (Rapid, Unpredictable, Paradoxical, Tangled), TUNA (Turbulent, Uncertain, Novel, Ambiguous), and PUMO (Polarised, Unthinkable, Metamorphic, Overheated)

Key drivers of this change include rapid technological advancement, geopolitical instability, evolving regulatory expectations, and environmental pressures. The accelerated adoption of digital technologies and artificial intelligence (AI) has created new operational dependencies while simultaneously introducing risks related to cybersecurity, data privacy, and system resilience. At the same time, geopolitical tensions and global economic shifts are disrupting trade flows, supply chains, and investment environments, requiring organisations to continuously adapt to changing conditions.

Regulatory complexity is also increasing, with organisations facing a growing volume of compliance requirements across jurisdictions. In parallel, climate change and broader environmental concerns are emerging as critical risk factors, influencing both physical assets and long-term business sustainability.

These structural drivers are not isolated; rather, they collectively contribute to a more uncertain and rapidly evolving operating environment. As a result, organisations have to navigate a landscape where external conditions are constantly shifting, and risks are becoming more difficult to anticipate using traditional approaches.

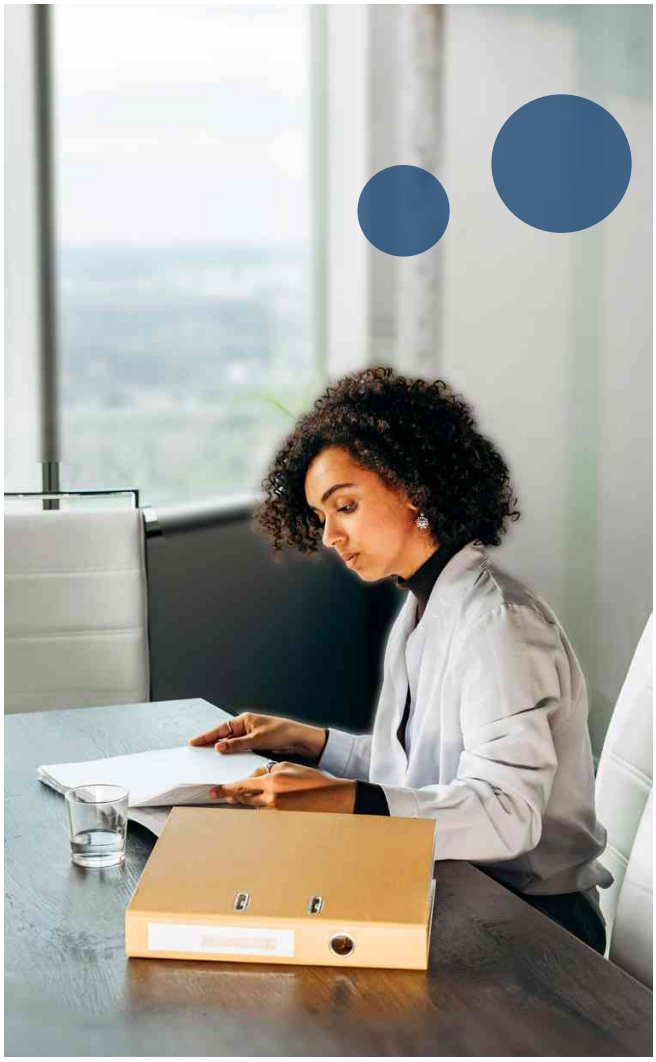
1.3 Evolution of the Global Risk Landscape

In response to these changing conditions, the nature of risks themselves has undergone a fundamental transformation. Risks are no longer discrete or isolated events; instead, they are increasingly interconnected, systemic, and capable of propagating across organisational and sectoral boundaries.

Modern risk environments are characterised by interdependency and non-linearity, where disruptions in one area can trigger cascading effects across multiple domains. For example, disruptions within supply chain networks can spread rapidly across interconnected partners, amplifying operational and financial impacts. Similarly, cybersecurity incidents affecting third-party vendors can extend beyond the initial point of failure, exposing entire ecosystems to risk.

This shift reflects a move from predictable, event-based risks to complex, networked risk systems. The increasing interconnections between technology, operations, and external stakeholders mean that risks can escalate quickly and with limited warning.

As a result, organisations must move beyond traditional approaches that assess risks in isolation and instead adopt methods that account for systemic relationships, dependencies, and potential ripple effects across the enterprise.



1.4 Limitations of Traditional Risk Management

Traditional risk management frameworks, while foundational, are increasingly inadequate in addressing the complexities of today's risk environment. Historically, these approaches were designed for relatively stable and predictable conditions, where risks could be identified, assessed, and mitigated within defined boundaries. However, in the current context of rapid change and heightened uncertainty, their effectiveness has become increasingly constrained.

One of the primary limitations of traditional risk management is its reactive orientation. Risks are often addressed only after they materialise or when their impact becomes evident, rather than being anticipated and proactively managed. This limits an organisation's ability to prepare for emerging threats or respond swiftly to evolving situations.

In addition, traditional frameworks tend to operate in silos, with risk ownership distributed across functions such as finance, operations, compliance, and technology. This fragmented approach restricts visibility across the enterprise and makes it difficult to capture interdependencies between risks. As a result, organisations may overlook broader systemic exposures and underestimate the potential for risks to interact and amplify one another.

Another significant constraint is the reliance on periodic risk assessments, which are typically conducted at fixed intervals. While these assessments provide structured insights, they do not capture the dynamic nature of risk in real time. In rapidly changing environments, risk profiles can shift faster than traditional review cycles allow, leading to outdated assessments and delayed responses.

Traditional approaches also rely heavily on historical data and past trends to evaluate risk likelihood and impact. While useful in stable environments, this retrospective focus is less effective in anticipating novel or unprecedented risks, such as those arising from technological disruption or global crises. Consequently, organisations may struggle to detect early warning signals or emerging patterns.

Furthermore, traditional risk management often lacks integration with strategic decision-making. Risk assessments are frequently treated as compliance exercises rather than as inputs into business strategy, investment planning, or operational design. This disconnect limits the ability of organisations to align risk management with value creation and long-term objectives.

The absence of real-time monitoring and data-driven insights further compounds these challenges. Without continuous visibility into risk indicators, organisations face delays in identifying changes in risk exposure and responding effectively.

Collectively, these limitations create a critical gap between risk awareness and actionable insight. While risks may be documented and reported, the ability to translate this awareness into timely, informed decisions remains constrained. Addressing this gap requires a shift away from static, fragmented approaches toward more integrated, dynamic, and responsive risk management frameworks.

1.5 Need for a Dynamic Risk Framework

The limitations of traditional approaches highlight the need for a more dynamic and integrated risk management framework. Addressing these gaps requires a shift away from static, periodic assessments toward continuously evolving systems that are capable of responding to rapidly changing risk conditions.

A dynamic risk framework enables continuous monitoring and timely assessment of risks, allowing organisations to identify changes in risk exposure as they occur. By leveraging data, analytics, and real-time indicators, such frameworks provide enhanced visibility into emerging trends and potential disruptions. This improves the organisation's ability to respond proactively rather than reactively.

In addition to real-time awareness, a dynamic framework promotes a holistic, enterprise-wide perspective, breaking down functional silos and enabling the identification of interdependencies across risks. This integrated view is critical in understanding how risks interact and propagate across different areas of the organisation.

Equally important is the alignment of risk management with strategic and operational decision-making. Rather than functioning as a standalone or compliance-driven activity, risk management must be embedded within core business processes, informing planning, investment decisions, and performance management. This integration ensures that risk considerations are incorporated into value creation rather than treated as separate constraints.

Leading research indicates that organisations need to transition from viewing risk management as a defensive function to positioning it as a strategic enabler of resilience and competitive advantage. Integrating enterprise risk management with resilience allows organisations to anticipate, adapt, and respond effectively to disruptions while maintaining continuity and long-term value creation.

Ultimately, a dynamic risk framework supports a more adaptive and responsive organisational posture, enabling organisations not only to manage uncertainty but also to leverage it as a source of strategic opportunity.

1.6 Introduction to Periodic Risk Tables and their role in Organisational Resilience

Periodic Risk Tables represent a structured and dynamic approach to risk management, enabling systematic identification, prioritisation, and monitoring of risks across the enterprise. Built on a 5×5 likelihood -impact model, they provide a consistent framework for assessing risks based on their probability and potential severity, supporting standardised and comparable risk evaluation.

The framework incorporates heatmap visualisation techniques to deliver a clear and intuitive representation of risk exposure. By enabling periodic updates, it facilitates continuous tracking of evolving risk profiles, allowing organisations to move beyond static assessments and maintain up-to-date visibility into their risk landscape.

Unlike traditional risk registers, which often reflect a point-in-time view, Periodic Risk Tables support structured, time-based tracking of risks. This allows organisations to identify shifts in risk levels, detect emerging patterns, and monitor changes in risk velocity and concentration over time. Such insights are critical in understanding not only individual risks but also broader trends and systemic exposures.

By enhancing visibility and enabling ongoing analysis, Periodic Risk Tables strengthen data-driven decision-making at both operational and strategic levels. They support more effective risk prioritisation, improve trend analysis, and provide early warning signals that allow organisations to respond proactively to potential disruptions.

Importantly, Periodic Risk Tables contribute directly to organisational resilience by aligning risk insights with strategic objectives. They enable organisations to anticipate and adapt to changing conditions, rather than reacting after risks materialise. As organisations increasingly adopt resilience-centric operating models, these tools offer a practical and scalable mechanism to embed risk awareness into decision-making processes and support sustained performance in an uncertain and evolving environment.

Chapter 2

Periodic Risk Tables – Framework Overview

2.1 Defining "Elements"of Risk

The Periodic Risk Tables framework is built on the fundamental concept of treating risks as distinct but interconnected elements within an organised system. In this framework, each "element" represents a specific, identifiable risk that can be clearly defined, described, and assessed in terms of its underlying drivers, potential impact, and likelihood of occurrence. A Risk element can be defined as the lowest practical unit of enterprise-level risk classification within the framework. Unlike traditional risk registers, where risks are often listed in isolation, the concept of risk elements emphasises structure, comparability, and interrelationship. Each element functions as a standardised unit of analysis, enabling consistent classification across sectors and facilitating aggregation into broader patterns.

Risk elements are not static; their significance, connectivity, and behaviour may evolve over time as internal and external conditions change. Hence these elements are defined not only by their immediate manifestation but also by the underlying drivers that generate them. For example, a cybersecurity breach, a data privacy violation, and a system outage may appear as distinct risks but are often linked by a common technological dependency. The framework captures both the individual identity of risks and their embedded connections within a wider system.

By decomposing the risk landscape into discrete elements, the Periodic Table approach enables organisations to move beyond fragmented identification toward a more systematic understanding of how risks originate, interact, and evolve over time.

2.2 Risk Families & Groups

To provide structure and coherence, individual risk elements are organised into broader families or groups based on shared characteristics and underlying drivers. These groups represent major dimensions of enterprise risk exposure and allow organisations to view risks at both granular and aggregated levels.

The major risk families can be summarised as follows:

Although these categories provide structural clarity, they are inherently interconnected. A single risk element may belong to multiple families depending on its context and impact. For example, a technology failure may simultaneously represent an operational disruption, a financial exposure, and a reputational risk.

The grouping process therefore does not create rigid silos but enables multi-dimensional classification, reflecting the complexity of modern risk environments.

Risk Family	Description	Example
Strategic	Risks affecting long-term positioning and business model viability	Market disruption, failed mergers
Financial	Exposure to market volatility, liquidity, and capital constraints	Currency fluctuations, credit risk
Operational	Risks arising from internal processes, people, or systems	Process failure, supply chain disruption
Regulatory	Risks from evolving compliance and policy environments	Non-compliance penalties
Technological	Risks linked to digital infrastructure and data systems	Cybersecurity breach
Environmental	Risks related to climate, resources, and sustainability	Climate transition risk
Social	Risks from workforce and stakeholder dynamics	Labour unrest
Governance & Ethical	Risks arising from weak governance structures or unethical practices	Fraud, misconduct
Geopolitical & External	Risks driven by external macroeconomic or geopolitical conditions	Trade restrictions, political instability

The nine risk families described above provide a high-level vocabulary for discussing enterprise risk with boards and senior management. They are deliberately broad, and a single risk element may sit in more than one family. They are not, however, the classification used to construct the Periodic Risk Tables themselves. For that purpose the study applies the IRM Risk Wheel, a more granular scheme described in Section 3.4, which assigns each risk element to exactly one category and thereby permits consistent aggregation across sectors. The two operate at different levels: the risk families are the language of the framework, while the IRM Risk Wheel is the coding scheme behind the tables. The two-letter code displayed on each element refers to the IRM Risk Wheel category, not to the risk family.

2.3 Risk Severity, Velocity, Interdependencies

A distinguishing feature of the Periodic Risk Table framework is its emphasis on understanding not only the existence of risks but also their behaviour across three critical dimensions: severity, velocity, and interdependency.

Risk severity captures the magnitude of potential impact and is assessed through a multi-dimensional lens that includes financial loss, operational disruption, regulatory consequences, reputational damage, safety implications, and systemic effects. Severity reflects the highest plausible enterprise impact across multiple dimensions rather than a single-point estimate.

Risk velocity refers to the speed at which a risk can materialise and propagate. High-velocity risks are typically associated with immediate and potentially severe impact, requiring rapid detection, escalation, and response mechanisms. In contrast, low-velocity risks often exhibit high persistence, with impacts accumulating gradually over time, but can ultimately become equally significant or more so if left unmanaged. In highly interconnected environments, certain risks—such as cyber incidents or reputational events—can escalate rapidly, leaving limited time for response, while others—such as climate risks or strategic misalignment—develop slowly but create sustained pressure on organisational performance. Interdependencies represent the relationships between risks and the pathways through which they interact. Risks rarely exist in isolation; instead, they form networks where disruptions in one area can trigger cascading effects across multiple domains. For example, a technology failure can disrupt operations, increase financial exposure, and trigger regulatory scrutiny, creating a chain of consequences.

Together, these three dimensions provide a dynamic understanding of risk, enabling organisations to move beyond static assessment toward a more system-oriented perspective.

2.4 Colour Coding, Category Codes, and Sector-Specific Adaptation

The visual representation of the Periodic Risk Table is a critical component of its effectiveness as a decision-support tool. Colour coding and alphabetic category coding are used to enhance clarity, simplify interpretation, and enable rapid identification of risk priorities. Category codes and textual indicators supplement colour coding to improve accessibility and reduce reliance on colour perception alone.

Colour coding is aligned with the likelihood–impact scoring framework based on a 5×5 matrix. Risks are classified into three categories based on their composite scores. For all the sectors risks with a composite score less than or equal to 8 are categorised as low-risk and represented in green. Risks with scores ranging from 9 to 14 are classified as moderate-risk and represented in yellow. Risks with composite scores greater than or equal to 15 are categorised as critical-risks and represented in red. This classification enables clear visual differentiation of risk intensity and supports prioritisation of management attention and resources.

Each element carries a two-letter alphabetic code denoting the risk category to which it belongs, drawn from the IRM Risk Wheel classification described in Section 3.4 and expanded in the category key printed beneath every table. This coding supplements the colour bands, so that risk category and risk level can each be read independently of colour perception.

Each risk element is represented within a structured visual box designed to convey multiple dimensions of information in a standardised format. The top-left edge of each box carries the two-letter code of the risk category to which the element belongs, while the top-right corner reflects the composite risk score. The central portion of the box contains the name of the risk, providing immediate identification. The bottom-left corner presents the element's unique reference number (R1, R2, …) together with its likelihood and impact scores, shown in the form L:x I:y, offering transparency into the underlying assessment. The bottom-right corner indicates the level of risk—categorised as Low, Moderate, or Critical—based on the defined scoring thresholds.

How to Read a Periodic Risk Table Element

Figure 2.1 shows the anatomy of a single element. Reading clockwise from the top-left: the coloured edge strip carries the two-letter risk category code; the top-right corner shows the composite score (likelihood × impact, range 1–25); the bottom-right corner shows the resulting risk band (LOW for scores of 8 or below, MOD for 9 to 14, CRIT for 15 and above); and the bottom-left corner carries the element's unique reference number together with its likelihood and impact scores in the form L:x I:y. The centre of the element shows its two-letter symbol and full risk name. The fill colour of the score and band panels repeats the band classification — green for low, amber for moderate, red for critical — so that priority can be read at a glance.

At a structural level, each row within the Periodic Risk Table represents a distinct risk category or family, enabling clear visual grouping and comparative analysis across related risks.

At the same time, the framework allows for sector-specific adaptation. While the structure of the Periodic Risk Table remains standardised, the interpretation of elements can vary based on industry context. Certain risks may carry higher significance in specific sectors, for example, safety risks in aviation, liquidity risks in financial services, or environmental risks in energy and infrastructure.

This adaptability ensures that the framework balances standardisation with contextual relevance, making it applicable across diverse industries without losing specificity.

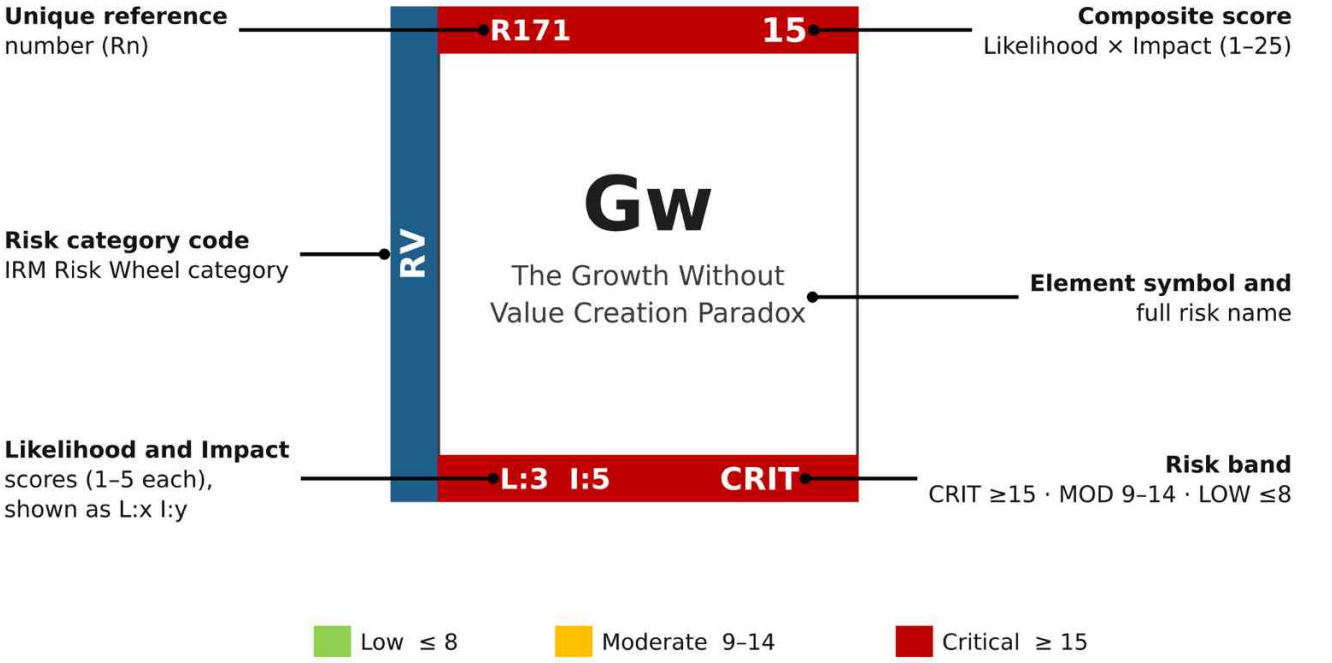
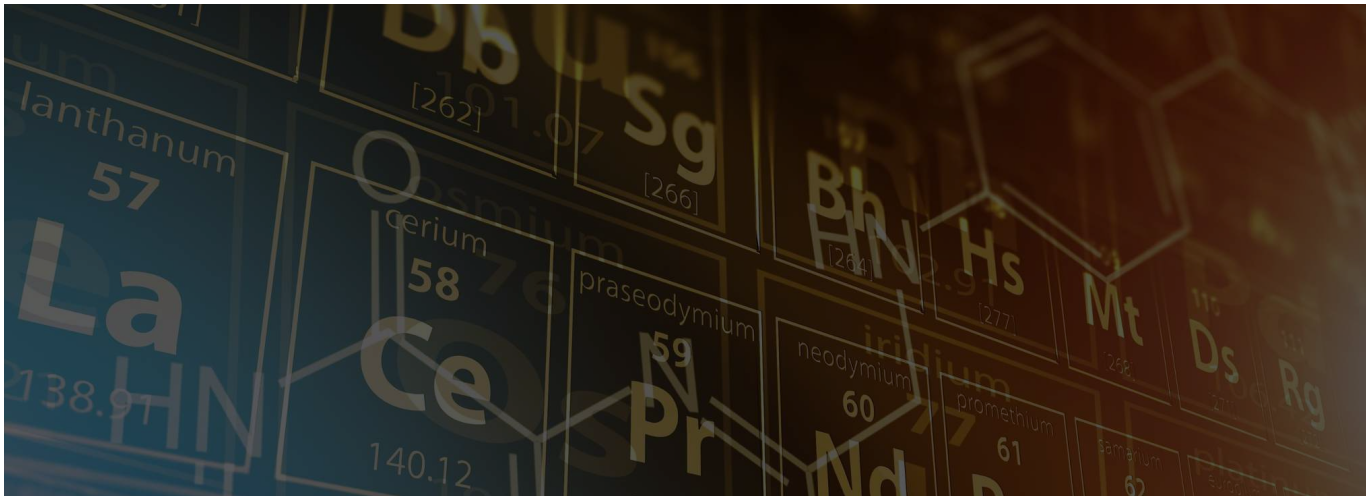


Figure 2.1: Anatomy of a Periodic Risk Table element. The example shown is a critical-band risk with likelihood 3 and impact 5, giving a composite score of 15.



2.5 Mapping Periodic Risk Tables to ERM Processes

The Periodic Risk Table framework is not intended to replace established ERM standards such as COSO ERM or ISO 31000; rather, it serves as a complementary analytic and visualisation layer that enhances risk identification, assessment, and monitoring within these frameworks. Its value lies in its ability to support each stage of the risk management process in a structured and consistent manner.

The framework is 'periodic' not only in its structured arrangement, but also because risk relationships evolve and require continuous reassessment. In the identification phase, the framework provides a comprehensive taxonomy that ensures systematic recognition of risks across categories and sectors. By organising risks into defined elements, it reduces the likelihood of omission and improves coverage of emerging and non-obvious risks.

During the assessment phase, the likelihood–impact scoring model enables consistent evaluation of risk severity, while the inclusion of velocity and interdependency considerations provides additional depth. This supports more informed prioritisation and resource allocation.

In the response phase, the Periodic Risk Table helps organisations align mitigation strategies with risk characteristics. High-velocity risks may require rapid detection and response mechanisms, while high-severity or systemic risks may require structural resilience measures.

Finally, in the monitoring phase, the framework supports continuous tracking of risk evolution. By enabling periodic updates and visualisation of changing risk profiles, it allows organisations to detect trends, identify emerging exposures, and adjust strategies accordingly. While not a dedicated scenario modelling tool, the framework supports scenario analysis and stress testing by revealing concentrations of interconnected risks and potential cascade pathways, thereby improving the design and relevance of stress scenarios.

By linking risk identification, assessment, response, and monitoring within a unified structure, the Periodic Risk Table transforms risk management from a static reporting exercise into a dynamic, continuous process aligned with organisational strategy and resilience objectives.

Chapter 3

Research Methodology

3.1 Methodological Approach

The Periodic Risk Tables (PRT) framework was developed using a mixed-methods research design combining structured industry inputs, faculty-led sectoral analysis, desk research, expert judgement, and risk scoring. The research integrates two primary input streams: a structured questionnaire capturing practitioner perspectives, and faculty-led risk identification supported by secondary research and domain expertise. A third component, the construction of illustrative sector case studies, is described in Section 3.13.

The study adopted an exploratory mixed-methods research design combining qualitative risk identification, structured expert input, and semi-quantitative scoring. Primary research was conducted through the questionnaire, while secondary research included analysis of industry reports, academic literature, regulatory publications, ESG disclosures, and publicly available data. Faculty-led synthesis integrated these inputs into sector-level risk perspectives.

The objective was to identify, classify, score, and compare key risks across major sectors of the economy while retaining the distinctive characteristics of each sector's operating environment.

The methodology was guided by three core principles. First, it required sufficient standardisation to enable comparison across sectors. Second, it needed to remain sector-sensitive, recognising that risks manifest differently across industries such as aviation, healthcare, financial services, telecom, agriculture, tourism, infrastructure, and public services. Third, it aimed to move beyond a descriptive listing of risks toward a structured understanding of risk interdependencies, systemic exposure, and emerging risk clusters.

These principles ensured that the framework remains both analytically rigorous and grounded in real-world industry perspectives, while also enabling cross-sector comparability.

3.2 Industry Coverage and Sector Allocation

The study covered nineteen industries: Healthcare and Pharma; Information Technology and IT-enabled Services; Hospitality; Tourism; Media; Retail; Oil and Gas; Aviation; Financial Services; Government and Public Services; Telecom; Education; Food; FMCG; Agriculture; Mining; Energy; Manufacturing; and Infrastructure. The selected sectors collectively represent significant components of the Indian economy in terms of GDP contribution, employment, and systemic relevance. While the study aimed to achieve broad sectoral coverage, certain niche or emerging industries were outside the scope of this phase.

Industries were allocated to Mahindra University faculty members based on their expertise, training, prior work experience, or research interests. Prof. Shivdasini Singh Amin analysed the sectors of hospitality, tourism, media, retail, and oil and gas; Assoc Prof. Keerti Pendyal analysed the sectors of aviation, financial services, government and public services, and telecommunications. Assoc Prof. Sri Kalyana Rama Jyosyula analysed mining, energy, manufacturing, and infrastructure. Asst Prof. Binay Pathak analysed education, food, FMCG, and agriculture. Asst Prof. Nidhi Goyal analysed the healthcare, pharmaceuticals, IT, and IT-enabled services.

For presentation in the report, industries were organised into sector groups. This enabled detailed sector-specific insights while also facilitating cross-sector comparison and identification of broader patterns. The grouping also helped distinguish risks that are unique to individual sectors, those that recur across related sectors, and those that cut across the economy.

3.3 Faculty Led Risk Identification

In addition to industry inputs, faculty members conducted sector-specific risk identification through expert analysis and structured secondary research sources Secondary sources included annual reports, sectoral publications, regulatory filings, ESG reports, policy papers, and publicly available industry analyses, providing both quantitative data points and qualitative insights into sector-specific risk conditions. This process included review of sectoral developments, regulatory and policy frameworks, industry reports, ESG disclosures, academic literature, and benchmarking against both Indian and global operating environments.

The purpose of this exercise was to develop a comprehensive view of sectoral risks, capturing not only frequently cited risks but also emerging and less visible exposures. The analysis covered a broad spectrum of risk types, including financial, operational, strategic, regulatory, technological, environmental, social, geo-political, reputational, and governance-related risks. It also incorporated sector-specific dependencies such as supply chains, critical infrastructure, workforce availability, digital platforms, and public policy frameworks.

Identified risks were recorded in a standardised risk register format capturing risk descriptions, drivers, IRM Risk Wheel classification, likelihood and impact scores, composite scores, and supporting notes. This approach ensured consistency while preserving sector-specific context. Where risks overlapped within a sector, they were consolidated where appropriate; however, sector-specific expressions were retained where differences in manifestation were material.

The number of risk elements identified varies by sector, reflecting differences in the level of granularity applied during sector-level analysis. Element counts should not be read as a measure of relative risk exposure between sectors.

3.4 IRM Risk Wheel – Based Classification

The IRM Risk Wheel was used as the common classification framework for organising identified risks across sectors. This ensured that risks were not assessed narrowly through a single dimension, such as financial loss or operational disruption, but instead evaluated through a broader enterprise risk management perspective.

The IRM Risk Wheel was selected due to its comprehensive enterprise-wide coverage and its suitability for cross-sector ERM analysis, enabling consistent classification of risks across diverse industries.

The IRM Risk Wheel comprises eighteen categories of enterprise risk, each of which is represented in the Periodic Risk Tables by a two-letter code: Strategic Objectives (SO), Governance (GV), Reputation & Ethics (RE), Legal Liability (LL), Political and Social (PS), Economic (EC), Credit & Market (CM), Liquidity (LQ), Reward & Value (RV), Technology (TE), Information (IN), Business Continuity (BC), Supply Chain (SC), Projects & Change (PC), Employment (EM), Personal Effectiveness (PE), Natural Events (NE), and Environment (EV). These codes appear on every element of every Periodic Risk Table and are expanded in the category key printed beneath each table. The Risk Wheel is illustrated in Figure 3.1 below, adapted from the framework published by the Institute of Risk Management.

Each identified risk was mapped to an appropriate category within the IRM framework. This ensured coverage across multiple risk types and reduced the likelihood of underrepresentation of risks such as people risk, governance risk, technology risk, compliance risk, or external environment risk.

The IRM-based classification also enabled cross-sector aggregation. Once risks from different industries were mapped into common categories, it became possible to identify recurring patterns and systemic themes, including technology disruption, cybersecurity risks, regulatory complexity, climate exposure, talent constraints, infrastructure dependency, and reputational vulnerability.

Figure 3.1: The IRM Risk Wheel — the eighteen risk categories used to classify every element in the Periodic Risk Tables, shown with the two-letter code by which each category appears on the tables. Adapted from the Institute of Risk Management.

3.5 Likelihood-Impact Scoring Framework

Each risk was assessed using a likelihood-impact scoring framework based on a five-point scale, where 1 represents very low likelihood or impact and 5 represents very high likelihood or impact. Composite risk scores were derived using a likelihood × impact approach and used to prioritise risks within each sector, forming the basis of the Periodic Risk Table.

The scoring framework provided a structured approach to distinguishing between low-, moderate- and critical-priority risks. Risks with both high likelihood and high impact were placed in the highest-priority zones, while low-likelihood but high-impact risks were also treated carefully, particularly in sectors where rare events can have systemic or irreversible consequences.

The scoring approach deliberately avoided a purely mechanical structure. Scores were calibrated to reflect sector realities rather than applying uniform thresholds across industries, recognising differences in scale, capital intensity, regulatory exposure, and stakeholder expectations.

Impact scores incorporated multiple dimensions, including financial loss, operational disruption, regulatory consequences, reputational and stakeholder impact, safety implications, public welfare, systemic consequences, and environmental effects. In several cases, the final score reflected the most severe impact dimension rather than an average, ensuring that high-consequence risks were not understated.

3.6 Sector-Calibrated Scoring, Composite Scores, and Heatmaps

While the 1–5 scoring scale provided a common structure, interpretation of likelihood and impact was calibrated to each sector's operating context. This calibration reflected differences in regulatory sensitivity, stakeholder expectations, operational dependencies, reputational exposure, and systemic importance. Calibration influenced interpretation within sectors but retained a common structural scale to preserve directional comparability across sectors.

Sector-specific calibration ensured that scoring remained meaningful within context. For example, aviation and oil and gas emphasised safety and catastrophic impact; financial services emphasised systemic interconnectedness; public sector analysis focused on citizen welfare; telecom prioritised infrastructure and data integrity; and consumer sectors emphasised reputational risk and demand sensitivity.

Heatmaps are intended not only as visual representations but as decision-support tools. They enable identification of concentrated zones of exposure and support prioritisation of mitigation strategies across prevention, detection, response, and resilience dimensions.

3.7 Cross-Sector Consolidation and Clustering

After sector-wise risk registers were developed, risks were analysed across sectors to identify broader themes and interdependencies. This involved comparing risk descriptions, drivers, classifications, scoring outcomes, and qualitative insights.

The clustering process was based on thematic grouping and interpretive synthesis rather than statistical clustering techniques. Risks were grouped based on conceptual similarity, underlying drivers, and observed interdependencies across sectors. Clusters were further refined iteratively through review and validation to minimise duplication and ensure conceptual consistency.

The clustering process was based on two key dimensions:

commonality and interdependency. Commonality refers to risks that appear across multiple sectors, such as cybersecurity, regulatory change, technology disruption, climate exposure, supply chain disruption, talent shortages, reputational risk, and geopolitical uncertainty.

Interdependency captures how risks propagate across sectors, creating cascading effects. For example, telecom disruptions can affect digital payments, logistics, public services, and IT-enabled services, while energy disruptions can affect manufacturing, infrastructure, transport, agriculture, and healthcare.

The outcome of this process was both sector-specific risk registers and cross-sector risk clusters, enabling the framework to support both operational risk management and system-level analysis.

3.8 Purpose of the Questionnaire

To ensure that the Periodic Risk Tables framework is grounded in practical, industry-led insights, a structured questionnaire was developed as a primary research instrument. The questionnaire was designed to systematically capture perceptions of risk, emerging trends, and organisational preparedness across multiple sectors. It aimed to bridge the gap between conceptual risk frameworks and real-world business environments by incorporating inputs from practitioners actively engaged in risk management, strategy, finance, and compliance functions.

The primary objective of the questionnaire was to identify the most significant current and emerging risks faced by organisations, while also understanding how these risks are prioritised and managed. Additionally, the questionnaire sought to capture insights into the interconnected nature of risks, assess organisational risk appetite and tolerance, and evaluate the readiness of organisations to respond to disruptions. These insights were used to support the development of Periodic Risk Tables as well as sector-specific risk analyses presented in this report.

The questionnaire utilised a combination of response formats to capture both qualitative and semi-quantitative insights. These included open-ended questions for detailed descriptive inputs, structured multiple-choice questions for categorical responses (such as low, moderate, and high), Likert scale-based questions (typically on a 1–5 scale) to assess levels of impact, importance, and preparedness, and ranking-based questions to prioritise key risks, governance enablers, and strategic focus areas. In addition, respondents were asked to provide semi-quantitative assessments, such as financial impact ranges and percentage allocations, enabling comparison across organisations. This combination of response types ensured that the questionnaire captured both depth of insight and consistency of interpretation, supporting robust cross-sector analysis.

3.9 Coverage and Respondent Profile

The questionnaire was administered to a targeted group of respondents representing the key sectors covered in this study. For each sector, the top five companies were identified based on market capitalisation, ensuring that the sample reflected leading organisations with significant market presence and operational scale. The questionnaire was shared with Chief Risk Officers (CROs) and other senior risk professionals within these organisations, along with domain experts across functions such as risk management, finance, strategy, and compliance.

The data collection exercise was conducted over a one-month period, allowing sufficient time for detailed and considered responses. A total of 38 responses were received, representing a combination of senior leadership perspectives and operational insights. This approach ensured that the findings captured both strategic viewpoints and ground-level realities of risk management practices.

The respondent base included senior leadership roles such as chief risk officers and functional heads, as well as domain specialists with direct responsibility for risk identification and mitigation. This mix enabled a balanced representation of perspectives across decision-making and implementation levels. Furthermore, the cross-sector nature of the sample facilitated the identification of common risk themes across industries while also highlighting sector -specific differences in risk exposure, priorities, and management approaches.

3.10 Structure of the Questionnaire

The questionnaire was structured to provide comprehensive coverage of the organisational risk landscape, with each section designed to capture a specific dimension of risk management.

The initial section focused on respondent and organisational profile, capturing basic details such as industry classification, organisational size, and respondent role. This information was used to contextualise responses and enable segmentation of findings during analysis.

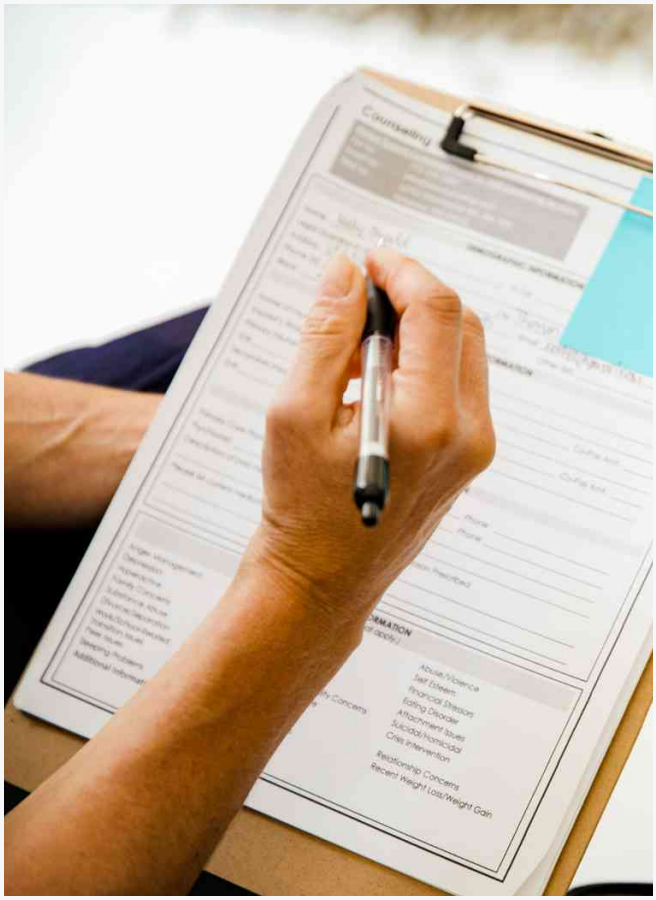
Subsequent sections examined the broader industry context, including key dependencies, external pressures, and sector-specific characteristics that influence risk exposure. Respondents were then asked to identify and describe the key risks they currently face, as well as those increasing in significance and those expected to emerge over time. This enabled the identification of both current and emerging risk themes.

Further sections explored organisational risk appetite and tolerance, seeking to understand how organisations define acceptable levels of risk and how these thresholds influence decision-making. Respondents were also asked to assess the impact and likelihood of identified risks, along with their organisation's level of preparedness and existing mitigation measures.

The questionnaire also included sections on governance, compliance, and risk culture, focusing on the extent to which risk management is embedded within organisational structures and decision-making processes. This was complemented by questions on the use of data, technology, and analytics in risk identification and monitoring, reflecting the growing importance of digital tools in modern risk management.

In addition, respondents were asked to provide insights into external environmental factors, such as regulatory changes, geopolitical developments, and macroeconomic conditions, and their influence on organisational risk profiles. The questionnaire also captured key barriers and constraints faced by organisations in managing risks effectively, including challenges related to data availability, resource limitations, and integration across functions.

Finally, a dedicated section was included to gather perspectives on emerging risks and recommended strategies for strengthening organisational resilience over time.



3.11 Data Usage in the Report

The responses collected through the questionnaire were aggregated and anonymised to ensure confidentiality and encourage candid participation. A thematic analysis approach was applied, with responses coded into recurring risk themes. Frequency and severity scores were combined to identify high-priority risks across sectors.

The insights derived from the questionnaire were used to inform multiple components of this report, including the identification of dominant risk themes, the development of cross-sectoral risk patterns, and the creation of sector-specific Periodic Risk Tables. The findings also supported the design of visual representations, such as risk heatmaps and infographics.

Given the perception-based nature of the responses, the analysis focused on deriving directional insights rather than statistically representative conclusions. The findings should therefore be interpreted as reflective of industry sentiment and practitioner experience.

3.12 Strengths and Limitations of the Questionnaire

The questionnaire-based approach provides several strengths that enhance the overall robustness and relevance of the research. Its structured design ensures consistency in data collection across respondents and sectors, while its flexibility enables the capture of both quantitative metrics and qualitative insights. This combination allows for comparability across industries while also preserving contextual depth, enabling the identification of both common risk themes and sector-specific variations.

The inclusion of respondents from multiple sectors further strengthens the framework by supporting cross-industry analysis and uncovering broader patterns within the risk landscape. In addition, the questionnaire incorporates a forward-looking perspective, capturing emerging risks and long-term strategic considerations beyond immediate conditions. By integrating practitioner perspectives, the research remains grounded in real-world experience, ensuring practical relevance for organisational decision-making and risk management practices.

At the same time, certain limitations must be acknowledged. The findings are based on perception-driven responses, which may be influenced by individual judgement, organisational context, and sector-specific priorities. Responses may also reflect organisational positioning or expectations, potentially resulting in overstatement of preparedness or alignment with best practices. Variations in respondent profiles and levels of experience may therefore affect the consistency and comparability of responses.

Given the rapidly evolving nature of geopolitical, technological, and regulatory risks, findings represent a time-sensitive assessment rather than a permanent risk baseline.

The selected approach to respondent sampling introduces additional considerations. The use of a targeted, non-random sample—focused on leading organisations based on market capitalisation—may result in selection bias, with insights more reflective of large, established entities. Consequently, the perspectives of smaller or less-represented organisations may not be fully captured.

Differences in response rates and participation levels across sectors may also influence the depth and breadth of insights obtained. In some cases, uneven sector representation may affect cross-sector comparability and the ability to generalise findings. The depth of insights is also dependent on the completeness and quality of responses provided by participants.

Finally, constraints related to sample size in certain sectors, combined with the time-bound nature of the data collection process, limit the statistical generalisability of results and the ability to fully capture rapidly evolving risk conditions. Accordingly, the insights derived from the questionnaire should be interpreted as directional indicators of risk trends and practitioner perspectives rather than definitive or statistically representative conclusions.

Despite these limitations, the questionnaire remains a critical input to the overall methodology, complementing faculty-led analysis and structured risk frameworks. Together, these elements provide a balanced and multi-dimensional view of risk, supporting both sector-specific insights and broader cross-sector risk analysis.

3.13 Construction of Sector Case Studies

In addition to the sector risk registers, a set of illustrative case studies was developed to demonstrate how the risks identified in this study manifest in practice. These case studies, presented in Chapter 7, are composites: each draws on documented sector patterns, regulatory experiences, and publicly observed risk management dynamics across multiple organisations, rather than on the experience of any single company. Company identities are masked, and financial and operational details have been generalised, in order to preserve confidentiality while retaining instructional accuracy.

Each composite was reviewed by the relevant sector faculty member for plausibility and for alignment with the risk elements identified in the corresponding Periodic Risk Table. The case studies are intended as teaching material illustrating risk dynamics and response patterns; they are not audited accounts of specific incidents and should not be read as such.

Chapter 4

Universal Risks & Cross-Sector Analysis

4.1 Introduction to Universal Risks

In an increasingly interconnected economic and operational environment, organisations are exposed to a set of risks that transcend sectoral boundaries. For the purposes of this study, universal risks are defined as risks that recur across multiple sectors due to shared structural dependencies and that possess the capacity to generate systemic, cascading, or economy-wide impacts.

Analysis of the compiled risk registers shows that these risks consistently recur across sectors and are embedded within the broader economic ecosystem. Risks related to cybersecurity, supply chain disruption, regulatory shifts, and climate events appear with high frequency across datasets, demonstrating that organisations are exposed to structurally common risk drivers.

Universal risks therefore reflect the underlying architecture of the modern Indian economy, where integration amplifies both efficiency and vulnerability. Understanding these risks provides a critical foundation for identifying cross-sector patterns and developing resilient, forward-looking organisational strategies.

4.2 Approach to Identifying Universal Risks

The identification of universal risks is based on the cross-sector consolidation and clustering process described in the Research Methodology section. After sector-wise risk registers were prepared, risks identified across the nineteen industries were compared to determine which risks recurred across sectors and which had the potential to create systemic or cascading effects across the economy.

The purpose of this exercise is not merely to count how often a risk appeared. Instead, the analysis sought to identify risks with broader enterprise relevance across industries, even when their sector-specific expressions differed. A risk is treated as potentially universal when it meets one or more of the following conditions: it appears across multiple sectoral risk registers; it is mapped to recurring IRM Risk Wheel categories; it reflects a common underlying driver such as technology, regulation, climate, talent, or supply chain dependence; or it has the potential to transmit disruption from one sector to another.

The analysis proceeded in four stages. First, the risks identified in the sector-level registers were reviewed using their risk names, descriptions, causes or drivers, IRM Risk Wheel classifications, likelihood scores, impact scores, and supporting qualitative notes. This helped distinguish between risks that were only superficially similar and risks that shared a deeper structural basis. For example, technology risk in financial services, telecom, healthcare, and government services may appear under different descriptions, but all may reflect dependence on digital infrastructure, cyber-security exposure, data governance challenges, and resilience of technology systems.

Second, similar or related risks were grouped into broader cross-sector clusters. Risk clustering was based on two dimensions: recurrence similarity (common appearance across sectors) and transmission dependency (capacity to create cascading cross-sector effects. Examples include cyber risk, regulatory change, technology disruption, climate exposure, supply chain disruption, talent shortage, reputational risk, and geopolitical uncertainty. Interdependency refers to risks that connect sectors or create cascading effects across the wider economy. For instance, telecom disruptions may affect digital payments, logistics, public services, and IT-enabled services; energy disruptions may affect manufacturing, infrastructure, transport, agriculture, and healthcare; and financial stress may spread through credit, investment, insurance, and consumer demand channels.

Third, the research team examined whether each cluster had sector -specific or systemic significance. This distinction is important because a risk may be universally present but not uniformly severe. Cyber risk, for example, is relevant to nearly every sector, but its implications differ across healthcare, financial services, telecom, education, and government services. In healthcare, cyber risk may affect patient data, clinical continuity, and trust in digital health systems. In financial services, it may affect payment systems, depositor confidence, and regulatory scrutiny. In telecom, it may affect network integrity and the national digital infrastructure. Similarly, climate risk appears across agriculture, infrastructure, tourism, energy, and insurance, but the mechanisms of exposure vary by physical assets, supply chains, demand patterns, natural resource dependence, and long-term insurability.

Fourth, the clusters were assessed for their relevance to enterprise risk governance. Risks were prioritised as universal risks where they were found to have cross-sector recurrence, high interdependency, strong potential for escalation, or relevance to board-level and strategic decision-making. This ensured that the universal risk categories were not limited to high-frequency risks but also included risks that could produce severe consequences through systemic transmission. Low-probability but high-impact risks were therefore carefully considered, especially where their consequences could extend beyond a single organisation or sector.

The output of this process is a set of cross-industry enterprise risks that complement the sector-specific Periodic Risk Tables. The sector -specific risk registers preserve industry-level detail and context, while the universal risk categories identify common patterns that cut across

the economy. Together, these two outputs allow the PRT framework to serve both operational and strategic purposes: operationally, by helping organisations understand risks within their own sectors; and strategically, by helping boards, policymakers, and risk professionals recognise interconnected risks that require broader governance attention.

The universal risks identified through this approach should therefore be read as economy-wide risk themes rather than generic risk labels. Their value lies in showing how risks recur, interact, and amplify across industries. This perspective is central to the Periodic Risk Tables framework, which is intended to move beyond static risk registers and support a more dynamic, interdependent, and resilience-oriented approach to enterprise risk management.

4.3 Key Universal Risk Categories

The analysis indicates that universal risks can be grouped into several core categories, each representing a distinct yet inter-connected dimension of risk exposure. These categories are not discrete silos; rather, they represent interrelated dimensions of enterprise vulnerability.

Technological and Cyber Risks represent one of the most dominant categories, driven by pervasive digitalisation across industries. Risks such as cyberattacks on critical infrastructure, large-scale data breaches, AI model failures, and cloud dependencies expose systemic vulnerabilities embedded within interconnected digital ecosystems.

Operational and Supply Chain Risks reflect widespread reliance on complex and often global networks for logistics, vendors, and critical inputs. Disruptions—including vendor failures, infra-structure outages, and logistics constraints—act as immediate operational shocks with cross-sector impact.

Financial and Liquidity Risks remain central, capturing exposure to interest rate volatility, currency fluctuations, macroeconomic cycles, and liquidity constraints. These risks often act as transmission channels through which operational, regulatory, or geopolitical disruptions translate into financial stress.

Regulatory and Compliance Risks arise from dynamic policy environments and evolving enforcement frameworks. Sudden regulatory shifts, increased scrutiny, and compliance failures can disrupt operations, delay decision-making, and increase cost burdens.

Human Capital Risks reflect challenges in talent availability, workforce stability, and skill alignment. In high-growth sectors, skill shortages and capability gaps directly constrain productivity, innovation, and execution capacity.

Geopolitical Risks arise from global instability, trade tensions, geopolitical conflicts, and shifting international alignments. These risks influence cross-border supply chains, energy availability, capital flows, and regulatory environments, often acting as external shock drivers that can trigger or amplify disruptions across sectors.

Strategic Risks relate to long-term organisational positioning, business model viability, and competitive dynamics. These include risks arising from market disruption, technological shifts, innovation gaps, misaligned investments, and failure to adapt to changing customer or regulatory expectations. Such risks directly affect growth trajectories, sustainability, and long-term value creation.

Environmental and Climate Risks are increasing in materiality, driven by extreme weather events, resource constraints, and sustainability pressures. These risks simultaneously affect physical assets, operations, regulatory expectations, and long-term viability.

Reputational and Ethical Risks operate as cross-cutting risks, amplified by digital media and heightened stakeholder scrutiny. Issues such as misinformation, governance failures, and ESG misalignment can rapidly erode stakeholder trust and market confidence.

4.4 Cross-Sector Interdependency Analysis

A central finding of the analysis is that risk is no longer bounded within sectors or institutions but is increasingly shaped by interdependencies across systems, infrastructure, and networks. Traditional approaches to risk management assumed that risks could be identified, bounded, and managed within discrete organisational or sectoral silos. However, this assumption no longer holds. Risks increasingly operate across functional, sectoral, and geographic boundaries, emerging from the connections between systems rather than from isolated sources.

Sectors now function as interconnected nodes within shared infrastructure and dependency networks, where disruptions in one domain propagate rapidly across others rather than remaining contained. For instance, a cyberattack on payment systems or telecom infrastructure can simultaneously disrupt operations across multiple sectors, affect financial systems, and generate reputational consequences. Similarly, disruptions in global supply chains—whether driven by geopolitical developments or environmental events—can cascade across industries, affecting production, logistics, pricing, and financial stability.

Climate-related events further illustrate this systemic behaviour. Extreme weather events can disrupt infrastructure, supply networks,

and workforce availability simultaneously, with cascading implications for insurance, regulatory response, and long-term investment patterns. These impacts are rarely confined to a single geography, often transmitting across interconnected global systems.

Sector-level observations reinforce the relational nature of risk. Risks identified across industries—including financial services, infrastructure, and public systems—consistently converge around shared dependencies such as technology infrastructure, governance frameworks, and supply chains. This convergence demonstrates that risks propagate through common systemic linkages rather than remaining sector-specific.

This interconnected risk structure reflects a broader shift toward a relational risk paradigm, where risk should be understood as an emergent system property arising from the structure, density, and fragility of interdependencies rather than from isolated events. Consequently, effective risk management requires moving beyond siloed frameworks toward a systems-based approach that explicitly accounts for dependencies, feedback loops, and cascading effects. In practical terms, these dynamics may manifest through pathways where a technological disruption triggers operational failure, leading to reputational impact, regulatory intervention, and financial stress, or where external shocks amplify vulnerabilities across multiple sectors simultaneously.

4.5 Systemic & Cascading Risks

Systemic risk is distinguished from conventional organisational risk by its ability to propagate across the boundaries of individual institutions, sectors, and geographies. The International Science Council's Briefing Note on Systemic Risk defines it through the lens of interconnectedness and non-linearity — characteristics that "set systemic risks apart from conventional risk assessment approaches and risk governance". This is precisely because their impacts transgress geopolitical boundaries and amplify across system elements. Unlike hazards that are contained at the point of origin, systemic risks exploit the very pathways of integration and efficiency that modern economies have constructed.

The term **polycrisis** — now firmly embedded in the global risk vocabulary — captures a related but distinct phenomenon: the simultaneous emergence of multiple, causally linked crises whose compound effects exceed the sum of their parts. A 2025 methodology paper in Nature Communications formalises this concept, proposing an assessment framework specifically designed for systemic risks that "compound and cascade within and between systems," with explicit attention to the political economy and transformational dimensions that conventional quantitative models overlook. The World Economic Forum's Global Risks Report 2025 — now in its 20th edition — reveals "an increasingly fractured global landscape, where escalating geopolitical, environmental, societal and technological challenges threaten stability and progress," noting that risk interconnections are deepening as the pace of systemic change accelerates.

The blockade of the Strait of Hormuz has resulted in disruption of supply of crude oil to many countries. Owing to this, the price of petroleum products like petrol, diesel, kerosene and aviation fuel has shot up in many countries. Countries that have petroleum reserves are resisting this price hike as of now. However, Products that are dependent on crude oil like asphalt, synthetic fibres, lubricants, and chemicals have been adversely affected. For example, construction of a one-kilometre-long asphalt road that would incur an estimated cost of Rs 30 lakhs to Rs 60 Lakhs, now costs close to Rs 1 crore.

On the other hand, during the Covid lockdown, prices of bicycles in India had increased significantly. It is believed that many exercise freaks resorted to cycling as an exercise since the gymnasiums were closed.

The Mechanics of Cascading Failure

Cascading risk operates through interdependency pathways — physical, digital, economic, and social. Engineering risk research has traditionally assessed direct impacts to individual systems; emerging scholarship now establishes a tiered taxonomy of consequence: **Tier 1 methods** capture direct, localised impacts, while **Tier 2 methods** assess second-order and cascading risks arising when disruption in one system propagates to connected sectors. The EU-funded ATLANTIS project, applying this multi-level approach to critical infrastructure across national borders, demonstrated that a holistic, cross-sector assessment methodology yielded measurable improvements in preparedness of 5 % to 55 %, depending on threat scenario and stakeholder group — a result unachievable through siloed infrastructure-by-infrastructure analysis.

The CrowdStrike software failure of July 2024 provided a vivid real-world demonstration of cascading dynamics. A single flawed software update simultaneously grounded flights globally, disrupted hospital patient records systems, froze banking transactions, and immobilised logistics networks. This was not a security breach — it was a system-level failure propagated across sectors that shared a common technological dependency. The incident underscored what resilience researchers have long argued: that the very efficiency gains from digital integration also compress the space for error correction and increase the velocity of contagion.

4.6 Networked Supply Chains

From Linear Chains to Complex Networks

The term "supply chain" has become a misnomer. What enterprises actually navigate are supply networks — highly interconnected, multi-tier, geographically distributed systems where each node has its own dependencies, vulnerabilities, and risk profiles. The OECD defines critical trade dependencies as those combining three characteristics: high risk of disruption, high economic or strategic importance, and constrained possibility of substitution. This definition captures the structural reality that has created some of the most consequential risk events of the current decade.

Global supply chain schedule reliability hovered between 50–55 % throughout 2024, down sharply from 70–85 % in the pre-COVID era. A Maersk survey of over 2,000 European shippers found that four out of five respondents identified geopolitical tensions and inter-state conflicts as the most pressing risk to their supply chains — risks further amplified by environmental disruptions and economic instability creating feedback loops that multiply disruption effects. The convergence of these risk sources — what Maersk terms a "polycrisis" operating environment — has moved supply chain risk from the operations function to the board agenda.

Implications for ERM Practice

For enterprise risk managers, the systemic dimension demands a fundamental shift in methodology. Risk registers built around probability-impact matrices for individual risk categories are insufficient when the interaction between risks — rather than any single risk — generates the most severe outcomes. Effective systemic risk assessment requires:

- **Network mapping** of dependencies across suppliers, technology platforms, regulators, and peer institutions
- **Scenario analysis** that models second and third-order effects, not merely direct impacts
- **Stress testing** of cross-sector linkages, particularly for shared digital infrastructure and common suppliers
- **Threshold identification**, recognising that systems may absorb shocks below critical thresholds but experience nonlinear collapse once those thresholds are crossed

The Cambridge University study on interconnected global risks, referenced in a 2024 UNCTAD analysis, reveals that crises such as climate change, pandemics, and geopolitical conflicts are causally linked, often intensifying each other's effects — a dynamic that underscores the fragility of global systems to cascading disruptions where a single crisis can trigger or amplify others.

Concentration and Chokepoint Vulnerabilities

The most structurally significant supply chain risk of 2025 and 2026 is resource concentration — the dependence of multiple sectors on materials or processing capabilities dominated by a single geography. China accounts for over 90 % of globally processed rare earth elements and rare earth permanent magnets. In 2025, China imposed export restrictions on some categories of rare earth metals, like europium, ytterbium, and terbium. Foreign companies had to obtain Chinese government approval for re-exports of products containing Chinese-origin rare earth materials.

The cross-sector impact of this single chokepoint is illustrative of networked supply chain risk in its most concentrated form. The disruptions simultaneously affected:

- **Semiconductor manufacturing:** Rare earths are essential inputs for chip fabrication equipment; ASML, the world's sole manufacturer of extreme ultraviolet lithography machines, was preparing for weeks-long shipment delays
- **Defence:** Rare earth magnets are critical for radar systems, guided munitions, and advanced propulsion
- **Clean energy:** Neodymium-iron-boron magnets using terbium and dysprosium are indispensable for EV motors and wind turbine generators
- **Consumer electronics:** From smartphones to medical devices, rare earth materials underpin miniaturised high-performance components

A CEPR analysis of Japanese multinational responses confirms that firms are responding not by retreating from globalisation but by diversifying supply chains — "friend-shoring" toward ASEAN economies — without full relocation of production. Geopolitical risk researchers at ScienceDirect find that geopolitical risk significantly weakens global supply chain resilience, with the effect amplified where property rights protections are weaker.

Risk Management Imperatives

The imperative for enterprise risk functions is multi-tier supply chain visibility — the ability to trace dependencies not just to direct suppliers but to second and third-tier nodes that may harbour concentration risks invisible at the surface level. The OECD's policy work on supply chain interdependencies identifies three complementary methodologies for identifying critical trade dependencies: detailed trade data analysis, input-output data techniques, and computable general equilibrium modelling. For ERM practitioners, this translates to supplier mapping tools, contractual resilience provisions, strategic inventory policies, and scenario-tested alternative sourcing arrangements calibrated to realistic disruption timelines.

4.7 Technology as a Horizontal Risk Driver

The Architecture of Technology Risk

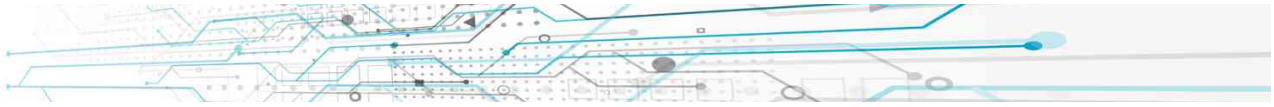
Technology has ceased to be a sector-specific risk domain and has become a horizontal risk driver — one that cuts across every industry, function, and geography simultaneously. When the same cloud platforms, software vendors, semiconductor architectures, and digital protocols underpin the operations of banks, hospitals, utilities, manufacturers, and governments, a vulnerability in any shared layer becomes a vulnerability for all. This is the architecture of modern technological risk: deeply interconnected, rapidly evolving, and resistant to containment within traditional risk perimeters.

The enterprise risk management market reflects this growing recognition. The ERM market is projected to grow from USD 6.00 billion in 2025 to USD 11.97 billion by 2030, at a compound annual growth rate of 14.8% — driven substantially by the need to integrate technology risk management across organisational and sectoral lines. Marsh's analysis of healthcare sector technology risk identifies four dimensions of technology risk amplification: amplifying current risk drivers, extending risk interactions, triggering risk cascades, and creating entirely new categories of risk — a typology that applies with equal force across financial services, energy, manufacturing, and government.

Artificial Intelligence as a Cross-Sector Risk Amplifier

AI has emerged as the paradigmatic horizontal technology risk. A 2024–2025 cross-quantile interdependency study, examining sectors from fintech to cybersecurity to clean energy, found that AI, fintech, and cybersecurity consistently act as net risk transmitters — exporting risk to connected sectors, particularly during market stress conditions. The WEF Global Risks Report 2025 notes that while adverse outcomes of AI rank relatively low on two-year risk severity scales, they are already a leading driver of misinformation and disinformation — the top-ranked global risk for 2025 — and are expected to rank 6th in severity on a ten-year outlook. The report explicitly cautions against complacency given the fast-paced nature of AI adoption and its increasing ubiquity across critical systems.

AI-assisted cyberattacks have increased by 72% since 2024. An estimated 40% of all cyberattacks are now AI-driven, enabling adaptive malware, automated phishing with convincing natural language, and adversarial model poisoning — attacks that target not just data but the AI decision-making systems that enterprises increasingly rely upon. The NIST AI Risk Management Framework, updated in 2026 to include a profile specifically for trustworthy AI in critical infrastructure, reflects the recognition that AI risk management must be integrated into sector-wide resilience planning rather than treated as a technology department concern.



Digital Concentration and Third-Party Dependency

Technology risk is further amplified by concentration in digital infrastructure. Across sectors, organisations share small numbers of dominant cloud providers, software platforms, and communications networks. This concentration creates correlated exposure: a failure, breach, or policy change affecting a single major technology vendor that would simultaneously impact thousands of organisations across multiple sectors. The Australian Government's 2025 Critical Infrastructure Annual Risk Review explicitly identifies "agentic AI and other cutting-edge technology" as generating new and more complex risks for critical infrastructure operators.

For ERM frameworks, the implication is that technology risk management must extend beyond internal IT controls to encompass:

- **Third-party and fourth-party risk assessment** mapped against critical operational dependencies
- **Scenario planning for single-point-of-failure technology events** affecting shared platforms
- **AI governance frameworks** aligned to NIST AI RMF or equivalent standards
- **Quantum computing transition planning**, recognising that current cryptographic protections face potential obsolescence by the late 2020s

Ransomware preparedness as an enterprise-level resilience challenge, not merely an IT security issue — a multi-case analysis of 16 major ransomware incidents between 2015 and 2025 confirms that direct and indirect costs systematically compound, with impacts ranging from operational shutdown to reputational damage and sector-wide vulnerability exposure

4.8 ESG as a Multi-Domain Risk

Beyond Compliance: ESG as a Risk Architecture

Environmental, Social, and Governance (ESG) factors have undergone a conceptual transformation in risk management discourse. Initially treated as a reputational or reporting compliance consideration, ESG has evolved into a multi-domain risk architecture — one where environmental stresses, social disruptions, and governance failures simultaneously affect financial performance, regulatory standing, operational continuity, and strategic positioning. A 2024 study published in the International Journal of Productivity and Performance Management confirms that ERM frameworks enhance an organisation's ability to navigate these emerging ESG risks, while COSO and the World Business Council for Sustainable Development (WBCSD) have jointly issued guidance integrating ESG risks within the full COSO ERM framework's five components and 20 principles.

For example, a significant drop in snow-fall at tourist destinations like Nainital and Manali will adversely impact winter tourism at those locations. This will have a substantial bearing on local businesses, thereby impacting the economy of the location.

The multi-domain nature of ESG risk is most clearly visible in its cross-sectoral propagation. Physical climate risks — flooding, extreme heat, water scarcity — directly affect agricultural output, energy generation capacity, logistics infrastructure, and population health. Transition risks — carbon pricing mechanisms, regulatory phase-outs of carbon-intensive activities, and the EU's Carbon Border Adjustment Mechanism (CBAM) — simultaneously reshape cost structures across steel, aluminium, cement, and energy-intensive manufacturing. Social risks — labour rights failures, community displacement, diversity and inclusion shortfalls — can trigger regulatory investigation, consumer boycotts, investor divestment, and employee attrition in cascades that amplify far beyond the originating incident.

The Financial Stability Dimension

Climate-related financial risks have graduated from an environmental niche to a systemic financial stability concern. The Financial Stability Board's Roadmap for Addressing Financial Risks from Climate Change, updated in July 2025, charts a comprehensive pathway for integrating climate risk into financial regulation and prudential oversight. The Bank of England's climate-related financial disclosure for 2025 details the organisation's own approach to managing climate risks, setting a governance standard for financial institutions. A bibliometric analysis of ESG-climate research finds a sharp acceleration in publications — from 6 papers in 2021 to 72 in 2024 — reflecting the rapid emergence of an evidence base that is simultaneously reshaping regulatory expectations and investment practice.

The integration imperative for ERM is clear: ESG risks are not a parallel programme to be managed alongside conventional risk frameworks, but are to be embedded within them. As ESG legal and risk advisory practitioners have noted, an ESG strategy that is "bolted on" rather than "built in" ultimately fails because ESG values are only loosely coupled with business objectives, creating dangerous gaps between reported positions and actual exposure. The COSO-WBCSD joint guidance provides structured guidance across seven modules — from governance to measurement to disclosure — offering a practical integration architecture that ERM practitioners can operationalise.

Double Materiality and Cross-Sector Amplification

The principle of double materiality — assessing both how ESG factors affect enterprise value and how enterprise activities affect society and the environment — is now central to leading ESG frameworks including the EU's Corporate Sustainability Reporting Directive (CSRD) and the IFRS S1 and S2 sustainability disclosure standards. For cross-sector risk management, double materiality expands the risk universe substantially: an organisation's supply chain labour practices create social risks that can cascade to regulatory sanction and reputational damage; its Scope 3 carbon emissions create transition risks not only for itself but for all firms in the same value chain.

Research across 30 high-risk Indonesian energy, mining, and manufacturing companies over 2020–2024 finds a positive and significant relationship between risk disclosure scores, ESG scores, and both financial and non-financial performance outcomes — reinforcing the integration of COSO ERM and global ESG standards (GRI, SASB, IFRS S1 and S2) as a performance imperative rather than merely a compliance exercise. ESG risks, properly integrated within ERM, strengthen rather than burden strategic decision-making.

4.9 National Critical Infrastructure Linkages

The System-of-Systems Problem

National critical infrastructure (NCI) — encompassing energy, water, telecommunications, transportation, finance, healthcare, and food systems — was once designed as a collection of largely independent sectoral networks. It now functions as a **system of systems:** tightly coupled, mutually dependent, and vulnerable to failures that propagate across sectoral boundaries with speed and force that traditional single-sector risk governance cannot contain.

The OECD's 2025 Government at a Glance report on critical infrastructure resilience emphasises that "a system-based, all-hazards approach to infrastructure resilience is crucial for maintaining service continuity in the face of various threats," and that infrastructure assets are "usually just a part of a wider system, which should be considered in its entirety." Among the twenty-three OECD countries surveyed, governance scores for critical infrastructure resilience ranged from 0.32 to 0.83 on a scale of 0 to 1, with an average of 0.59 — indicating significant gaps in multi-sector governance and interdependency management even among advanced economies. Fourteen of the twenty-three countries have a national policy or strategy for infrastructure resilience, while six have embedded it in legislation.

A 2025 academic study on resilience in critical infrastructure from Multi Research Journal identifies a convergent risk ecosystem where "disruptions in one domain can propagate rapidly across others, leading to cascading failures with severe societal and economic consequences." The illustrative scenario offered is precise: a cyberattack on a power grid can simultaneously disrupt healthcare delivery and financial transactions, while communication failures impede crisis coordination. This system-of-systems dynamic is no longer theoretical — it is the lived risk environment that critical infrastructure operators must navigate.

India's Critical Infrastructure Risk Landscape

For Indian enterprises and policymakers, the critical infrastructure risk challenge carries specific structural dimensions. India's National Critical Information Infrastructure Protection Centre (NCIIPC) currently focuses on information assets, leaving physical infrastructures and sectoral interdependencies outside effective regulatory oversight. A foundational analysis published in December 2025 proposes an integrated statutory architecture — a Critical Infrastructure Protection Act (CIPA) paired with a Bharat National Resilience Index (BNRI) — specifically designed to address India's "system-of-systems vulnerabilities, federal asymmetry and hybrid threat exposure". This framework explicitly captures India-specific sectoral clusters and moves beyond Western standalone critical-sector templates.

India's cybersecurity exposure in critical sectors is escalating. Carnegie Endowment for International Peace research published in September 2025 maps India's cybersecurity administration across critical infrastructure domains, highlighting the alignment gaps between the pace of cyber threat evolution and the architecture of current governance. Pakistan-linked cyber operations reportedly launched over 1.5 million attacks on Indian defence and power sectors during Operation Sindoor in 2025 — illustrating how geopolitical tensions directly materialise as infrastructure risk events, not merely as abstract threat intelligence.

Cross-Sector Governance Frameworks

The NERC 2025 RISC (Reliability Issues Steering Committee) report identifies cybersecurity, supply chain dependencies, and critical infrastructure interdependencies among the top reliability risks for the energy sector. The Australian Government's 2025 Critical Infrastructure Annual Risk Review similarly notes that critical sectors — energy, water, food, healthcare, transport, finance, and communications — are "increasingly intertwined with global supply chain dependencies exposed to third-party and geopolitical disruption," and identifies agentic AI as an emerging source of complex new risks. These international assessments converge on a common finding: single-sector risk governance is structurally unable to address cross-sector interdependency risks. Multi-sector governance structures, information sharing frameworks, and binding cross-sectoral response capabilities are required.

For enterprise risk practitioners operating in or adjacent to critical infrastructure sectors, the governance imperatives include:

- **Dependency mapping** extending across sectoral boundaries to identify where operational continuity depends on the health of adjacent infrastructure systems
- **Joint scenario exercises** with sector peers, regulators, and government agencies that simulate cross-sector cascades
- **Information sharing protocols** for threat intelligence across competing organisations within sectors, and across sectors at national level
- **Resilience investment prioritisation** guided by systems-level vulnerability analysis, not solely enterprise-level risk registers
- **Alignment with national resilience standards** and emerging regulatory requirements, including India's evolving NCIIPC and proposed CIPA frameworks

Synthesis: Integrating Cross-Sector Risk Intelligence into ERM

The five dimensions explored in this chapter — systemic and cascading dynamics, networked supply chains, horizontal technology risk, ESG multi-domain exposure, and critical infrastructure linkages — are not independent risk categories to be managed in parallel. They are interconnected lenses on a single underlying reality: that risk in the contemporary operating environment is fundamentally relational, emergent, and cross-boundary.

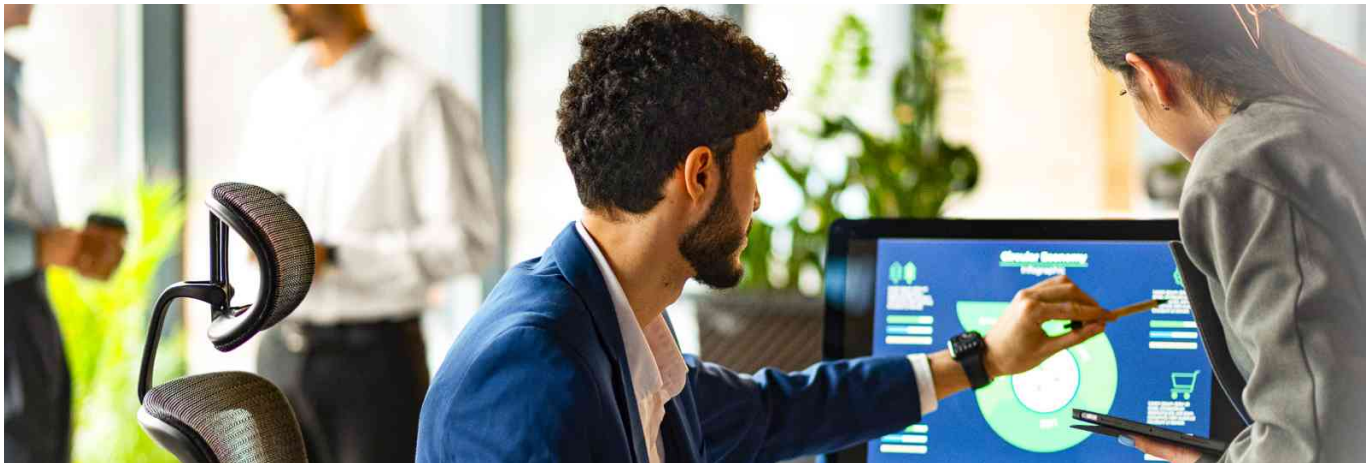
Three integration principles follow from this analysis:

First, risk identification must become network-centric. Conventional risk registers map risk against organisational objectives. Network-centric risk identification maps the dependencies that connect an organisation to the wider systems within which it operates — supply networks, technology platforms, regulatory environments, and infrastructure systems. The failure point may not lie within the enterprise at all; it may lie two or three nodes away in a supply network or in a shared technology dependency.

Second, risk assessment must account for cascade dynamics. Static probability-impact assessment underestimates cross-sector risk because it fails to model the propagation of failure across interdependent systems. Stress testing and scenario analysis must extend to second and third-order effects, incorporating the possibility that risks interact in ways that amplify rather than simply add.

Third, risk governance must operate at the systemic level. Individual enterprises cannot manage systemic risk alone. Cross-sector risk governance — through regulatory frameworks, industry bodies, information sharing platforms, and national resilience programmes — is a structural complement to enterprise-level risk management. For boards and senior risk leaders, participation in these cross-sector governance mechanisms is itself a risk management activity.

The *Global Risks Report 2026* confirms that interconnected and compounding risks are reshaping operational, societal, and geopolitical stability, calling for "proactive, cross-sectoral strategies to mitigate cascading impacts across regions and sectors". For the enterprise risk function, this is both a challenge and a mandate: to evolve from a guardian of organisational risk registers to an architect of cross-sector risk intelligence.



4.10 Cross-Sector Risk Patterns & Trends

The analysis highlights several defining patterns shaping the evolving risk landscape.

A key trend is the systemic digitisation of risk, where technology functions simultaneously as an enabler of efficiency and a source of concentration risk. Increasing reliance on interconnected digital ecosystems amplifies both the scale and speed of disruption.

Another defining pattern is the rise of cascading risk dynamics, where disruptions propagate across interconnected systems, transforming localised events into enterprise-wide or sector-wide impacts.

There is also a shift from episodic disruptions to persistent risk environments, particularly in areas such as cybersecurity and climate, where risks are continuous, evolving, and less predictable.

The analysis further highlights the growing influence of perception -driven risk, referring to situations where stakeholder perception, shaped by media narratives, social amplification, public sentiment, and regulatory signalling, plays a decisive role in determining outcomes, sometimes independent of underlying operational or financial reality. In such cases, the speed and scale of information flows can amplify isolated incidents into broader reputational, regulatory, or market consequences, affecting investor confidence, customer behaviour, and policy responses. As a result, organisations must recognise that risk materialisation is increasingly influenced not only by actual events but also by how those events are interpreted, communicated, and perceived across stakeholders.

Finally, a recurring pattern is the capacity versus scale imbalance, where rapid expansion in infrastructure, digital systems, and operations outpaces organisational and institutional capabilities, increasing systemic vulnerability.

4.11 Implications for Organisations

The prevalence of universal risks has significant implications for organisational risk management. Organisations must move beyond siloed approaches and implement integrated risk management frameworks that explicitly account for cross-functional and cross-sector dependencies. This includes strengthening capabilities in cyber resilience, supply chain diversification, and enterprise-wide scenario planning, as well as embedding systemic risk governance mechanisms, such as cross-functional risk committees and integrated risk dashboards that monitor interdependent exposures across business units.

Given the speed at which risks evolve, organisations must invest in real-time risk sensing and data-driven decision-making capabilities, supported by robust governance and control frameworks. This includes the use of early warning indicators, continuous monitoring tools, and structured stress testing and scenario analysis to assess how multiple risks—such as supply chain disruption combined with liquidity stress—may impact operations under adverse conditions.

There is also a strategic imperative to prioritise resilience alongside efficiency. Optimisation strategies must be balanced with redundancy, flexibility, and adaptability, particularly across supply chains, infrastructure, and workforce models. In practice, this requires organisations to incorporate resilience-oriented metrics, such as recovery time objectives, buffer capacity levels, and system availability thresholds, alongside traditional cost and efficiency measures.

In parallel, managing reputational and stakeholder risks requires proactive engagement, transparent communication, and alignment with evolving ESG expectations, as these factors increasingly influence regulatory outcomes and market behaviour. This also necessitates periodic recalibration of risk appetite and tolerance thresholds, particularly in areas such as data privacy, climate exposure, and operational continuity, where stakeholder expectations and regulatory standards are evolving rapidly.

4.12 Link to Sector-Specific Analysis

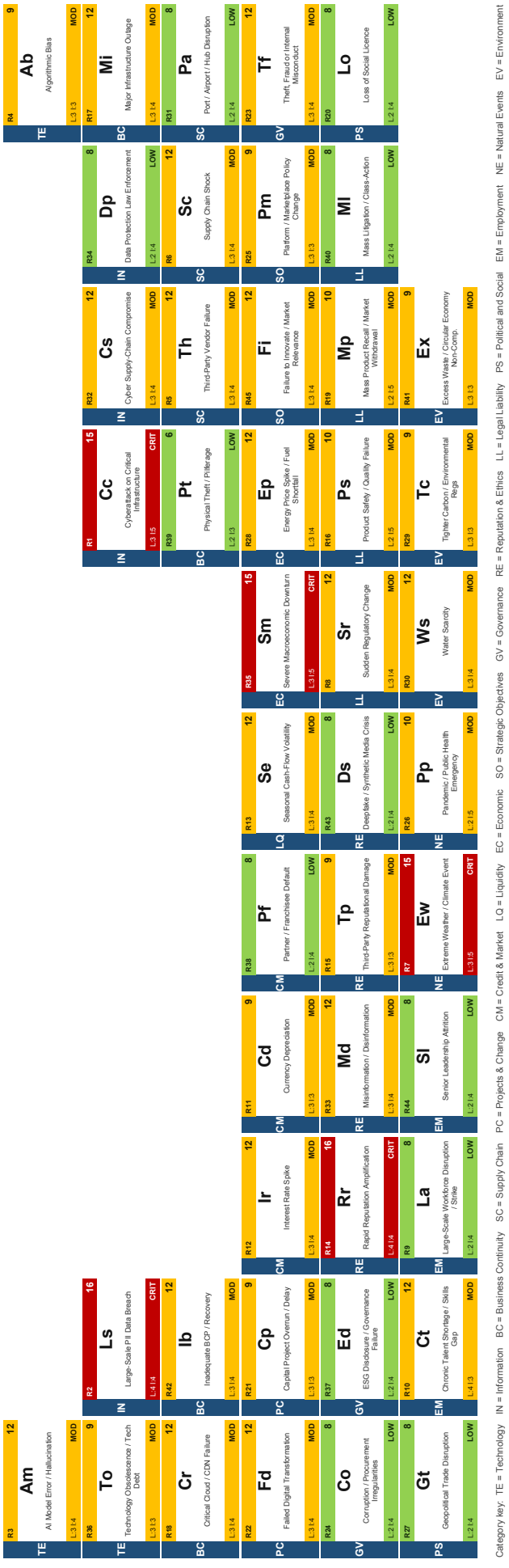
While universal risks provide a macro-level view of systemic vulnerabilities, their manifestation varies across sectors based on industry-specific characteristics, operational models, and regulatory environments.

The sector-specific analyses that follow build on this universal framework by illustrating how these risks materialise in distinct contexts. For example, cyber risks in aviation may affect operational systems and navigation infrastructure, whereas in financial services they are more closely tied to digital payments and customer data security.

This linkage ensures that Periodic Risk Tables remain both standardised and contextually relevant, enabling organisations to apply a consistent framework while accounting for sector-specific nuances.

By integrating universal risk patterns with sector-level insights, the analysis provides a comprehensive and actionable understanding of the risk landscape, supporting informed decision-making and long-term resilience.

4.13 Universal Periodic Risk Table



Chapter 5

Sector Specific Risks

While universal risks provide a macro-level view of systemic vulnerabilities, their manifestation varies significantly across sectors due to differences in operating models, regulatory environments, and dependency structures. This chapter presents a sectoral deep dive across multiple industries, highlighting how risks materialise within each domain.

The analysis integrates primary dataset insights, sectoral perspectives, and systemic risk frameworks to present a multi-dimensional understanding of sector-specific risks, supported by Periodic Risk Tables (PRTs).

5.1 Aviation, Financial Services, Government & Public Services, Telecom

About the researchers

Dr. Keerti Pendyal

Associate Professor of Economics and Economics Area Chair at Mahindra University School of Management

Dr. Keerti Pendyal is an Associate Professor of Economics and Economics Area Chair at Mahindra University School of Management, with a PhD from IIM Calcutta, an MBA from IIM Ahmedabad, and IRM Level 2 certification. His expertise spans institutional economics, enterprise risk management, public policy, and governance systems. He has co-authored multiple editions of the India Risk Report with ICICI Lombard and IRM India, and has delivered executive risk management programmes for senior leaders and government officers. At the Mahindra University–IRM India Global Centre for Enterprise Risk Management, he brings economic foresight, policy intelligence, and strategic risk expertise to help leaders navigate technological, geopolitical, and financial uncertainty.

Chanakya Naidu

IRM level 1 certified, final-year BBA (Digital Technologies) student at Mahindra University

Chanakya Naidu is an IRM level 1 certified, final-year BBA (Digital Technologies) student at Mahindra University. His areas of interest are corporate strategy, organisational risk, and business analytics.

5.1.1 Aviation

5.1.1.1 Overview

Aviation is among the most safety-critical and tightly coupled industries globally, where system-wide disruptions can emerge from seemingly minor operational deviations. The industry ecosystem comprises airlines, cargo operators, airports, Maintenance Repair and Overhaul (MRO) providers, and an extensive ancillary ecosystem that includes ground handling, fuel logistics, training institutions, and regulatory bodies. The ancillary ecosystem plays a crucial enabling role by supporting operational continuity, even though it lies outside core airline operations.

From an economic standpoint, aviation contributes significantly to national development by facilitating trade, tourism, and regional connectivity. At the same time, it operates under structural constraints such as high capital intensity, thin operating margins, and sensitivity to macroeconomic variables including fuel costs, demand cycles, and currency volatility.

The sector is governed by a stringent regulatory framework, encompassing global bodies such as ICAO and national regulators such as DGCA, with a strong emphasis on safety, compliance, and operational discipline. As a result, aviation has traditionally been viewed through the lens of reliability and procedural precision, with risk management focused primarily on safety and operational continuity.

However, the nature of risk within the sector has evolved significantly. While operational and safety risks remain central, the risk landscape now extends to include financial fragility, supply chain dependencies, digital vulnerabilities, climate exposure, and governance challenges. In addition, sector-specific pressures such as engine grounding events (e.g., Pratt & Whitney issues), post-COVID workforce shortages, and air traffic congestion in major hubs have further intensified operational and strategic risk exposure. A defining characteristic of the sector is the asymmetry between likelihood and impact, where high-impact events may remain statistically rare but can generate severe and long-lasting consequences when they materialise.

Aviation increasingly reflects the characteristics of a complex adaptive system, where risks do not emerge in isolation but arise from interactions across interconnected subsystems. Operational disruptions—such as engine groundings, maintenance delays, crew shortages, or air traffic congestion—do not remain confined to technical domains but can quickly propagate across capacity, liquidity, regulatory compliance, and customer experience.

This interconnectedness implies that small disruptions can escalate into system-wide challenges through cascading effects. A core structural driver of this dynamic is the growing mismatch between rapid sectoral expansion and the pace of development of supporting human, infrastructural, and institutional capacity. Consequently, the emphasis has shifted from managing discrete risks to understanding how risks accumulate, interact, and amplify over time, underscoring the need for dynamic, forward-looking tools that support continuous monitoring and adaptive decision-making.

5.1.1.2 Key Risk Themes

A comprehensive assessment of the aviation sector resulted in the identification of over 180 distinct risks spanning operational, strategic, financial, governance, environmental, and technological domains. Of these, 15 risks were classified as critical, 61 as moderate, and 106 as low based on the defined likelihood–impact scoring framework. These risks collectively highlight a transition from isolated risk events to a deeply interconnected risk system, where vulnerabilities are shaped by structural interdependencies and scale.

A dominant theme emerging from the analysis is the growing strain on human capital and safety systems. Human capital constraints are emerging not merely as operational risks, but as structural limits to system scalability. Rapid expansion in fleet size, traffic volumes, and infrastructure has outpaced the development of skilled personnel, resulting in risks related to fatigue, cognitive overload, training bottlenecks, and reduced depth of experience. These pressures are observed across pilots, maintenance engineers, air traffic controllers, and ground staff, and are particularly critical in a high-reliability environment. Over time, such risks tend to accumulate gradually and remain latent until triggered by stress events, contributing to the erosion of safety margins even when formal compliance indicators remain within acceptable limits.

Closely linked to this is the sector's **dependence on engine manufacturers and original equipment manufacturers (OEMs)**, which introduces a concentration risk within the technical ecosystem, creating a quasi-single-point-of-failure risks within a globally distributed system. Issues such as engine durability challenges, limited availability of spare parts, and constraints in global MRO capacity can disrupt fleet availability at scale. These disruptions do not remain confined to technical domains; they translate into reduced operational capacity, liquidity stress, pressure on leasing arrangements, and increased strain on already stressed supply chains. This reflects a broader pattern in which technical risks act as transmission mechanisms, linking operational breakdowns with financial and reputational consequences.

Another critical area of concern relates to **supply chain fragility**

and infrastructure dependencies. The aviation ecosystem relies on highly specialised and often concentrated supply chains for spare parts, maintenance services, and fuel logistics, where substitution is both limited and time-intensive. Disruptions within these networks can therefore have disproportionate operational consequences. At the same time, large-scale infrastructure expansion, including new airports and hubs, introduces risks associated with coordination challenges and timing mismatches between capacity creation and ecosystem readiness. These risks arise less from absolute capacity shortages and more from the lack of synchronisation across airports, air traffic systems, ground handling, and airline operations.

Governance and institutional capacity represent another important dimension of risk. As the sector expands rapidly, regulatory and supervisory systems must evolve to manage increasing complexity. However, institutional capability does not always scale at the same pace, resulting in gaps in oversight, delays in enforcement, and a tendency to rely on procedural compliance rather than risk-based supervision. These gaps extend beyond compliance concerns and directly affect transparency, stakeholder confidence, and the credibility of safety oversight—factors that are central to maintaining trust in the aviation system.

The **financial structure** of the aviation industry further amplifies risk exposure. High leverage, reliance on leasing arrangements, and sensitivity to external shocks create conditions in which even moderate disruptions can lead to disproportionate financial stress. This financial stress often emerges as a second-order effect of operational disruptions, rather than independent triggers. Operational disruptions—such as aircraft groundings or demand fluctuations—can rapidly transmit into liquidity pressures, credit constraints, and pricing instability due to the sector's high fixed-cost structure. This results in a cyclical dynamic where risks materialise in a non-linear manner, often becoming visible only under stress conditions.

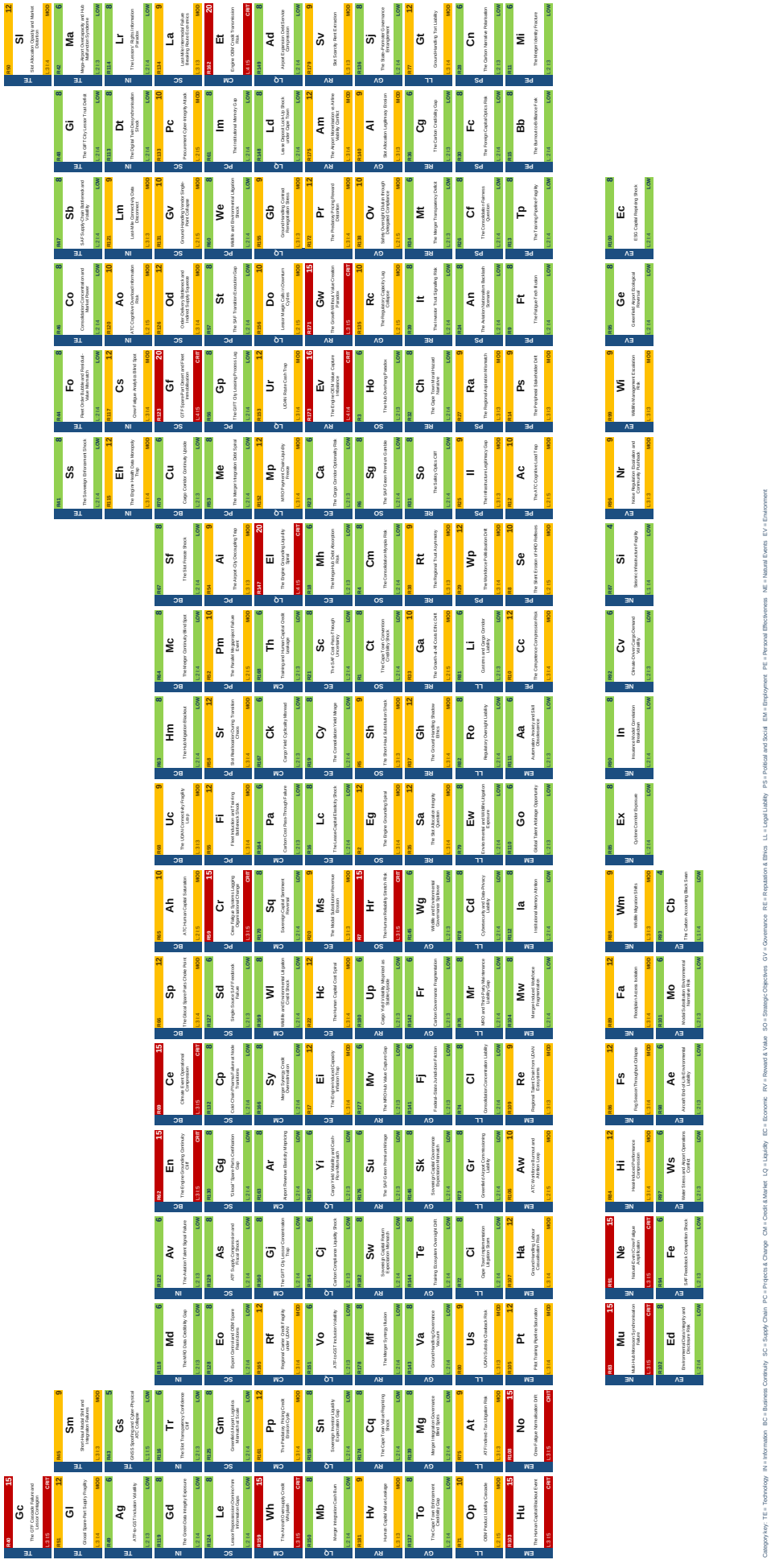
Environmental and climate-related risks are also emerging as structural drivers of uncertainty. Increasing frequency of extreme weather events, rising temperatures, and shifting climate patterns affect operations, infrastructure planning, and network reliability. These risks are often correlated across geographies, reducing the effectiveness of diversification strategies and increasing the likelihood of simultaneous disruptions across multiple locations.

Technological transformation introduces another layer of complexity. While digitalisation enhances efficiency, coordination, and predictive capabilities, it also creates dependencies on data systems, platforms, and external providers. Risks related to cybersecurity, data integrity, and system interoperability are becoming increasingly material, particularly as aviation systems become more integrated. Concentration of control over critical operational data among a limited set of stakeholders may also lead to asymmetries in information access and decision-making capability.

Finally, the sector faces a growing set of **reputational and perception-based risks**. In aviation, public trust is a critical asset, and perceptions of safety, transparency, and fairness can significantly influence regulatory responses, investor sentiment, and passenger behaviour. These risks are inherently asymmetric, where a single incident, operational disruption, or narrative can have disproportionate consequences across the ecosystem.

Overall, the aviation risk landscape reflects a system where risks are tightly interconnected and mutually reinforcing. Operational, financial, human, technological, infrastructural, and governance risks do not operate independently but interact continuously, making isolated risk management approaches insufficient. Effective risk management in aviation therefore requires an integrated perspective that recognises interdependencies and supports coordinated responses across the ecosystem. Periodic Risk Tables (PRTs) provide a structured mechanism to track how these interdependent risks evolve over time, particularly in response to stress events.

5.1.1.3 The Periodic Risk Table



5.1.2 Financial Services

5.1.2.1 Overview

The financial services sector sits at the core of modern economies, acting simultaneously as a stabilising force and a high-speed transmission channel for systemic risk. The sector encompasses banking institutions, insurance providers, capital markets, and an increasingly prominent fintech ecosystem, alongside non-banking financial companies, payment intermediaries, and a growing network of technology and outsourcing partners. Its importance lies not only in its economic contribution—spanning credit intermediation, payments, savings, investment, and insurance—but also in its role as a systemic stabiliser, where confidence, liquidity, and trust are critical to sustained functioning. Recent episodes of rapid digital withdrawals and payment system disruptions illustrate how quickly liquidity and trust shocks can propagate in a digitised environment.

Unlike most other sectors, financial services operate within a highly regulated environment characterised by continuous oversight, prudential norms, and macroeconomic sensitivity. Regulatory institutions play a central role in shaping operational behaviour, capital adequacy, and risk exposure. However, the effectiveness of these frameworks depends on their alignment with evolving financial innovation, including digital public infrastructure, real-time payment systems, embedded finance, open banking, and AI-enabled decision-making. These developments have also intensified supervisory expectations and heightened the importance of customer-centric considerations such as fairness, transparency, convenience, and data protection.

From an academic perspective, financial systems are often described complex adaptive networks, where institutions are interconnected through credit relationships, capital flows, shared market exposures, and digital platforms. This interconnectedness implies that risks are rarely contained within a single entity and can propagate rapidly across the system. As a result, financial risk is fundamentally systemic in nature, characterised by contagion effects, where disruptions originating in one institution, vendor, payment rail, or customer segment can quickly transmit through channels of liquidity, market sentiment, regulatory responses, and even social media amplification.

The sector has also undergone significant transformation due to digitalisation, which has enhanced efficiency, inclusion, and access while simultaneously introducing new forms of vulnerability. The emergence of fintech platforms, digital payments, and algorithm-driven decision-making has expanded the scope of risk from traditional credit and market risks to include cybersecurity threats, operational resilience challenges, data integrity concerns, and dependencies on third-party service providers.

Consequently, the risk landscape in financial services has become increasingly multidimensional, extending beyond financial exposures to encompass governance, technology infrastructure, human capability, business continuity, legal liability, and reputational considerations. This broadened risk spectrum underscores that the sector's exposure is driven not only by financial variables but also by the interplay of digital infrastructure, regulatory scrutiny, customer trust, and the continuity of critical services. In this context, effective risk management requires an integrated approach that aligns financial resilience with technological robustness, strong governance practices, consumer protection, and sustained confidence in the wider financial ecosystem.

5.1.2.2 Key Risk Themes

A comprehensive assessment of the financial services sector highlights a set of deeply interconnected risk themes that extend beyond conventional classifications. These risks are driven by both structural dependencies and evolving market conditions, resulting in a dynamic and often fragile risk landscape. Increasingly, this landscape reflects not only financial exposures but also the interaction between human capital, technology systems, governance structures, and customer trust.

Credit and market risks increasingly reflect systemic inter connectedness rather than isolated institutional exposures. Economic downturns, interest rate volatility, and asset quality deterioration can lead to rapid erosion of capital buffers. However, these risks are increasingly influenced by shifting structural factors, including unsecured retail lending growth, liquidity asymmetries between banks and non-banking institutions, asset-liability mismatches, and borrower-level vulnerabilities such as MSME cash flow instability and rural climate-related stress. As a result, financial shocks are often transmitted simultaneously across institutions through tightly coupled channels of liquidity, credit quality, and market confidence, amplifying their overall systemic impact.

Alongside financial risk, **people and conduct-related risks** have emerged as critical drivers of sectoral vulnerability. Workforce instability, particularly frontline attrition and sustained churn, can weaken service delivery and internal control environments. These challenges are reinforced by performance pressures, incentive -driven mis-selling behaviours, cognitive overload in compliance roles, and reduced psychological safety within institutions. Over time, such conditions can erode ethical standards, suppress escalation mechanisms, and normalise conduct breaches. This suggests that financial sector risk is not solely balance-sheet

driven but also deeply embedded in human capital dynamics, organisational culture, and execution quality.

> "Banks are aggressively shrinking their tolerance for operational and regulatory slip-ups while taking calculated, strategic risks to avoid digital obsolescence."
>
> **Banking respondent**,
> when asked about the industry's overall risk appetite

Another critical area is the growing significance of **cyber security and digital infrastructure risks.** As financial services become increasingly digitised and reliant on real-time transaction systems, dependencies on interconnected digital platforms have inten sified. Operational disruptions are increasingly characterised by high -frequency, low-duration failures with high systemic amplification potential. Risks associated with payment rails, API integrations, cloud concentration, and national digital infrastructure create high-velocity operational vulnerabilities. Even minor technical disruptions—such as system latency, switch congestion, or masked downtime—can escalate into ecosystem-wide incidents due to repeated transaction attempts, settlement backlogs, and customer reactions. The shift towards 24x7 digital finance has therefore increased both the speed and scale at which operational risks can materialise.

Operational resilience has consequently evolved into a broader concern encompassing not only internal systems but also **third-party dependencies and infrastructure ecosystems**, creating a structural shift where critical risk control points move outside regulated entities. Financial institutions rely extensively on vendors, fintech partnerships, cloud providers, telecom networks, and payment aggregators. While these arrangements enhance efficiency and scalability, they introduce concentration risks and reduce direct institutional control. Disruptions within vendor networks or critical infrastructure—such as data centres, telecom systems, or payment switches—can have cascading effects across the sector, particularly given the interdependence of service delivery channels.

Regulatory and governance risks continue to define the sector, though their complexity has increased significantly. The evolution of regulatory frameworks has introduced heightened expectations around transparency, data protection, governance oversight, and accountability. Risks related to group-level opacity, related-party transactions, board independence, and information asymmetry, particularly within multi-layered financial structures, highlight the limitations of formal compliance approaches. Governance risks increasingly arise not from lack of rules, but from inadequate interpretability, coordination, and real-time enforcement across complex institutional structures. This challenge is further compounded as emerging data protection regimes and cross-border data requirements have introduced new legal and operational challenges. Effective governance now requires not only adherence to rules but also real-time visibility, clear accountability across entities, and robust oversight of third-party and fintech ecosystems.

Liquidity risk remains a central amplification mechanism, where stress in funding markets can rapidly escalate into solvency concerns. The interaction between liquidity availability, depositor confidence, funding concentration, and regulatory response creates non-linear outcomes, particularly during stress events. Digital financial behaviour, particularly rapid withdrawals enabled by real-time banking systems and mobile platforms, further accelerates liquidity transmission, increasing the speed at which localised stress can evolve into broader systemic instability. Unlike traditional liquidity stress events, where response windows could extend over days, digital withdrawals compress reaction time to hours, significantly constraining the effectiveness of conventional intervention mechanisms.

Reputational and trust-based risks represent another critical and cross-cutting dimension. In financial services, trust functions as a core operating asset. Events such as data breaches, service disruptions, perceived customer harm, or unethical practices can trigger rapid and amplified responses through social media, public narratives, and regulatory scrutiny. Negative perceptions—whether linked to opaque pricing, aggressive recovery practices, or algorithmic bias—can influence customer retention, deposit stability, credit demand, and the legitimacy of innovation in digital finance. These risks often propagate faster than formal regulatory interventions, making them particularly difficult to contain.

The increasing use of advanced analytics, AI, and data-driven decision-making has introduced a further layer of **structural risk**. Model reliability, data integrity, algorithmic bias, and the potential misuse of customer data are emerging as critical concerns. Risks such as AI-driven credit assessment errors, identity fraud enabled by generative technologies, unauthorised data usage, and insufficient model explainability extend beyond traditional modelling challenges. These issues affect underwriting accuracy, fairness in customer outcomes, auditability, and regulatory compliance, necessitating stronger governance over data provenance, validation processes, and ethical use frameworks.

Finally, **business continuity and physical resilience risks** are becoming closely tied to broader infrastructure and environmental dependencies. Financial services operations are increasingly concentrated in urban hubs and reliant on external systems such as power grids, telecom networks, cloud infrastructure, and data centres. Climate-related disruptions, infrastructure failures, and geopolitical or cyber threats can therefore affect not just individual

institutions but the continuity of critical financial services. Such vulnerabilities highlight that resilience must extend beyond institutional boundaries to encompass the entire supporting ecosystem.

Fraud and financial crime risks have become one of the most rapidly escalating exposures in the sector, particularly as digital adoption widens the surface for criminal activity. The expansion of real-time payments, mobile banking, and digital onboarding has been accompanied by a marked rise in social engineering scams, account takeover, synthetic identity fraud, mule account networks, and authorised push payment fraud. At the same time, institutions face heightened obligations relating to anti-money laundering, combating the financing of terrorism, sanctions screening, and know-your-customer compliance. Weaknesses in transaction monitoring, customer due diligence, or the detection of illicit fund flows can result in significant regulatory penalties, remediation costs, and reputational harm. Because fraud and financial crime increasingly operate across institutional and jurisdictional boundaries, they represent a systemic rather than purely institutional concern, requiring coordinated detection, intelligence sharing, and controls across the wider ecosystem.

Climate, environmental, and ESG-related risks are emerging as material financial risks rather than peripheral sustainability considerations. Physical risks, such as floods, cyclones, heatwaves, and rural climate stress, can impair asset quality within lending and insurance portfolios, while transition risks arising from decarbonisation, evolving policy, and shifting market preferences can affect the valuation of carbon-intensive exposures. Financial institutions are increasingly expected to assess climate-related risk within credit underwriting, investment decisions, and capital planning, and to conduct climate scenario analysis and stress testing. In parallel, expanding ESG disclosure obligations and heightened scrutiny of greenwashing introduce compliance, legal, and reputational exposure. These risks are inherently long-dated, non-linear, and interconnected with credit, market, and operational risk, and therefore require integration into core risk frameworks rather than isolated treatment.

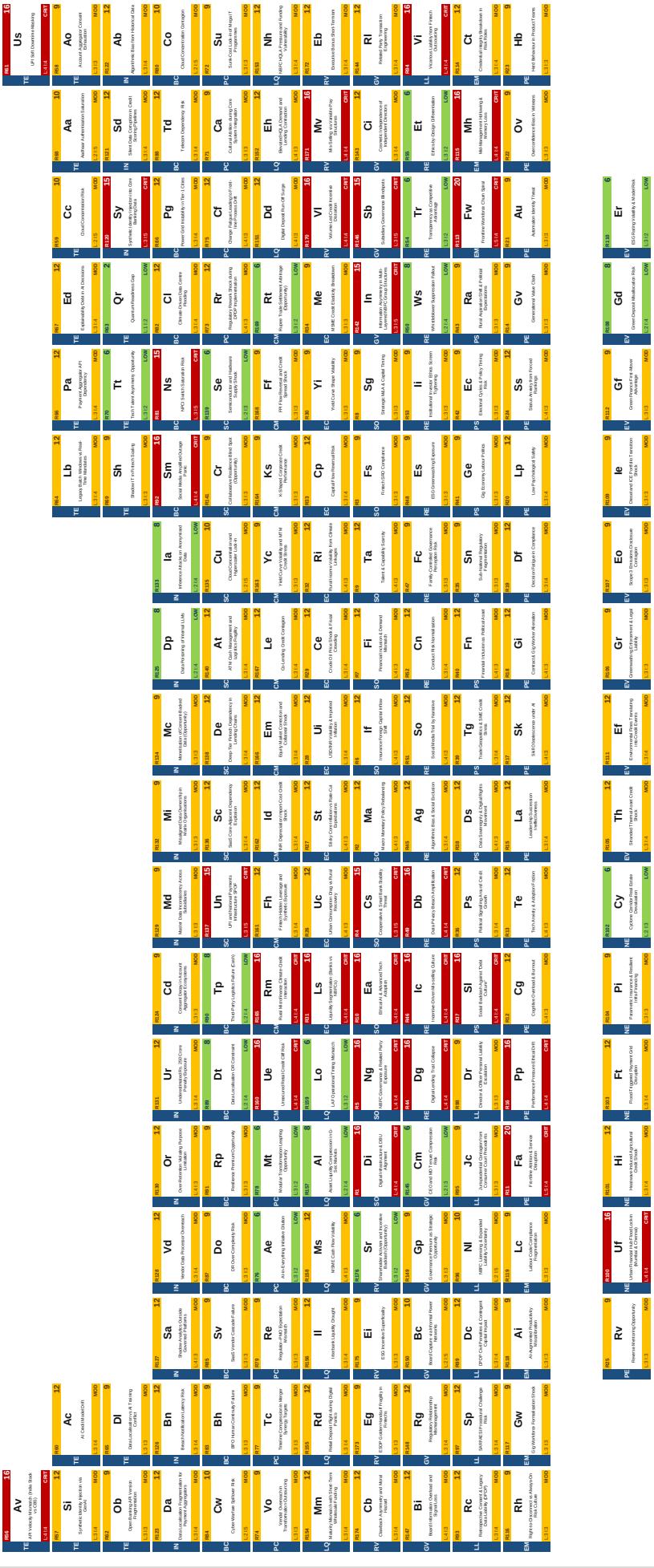
Underwriting and actuarial risks add a further dimension to the sector's risk profile for insurance and long-term savings providers. Mispricing, inadequate reserving, and flawed assumptions regarding mortality, morbidity, longevity, or persistency can undermine solvency over time. Exposure to catastrophic and correlated events, including natural catastrophes, pandemics, and climate-driven losses, can generate large and simultaneous claims that strain capital adequacy. These risks are compounded by asset-liability management challenges, where the need to match long-duration liabilities with suitable assets interacts with interest rate movements and market volatility. Effective management therefore depends on robust actuarial governance, reinsurance arrangements, and disciplined capital and reserving practices.

Macroeconomic, monetary, and capital adequacy risks represent a pervasive influence that shapes the sector's overall stability. Interest rate cycles, inflationary pressures, exchange rate volatility, and shifts in monetary policy directly affect funding costs, net interest margins, asset valuations, and borrower repayment capacity. Sudden changes in the macroeconomic environment can simultaneously affect credit quality, liquidity, and capital positions, underscoring the importance of maintaining adequate capital buffers, prudent asset-liability management, and forward-looking stress testing. For internationally exposed institutions, global economic cycles, capital flow reversals, and geopolitical developments can further amplify volatility and its transmission across markets.

Overall, the financial services sector exemplifies a system where risks are highly interconnected, multi-dimensional, and self-reinforcing. Workforce instability can weaken control environments; incentive structures can distort credit origination; digital infrastructure failures can trigger liquidity and reputational consequences; governance gaps can amplify contagion across group structures; and external disruptions can affect both operational continuity and financial stability. The core implication is that risk management in financial services must move towards an integrated, enterprise-wide framework that aligns prudential risk oversight with human capital management, technology resilience, data governance, third-party risk management, and the preservation of systemic trust.

> "Agentic AI and autonomous financial crime represents the next frontier — AI systems gaining the ability to act autonomously, executing transactions, managing accounts, and interacting with financial institutions without human intervention."
>
> **— Anti-Financial Crime respondent,**
> when asked which risks will emerge or intensify over the next 3–5 years

5.1.2.3 The Periodic Risk Table



5.1.3 Government and Public Services

5.1.3.1 Overview

The government and public services sector forms the institutional backbone of the economy, where risks have far-reaching implications for economic stability, social cohesion, and public trust. It encompasses a wide range of functions, including policymaking, infrastructure development, service delivery, fiscal stewardship, and regulatory oversight. Unlike private sector entities, public institutions operate within a framework where objectives extend beyond financial performance to include public welfare, equity, sovereign credibility, and long-term national development priorities. Consequently, the impact of risk in this sector is multidimensional, affecting not only financial outcomes but also citizen welfare, institutional trust, legal accountability, and social cohesion.

From a risk perspective, this sector is characterised by scale, complexity, and stakeholder diversity. Public systems often operate across multiple levels of governance, involving coordination between central, state, and local authorities. This multi-layered structure introduces both resilience and vulnerability, as differences in administrative capacity, fiscal resources, and governance quality can create uneven outcomes. Coordination challenges across jurisdictions, combined with high levels of public scrutiny, can lead to execution gaps, delays, and inconsistencies in service delivery.

Academic perspectives often describe public sector risk as a function of institutional capacity and governance effectiveness. Risks emerge not only from external pressures but also from internal constraints, such as bureaucratic processes, resource limitations, legacy systems, and policy implementation challenges. These structural factors often interact with evolving external conditions—including rapid urbanisation, climate stress, and fiscal pressures—creating a risk environment where long-term vulnerabilities can be amplified by short-term shocks.

> "Technology and data analytics are shifting risk management from retrospective reporting to real-time visibility and predictive intervention. Over the next 3–5 years, technology will evolve from risk monitoring to risk orchestration."
>
> **— Financial Infrastructure Advisory respondent,** when asked about the role of technology and data analytics in risk management

The increasing digitalisation of public services has added a significant new dimension to this landscape. Governments are adopting digital public infrastructure, data-driven governance models, direct benefit transfer mechanisms, and integrated service platforms to improve efficiency, transparency, and scale. While these developments enhance accessibility and delivery capability, they also introduce risks related to cybersecurity, data governance, system reliability, and digital exclusion. Dependence on interconnected digital systems can create systemic vulnerabilities, where failures or disruptions have wide-reaching implications for service continuity and public trust.

At the same time, the sector continues to operate within legacy administrative and institutional frameworks, resulting in a dual transformation dynamic. Traditional constraints—such as municipal finance limitations, fragmented planning processes, and capacity gaps—coexist with increasingly complex, technology-enabled delivery systems. This interplay makes the risk environment highly interdependent, where governance effectiveness, technological resilience, fiscal capacity, and citizen trust are closely linked.

The most significant risks in this sector arise where structural weaknesses intersect with rapidly evolving external pressures. Factors such as climate volatility, water stress, infrastructure strain, cyber dependence, project execution delays, and institutional coordination failures rarely operate in isolation. Instead, they tend to compound, leading to service disruption, increased public grievance, reputational erosion, and higher remediation costs.

Overall, the government and public services sector can be understood as a system of interconnected risks rather than isolated administrative challenges. The risk landscape reflects broader systemic exposure, where outcomes are shaped by the interaction of policy design, institutional capacity, technological systems, environmental conditions, and citizen expectations. Effective risk management in this context therefore requires an integrated approach that aligns governance reform, digital resilience, fiscal sustainability, and public trust within a unified framework.

5.1.3.2 Key Risk Themes

The risk landscape within government and public services is shaped by a combination of structural, operational, and perception -driven factors, increasingly influenced by the interaction between governance systems, environmental pressures, digital infrastructure, and public expectations. Through our analysis we identified over 200 risks, with a significant proportion concentrated in execution and infrastructure-related risks, alongside notable exposure to digital system dependencies and governance-driven systemic risks.

One of the most significant risks relates to **policy execution and implementation gaps.** These risks are often observable through indicators such as project delays, cost overruns, pending approvals, and grievance volumes. While policy frameworks may be robust in design, challenges often arise during execution due to coordination issues, capacity constraints, and regional variations. The multi-layered nature of governance, combined with overlapping institutional mandates, can result in delays, inconsistencies, and inefficiencies. Factors such as slow decision-making processes, judicial delays, and risk-averse administrative behaviour—driven by fear of scrutiny—further contribute to execution bottlenecks. This creates a disconnect between policy intent and outcomes, affecting service delivery, increasing project costs, and eroding stakeholder confidence.

Infrastructure-related risks are also prominent, particularly in areas such as transportation, energy, and urban development. Recent disruptions in digital service delivery platforms and delays in large-scale infrastructure projects illustrate how execution and system risks can directly affect citizen welfare. Large-scale infrastructure projects involve long timelines, high capital investments, and multiple stakeholders, increasing exposure to delays, cost overruns, and operational inefficiencies. These risks are compounded by rapid urbanisation, fiscal constraints, and coordination challenges across agencies. In addition, climate-related factors such as flooding, heatwaves, water scarcity, and environmental degradation are no longer isolated events but persistent conditions that affect infrastructure planning, asset resilience, and long-term viability of urban systems.

Cybersecurity and digital infrastructure risks have emerged as critical areas of concern, given the increasing reliance on digital platforms for public service delivery. The expansion of digital public infrastructure, direct benefit transfer systems, and integrated service platforms has improved scale and efficiency but has also created concentrated dependencies on interconnected systems. Risks related to API failures, platform concentration, data inaccuracies in benefit delivery systems, and cybersecurity threats such as ransomware or coordinated attacks can disrupt essential services and trigger cascading effects across welfare delivery, public finance, and citizen trust. Failures in identity verification or authentication systems can lead to exclusion errors at scale, further affecting welfare access. Furthermore, challenges in integrating legacy systems with modern digital platforms, along with issues of algorithmic transparency and data governance, add to operational complexity.

Governance and accountability risks remain central to the sector, as public institutions operate under high levels of scrutiny from citizens, media, and oversight bodies. Issues related to transparency, ethical conduct, and decision-making processes can have significant reputational and political consequences. In addition, structural governance risks—such as inefficient allocation of public resources, weak strategic direction in state-owned entities, and inconsistencies in policy implementation—can limit the effectiveness of public interventions and weaken long-term institutional credibility.

Capacity constraints represent another key risk factor, reflecting not just resource limitations but skill mismatches in digitally enabled governance systems. Rapid changes in economic, technological, and environmental conditions require adaptive capabilities, which may be limited by resource availability, institutional rigidity, and skill gaps within the public sector. These constraints are particularly visible in large, complex programmes that require cross-sector coordination, data integration, and sustained administrative oversight.

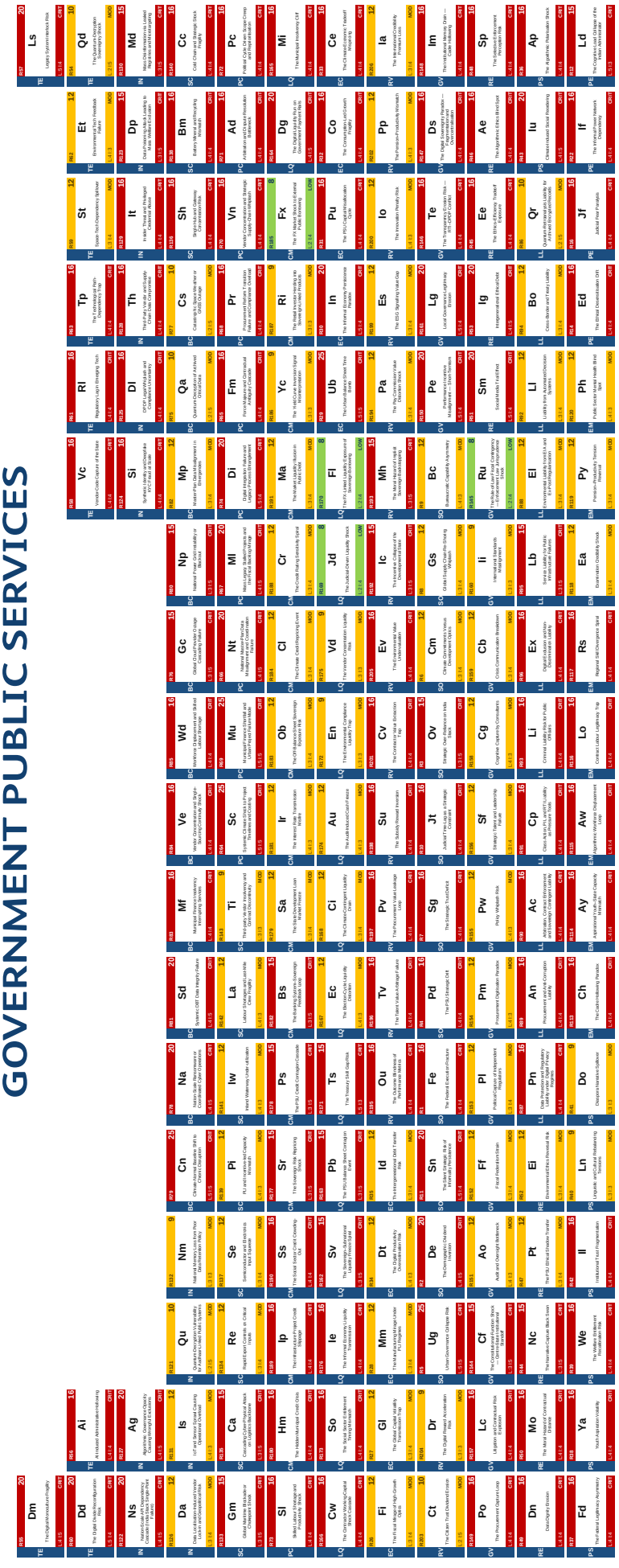
A defining feature of risks in this sector is their strong perception component, where public trust and confidence play a critical role. Public trust functions as a core institutional asset, influencing citizen compliance, programme adoption, and the effectiveness of policy interventions. Failures in service delivery, perceived unfairness, lack of transparency, or exclusion—particularly in digital systems—can lead to widespread dissatisfaction, social backlash, and reputational damage. In a high-visibility environment shaped by media and social platforms, even minor operational issues can escalate into broader legitimacy challenges if they are perceived as systemic or unjust.

> "The industry is moderately prepared for risk events it has seen before and materially underprepared for those it has not."
>
> **— Anti-Financial Crime respondent,**
> when asked how prepared the industry is for a major crisis

In addition, **macro-governance risks** linked to employment generation, informality, fiscal sustainability, and broader economic assumptions play a crucial role in shaping the sector's risk profile. Challenges such as limited job creation, persistent informal economic activity, inefficient public capital deployment, and dependence on consumption-led growth can constrain inclusive development and increase fiscal pressure. These dynamics highlight that risks in government and public services extend beyond administrative or operational issues to include the possibility that underlying economic and policy assumptions may not materialise as expected.materialise as expected.

Overall, the government and public services sector exhibits a highly interconnected risk environment where individual risks rarely operate in isolation. Policy execution gaps can exacerbate infrastructure challenges; climate pressures can intensify fiscal and service delivery risks; digital system failures can trigger welfare disruption and reputational consequences; and governance weaknesses can amplify systemic inefficiencies. This interconnectedness underscores the need for a holistic and integrated approach to risk management, where risks are assessed not only individually but also in terms of their capacity to reinforce and amplify one another across the public service ecosystem.

5.1.3.3 The Periodic Risk Table



5.1.4 Telecom

5.1.4.1 Overview

The telecom sector underpins the digital economy, functioning as critical infrastructure through which economic activity, financial systems, and public services operate in real time. It supports critical infrastructure such as financial systems, government services, enterprise operations, digital payments, e-commerce, logistics, and emergency communication, making it a key component of national resilience and the broader digital public infrastructure ecosystem. Its systemic importance lies in its role as the foundational layer upon which modern economic and social activity depends.

The sector is characterised by high capital intensity, rapid technological evolution, and strong regulatory oversight, functioning as a 'system-of-systems' layer, where failures propagate across interconnected sectors rather than remaining contained. It operates within a competitive market environment while simultaneously delivering essential public infrastructure, creating a balance between commercial viability and strategic national priorities. Ongoing transformations—including the rollout of 5G networks, expansion of fibre connectivity, adoption of cloud and edge computing architectures, emergence of software-defined networks, and the incorporation of AI in network management—are reshaping the sector. At the same time, developments such as satellite communication, Open RAN architectures, and early-stage planning for 6G are redefining long-term competitiveness and technological positioning.

From a systems perspective, telecom networks can be understood as critical infrastructure networks, where reliability, scalability, and availability are essential. This creates concentrated points of failure where localised disruptions can result in disproportionate system-wide impact. The increasing integration of telecom systems with digital platforms, cloud infrastructure, Internet of Things (IoT) ecosystems, and data-driven services has expanded their functional role but also increased their exposure to systemic vulnerabilities. These dependencies create interlinked risk pathways across sectors, where disruptions are not contained within telecom networks alone but can cascade into broader economic and social systems.

A defining characteristic of the telecom sector is its high degree of systemic relevance. Telecom networks increasingly represent strategic targets, extending cyber risk into national security domains. Disruptions in telecommunications infrastructure, whether due to technical failure, cyber incidents, energy constraints, or policy-related issues, can rapidly propagate across interconnected sectors, affecting payments systems, logistics operations, healthcare delivery, education access, business continuity, and citizen communication. This interconnectedness underscores that telecommunications risk extends beyond network operations to encompass broader economic and societal stability.

The sector's risk profile is increasingly shaped by the interaction of multiple structural factors, including infrastructure fragility, regulatory and policy dynamics, cybersecurity and data exposure, capital investment pressures, energy dependence, vendor concentration, workforce capability, and public trust. Municipal-level execution challenges, such as right-of-way permissions and infrastructure deployment delays, further complicate network expansion and reliability. As a result, telecom risk is multidimensional, requiring coordination across technical, financial, regulatory, and operational domains.

In this context, effective risk management in the telecom sector requires an integrated approach that aligns network resilience with regulatory legitimacy, technological sovereignty, financial sustainability, and societal trust. These dimensions are not independent; rather, they are mutually reinforcing, collectively determining the sector's ability to support a resilient and inclusive digital economy.

5.1.4.2 Key Risk Themes

The telecom sector faces a range of risks that are both operational and systemic in nature, reflecting its central role in enabling connectivity across the digital economy. These risks are increasingly shaped by the interaction between physical infrastructure, technology architecture, regulatory dynamics, financial pressures, and public trust.

One of the most critical risks is related to **network reliability and infrastructure resilience**. Failures in network systems can lead to widespread disruptions, affecting multiple sectors simultaneously. However, network resilience is not determined solely by core technology; it is also heavily dependent on supporting physical infrastructure such as fibre networks, access routes, and municipal coordination. Risks related to fibre fragility, co-located infrastructure, and disruptions caused by construction activity, flooding, or maintenance constraints can lead to cascading service degradation. In addition, delays and inconsistencies in right-of-way approvals across local authorities can slow network expansion, increase deployment costs, and affect the rollout of advanced technologies such as 5G.

Cybersecurity risks are particularly significant, as telecom networks are frequent targets for cyberattacks. Breaches can compromise sensitive data, disrupt services, and create vulnerabilities in connected systems. As networks evolve towards software-defined and virtualised architectures, the attack surface expands, introducing new risks related to system opacity, automation dependencies, and integration across multiple vendors and platforms. These developments also create interdependencies between cybersecurity, data governance, and operational continuity.

Vendor concentration and supply chain dependencies represent another major risk factor. The sector relies on a limited number of global equipment providers, as well as broader eco-systems involving semiconductor supply chains, cloud providers, satellite systems, and undersea cable infrastructure. These dependencies create exposure to geopolitical tensions, export restrictions, and disruptions in global supply chains, affecting both operational continuity and strategic autonomy.

Regulatory and policy risks are also central to the telecom sector. The sector operates at the intersection of commercial viability, regulatory mandates, and public expectations, creating inherent structural tensions. Issues related to spectrum allocation, pricing regulations, compliance requirements, and lawful interception obligations influence both operational and financial performance. At the same time, telecommunications providers must navigate the balance between regulatory compliance and public expectations of neutral, open connectivity. Actions such as internet shutdowns, opaque data practices, or inadequate communication during outages can transform regulatory compliance into reputational risk, affecting the sector's social licence to operate.

Technological change introduces additional complexity, as the transition to new generations of technology, such as 5G and beyond, requires significant investment and coordination. While these advancements enable innovation and efficiency, they also increase exposure to execution risks, interoperability challenges, and potential systemic vulnerabilities arising from tightly integrated digital ecosystems.

Financial sustainability represents a critical and often under-emphasised risk dimension. The telecom sector combines high capital intensity with relatively weak monetisation, where rapid growth in data consumption does not necessarily translate into proportional revenue gains. Spectrum costs, statutory obligations, competitive pricing pressures, and mandated inclusion can compress margins and strain liquidity. Financial stress in telecom operators can also propagate into the broader financial system through lender exposure and reduced infrastructure investment. Financial stress within telecom operators can have cascading effects on tower companies, infrastructure providers, vendors, lenders, and future investment in network expansion and next-generation technologies.

The sector is also exposed to **capacity and demand risks,** where rapid growth in data consumption can strain infrastructure and require continuous scaling. Failure to keep pace with demand can result in service degradation, congestion, and customer dissatisfaction, further impacting trust and revenue models.

In addition, **climate, energy, and physical resilience risks** are becoming increasingly material. Telecom infrastructure—including towers, fibre networks, data centres, and power systems—is vulnerable to environmental factors such as heatwaves, floods, cyclones, and power outages. These risks not only affect operational continuity but also increase maintenance costs and require adaptation in network design, energy sourcing, and backup systems. Long-term pressures related to decarbonisation and environmental compliance further add to operational complexity.

Governance, workforce capability, and institutional effectiveness also play a crucial role in shaping risk outcomes. The increasing complexity of telecom systems requires specialised technical expertise, while competition for skilled talent from global technology firms can create capability gaps. At the same time, governance bodies must navigate issues related to infrastructure resilience, cybersecurity, data protection, capital allocation, and regulatory obligations. Weaknesses in these areas can turn manageable operational risks into broader strategic challenges.

A defining feature of risks in the telecom sector is the **centrality of trust and legitimacy.** In a highly connected and digitally dependent society, public perception of reliability, fairness, and transparency plays a critical role in sustaining operations. Poor communication during outages, perceived exclusion of underserved regions, or concerns around surveillance and data usage can erode trust rapidly, with implications for both regulatory relationships and customer confidence. Overall, the telecom sector exhibits a deeply interconnected risk environment where individual risks rarely operate in isolation. Municipal-level execution challenges can delay fibre deployment; infrastructure fragility can disrupt critical services such as payments and public systems; financial stress can constrain investment in resilience; technology dependencies can introduce cybersecurity and sovereignty risks; and climate events can affect network continuity. This interconnectedness highlights the need for an integrated approach to risk management that aligns infrastructure resilience, financial sustainability, regulatory engagement, technological governance, environmental adaptation, workforce capability, and public trust within a unified framework.

5.1.4.3 The Periodic Risk Table

5.1.5 Mitigation Strategies

Across aviation, financial services, government, and telecom sectors, risks are increasingly interconnected, dynamic, and capable of cascading across organisational and sectoral boundaries. As a result, mitigation can no longer rely on isolated controls or static frameworks. Organisations must adopt an integrated, lifecycle-based approach that evolves continuously alongside the risk environment.

The mitigation framework is structured as a closed-loop system linking prevention, detection, response, and resilience into a continuous cycle. It aligns with core risk treatment strategies by reducing likelihood, limiting impact, transferring exposure where appropriate, and accepting residual risks where necessary. In complex systems, risks cannot be entirely eliminated; therefore, the emphasis shifts toward controlling how risks propagate and strengthening the organisation's capacity to adapt.

5.1.5.1 Prevention (Risk Avoidance and Reduction)

Prevention represents the first and most critical layer of the framework, focused on reducing the likelihood of disruption through robust system design and forward-looking controls. This requires a deliberate shift from efficiency-oriented models toward resilience-oriented architectures. Organisations must embed layered cybersecurity controls, segregate critical systems from non-critical networks, and enforce strong encryption and data protection practices to minimise vulnerability.

Infrastructure resilience must be built into system design through redundancy and distribution, including backup power capabilities, dual network pathways, and decentralised operational structures. In digital environments, reducing dependency risk requires diversification through multi-cloud strategies and platform alternatives, ensuring that failure in a single provider does not translate into systemic disruption.

Supply chain resilience is equally central to prevention. Organisations must proactively diversify vendor bases, monitor supplier stability, and establish alternative sourcing arrangements, particularly in sectors where dependencies are concentrated and substitution is limited. Alongside structural measures, governance and human capital play a foundational role. Strong internal controls, clear accountability mechanisms, and ongoing workforce capability development ensure that risk awareness is embedded across operations.

In this context, prevention enables a transition from reactive risk management to proactive risk control, addressing vulnerabilities before they materialise into disruption.

5.1.5.2 Detection (Monitoring and Early Warning Systems)

While prevention reduces exposure, it cannot fully eliminate risk. Detection mechanisms therefore become critical in identifying early signals of emerging threats and enabling timely intervention. In modern risk environments, detection must operate as a continuous, real-time process, supported by integrated monitoring systems that provide visibility across operational, technological, and external domains.

Organisations increasingly rely on centralised dashboards, security operations centres, and automated alert systems to track system behaviour and identify deviations. A key component of this capability is the use of Key Risk Indicators, which provide measurable signals of potential disruption. Metrics such as system downtime, intrusion attempts, vendor risk scores, and capacity utilisation enable organisations to detect emerging vulnerabilities before they fully materialise.

Advancements in analytics and artificial intelligence further enhance detection capabilities by enabling anomaly identification and predictive insights. This shifts organisations from reactive monitoring toward anticipatory risk sensing. In parallel, detection must incorporate external intelligence, including regulatory developments, geopolitical shifts, and emerging threat patterns, as these external factors increasingly influence internal risk exposure.

Ultimately, effective detection reduces the time between risk emergence and organisational awareness, significantly improving the effectiveness of subsequent response actions.

5.1.5.3 Response (Incident and Crisis Management)

Response capability determines how effectively an organisation manages disruption once it occurs. Even with strong preventive and detection mechanisms, complex systems inherently carry residual risk, making response preparedness a critical component of resilience.

Effective response requires well-defined incident management structures, supported by clear escalation protocols, decision-making hierarchies, and predefined roles and responsibilities. These elements ensure coordination and speed during high-pressure situations, reducing the risk of delayed or fragmented decision-making.

Business continuity and disaster recovery frameworks form the operational backbone of response. These frameworks rely on backup systems, alternate operating models, and recovery infrastructure capable of sustaining operations during disruption. Their effectiveness depends on regular testing and simulation under realistic conditions.

Operational containment is equally important, particularly in environments where disruption can escalate rapidly. Measures such as isolating affected systems, rerouting operations, or implementing controlled shutdowns limit the extent of damage and prevent wider system impact. Financial risk transfer mechanisms, including insurance, provide an additional layer of protection by mitigating economic loss. At the same time, timely and transparent stakeholder communication is essential in managing reputational risk and maintaining trust.

Strong response capability is ultimately defined by speed, coordination, and decisiveness, ensuring that incidents are contained before they evolve into systemic crises.

5.1.5.4 Resilience (Recovery and Adaptive Capability)

Resilience extends beyond recovery to encompass an organisation's ability to adapt, learn, and strengthen in response to disruption. Unlike traditional approaches that focus on restoring operations to pre-incident levels, modern resilience frameworks emphasise continuous adaptation and long-term system improvement.

A critical component of resilience is the establishment of redundancy and failover mechanisms that allow operations to continue despite system failure. This includes diversification across geographies, infrastructure, and operational processes, reducing reliance on single points of failure.

Equally important is post-incident learning. Organisations must systematically analyse disruptions to identify root causes, structural weaknesses, and process gaps. These insights must then be integrated into prevention and detection frameworks, creating a continuous feedback loop that strengthens overall system resilience.

Resilience also requires flexibility in operating models. Organisations must maintain the ability to dynamically allocate resources, adjust capacity, and adapt strategies in response to evolving conditions. This includes scaling operations efficiently during periods of disruption or recovery.

In this way, resilience transforms risk management from a defensive mechanism into a strategic capability, enabling organisations to absorb shocks while sustaining long-term performance.

5.1.5.5 KRIs and Governance

The effectiveness of the mitigation framework depends on how well risk monitoring is embedded within governance structures. Key Risk Indicators must be fully integrated into organisational dashboards, reporting systems, and periodic review processes, ensuring that risk signals are continuously monitored and acted upon.

This integration enables alignment between risk management and strategic decision-making, ensuring that leadership has timely visibility into emerging exposures. Linking KRIs with frameworks such as Periodic Risk Tables further enhances this capability by providing a dynamic and evolving view of organisational risk.

The strength of the overall framework ultimately depends on a combination of governance, culture, and technology. Clear accountability, data-driven decision-making, and strong cross-functional coordination are critical enablers. Regular testing and validation of systems ensure that both preventive and response mechanisms remain effective under changing conditions.

When effectively embedded, the mitigation framework ensures that risk management is not treated as a standalone function, but as an integral component of organisational strategy, supporting resilience, adaptability, and sustained value creation.

Aviation, Government & Public Services, Financial Services, & Telecom

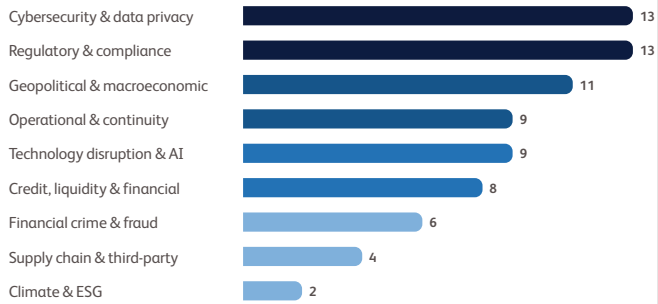
15
RESPONDENTS

93%
SAY THEY ARE GROWING
1 of 15 reports Stable

3.7/5
AVG RISK EXPOSURE
7 rate 3 . 5 rate 4 . 3 rate 5

~10%
MEDIAN RESOURCES TO RISK MGMT
Range 2% (telecom) to 25-30% (NBFC)

What keeps these industries up at night - top-five risk mentions



75 mentions = 15 respondents * 5 risks each.

The risk outlook - what's rising now, what's coming next

RISING FASTEST . LAST 3 YEARS

- Cyber & digital fraud
- AI-enabled fraud & deepfakes
- Third-party / hyperscaler dependency
- Geopolitical instability
- Regulatory velocity
- Model & conduct risk

→

EMERGING . NEXT 3-5 YEARS

- AI governance
- Deepfake & agentic-AI fraud
- Quantum encryption risk
- Cloud & hyperscaler concentration
- Climate-linked credit risk
- Regulatory fragmentation
- Geopolitical realignment
- Unsecured retail stress
- DeFi / digital-asset layering

Driven by: Rapid digitalisation & technology dependence; Customer / borrower stress and over-leverage; Regulatory velocity & supervisory tightening; Geopolitical and macroeconomic uncertainty.

Risk appetite - segment average by dimension

FINANCIAL	OPERATIONAL	REGULATORY	STRATEGIC
3.0/5	2.2/5	1.7/5	3.5/5
Moderate	Low	Very Low to Low	Moderate to Mod-High
from 13 stated answers	from 13 stated answers	from 12 stated answers	from 12 stated answers

A low score means the segment has little appetite for that type of risk-failures there are treated as unacceptable and are tightly controlled rather than taken on. A high score means the segment is willing to accept more of that risk in pursuit of growth, innovation and returns.

How far ahead these industries plan

Now - 12 months	Liquidity, payments, cyber & fraud-watched daily to 90 days
1 - 3 years	Credit cycles, capital planning, profitability & deposit competition
3 - 5 years	AI governance, cloud concentration, regulatory & business- model shifts
5 years +	Climate-linked credit, quantum encryption, structural change

Crisis preparedness --- self-assessed, by segment

The dependency chain - what operations cannot run without

1. Cloud hyperscalers & core-banking technology
2. UPI / NPCI payment rails & credit bureaus
3. Aadhaar e-KYC & digital identity infrastructure
4. Telecom networks & data centres
5. Reinsurers, insurers & funding markets
6. Regulators RBI, IRDAI, PFRDA

12 of 15 report active industry-level risk collaborations. Effectiveness is rated moderate to high- SROS and FIU-IND-guided platforms (MuleHunter.AI, DPIP) are called "very effective"; voluntary intelligence-sharing between competitors remains underdeveloped.

From gaps to action

WHAT'S MISSING TODAY

- ✕ Cyber, AI & analytics talent shortage
- ✕ Fragmented risk data & legacy architecture
- ✕ Inconsistent first-line owner ship & board engagement
- ✕ Limited predictive analytics & early warning
- ✕ Barrier: Legacy technology & data silos

WHAT WOULD CLOSE THE GAP

- ✓ Upskill people and fund compliance to match actual risk exposure
- ✓ Invest in AI-driven analytics, data governance & secure infrastructure
- ✓ Build shared fraud & threat-intelligence platforms
- ✓ Make boards genuinely own financial-crime and cyber risk
- ✓ Run deeper cyber-simulation and crisis exercises

Already in play: Zero-trust security architecture, AI & model-risk governance, Early warning systems, Co-lending & risk transfer.

The agenda - what these industries say they must do next

TOP COMPLIANCE PRIORITY
Active board oversight
then: Keeping pace with regulatory change

MOST PRESSING SHARED CHALLENGE
Strengthening governance & culture
then: Integrating cybersecurity & data privacy

#1 FOCUS NEXT 12-24 MONTHS
Accelerating digital transformation
6 of 15 review tolerance limits quarterly

What enables it (importance / 5): Culture & values **4.47**. Continuous risk assessment **4.47** Technology & data **4.40** Maturity of risk & compliance functions **4.33**. **Hardest rules to live with:** Data privacy (DPDP) & cybersecurity directions; KYC / AML & sanctions screening; Digital lending & outsourcing norms.

"Regulation defines the operating licence; analytics is shifting risk management left — from retrospective reporting to real-time, predictive intervention."

5.2 Food Security, Fast Moving Consumer Goods, Agriculture

About the researchers

Dr. Binay Kumar Pathak

Assistant Professor
Indira Mahindra School of Education,
Mahindra University.

Dr. Binay Kumar Pathak is an Assistant Professor and PhD Programme Coordinator at Indira Mahindra School of Education, Mahindra University. His research interests revolve around issues of development, economics of Information, education policy, economics of knowledge, and research ecosystems. He has authored working papers on Agriculture, Food Security, Water Security, and Demographics for a strategic trends project. He is an IRM Level 1 certified professional.

Chennamenani Parikshit Rao

final-year BBA (Computational Business Analytics) Student at Mahindra University
IRM Level 1 certified professional

Chennamenani Parikshit Rao is a final-year BBA (Computational Business Analytics) Student at Mahindra University and is an IRM Level 1 certified professional. He contributed to the sectors of Agriculture, Food, FMCG, and Education.

5.2.1 Food Security

5.2.1.1 Overview

Food security represents a foundational pillar of economic stability, public health, and social welfare, encompassing the availability, accessibility, safety, and affordability of food across populations. It operates as a multi-dimensional system spanning agricultural production, procurement, storage, logistics, distribution, and welfare delivery mechanisms supported by extensive institutional and regulatory frameworks.

The sector functions within a highly interconnected ecosystem influenced by environmental variability, infrastructure capacity, macroeconomic conditions, and policy interventions. Unlike purely commercial sectors, food systems are governed by a public welfare imperative, where disruptions directly affect nutritional outcomes, inflation, and social stability rather than only financial performance.

Increasing exposure to climate variability, global trade dynamics, and resource constraints has transformed food security from a production-centric issue into a system-wide challenge. Risks now emerge across multiple nodes simultaneously, with vulnerabilities in production, storage, delivery, and policy frameworks reinforcing one another.

As a result, food security operates as a tightly coupled system in which environmental, logistical, economic, and institutional factors collectively determine resilience and stability.

5.2.1.2 Key Risk Themes

The food security risk landscape is driven by the interaction of climate dynamics, infrastructure constraints, economic volatility, and welfare delivery complexity.

Climate variability is a primary risk driver, with erratic monsoons, rising temperatures, and land degradation directly affecting crop yields, supply stability, and price volatility

Supply chain and infrastructure risks are equally significant. Dependence on large-scale storage and transport systems creates exposure to post-harvest losses, spoilage, and inefficiencies, particularly in regions with inadequate warehousing and cold-chain infrastructure. Weaknesses in warehousing quality, regional infrastructure gaps, and transit inefficiencies reduce effective supply and increase system-wide costs.

Macroeconomic factors further amplify risk exposure. Volatility in global commodity prices and input costs—such as fertilisers and fuel—affects both production incentives and retail prices, with direct implications for food inflation and overall economic stability. Given the weight of food in inflation indices, these pressures can quickly translate into broader economic instability.

Distribution and welfare delivery risks represent a critical operational dimension. Food systems rely on large-scale public distribution networks and digital identification systems, where inefficiencies such as leakage, authentication failures, and quality issues can undermine both access and trust. In such systems, operational reliability becomes directly linked to public health outcomes.

Regulatory and policy risks add additional complexity. Changes in procurement policies, subsidy structures, trade restrictions, and stock limits can alter supply incentives, distribution patterns, and pricing dynamics. Frequent or unpredictable changes in procurement policies, subsidies, and trade restrictions can distort supply incentives and pricing signal.

Resource depletion and sustainability constraints are emerging as long-term structural risks. Declining groundwater levels, soil degradation, and unsustainable cropping patterns threaten future production capacity, reducing the system's ability to absorb shocks.

Workforce and rural dynamics also influence sector resilience. Labour shortages, demographic shifts, and skill gaps affect agricultural operations and downstream supply chain efficiency, particularly in labour-intensive segments.

Overall, food security reflects a highly interconnected system where climate, infrastructure, economic, and institutional risks interact continuously. Effective risk management requires an integrated approach that strengthens production resilience, modernises infrastructure, ensures distribution integrity, and supports long-term resource sustainability.

> "The industry will remain fundamentally resilient, but the risk mix will become more non-financial and more interconnected."
>
> **— FMCG respondent,**
> when asked how the risk landscape will evolve

5.2.1.3 The Periodic Risk Table

5.2.2 Fast Moving Consumer Goods

5.2.2.1 Overview

The Fast-Moving Consumer Goods (FMCG) sector is a high-volume, consumption-driven industry encompassing food, personal care, and household products. It plays a central role in economic activity by linking manufacturing value chains with daily consumer demand across urban and rural markets.

The sector is characterised by rapid inventory turnover, extensive distribution networks, and strong dependence on demand predictability. Its operating model is highly sensitive to supply chain efficiency, input cost dynamics, and consumer behaviour, resulting in a constant trade-off between speed, cost, and reliability.

In recent years, the FMCG landscape has undergone structural transformation driven by digital distribution platforms, quick-commerce expansion, and evolving consumption patterns. This shift has increased reliance on technology and platform intermediaries while intensifying competition and margin pressure.

As a result, FMCG operates within a tightly coupled system where operational efficiency, demand volatility, and distribution dynamics interact continuously, amplifying both opportunity and risk.

5.2.2.2 Key Risk Themes

The FMCG risk landscape is shaped by the interplay of supply chain complexity, cost pressures, digital transformation, and consumer dynamics.

Supply chain and distribution risks remain central. High dependency on logistics networks, warehousing systems, and supplier ecosystems creates vulnerability to disruptions, particularly given the time-sensitive nature of products, where disruptions can rapidly result in stockouts, lost sales, and reduced shelf availability. Failures in transport, inventory management, or last-mile delivery can quickly translate into stockouts and revenue loss.

Channel transformation represents a key structural risk. The rapid growth of e-commerce and quick-commerce platforms is shifting demand toward platform-driven channels, increasing dependency on intermediaries, altering bargaining power, and compressing margins. This transition requires continuous adaptation of omnichannel strategies.

Input cost volatility introduces significant financial pressure. Fluctuations in raw materials, packaging, and energy costs directly affect margins, while limited pricing flexibility—due to consumer sensitivity—restricts cost pass-through mechanisms.

Demand-side uncertainty further complicates operations. Changing consumer preferences, price sensitivity, and the increasing influence of digital platforms and targeted marketing, leading to inventory imbalances and efficiency losses.

Reputational risk is particularly pronounced. In a digitally connected environment, product issues, quality failures, or negative publicity can rapidly impact brand perception and consumer trust, with immediate effects on sales.

Technology and data-related risks are increasing in importance. Growing reliance on digital platforms, data-driven marketing, and customer analytics introduces exposure to cybersecurity threats, data privacy issues, and system disruptions.

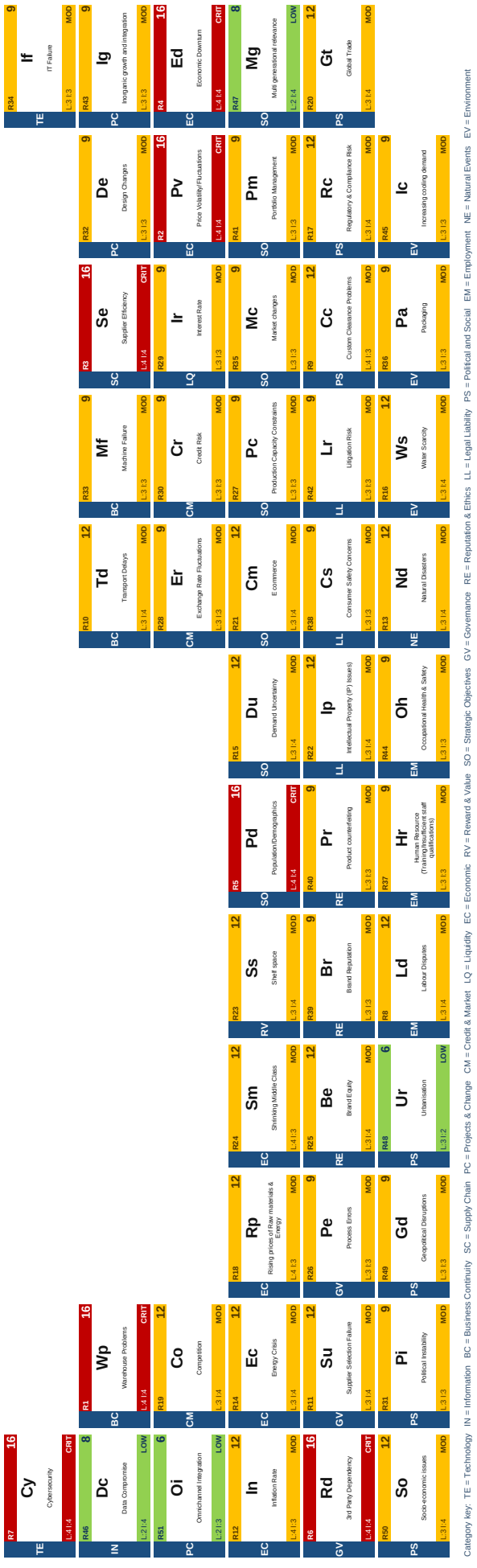
Regulatory and ESG risks are expanding, particularly in areas such as product safety, labelling, environmental compliance, and packaging regulations. Compliance failures can result in penalties, recalls, and reputational damage, while sustainability expectations along with increasing regulatory scrutiny and alignment with global ESG standards are increasingly influencing market positioning.

Workforce-related risks also remain relevant, particularly in frontline sales, logistics, and emerging digital roles. Skill gaps and attrition can affect execution quality and transformation capability.

Overall, the FMCG sector operates within a high-speed, demand-driven system where operational efficiency, cost management, and consumer responsiveness are tightly interconnected. Managing this environment requires balancing supply chain agility with diversification, digital capability, and strong brand governance.

> "One crop season for operating risk. Three to five years for climate, portfolio and capex risk."
>
> **— Agriculture & agri-inputs respondent,**
> when asked which time horizon matters most for risk planning

5.2.2.3 The Periodic Risk Table



5.2.3 Agriculture

5.2.3.1 Overview

The agriculture sector forms the backbone of the food ecosystem, playing a critical role in employment, rural livelihoods, and economic stability. It encompasses crop cultivation, livestock, horticulture, and allied activities, supported by input supply chains nd market linkages.

The sector is inherently dependent on natural resources such as land, water, and climate, making it highly exposed to environmental variability and external shocks. Unlike controlled industrial systems, agricultural production is influenced by biological and ecological factors, resulting in high uncertainty and variability.

Structural characteristics such as fragmented landholdings, seasonal production cycles, and limited technological adoption further shape the sector's performance. At the same time, increasing integration with markets, policy frameworks, and consumption patterns has added complexity to the operating environment.

As a result, agriculture functions as an interconnected system where environmental, economic, and institutional factors collectively determine productivity and resilience.

5.2.3.2 Key Risk Themes

Agricultural risks are driven by environmental dependence, resource constraints, and structural limitations, with strong interconnections across these dimensions.

Climate-related risks remain the most significant. Irregular rainfall, extreme weather events, and shifting seasonal patterns directly impact crop yields and quality. These disruptions create production volatility and income uncertainty, increasing regulatory scrutiny and alignment with global ESG standards.

Water scarcity represents a critical long-term constraint. Over -extraction of groundwater and inefficient irrigation practices are reducing resource availability, threatening both productivity and sustainability across regions.

Soil degradation and declining fertility further weaken long-term yield potential. Intensive farming practices and overuse of chemical inputs have reduced soil health, increasing dependence on external inputs and raising production costs.

Input cost volatility adds financial pressure, particularly for small and marginal farmers. Fluctuations in fertilisers, seeds, fuel, and labour costs reduce profitability and increase vulnerability to shocks.

Market inefficiencies amplify risk exposure. Limited access to storage, processing, and transportation infrastructure leads to post-harvest losses and price volatility, reducing realised income and increasing supply-side instability.

Structural fragmentation of landholdings restricts economies of scale and limits adoption of mechanisation and advanced technologies. This reduces productivity and bargaining power, particularly in fragmented rural markets.

Policy and regulatory uncertainty introduces additional complexity. Changes in pricing mechanisms, subsidies, and trade policies influence production decisions and market dynamics, often creating unpredictability in planning and investment.

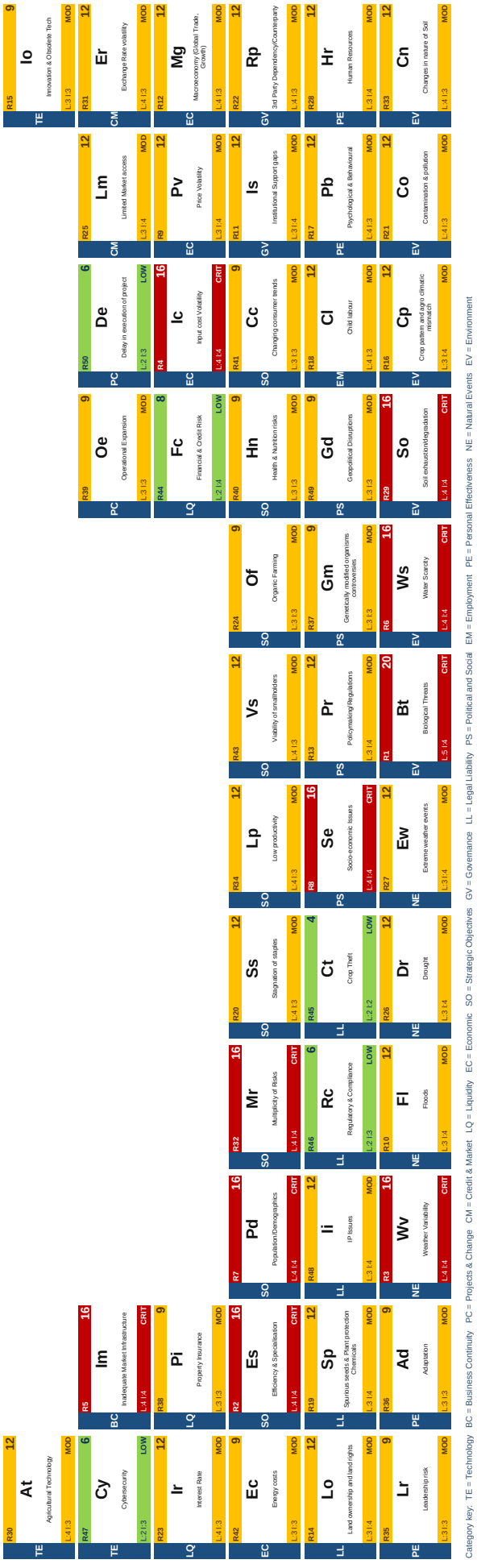
Biological risks, including pests and diseases, further increase variability which can spread rapidly and cause concentrated crop losses, particularly in the absence of effective mitigation systems.

Labour availability and demographic shifts also influence sector performance. Migration to urban areas, ageing farming populations, and skill gaps affect operational timing and efficiency, with affecting critical farming operations such as sowing and harvesting cycles.

Overall, the agriculture sector reflects a structurally fragile system where environmental volatility, resource constraints, market inefficiencies, and institutional limitations interact continuously. Strengthening resilience requires integrated interventions across climate adaptation, resource management, infrastructure development, market access, and technological adoption.

> "We map dependencies as granular as a farmer with one hectare of land, or a trader who trades no more than 1,000 kg of grains a quarter — to protect supplies, continuity planning and foresight."
>
> **— Agriculture respondent,**
> when asked about critical external dependencies

5.2.3.3 The Periodic Risk Table



5.2.4 Mitigation Strategies

5.2.4.1 Prevention (Risk Avoidance and Reduction)

Prevention within the food, FMCG, and agriculture ecosystem is primarily focused on reducing exposure to structural and recurring risks through proactive system design and operational controls. Given the sector's dependence on environmental conditions, supply chains, and quality standards, prevention strategies emphasise resilience at the source of risk.

A key priority lies in addressing climate and environmental risks, including weather variability, extreme events, and water scarcity. Organisations increasingly adopt diversified sourcing strategies across geographies to reduce dependence on single climatic zones, while maintaining seasonal buffer stocks to stabilise supply. Infrastructure strengthening, including hardened facilities and climate-resilient supply chains, further mitigates the risk of physical disruption. Water conservation measures, recycling systems, and alternative sourcing arrangements are also critical in addressing long-term resource constraints.

Food safety and quality risks are managed through stringent preventive controls, including enhanced hygiene protocols, supplier certifications, and routine testing of inputs. Measures such as batch-level traceability, integrated supplier monitoring, and strict chemical and biological controls reduce the likelihood of contamination, adulteration, and product failures. These controls are particularly critical in maintaining regulatory compliance and consumer trust.

Supply chain risk prevention focuses on reducing concentration and dependency. Organisations mitigate these risks by limiting reliance on single suppliers, conducting periodic financial and performance assessments, and maintaining pre-qualified alternative vendors. Investments in cold chain infrastructure, storage capacity, and logistics flexibility further help prevent disruptions in product flow and quality degradation.

Economic and financial risks are addressed through price stabilisation and hedging strategies, including forward contracts, diversified sourcing, and flexible procurement models. Similarly, technology and cybersecurity risks are reduced through layered security architectures, system upgrades, and continuous monitoring, ensuring that growing digital integration does not create new vulnerabilities.

Overall, prevention strategies reflect a shift toward anticipating risk conditions and embedding resilience directly into system design, rather than reacting to disruptions after they occur.

5.2.4.2 Detection (Monitoring and Early Warning Systems)

Detection mechanisms are designed to provide continuous visibility into risk conditions, enabling early identification of vulnerabilities before they escalate into disruptions. Given the dynamic nature of risks in these sectors, detection relies heavily on real-time monitoring systems and clearly defined performance indicators.

Key Risk Indicators play a central role in detection by translating complex risks into measurable signals. In environmental contexts, metrics such as crop yield variation, water availability indices, and early weather alerts provide advance warning of potential supply disruptions. Similarly, monitoring of temperature excursions within cold chains, spoilage rates, and quality rejection trends enables early identification of operational failures.

Supply chain visibility is enhanced through tracking systems that monitor delivery timelines, supplier performance, and logistics disruptions. Indicators such as on-time delivery rates, transit delays, and supplier concentration ratios help organisations identify emerging bottlenecks within the value chain.

In financial and market contexts, indicators such as input price movements, revenue variability, exchange rate fluctuations, and interest coverage ratios provide insight into economic stress conditions. Continuous monitoring of these indicators allows organisations to adjust procurement, pricing, and investment strategies in a timely manner.

Technology-related risks are monitored through cybersecurity indicators such as the frequency of intrusion attempts, system downtime, and recovery times. Real-time monitoring platforms and incident tracking systems ensure that vulnerabilities are detected quickly and addressed promptly.

The effectiveness of detection systems depends on high-frequency monitoring and integration of data across operational, financial, and external sources, including meteorological agencies, regulatory platforms, and internal ERP systems. This ensures that organisations maintain a forward-looking view of risk conditions.

5.2.4.3 Response (Incident and Crisis Management)

Response strategies focus on managing disruptions effectively once they materialise, ensuring that operational, financial, and reputational impacts are contained. Given the interconnected nature of risks in these sectors, response mechanisms must be both rapid and coordinated across multiple functions.

Operational response primarily involves containment and continuity measures, such as activating contingency logistics plans, switching

to alternate suppliers, and rerouting transportation networks. In food systems, rapid recall mechanisms and coordination with public health authorities are critical in managing contamination incidents and limiting consumer impact.

Financial response strategies complement operational measures by reducing exposure to losses. Insurance mechanisms are widely used to transfer risks related to extreme weather, supply chain disruptions, and cyber incidents. Hedging instruments and liquidity buffers further help organisations manage financial volatility during periods of disruption.

Crisis communication plays a crucial role in response, particularly in sectors where consumer trust and brand reputation are critical. Real-time monitoring of consumer sentiment, coupled with transparent communication and remediation efforts, helps limit reputational damage and restore confidence.

In workforce-related disruptions, including pandemics or labour shortages, response mechanisms focus on maintaining operational continuity through flexible staffing models, health protocols, and coordination with external agencies.

Overall, response capability is defined by the ability to act quickly, minimise impact, and prevent the escalation of localised incidents into wider systemic disruptions.

5.2.4.4 Resilience (Recovery and Adaptive Capability)

Resilience reflects the ability of organisations to recover from disruptions and adapt to evolving risk conditions. In the context of food, FMCG, and agriculture sectors, resilience is closely linked to the ability to maintain continuity in the face of environmental, operational, and market uncertainties.

At a structural level, resilience is achieved through redundancy and diversification, including multiple sourcing options, backup infrastructure, and alternate distribution channels. Investments in storage facilities, aggregation networks, and shared infrastructure further enhance the ability to absorb shocks and stabilise supply.

Operational resilience is strengthened through flexibility in production, logistics, and workforce management. This includes the ability to scale operations dynamically, adjust production schedules, and reallocate resources in response to changing demand or supply conditions.

A critical component of resilience is continuous learning and adaptation. Post-incident analysis enables organisations to identify root causes, refine processes, and strengthen preventive and detection mechanisms. Over time, this creates a feedback loop in which each disruption contributes to improving overall system robustness.

Innovation also plays a key role in building resilience, particularly in responding to changing consumer preferences and market dynamics. Organisations invest in product innovation, digital solutions, and partnerships to remain competitive while adapting to new risk conditions.

Ultimately, resilience transforms risk management from a reactive function into a strategic capability, enabling sustained performance in uncertain environments.

5.2.4.5 KRIs and Governance

Effective risk mitigation requires strong integration of monitoring systems with governance structures. Key Risk Indicators serve as the primary link between operational activity and strategic oversight, providing measurable insights into evolving risk conditions.

These indicators are embedded within organisational reporting frameworks, with defined data sources, ownership, and review frequencies. High-frequency monitoring—ranging from daily tracking of operational indicators such as temperature deviations and logistics delays to monthly reviews of financial metrics—ensures that risks are continuously assessed and updated.

Governance mechanisms ensure that risk signals are not only monitored but also acted upon. Regular review cycles, escalation protocols, and cross-functional coordination enable timely decision-making and alignment across organisational levels. External data sources, including regulatory updates, weather alerts, and market intelligence, are integrated into governance systems to provide a comprehensive view of the risk environment.

A key feature of effective governance is its ability to translate data into action, ensuring that insights from KRIs inform both immediate response measures and long-term strategic decisions. This integration enables organisations to maintain a dynamic and forward-looking risk management approach.

> "In this sector, reputation can move faster than facts, so response speed matters."
>
> **— FMCG respondent,**
> when asked about the most significant reputational threats

5.3 Healthcare & Pharma, Information Technology

About the researchers

Dr. Nidhi Goyal

Assistant Professor
Department of Computer Science and Engineering at Ecole Centrale School of Engineering

Dr. Nidhi Goyal is an Assistant Professor in the Department of Computer Science and Engineering at the Ecole Centrale School of Engineering. She is a faculty expert at the Global Centre for Enterprise Risk Management and an IRM-certified Global Level 1 Professional in Enterprise Risk Management. She holds a Ph.D. (CSE) from IIIT-Delhi and was granted the Prime Minister's Fellowship for Doctoral Research to conduct academic research in collaboration with Info Edge India Limited.

Karri Hasini

BBA (Computational Business Analytics)
Student at Mahindra University

Karri Hasini is a BBA (Computational Business Analytics) student at Mahindra University and has contributed to the Healthcare & Pharmaceutical sector analysis.

Sanjana Ailani

B.Tech (Artificial Intelligence)
student at Mahindra University
IRM Level 1 certified professional

Sanjana Ailani, is a B.Tech (Artificial Intelligence) student at Mahindra University and has IRM Level 1 qualification, and she worked on the Information Technology sector analysis.

5.3.1 Healthcare & Pharma

5.3.1.1 Overview

The healthcare and pharmaceutical sector is a critical pillar of economic stability and public welfare, operating at the intersection of scientific innovation, regulatory frameworks, and societal impact. It encompasses pharmaceutical manufacturing, biotechnology, clinical research, diagnostics, hospital care, and broader healthcare delivery systems, all of which contribute to the availability, quality, and accessibility of medical products and services.

The sector is characterised by long product development cycles, high research and development costs, and stringent regulatory oversight. Drug discovery and clinical development involve significant uncertainty, with high failure rates and extended timelines, while manufacturing and distribution systems are required to maintain strict quality standards to ensure patient safety.

The sector is also deeply dependent on global supply chains, particularly for active pharmaceutical ingredients (APIs), specialised chemicals, and manufacturing inputs. This interconnectedness creates exposure to geopolitical developments, trade policies, and supplier concentration risks. At the same time, healthcare delivery systems depend on a combination of hospital infrastructure, insurance networks, digital health platforms, and public policy frameworks, further expanding the scope of interdependencies.

Rapid scientific advancement and technological integration are reshaping the operating landscape. Developments in biologics, advanced therapies, digital health, and data-driven diagnostics are transforming traditional models while introducing new layers of complexity. Increasing adoption of digital systems across clinical research, patient care, and supply chains has enhanced efficiency but also introduced new risks related to cybersecurity, data privacy, and system reliability.

A defining characteristic of the sector is its direct impact on human life, which significantly lowers tolerance for failure. As a result, safety, compliance, traceability, and ethical governance are central to sector operations. The risk landscape has therefore evolved beyond traditional compliance concerns to include scientific uncertainty, supply chain fragility, technological vulnerability, pricing pressures, and public health responsiveness.

5.3.1.2 Key Risk Themes

The healthcare and pharmaceutical risk landscape is shaped by the interaction of regulatory intensity, scientific uncertainty, supply chain dependencies, and technology integration.

Regulatory compliance and quality assurance represent the most critical risk dimension. The sector operates under complex and multi-jurisdictional regulatory frameworks, including domestic authorities and international agencies such as the US FDA and EMA. Risks such as manufacturing quality failures, Good Manufacturing Practice (GMP) deficiencies, inspection observations, and data integrity issues can lead to product recalls, market restrictions, and reputational damage. Maintaining robust quality systems and regulatory alignment is therefore essential for operational continuity and global competitiveness.

Supply chain vulnerability remains a key systemic risk, driven by dependence on concentrated geographies for APIs and critical inputs. Disruptions arising from geopolitical tensions, export restrictions, supplier quality variability, or logistics constraints can directly affect manufacturing continuity and product availability. Given the critical nature of pharmaceutical products, such disruptions have immediate implications for public health and pricing stability.

Research and development uncertainty introduces significant financial and strategic risk. Drug discovery and clinical development involve high capital investment, long timelines, and low success probabilities. Late-stage failures, regulatory rejections, or weak market adoption can result in substantial financial losses and portfolio instability. Balancing innovation pipelines with commercial viability remains a central challenge.

Patient safety and pharmacovigilance risks are fundamental to sector operations. Adverse drug reactions, contamination, incorrect dosing, and delayed identification of safety signals can lead to severe patient harm. Effective pharmacovigilance systems are required to monitor real-world drug performance and enable timely intervention.

Technology-related risks are expanding as the sector becomes increasingly digitalised. The use of electronic health records, telemedicine platforms, AI-driven diagnostics, and connected medical devices introduces exposure to cybersecurity threats, data breaches, and system failures. Given the sensitivity of patient data, data governance and privacy protection have become critical regulatory and ethical priorities.

Emerging risks associated with AI further amplify complexity. Issues such as algorithmic bias, lack of explainability, and model reliability can affect clinical decision-making and patient outcomes, requiring robust governance and oversight frameworks.

Market access, pricing pressure, and reimbursement constraints represent a significant financial risk dimension. Governments, insurers, and healthcare providers exert increasing pressure to control drug prices, while generic competition and regulatory pricing interventions affect profitability. Delays in reimbursement

and market approval processes can further impact revenue realisation.

Operational risks within manufacturing and distribution also remain critical. Process deviations, cold chain failures, and logistical inefficiencies, including batch failures and distribution delays, can compromise product quality and availability, leading to regulatory action and reputational damage.

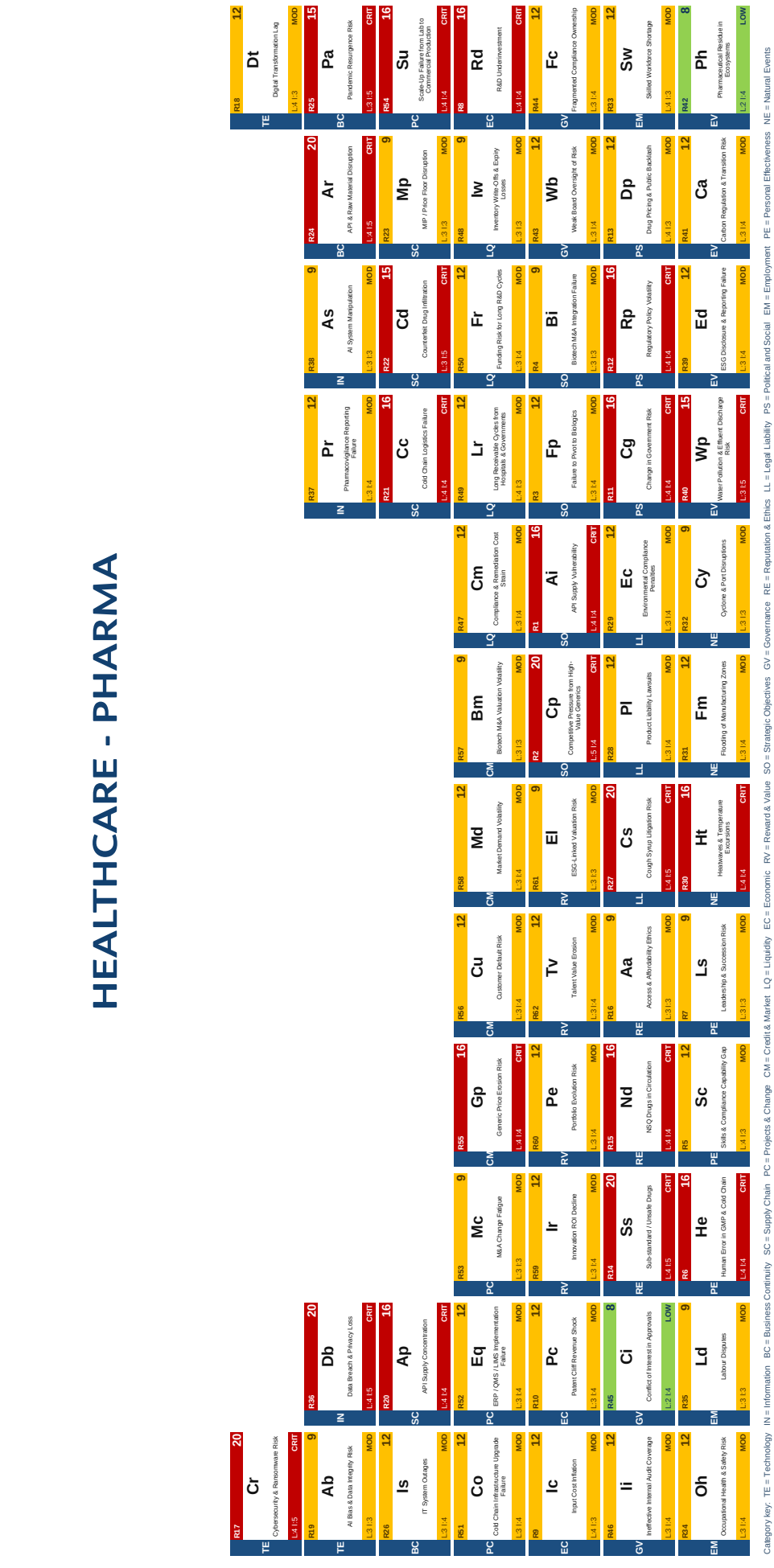
The sector is further exposed to external shocks, including pandemics, public health emergencies, and geopolitical disruptions. These events can simultaneously affect demand patterns, supply chain capacity, regulatory processes, and workforce availability, creating high levels of volatility.

Reputational and ethical risks are closely intertwined with all other risk dimensions. Public trust, regulatory perception, and stakeholder scrutiny are strongly influenced by issues such as drug pricing, accessibility, safety standards, and transparency. Failures in these areas can have wide-ranging and lasting consequences.

> "Traditional risks around clinical quality, patient safety and compliance will remain critical, but they will increasingly converge with digital, cyber and AI-driven exposures."
>
> **— Healthcare respondent,**
> when asked how the risk landscape will evolve over 5–10 years

> "The pharmaceutical industry is considerably more prepared for major risk events today than in the past, particularly following lessons learned from the pandemic, global supply disruptions and increasing cyber security threats."
>
> **— Pharmaceuticals respondent,**
> when asked about crisis preparedness

5.3.1.3 The Periodic Risk Table



5.3.2 Information Technology

5.3.2.1 Overview

One of the main pillars of contemporary economic systems is the information technology (IT) industry. It has made digital transformation possible in a number of sectors, including banking, retail, manufacturing, healthcare, and education. Software services, cloud computing, artificial intelligence, cybersecurity, data analytics, SaaS platforms, and digital infrastructure development are the main drivers of this industry in India and around the world.

The sector is characterised by high innovation intensity, rapid technological evolution, and strong global integration. It operates through distributed delivery models and cross-border service networks, making it both highly scalable and deeply dependent on global regulatory, geopolitical, and infrastructure conditions. As organisations across industries become increasingly reliant on digital systems, technology providers function as central nodes within a broader interconnected ecosystem supporting financial services, governance, healthcare, supply chains, and consumer platforms.

This expanded systemic role has increased both the importance of the sector and its exposure to risk. A defining characteristic of IT risk is its speed and interdependence, where disruptions in one layer—such as cloud infrastructure, cyber systems, or talent availability—can cascade across multiple clients, geographies, and industries. Unlike traditional sectors, risk is largely non-physical, emerging at the level of systems, networks, and digital dependencies.

The pace of technological change further intensifies risk exposure, creating continuous challenges related to technological obsolescence, operational complexity, and evolving threat landscapes. Emerging technologies such as generative AI, automation, and advanced computing systems are reshaping business models while introducing new governance, ethical, and accountability risks. As a result, the sector operates within a highly dynamic environment where resilience depends on adaptability, continuous innovation, and effective management of systemic interdependencies.

5.3.2.2 Key Risk Themes

The technology sector operates within a continuous and evolving risk environment, where exposure is shaped by system interconnectivity, technological acceleration, and external dependencies.

Cybersecurity remains the most critical risk dimension. Threats such as data breaches, ransomware attacks, and unauthorised system access are increasing in sophistication due to expanded attack surfaces across cloud environments, APIs, remote systems, and third-party integrations. Cyber incidents have the potential to disrupt operations, compromise sensitive data, and trigger regulatory, financial, and reputational consequences at scale, while also exposing organisations to regulatory penalties and contractual liabilities.

Identity and access vulnerabilities represent a key entry point for broader system compromise. Weak authentication controls, misuse of privileged access, and compromised machine identities can enable persistent and difficult-to-detect intrusions, amplifying downstream risk across interconnected systems.

Third-party and cloud dependencies introduce **systemic concentration risk.** Reliance on hyperscale cloud providers, SaaS ecosystems, and external vendors creates exposure to outages, service degradation, and vendor lock-in. Disruptions within a single platform can cascade across multiple organisations simultaneously, highlighting the sector's dependence on a limited number of global technology providers.

Operational risks remain significant, arising from configuration errors, process failures, and inadequate change management, including failed deployments, and integration breakdowns. In highly complex digital environments, minor misconfigurations or system integration failures can result in large-scale outages, service disruptions, and contractual penalties.

Technological disruption driven by artificial intelligence and automation is reshaping risk exposure. The adoption of generative AI introduces risks related to model reliability, data leakage, unauthorised use of AI systems, and dependency on third-party models. At the same time, automation is altering traditional service delivery structures, creating pressures on margins, workforce models, and long-term business sustainability.

Ethical and governance risks related to AI are emerging as enterprise-wide concerns. Issues such as algorithmic bias, lack of transparency, explainability challenges, privacy violations, and intellectual property disputes can affect decision-making across areas including finance, healthcare, recruitment, and customer engagement. The rapid pace of AI adoption often outpaces governance frameworks, creating gaps in oversight, accountability, and regulatory compliance.

Talent-related risks represent a structural challenge. The sector faces persistent shortages of skilled professionals in areas such as AI, cybersecurity, and advanced software systems, alongside high attrition rates and competitive global labour markets. Rapid technological change also accelerates skill obsolescence, making continuous reskilling a critical component of operational resilience.

Geopolitical and regulatory risks are increasing in importance due to the global nature of IT operations. Cross-border service delivery exposes organisations to data localisation requirements,

regulatory fragmentation, export controls, and compliance complexity. Geopolitical tensions can influence outsourcing decisions, client relationships, and operational continuity, particularly in sensitive or regulated sectors.

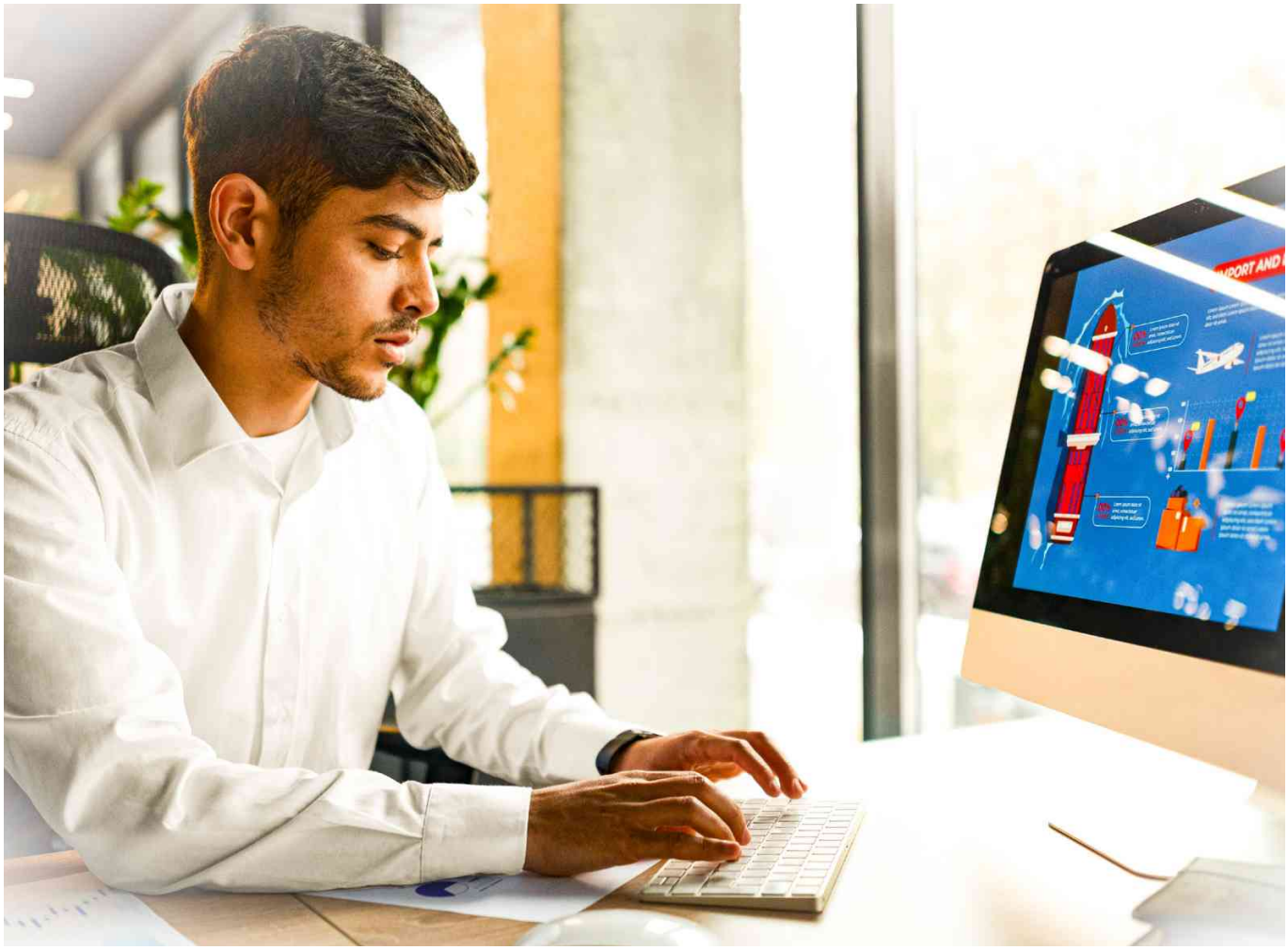
Business continuity and concentration risks further shape the sector's risk profile. Dependence on large clients, specific industries, or key technology platforms can create revenue volatility, while system outages or infrastructure failures can disrupt service delivery across multiple engagements simultaneously.

Overall, the technology sector reflects a highly interconnected digital ecosystem, where risks are dynamic, interdependent, and capable of propagating rapidly across organisational and sectoral boundaries. Cyber threats, platform dependencies, technological disruption, talent dynamics, and regulatory complexity interact continuously, amplifying both the scale and speed of potential disruption.

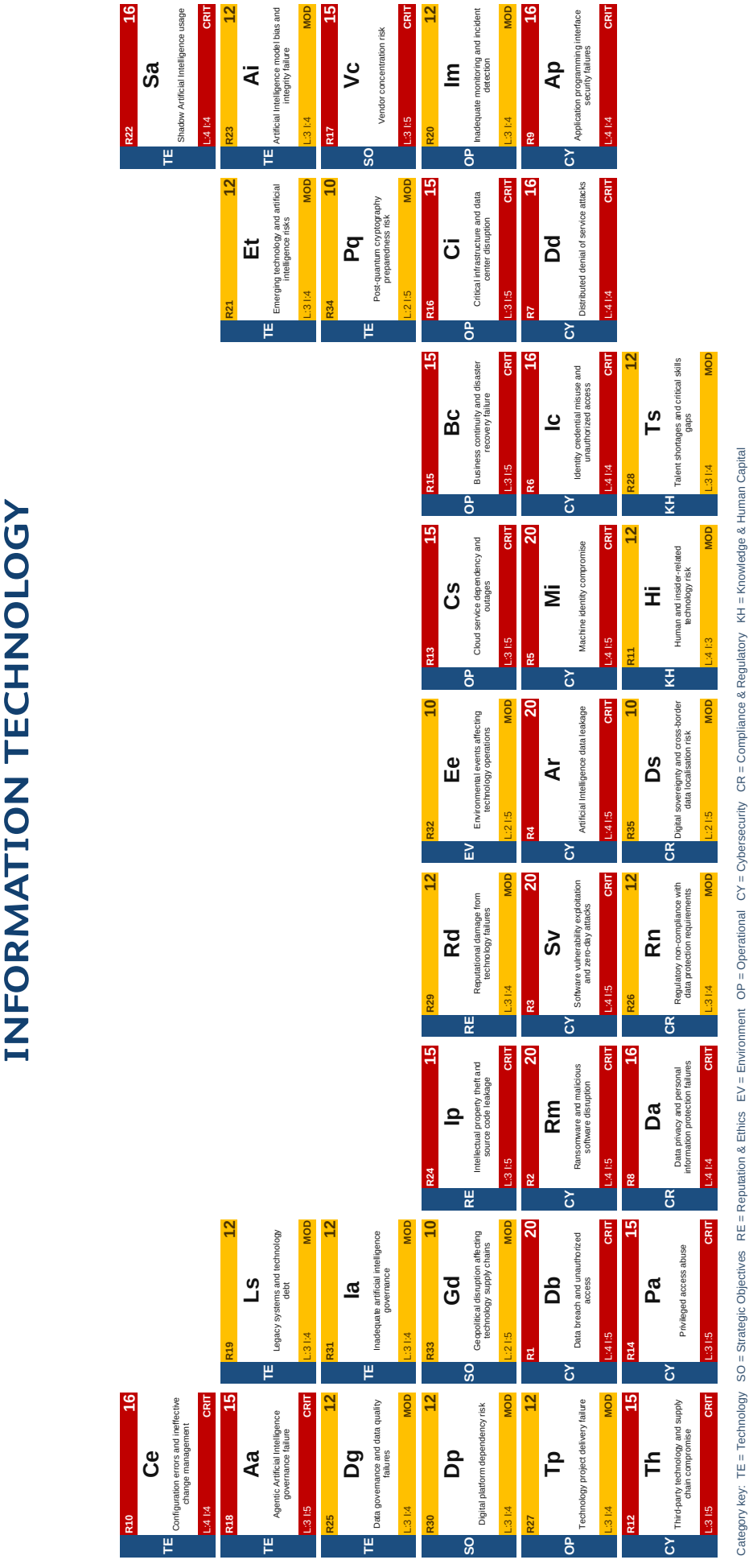
Effective risk management in this environment requires an integrated approach that combines cyber resilience, identity governance, diversification of dependencies, workforce capability development, regulatory alignment, and robust frameworks for responsible and ethical technology use.

> "The ITES industry has a moderate to high appetite for strategic and technology-related risks to support innovation and growth, but maintains a low tolerance for cybersecurity, regulatory, operational and reputational risk."
>
> **— ITES respondent,**
> when asked about the industry's risk appetite

> "The industry would benefit from more collaborative platforms for sharing risk intelligence, counterfeit -drug alerts, cyber-threat information and supply-shortage data across manufacturers, regulators and healthcare systems."
>
> **— Pharmaceuticals respondent,**
> when asked what would most improve resilience



5.3.2.3 The Periodic Risk Table



5.3.3 Mitigation Strategies

5.3.3.1 Prevention (Risk Avoidance and Reduction)

Prevention strategies across the healthcare, pharmaceutical, and technology sectors are focused on reducing exposure to systemic risks through robust system design, disciplined governance, and proactive control frameworks. Given the criticality of operations, sensitivity of data, and intensity of regulatory oversight, prevention centres on securing digital infrastructure, strengthening operational integrity, and reducing dependency risk.

Cybersecurity and data protection form a core pillar of preventive control. Organisations implement layered security architectures that combine strict access management, encryption, and continuous system hardening to minimise exposure to unauthorised access. Approaches such as least-privilege access models and enhanced authentication mechanisms ensure that vulnerabilities are contained at the system level.

Operational risk prevention is equally dependent on disciplined system management. Configuration errors, uncontrolled system changes, and legacy infrastructure represent persistent sources of vulnerability. Structured change management processes, supported by rigorous testing and validation protocols, reduce the likelihood of failures arising from system modifications. At the same time, ongoing modernisation initiatives address technical debt and reduce reliance on outdated systems that are inherently more difficult to secure.

Supply chain vulnerabilities are mitigated through strengthened third-party governance. Vendor assurance frameworks, including security validation, contractual safeguards, and continuous monitoring, reduce exposure to risks arising from external dependencies. Ensuring transparency in software components and enforcing timely updates further limits the introduction of vulnerabilities through supply chains.

Human-related risks are managed through strong governance, role-based access controls, and sustained training programmes. These measures reduce both insider threats and operational errors. Emerging risks from artificial intelligence are addressed through structured model governance, ensuring validation, oversight, and accountability in deployment.

Prevention, in this context, focuses on embedding resilience within systems and processes, reducing the likelihood of disruption before it materialises.

5.3.3.2 Detection (Monitoring and Early Warning Systems)

Detection mechanisms are designed to provide continuous visibility into system behaviour, enabling early identification of vulnerabilities and emerging threats. In sectors where disruption can escalate rapidly, real-time monitoring is a critical capability.

Detection frameworks rely on integrated monitoring systems that consolidate data across infrastructure, applications, and networks. Centralised platforms, supported by specialised operations centres and event management tools, enable organisations to identify anomalies and respond with speed. Indicators such as unauthorised access attempts, system irregularities, and incident detection timelines provide measurable signals of emerging risk.

Beyond technical monitoring, detection extends to operational processes. Metrics related to system changes, deployment failures, and configuration issues offer early insight into process breakdowns, allowing intervention before failures scale.

Behavioural monitoring adds an additional layer of protection by analysing patterns in user activity. Unusual access behaviour, privilege escalation, or deviation from established patterns can signal credential compromise or insider risk, enabling early containment.

Detection is further strengthened through external intelligence, including vulnerability disclosures, threat intelligence feeds, and vendor risk monitoring. These inputs provide a broader understanding of the evolving threat landscape and its potential impact on internal systems.

By compressing the time between risk emergence and organisational awareness, detection capability significantly improves the effectiveness of response actions and reduces the likelihood of large-scale disruption.

5.3.3.3 Response (Incident and Crisis Management)

Response strategies focus on managing disruptions effectively once they occur, with the objective of rapid containment and minimisation of impact. In healthcare, pharma, and technology environments, where disruptions can have immediate operational and societal consequences, response frameworks must be precise, coordinated, and decisive.

Structured incident management protocols define how risks are identified, escalated, and addressed. Clear decision-making hierarchies and predefined responsibilities ensure that response actions are executed without delay or ambiguity.

In cybersecurity incidents, immediate containment actions such as isolating affected systems, restoring data from secure backups, and initiating forensic analysis are critical in limiting spread and damage. Regular testing through simulations and exercises ensures operational readiness in real scenarios.

Business continuity and disaster recovery capabilities underpin response effectiveness. Redundant systems, alternative operating environments, and failover mechanisms allow organisations to maintain critical functions during disruption. These capabilities are particularly important in technology-enabled environments, where downtime can have cascading effects across sectors.

Response frameworks also extend to third-party incidents, requiring rapid assessment of exposure and activation of contingency arrangements. Given the dependency on external ecosystems, such coordination is essential to limiting operational impact.

In regulated environments, response includes compliance with reporting obligations and management of stakeholder communication. Transparent engagement is critical in maintaining trust and mitigating reputational impact.

Response capability is ultimately defined by speed, coordination, and execution discipline, ensuring that disruption is contained before it evolves into wider systemic failure.

5.3.3.4 Resilience (Recovery and Adaptive Capability)

Resilience reflects an organisation's ability not only to recover from disruption but also to adapt and strengthen in response to it. In healthcare, pharma, and technology sectors, resilience is closely tied to infrastructure reliability and the continuity of critical services.

A central element of resilience is the design of systems that can continue operating under failure conditions. Distributed architectures, multi-region deployments, and built-in redundancy ensure that disruptions in one component do not result in total system failure.

Recovery capability is driven by well-tested disaster recovery frameworks, which ensure that systems can be restored within defined parameters. Regular validation of backup mechanisms and restoration processes ensures that recovery actions are reliable and effective when required.

Addressing underlying structural issues is equally important. Technical debt and legacy systems represent persistent sources of fragility, and their gradual modernisation enhances long-term stability and security.

Resilience also depends on continuous learning. Post-incident analysis provides critical insights into root causes and system weaknesses, which are then incorporated into preventive and detection frameworks. This creates a reinforcing feedback loop that strengthens overall system capability.

As emerging technologies such as artificial intelligence become more embedded, resilience must also incorporate governance over these systems, ensuring reliability, transparency, and accountability.

Resilience, therefore, extends beyond recovery to adaptive capability, enabling organisations to respond effectively to evolving and unforeseen risks.

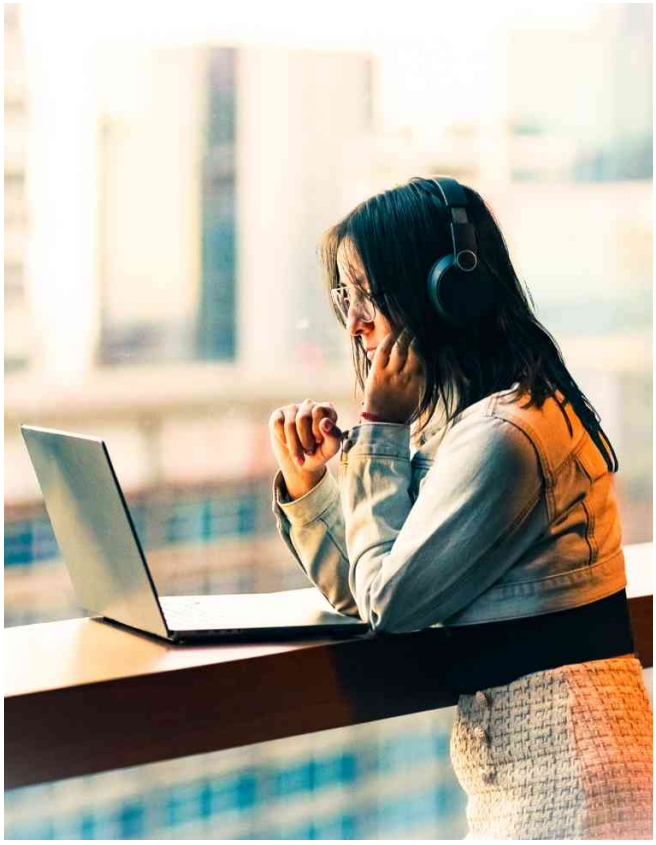
5.3.3.5 KRIs and Governance

Key Risk Indicators and governance frameworks provide the foundation for effective and continuous risk management. KRIs translate complex risk signals into measurable indicators, enabling organisations to monitor exposure and act proactively.

In cybersecurity and technology environments, indicators such as attempted breaches, incident frequency, and response times provide insight into system strength and vulnerability. Operational indicators, including system downtime, failed implementations, and change-related incidents, offer visibility into process stability.

These indicators are embedded within governance structures through centralised dashboards, reporting systems, and defined review processes. Continuous monitoring ensures that critical risks are tracked in real time, while periodic reviews support strategic oversight and alignment.

Governance effectiveness depends on linking monitoring to action. Insights derived from KRIs must inform operational adjustments, investment decisions, and long-term planning. Integration with broader frameworks, including Periodic Risk Tables, enables a dynamic view of evolving risk exposure.



5.4 Hospitality, Tourism, Retail, Media

About the researchers

Dr. Shivdasini S. Amin

Head of the Global Centre for Enterprise Risk Management at Mahindra University

Dr. Shivdasini S. Amin is a distinguished academic leader, Professor, and Master Certified Coach (MCC-ICF), ACTC with over 25 years of experience spanning higher education, leadership development, organisational behaviour, and enterprise risk management. She currently serves as the Head of the Global Centre for Enterprise Risk Management at Mahindra University, where she drives research, industry partnerships, and academic innovation. She is also the head of the department of humanities and social sciences at Mahindra University. She is recognised among the world's most influential coaching leaders, she has coached senior executives, mentored doctoral scholars, and led transformative initiatives across academia and industry. Her work is guided by a deep commitment to developing human potential, fostering institutional excellence, and creating meaningful impact through leadership, learning, and research.

Akshaya Buri

Bachelor of Business Administration (BBA) degree from Mahindra University
IRM level 1 certified professional

Akshaya Buri is a student of Bachelor of Business Administration (BBA) degree from Mahindra University, and is currently affiliated with D.E. Shaw. She is an IRM level 1 certified professional, and her interests include enterprise risk management, business strategy, and industry research. She contributed to the development of risk registers and mitigation frameworks for the Oil & Gas, Hospitality, Tourism, Retail, and Media sectors, with a focus on identifying emerging risks and evaluating their potential impact on the Indian business environment.

5.4.1 Hospitality

5.4.1.1 Overview

The hospitality sector operates at the intersection of discretionary consumption and service experience, making it highly sensitive to demand fluctuations and consumer sentiment. It encompasses hotels, resorts, restaurants, serviced apartments, homestays, convention centres, and related guest experiences, serving both domestic and international travellers. As a significant contributor to the service economy, the sector supports employment generation, tourism development, business travel, foreign exchange earnings, and regional economic growth.

Profitability within the sector is strongly dependent on occupancy levels, pricing strategies, and operational efficiency, while capital intensity and high fixed cost structures—associated with real estate, utilities, staffing, and maintenance—limit financial flexibility. The sector functions within a complex ecosystem shaped by digital platforms, supply chain networks, workforce availability, infrastructure development, and regulatory requirements. Increasing reliance on technology-enabled distribution channels, online booking platforms, customer engagement tools, and data-driven pricing mechanisms has enhanced efficiency and market reach but has also introduced new operational and technological dependencies.

In recent years, the industry has undergone rapid transformation driven by the growth of digital booking platforms, evolving customer expectations, increased demand for personalised and experiential travel, and the expansion of branded hospitality networks into Tier-2 and Tier-3 markets. At the same time, the sector operates in a highly dynamic environment where performance is closely influenced by macroeconomic conditions, travel patterns, consumer confidence, public health developments, and broader infrastructure ecosystems. Recent demand shocks, such as the sharp decline in travel during public health crises, have highlighted the sector's vulnerability to abrupt occupancy collapses.

Unlike many industries, hospitality businesses are inherently experience-centric and heavily reliant on service quality and customer perception. As a result, reputational sensitivity is particularly high, with service disruptions or negative customer experiences having the potential to rapidly affect brand value and demand. Hospitality operates as a demand-amplified system, where small changes in demand conditions can result in disproportionate financial and operational impacts. The sector is also highly sensitive to external shocks, including economic downturns, public health crises, geopolitical events, and climate-related disruptions, which can significantly impact travel flows and occupancy levels.

From a risk perspective, the hospitality sector is characterised by a multidimensional and interconnected risk landscape spanning strategic, financial, operational, technological, informational, reputational, employment, business continuity, legal, environmental, and governance domains. Risks within these categories are often interdependent, where disruptions in one area—such as workforce availability, digital platforms, or supply chains—can quickly cascade into operational challenges, financial stress, and reputational impact.

A defining characteristic of the sector is its high dependence on demand stability combined with limited operational flexibility, making it particularly vulnerable to abrupt changes in external conditions. To effectively manage this complexity, risk assessment frameworks typically evaluate risks based on both likelihood and impact, enabling organisations to prioritise high-severity exposures and strengthen resilience across interconnected risk domains.

> "The risk landscape in the retail industry is expected to become more complex and technology-driven over the next five to ten years."
>
> **— Retail respondent,**
> when asked how the risk landscape will evolve

> "Cybersecurity breaches, customer data privacy failures, product quality or safety issues, unethical business practices, regulatory non-compliance and poor customer service pose the most significant reputational threats."
>
> **— Retail respondent,**
> when asked about the biggest reputational risks

5.4.1.2 Key Risk Themes

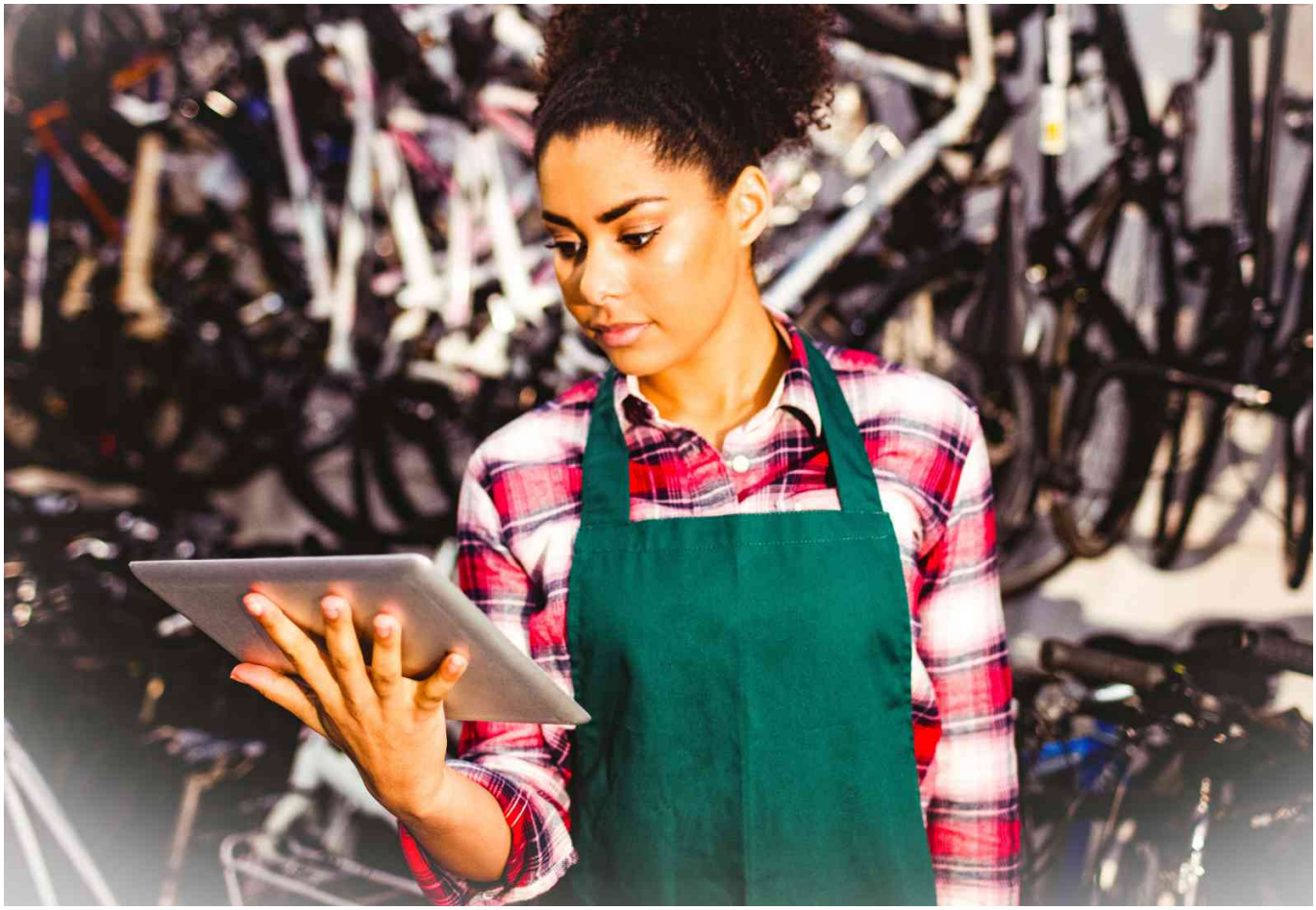
The hospitality risk landscape is shaped by a combination of demand volatility, structural rigidity, and operational exposure, with risks increasingly reflecting the interplay between financial dynamics, workforce capability, technology dependence, and customer perception.

Revenue volatility and demand concentration represent a fundamental risk dimension. The sector remains highly sensitive to fluctuations in travel demand, including seasonal variations, dependence on corporate and MICE (meetings, incentives, conferences, and exhibitions) segments, and broader macro-economic conditions. Short-term disruptions—such as economic downturns or public health events—can have disproportionate impacts on occupancy rates and pricing, thereby affecting profitability. This sensitivity is amplified by the sector's high fixed cost base, creating structural financial fragility where even temporary demand shocks can significantly affect performance. As a result, demand diversification and revenue resilience are critical to sustaining long-term stability.

Platform dependency represents another critical risk, with heavy reliance on online travel agencies (OTAs) and digital booking platforms for customer acquisition. This creates an asymmetric dependency where control over demand visibility increasingly shifts to platform intermediaries, exposing operators to changes in algorithms, commission structures, and visibility rankings that directly influence occupancy levels and pricing power. In an increasingly digital marketplace, this dependence also links closely with reputational dynamics, as platform ratings and reviews influence booking behaviour.

The asset-heavy nature of the sector further contributes to financial rigidity. High levels of capital investment in real estate and infrastructure, combined with ongoing operating costs, constrain the ability to respond flexibly to downturns. Strategic risks related to expansion—such as overinvestment in under performing locations, ineffective revenue management, or declining asset valuations—can have long-term financial implications due to the illiquid nature of hospitality assets.

Operational risks remain significant, particularly in areas such as food safety, service quality, infrastructure reliability, and vendor dependency. Failures in these domains can trigger immediate customer dissatisfaction, regulatory scrutiny, and long-term reputational damage. Risks associated with power outages, water scarcity, supply chain disruptions, and inadequate insurance coverage further highlight the sector's exposure to physical and logistical vulnerabilities. These risks underscore the importance of strong business continuity planning and infrastructure resilience in maintaining uninterrupted service delivery.



Human capital challenges are central to the sector's risk profile. Hospitality remains fundamentally dependent on frontline service delivery, making workforce capability a critical determinant of performance. High attrition, shortages of skilled personnel, wage inflation, and evolving employee expectations can reduce service consistency and operational effectiveness. Workforce instability directly affects customer experience, online reviews, and brand perception, linking human capital risk closely with revenue and competitive positioning.

Reputational risk is a defining feature of the sector, driven by real-time customer feedback and digital amplification. Negative guest experiences, food safety incidents, or service failures can rapidly spread through online reviews and social media, influencing booking decisions and brand perception. In an environment where digital platforms serve as primary discovery channels, even isolated incidents can have prolonged effects on occupancy and revenue recovery. Trust and brand consistency across properties therefore represent critical strategic assets.

Technology-related risks, including cybersecurity threats and system failures, are increasing in importance as operations become more digitised. Hospitality organisations manage significant volumes of customer data through booking systems, payment platforms, and loyalty programmes, making them vulnerable to breaches, fraud, and regulatory non-compliance. Technology failures can disrupt operations while simultaneously affecting customer trust and financial performance, highlighting the convergence of digital and operational risk.

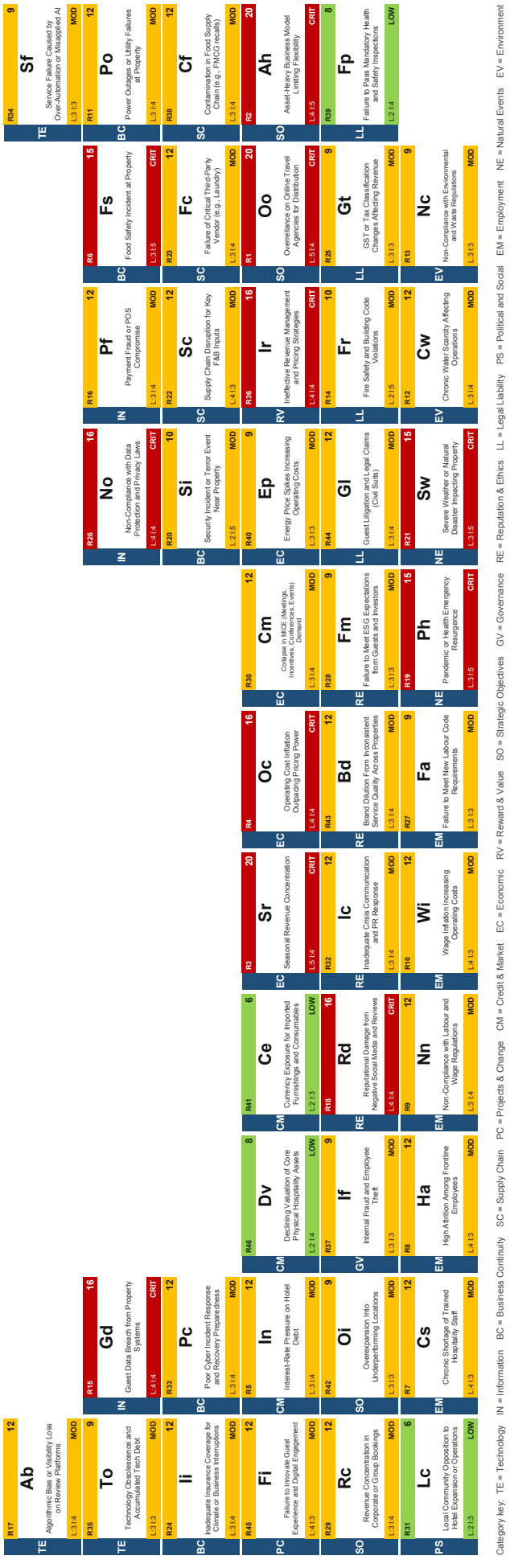
Regulatory and compliance risks are also expanding in scope. Requirements related to labour laws, health and safety standards, data protection, taxation, and environmental regulations impose increasing obligations on operators. In addition, evolving expectations around environmental, social, and governance (ESG) performance are influencing investor sentiment, financing conditions, and customer preferences, elevating compliance from a legal requirement to a strategic consideration.

External risks, including **climate variability, water scarcity, natural disasters, and public health events,** directly affect both demand and operational continuity. The increasing frequency and severity of climate-related disruptions are transforming previously episodic risks into structural challenges, requiring investment in resilient infrastructure, resource management, and adaptive operational strategies.

Overall, the hospitality sector reflects a highly interconnected, demand-sensitive system where financial performance, service quality, workforce capability, technology resilience, and reputational strength are tightly coupled. Demand shocks can affect occupancy and revenue; workforce challenges can degrade service standards and brand perception; digital disruptions can impact both operations and trust; and external events can influence both demand patterns and infrastructure reliability.

Hospitality organisations must therefore adopt an integrated risk management approach that combines demand diversification, workforce resilience, digital security, infrastructure preparedness, regulatory compliance, and disciplined strategic planning. Such an approach is essential to managing volatility and sustaining competitiveness in an increasingly dynamic and experience-driven operating environment.

5.4.1.3 The Periodic Risk Table



5.4.2 Tourism

5.4.2.1 Overview

The tourism sector operates as a demand-generating ecosystem driven by mobility, perception, and destination competitiveness, making it inherently sensitive to shifts in demand conditions and narrative dynamics. It plays a critical role in economic development, employment generation, foreign exchange earnings, regional growth, and cultural preservation. The sector spans multiple segments, including leisure tourism, pilgrimage tourism, business travel, medical tourism, eco-tourism, and emerging experiential travel formats, reflecting a highly diversified yet interdependent system of economic activity.

The sector is inherently dependent on mobility, connectivity, and perception, making it highly sensitive to geopolitical developments, environmental conditions, economic trends, public health events, and shifts in traveller sentiment. Tourism performance is not driven solely by market demand but also by a complex interplay of factors such as infrastructure quality, safety standards, environmental sustainability, and policy frameworks. Its fragmented governance structure, involving multiple stakeholders—including government agencies, local communities, transport providers, hospitality operators, and destination management bodies—adds further complexity to planning, coordination, and execution.

This high degree of stakeholder interdependence distinguishes tourism from more vertically integrated industries. Risks are rarely confined to a single segment and often emerge from across the value chain, making the sector particularly vulnerable to both internal inefficiencies and external disruptions. Coordination gaps, inconsistent policies, and variability in service standards can directly affect destination competitiveness and visitor experience.

Digital platforms have significantly improved accessibility, visibility, and market reach, enabling destinations to connect with global audiences more efficiently. However, this transformation has also introduced new dependencies and risks related to cybersecurity, misinformation, digital concentration, and platform-driven visibility. As digital channels increasingly shape traveller decision-making, online narratives, reviews, and information flows play a central role in influencing demand patterns.

Tourism operates as a perception-driven industry, where both real and perceived risks can significantly influence travel behaviour. Traveller confidence is shaped not only by objective conditions but also by reputation, safety perceptions, and broader narratives. Consequently, risks related to reputation, destination image, and public communication have a disproportionate impact on demand outcomes.

From a risk perspective, the tourism sector is characterised by a multidimensional landscape spanning strategic, operational, financial, environmental, social, technological, regulatory, business continuity, and governance domains. Increasingly, factors such as climate resilience, sustainability of destinations, quality of infrastructure, stakeholder coordination, and community acceptance are emerging as critical determinants of long-term sector viability.

A defining characteristic of tourism risk is its external orientation and interconnected nature. Sector performance is shaped as much by global and national developments as by local operational conditions. To effectively manage this complexity, risk assessment approaches typically evaluate both likelihood and impact, enabling prioritisation of the most significant risks affecting tourism growth, destination competitiveness, and overall visitor experience.

> "There is a higher willingness to take strategic and technology-related risks to support digital transformation and market expansion."
>
> **— Retail respondent,**
> when asked about the industry's risk appetite

5.4.2.2 Key Risk Themes

The tourism risk landscape is primarily shaped by external factors, reflecting the sector's dependence on broader economic, environmental, social, and infrastructural conditions. These risks are interconnected and often amplified through perception, making tourism particularly sensitive to both real and perceived disruptions.

Demand volatility and concentration represent a key risk dimension. Dependence on specific source markets, seasonal travel patterns, and discretionary consumer spending creates exposure to sudden demand shocks arising from macroeconomic

shifts, travel restrictions, geopolitical developments, or changes in investor and traveller confidence. Because tourism demand is highly elastic, even short-term disruptions can lead to significant declines in visitor arrivals and revenue, particularly in destinations with limited diversification across markets or product segments.

Destination accessibility and infrastructure constraints further shape risk exposure. Inadequate transport capacity, aviation disruptions, limited last-mile connectivity, insufficient cruise and support infrastructure, and weak destination monitoring systems can reduce accessibility and adversely affect visitor experience. Infrastructure risk often arises not from isolated capacity constraints but from a lack of synchronisation across transport, accommodation, and destination services, directly impacting destination competitiveness and visitor flows. Effective coordination across these components is therefore critical to maintaining sector performance.

Environmental risks are increasingly material, particularly in the context of climate change and sustainability. Factors such as climate variability, coastal erosion, biodiversity loss, pollution, flooding, and extreme weather events affect both the physical viability and attractiveness of destinations. In environmentally sensitive areas, risks related to carrying-capacity exceedance and ecological degradation can further reduce long-term sustainability. Importantly, environmental risks also influence perception, where media coverage or public narratives around environmental decline can affect demand independently of actual conditions.

Governance complexity introduces significant regulatory and execution risk. Fragmented decision-making across multiple administrative levels, coupled with policy uncertainty, permitting delays, inconsistent enforcement, and funding constraints, can hinder investment and infrastructure development. Tourism outcomes depend on coordinated performance across domains such as transportation, sanitation, conservation, and promotion, making governance effectiveness a critical determinant of sector resilience and growth.

Health and safety risks remain a central concern, particularly in the context of pandemics, public health emergencies, and limited emergency response capacity. Risks related to crowd management failures, unlicensed operators, visitor security, and inadequate medical infrastructure can result in immediate and severe demand disruption. High-visibility safety incidents can have spillover effects across regions and markets due to global information flows, especially when amplified through travel advisories and international perception channels.

Reputational risk is significantly amplified through digital and social media ecosystems. Misinformation, negative publicity, and viral narratives can rapidly influence traveller behaviour, reshape destination image, and alter demand patterns. In a highly connected environment, even isolated incidents can escalate into broader perception risks, making proactive communication and reputation management critical components of tourism risk mitigation.

Community acceptance and social licence to operate are emerging as important risk dimensions. Issues such as land-use conflicts, commercialisation of cultural assets, housing pressures from tourism activity, and perceived inequitable distribution of economic benefits can lead to local resistance. Community resistance can act as a structural constraint on growth, influencing both policy direction and investor confidence, particularly where tourism is perceived as disruptive or exclusionary.

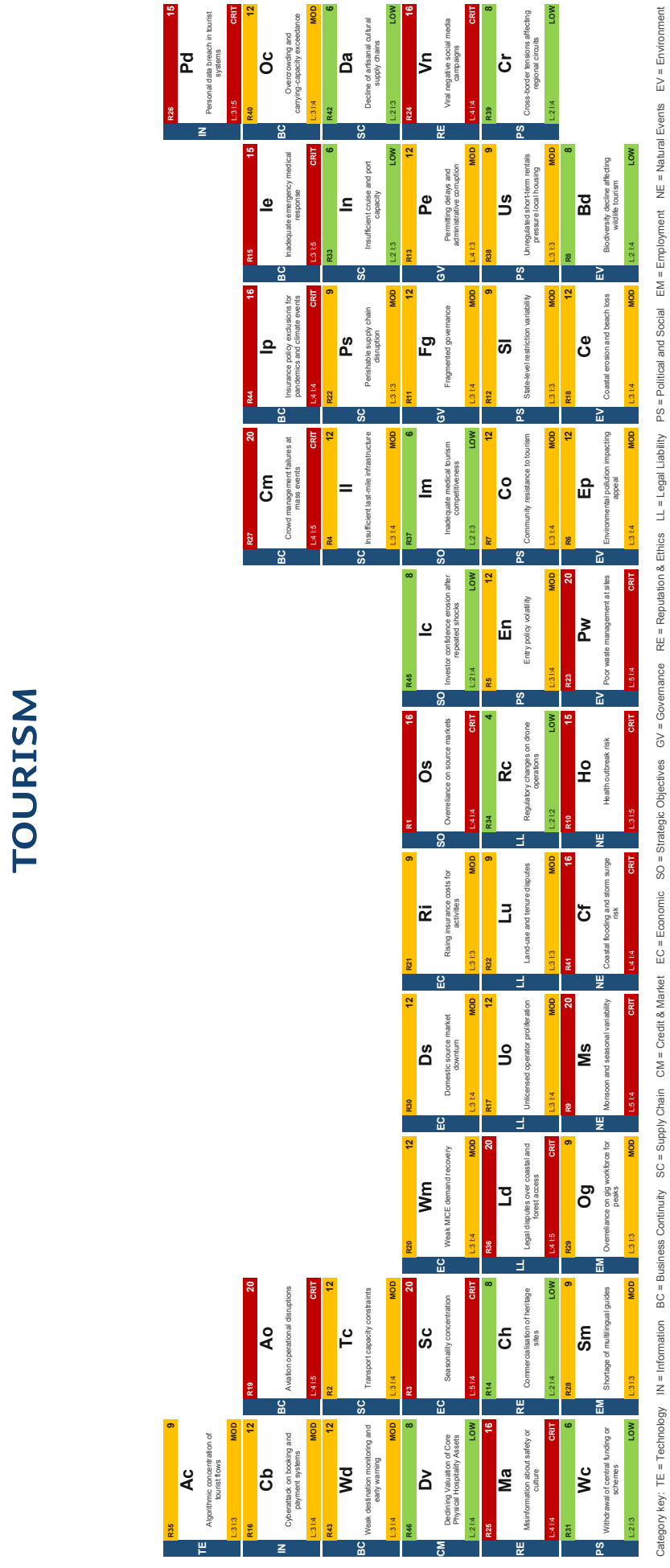
Technology-related risks, including cybersecurity threats, data breaches, and reliance on digital platforms, are also increasing in importance. While digital platforms improve visibility and accessibility, they introduce dependencies related to platform concentration, algorithm-driven demand flows, and data governance. Additionally, misinformation campaigns and digital manipulation can distort traveller perceptions, further reinforcing the sector's vulnerability to perception-driven risks.

Operational risks, including crowd management failures, over-capacity, and unregulated tourism activities, place additional strain on infrastructure and environmental systems, particularly in high-density or ecologically sensitive destinations. These risks can degrade visitor experience, accelerate environmental damage, and undermine long-term sustainability if not effectively managed.

Overall, the tourism sector reflects a highly interconnected and perception-driven system, where infrastructure quality, environmental sustainability, governance effectiveness, community acceptance, and economic conditions collectively shape performance. Risks do not operate in isolation; environmental degradation can affect reputation, governance failures can delay infrastructure, safety incidents can reduce demand, and community opposition can restrict growth.

Tourism resilience therefore requires a holistic approach that integrates demand diversification, infrastructure development, climate adaptation, stakeholder coordination, safety management, digital resilience, and community engagement. Destinations that effectively manage these interconnected risks will be better positioned to sustain growth, preserve cultural and environmental assets, and maintain long-term competitiveness in an increasingly dynamic global tourism landscape.

5.4.2.3 The Periodic Risk Table



5.4.3 Retail

5.4.3.1 Overview

The retail sector occupies a central position within the economy, functioning as the primary interface between producers and consumers across a wide range of product categories, including food and grocery, apparel, electronics, and lifestyle goods. It encompasses traditional retail formats such as kirana stores along side organised retail chains, e-commerce platforms, quick -commerce operators, marketplaces, and increasingly integrated omnichannel models. Beyond its role in consumption, the sector contributes significantly to employment generation, supply chain development, and urban economic activity.

The sector is undergoing a period of structural transformation driven by rapid digitalisation, evolving consumer preferences, and the expansion of technology-enabled retail models. Increasing smartphone penetration, the rise of e-commerce and quick-commerce platforms, and the adoption of data analytics have reshaped how consumers discover, evaluate, and purchase products. Recent rapid growth in quick-commerce and intense price competition across e-commerce platforms illustrates how quickly demand patterns and competitive dynamics can reshape retail performance, while expectations around convenience, delivery speed, personalisation, and pricing transparency continue to intensify, requiring retailers to continuously adapt their operating models.

Retail operates within a highly competitive and dynamic environment characterised by thin margins, rising operating costs, and complex supply chain dependencies. The sector must balance physical and digital channels while responding to frequent shifts in consumer behaviour, which can be influenced by digital platforms, social media trends, and technological adoption. This responsiveness makes retail particularly sensitive to rapid changes in demand patterns and competitive positioning.

From a risk perspective, the retail sector extends beyond traditional concerns related to inventory management and sales performance. Increasingly, risks arise across a broad spectrum of domains, including strategic positioning, financial sustainability, operational efficiency, technology reliability, data management, workforce capability, supply chain resilience, regulatory compliance, and reputation. The sector's performance is closely linked to its ability to integrate digital capabilities, maintain customer trust, and ensure continuity across complex and often fragmented supply networks.

A defining characteristic of retail risk is the speed at which external and internal factors can interact to reshape outcomes. Changes in consumer behaviour, platform dynamics, competitive intensity, and regulatory expectations can occur rapidly, requiring organisations to adopt flexible, data-driven, and adaptive strategies. As a result, effective risk management in retail increasingly requires a holistic approach that integrates operational agility, technological capability, supply chain coordination, and customer-centric decision-making to sustain long-term competitiveness.

5.4.3.2 Key Risk Themes

The retail risk landscape is shaped by a combination of financial pressures, operational complexity, digital transformation, and evolving consumer behaviour. These risks are highly interconnected, with changes in one domain often rapidly affecting performance across the entire value chain.

Margin pressure and profitability represent a central risk dimension. The sector operates within highly competitive and price-sensitive markets, where sustained discounting, rising operating costs, and macroeconomic fluctuations constrain pricing power. Factors such as inflation, currency volatility affecting imports, increasing compliance costs, and shifting interest rate environments further compress margins. Retailers often face limited ability to pass on cost increases without impacting demand, making profitability highly sensitive to cost control, operational efficiency, and pricing discipline.

Digital transformation and omnichannel execution introduce another layer of complexity. As retail increasingly shifts toward integrated multi-channel models, organisations must align physical stores, e-commerce platforms, mobile applications, and delivery systems into a seamless customer experience. Omni-channel execution risk often arises from fragmentation between legacy systems and new digital platforms, leading to operational inefficiencies, increased costs, and declining customer engagement when integration is not effectively managed. Given the pace of competition from digital-native players, delays or missteps in transformation can significantly weaken market positioning.

Supply chain and inventory management risks remain critical to operational performance. Retail success depends on maintaining product availability while controlling inventory levels across geographically dispersed networks. Retail supply chains are increasingly exposed to demand volatility, where forecasting errors can quickly translate into stock imbalances and fulfilment inefficiencies. Disruptions arising from supplier concentration, logistics bottlenecks, import dependencies, and last-mile delivery failures can further exacerbate these imbalances, leading to stockouts, excess inventory, or delayed fulfilment. The rise of quick-commerce models has further increased expectations around speed and availability, reducing tolerance for supply chain variability and raising the operational stakes.

Customer trust, brand reputation, and consumer protection form a central and cross-cutting risk theme. In a digitally connected environment, negative customer experiences, product quality issues, pricing disputes, or unethical practices can rapidly escalate through social media and influence purchasing decisions at scale. Reputation directly affects customer acquisition, retention, and lifetime value, while increasing regulatory scrutiny around consumer protection, data usage, and pricing transparency further heightens exposure. As a result, reputational risk and regulatory risk are closely intertwined.

Technology, cybersecurity, and data protection risks are becoming increasingly significant as retail operations digitise. Retailers manage large volumes of customer data through transactions, loyalty programmes, and online platforms, creating exposure to data breaches, fraud, and misuse of information. System outages or cyber incidents can disrupt sales channels while simultaneously undermining customer trust and triggering regulatory consequences. Dependence on third-party technology providers and platform intermediaries further amplifies systemic vulnerabilities.

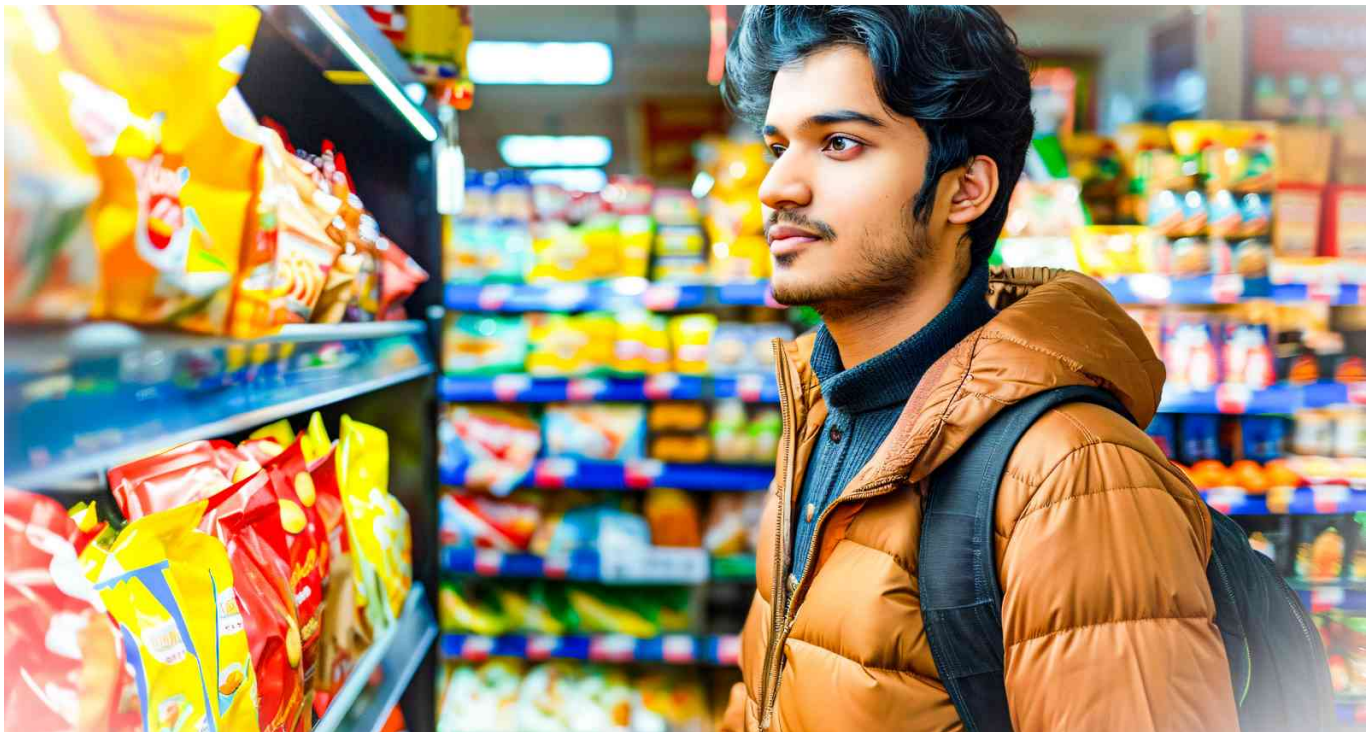
Workforce capability remains an important driver of risk, particularly in balancing frontline service delivery with the need for advanced digital and analytical skills. High attrition, workforce shortages during peak demand periods, and skill gaps in technology-driven roles can weaken both operational execution and customer experience. As retail operations become more technology-intensive, continuous reskilling and effective workforce management are essential to maintaining performance and adaptability.

Regulatory, compliance, and ESG-related risks are expanding in scope and importance. Increasing requirements related to data protection, environmental standards, consumer rights, and ethical sourcing create a more complex regulatory environment. Regulatory compliance increasingly intersects with brand positioning and investor perception, as growing expectations around sustainability, governance, and responsible business conduct mean that compliance is no longer limited to legal obligations but has become a strategic consideration affecting reputation and access to capital.

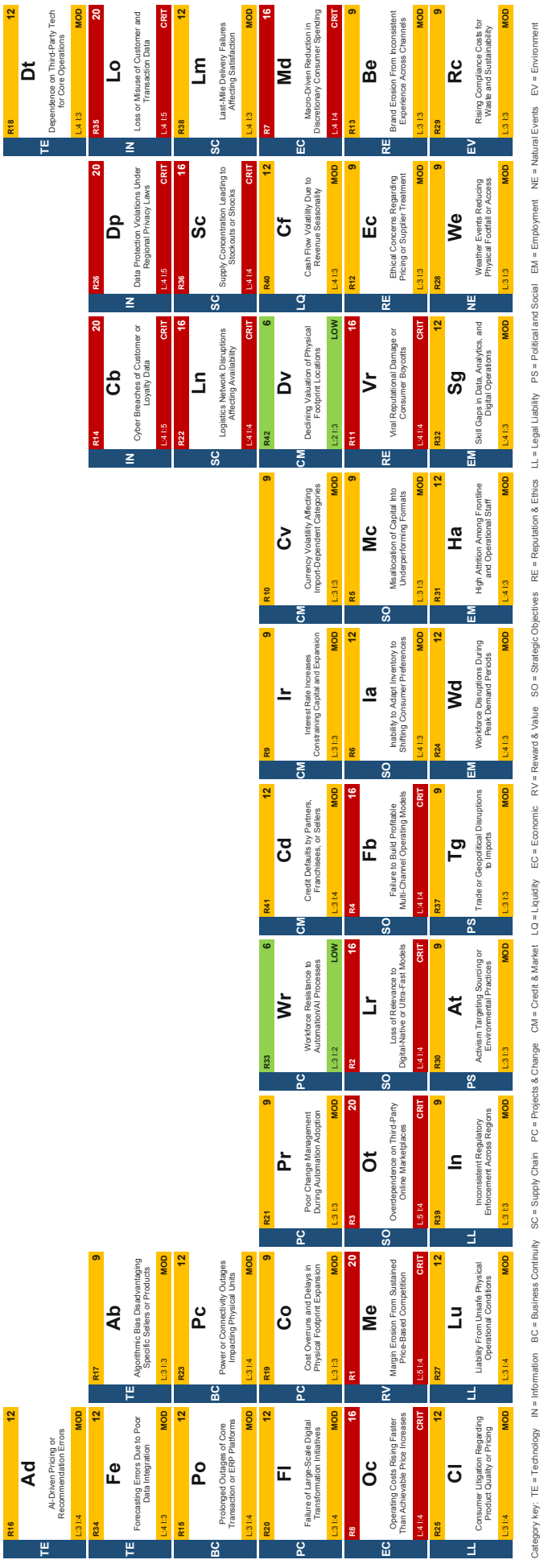
The retail sector's risk profile is defined by the interaction of consumer behaviour, digital ecosystems, supply chain networks, and financial performance, where disruptions in any one area can cascade across operations, customer experience, and brand outcomes.

Competitive advantage increasingly depends on the ability to coordinate these dimensions effectively while adapting to rapidly evolving market conditions.

> "Greater investment in technology and data analytics, stronger cyber security frameworks, improved supply-chain visibility and more effective business-continuity planning would significantly improve resilience."
>
> **— Retail respondent,**
> when asked what would most improve industry resilience



5.4.3.3 The Periodic Risk Table



5.4.4 Media

5.4.4.1 Overview

The media sector encompasses traditional platforms such as print and television, as well as digital platforms, streaming services, and content creators. The media sector operates as a critical component of the information ecosystem, shaping public discourse, influencing perception, and serving as a primary interface between information producers, platforms, and audiences, while also serving as a key channel for advertising and communication.

The sector is undergoing significant transformation due to digital disruption, changing consumer behaviour, and the rise of platform-based distribution models. As audiences increasingly shift toward digital and on-demand content, traditional business models are being challenged, creating both opportunities and risks.

Media organisations operate within a complex environment shaped by regulatory oversight, political dynamics, and technological change. Media increasingly functions as a platform-mediated ecosystem, where content creation, distribution, monetisation, and audience engagement are tightly interlinked across digital networks, amplifying the sector's reliance on audience trust and credibility and increasing exposure to reputational and ethical risks.

5.4.4.2 Key Risk Themes

The media sector faces a distinct set of risks driven by structural transformation, technological disruption, and heightened external scrutiny. These risks are increasingly interconnected, reflecting the convergence of content creation, technology platforms, regulatory oversight, and audience behaviour.

Platform dependency represents a primary strategic vulnerability. Media organisations increasingly rely on third-party digital platforms for content distribution, audience discovery, and monetisation. Changes in platform algorithms, recommendation systems, content moderation policies, or revenue-sharing models can significantly impact visibility, audience engagement, and advertising income. This creates an asymmetric dynamic, where control over distribution and monetisation is concentrated in a small number of platform intermediaries, reducing the autonomy of media organisations over their own reach and revenue streams.

Audience trust, reputation, and information integrity form a central and cross-cutting risk dimension. The sector's sustainability is closely tied to credibility, as risks such as misinformation, perceived editorial bias, inaccurate reporting, and privacy violations can rapidly erode public confidence. In a highly competitive and fragmented information environment, trust functions as a core business asset influencing audience retention, advertiser confidence, and regulatory relationships. The speed of information dissemination through digital channels further amplifies these risks, allowing reputational damage to propagate quickly across platforms and stakeholders.

Technological risks are becoming increasingly structural, particularly with the integration of artificial intelligence and data-driven content systems. AI introduces a shift from content scarcity to content overabundance, complicating verification and quality control, as the emergence of synthetic media, deepfakes, AI-generated content, and algorithmic bias creates complex challenges related to authenticity, accountability, and editorial oversight. While AI enhances efficiency in content production and distribution, it also increases exposure to misinformation, intellectual property concerns, and declining human control over content quality. These developments require media organisations to balance technological adoption with robust governance frameworks to preserve integrity and trust.

Revenue model disruption and financial sustainability remain critical concerns. Traditional reliance on advertising revenue is increasingly challenged by digital consumption patterns, audience fragmentation, and competition from global platform operators. A structural imbalance has emerged where platforms capture a disproportionate share of digital advertising revenue, contributing to volatility in advertising markets, rising content production costs, and slower growth in subscription revenues. As a result, organisations face pressure to diversify revenue streams and develop more resilient business models that are less dependent on cyclical advertising and platform-driven monetisation.

Regulatory, legal, and political risks are particularly significant given the sector's role in shaping public discourse. Media organisations operate within a sensitive environment where content is subject to regulatory scrutiny, legal liability, and potential political intervention. Changes in content regulations, data protection requirements, intermediary liability frameworks, and election-related restrictions can directly affect editorial decisions, distribution models, and operational flexibility. These risks are often interconnected with reputational and technological factors, where a single incident can trigger regulatory action and public backlash simultaneously.

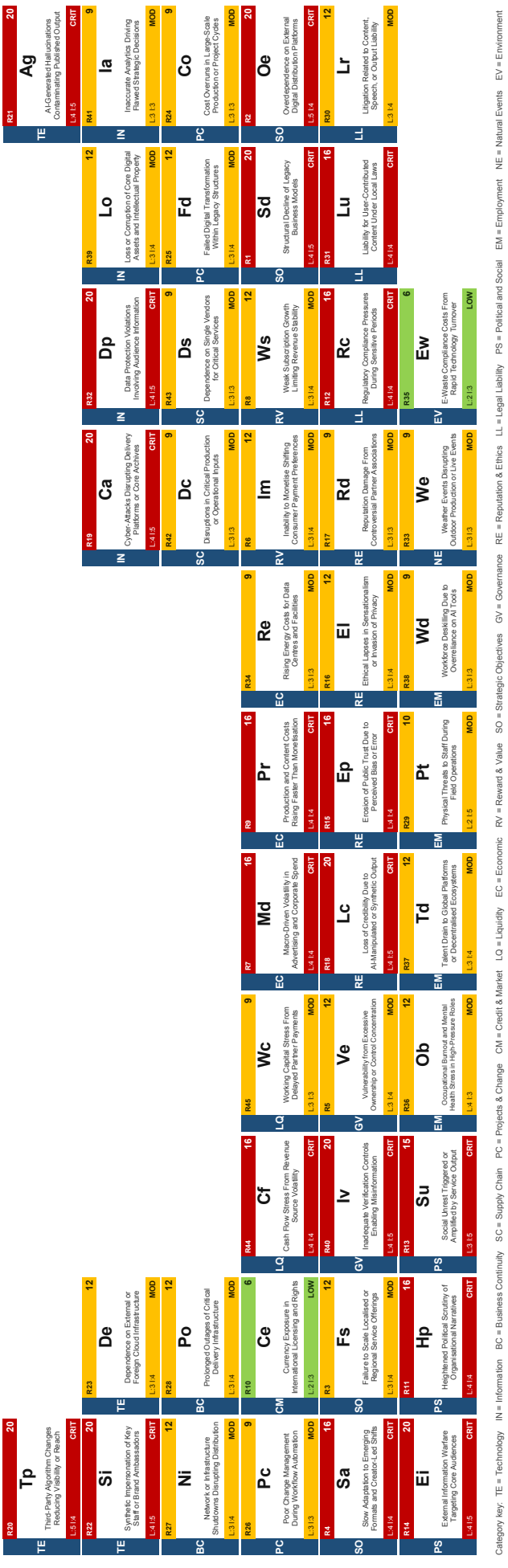
Cybersecurity, data protection, and digital infrastructure risks are also expanding in importance. Media organisations manage large volumes of subscriber data, proprietary content, and digital assets, making them targets for cyberattacks, data breaches, and intellectual property theft. Dependence on cloud infrastructure, content delivery networks, and third-party technology providers introduces additional vulnerabilities. Disruptions affecting these systems can impact operations, compromise sensitive information, and damage audience trust.

Human capital risks further influence sector performance, particularly in the context of rapid technological change and evolving content ecosystems. Media organisations face challenges related to talent retention, workforce burnout, skill gaps in digital and analytical capabilities, and competition from global platforms and creator -driven models. At the same time, increasing reliance on automation and AI tools can lead to deskilling and reduced editorial oversight, creating additional governance challenges.

The media sector's risk profile is defined by the interaction of platform ecosystems, technological disruption, regulatory oversight, financial pressures, and audience trust, where shocks in one area can cascade across visibility, revenues, and credibility.

Competitive advantage increasingly depends on the ability to adapt across editorial, technological, and commercial dimensions while maintaining integrity and resilience in a rapidly evolving information environment.

5.4.4.3 The Periodic Risk Table



5.4.5 Mitigation Strategies

5.4.5.1 Prevention (Risk Avoidance and Reduction)

Prevention across the hospitality, tourism, retail, and media sectors is focused on reducing exposure to structurally recurring risks through stronger system design, diversified dependencies, and embedded governance. Given the high reliance on digital platforms, supply chains, and customer-facing operations, preventive strategies must simultaneously address operational continuity and reputational protection.

A central priority is the mitigation of dependency risk, particularly on external platforms and third-party ecosystems. Organisations increasingly diversify distribution channels, strengthen direct customer engagement through owned platforms and loyalty programmes, and reduce revenue concentration from intermediaries. Vendor-related risks are similarly managed through exposure limits, vendor due diligence, and the development of alternative sourcing arrangements, ensuring continuity in the event of disruption.

Technology and data protection form another critical layer of prevention. As these sectors rely heavily on digital infrastructure for transactions, engagement, and content delivery, organisations implement robust security architectures combining access controls, encryption, and system hardening. Data governance frameworks, including controlled access, regular backup, and recovery protocols, ensure both protection and resilience of critical information.

Operational resilience is reinforced through investments in infrastructure reliability and supply chain stability. Contingency logistics, backup utilities, and inventory buffers reduce exposure to disruptions in supply and infrastructure. Preventive controls in quality and safety, particularly in customer-facing environments, ensure compliance and reduce the likelihood of service failures.

Reputational risk prevention is embedded at the source through strong supplier governance, ESG alignment, and internal quality assurance. As public scrutiny and digital amplification increase, organisations prioritise consistency, transparency, and proactive risk management in customer interactions and product delivery.

Overall, prevention focuses on building structural resilience, addressing vulnerabilities early, and reducing the probability of disruption across interconnected systems.

5.4.5.2 Detection (Monitoring and Early Warning Systems)

Detection mechanisms are designed to provide continuous visibility into operations, customer sentiment, and system performance, enabling early identification of emerging risks. In sectors characterised by high customer interaction and rapid information flow, the ability to detect anomalies early is critical.

Organisations rely on integrated monitoring systems that bring together operational, technological, and external data. Key Risk Indicators play a central role, offering measurable signals of potential disruptions through metrics such as service delays, system alerts, supply chain variability, and customer complaint trends.

Digital monitoring tools enhance detection capabilities by capturing both internal performance and external perception. Social listening platforms provide real-time insight into customer sentiment, allowing organisations to identify reputational risks before escalation. At the same time, analytics platforms monitor booking trends, traffic patterns, and conversion metrics, helping detect shifts in demand or platform visibility.

Operational detection focuses on supplier performance, logistics timelines, and infrastructure reliability. Deviations in service levels, delivery timelines, or inventory patterns provide early indicators of stress within the system.

In parallel, cybersecurity monitoring systems track anomalies within digital environments, identifying potential breaches, system irregularities, and configuration errors. Integration of external intelligence, including vendor signals and threat updates, further strengthens detection capability.

The core objective of detection is to shorten the time between risk emergence and awareness, enabling timely intervention before disruption escalates.

5.4.5.3 Response (Incident and Crisis Management)

Response strategies focus on managing disruptions swiftly while minimising operational impact and protecting brand reputation. In these sectors, where customer experience and public perception are directly affected, response capability must be rapid, coordinated, and clearly defined.

Structured crisis management frameworks establish escalation protocols, decision-making authority, and communication pathways. In reputational scenarios, rapid-response communication systems enable organisations to address issues proactively through coordinated messaging and customer engagement.

Operational response mechanisms prioritise continuity by activating contingency arrangements, including alternative suppliers, rerouted logistics, and backup facilities. Maintaining service delivery during disruption is critical to preventing revenue loss and customer dissatisfaction.

Technology-related incidents are managed through defined response plans involving system isolation, data restoration, and investigation processes. Regular testing through simulations ensures readiness to handle high-impact scenarios effectively.

Response also extends to managing third-party disruptions, requiring rapid assessment of exposure and activation of contingency arrangements. This is particularly critical in environments with high reliance on external platforms and vendors.

Financial safeguards, including insurance and contingency funding, support response efforts by limiting economic impact, particularly in cases of large-scale disruptions.

Effective response is ultimately defined by speed, coordination, and clarity of execution, ensuring that incidents are contained before they affect broader operations or stakeholder trust.

5.4.5.4 Resilience (Recovery and Adaptive Capability)

Resilience reflects the organisation's capacity to recover from disruptions while adapting to evolving risk conditions. In hospitality, tourism, retail, and media sectors, resilience is closely linked to sustaining customer trust while maintaining continuity of operations.

A key element of resilience lies in diversification and redundancy. Multiple distribution channels, backup infrastructure, and alternative supply arrangements ensure that disruptions in one part of the system do not lead to complete operational failure.

Recovery capability is supported by structured processes for restoring operations, including data recovery, infrastructure repair, and service reactivation. Regular validation of these processes ensures that recovery timelines remain realistic and effective.

Financial and operational flexibility are equally critical, particularly in sectors with demand volatility and seasonal dependencies. Liquidity buffers, flexible cost structures, and adaptive pricing strategies enable organisations to absorb shocks and stabilise performance.

Resilience also depends on continuous learning. Post-incident reviews identify underlying weaknesses and inform improvements in preventive and detection mechanisms, strengthening overall system capability.

In addition, long-term resilience requires adaptability to evolving consumer behaviour, technological change, and market expectations. Organisations that continuously innovate and adjust engagement strategies are better positioned to sustain relevance in dynamic environments.

Resilience therefore extends beyond recovery, enabling organisations to adapt to changing conditions while maintaining competitive advantage.

5.4.5.5 KRIs and Governance

The effectiveness of mitigation strategies depends on the integration of monitoring systems with governance frameworks. Key Risk Indicators translate operational and strategic risks into measurable signals, enabling organisations to maintain continuous visibility over evolving exposures.

KRIs are embedded within dashboards and reporting systems, covering areas such as service performance, supply chain reliability, cybersecurity alerts, and customer sentiment. These indicators draw on multiple data sources, including operational systems, analytics platforms, and external monitoring tools.

Structured review processes ensure consistent monitoring. Critical indicators are tracked in real time, while broader strategic metrics are assessed periodically, supporting both operational responsiveness and long-term oversight.

Governance frameworks ensure that monitoring translates into action. Defined escalation protocols, cross-functional coordination, and leadership oversight enable timely decision-making and alignment across the organisation. Integration with regulatory compliance systems further ensures alignment with external requirements.

Strong governance enables a dynamic and continuously updated view of risk, linking monitoring, decision-making, and adaptation. When effectively implemented, it ensures that risk management remains aligned with organisational strategy and supports sustained resilience in a rapidly evolving environment.

5.5 Education

About the researchers

Dr. Binay Kumar Pathak

Assistant Professor
Indira Mahindra School of Education,
Mahindra University.

Dr. Binay Kumar Pathak is an Assistant Professor and PhD Programme Coordinator at Indira Mahindra School of Education, Mahindra University. His research interests revolve around issues of development, economics of Information, education policy, economics of knowledge, and research ecosystems. He has authored working papers on Agriculture, Food Security, Water Security, and Demographics for a strategic trends project. He is an IRM Level 1 certified professional.

Chennamenani Parikshit Rao

final-year BBA (Computational Business Analytics) Student at Mahindra University
IRM Level 1 certified professional

Chennamenani Parikshit Rao is a final-year BBA (Computational Business Analytics) Student at Mahindra University and is an IRM Level 1 certified professional. He contributed to the sectors of Agriculture, Food, FMCG, and Education.

5.5.1 Education

5.5.1.1 Overview

The education sector represents a critical pillar of socio-economic development, responsible for building human capital, enabling innovation, and supporting long-term economic growth. It encompasses a wide spectrum of institutions and delivery models, including schools, higher education institutions, coaching centres, and an expanding ecosystem of edtech platforms and hybrid learning models.

The sector operates across multiple stages of learning, from foundational education to professional upskilling, serving a diverse and large population base with varying socio-economic, geographic, and developmental needs. This diversity introduces inherent complexity, as educational systems must address issues of accessibility and quality simultaneously.

In recent years, the sector has undergone significant transformation driven by digitisation, globalisation, and evolving labour market expectations. The integration of information and communication technologies has reshaped instructional delivery, assessment mechanisms, and content creation, enabling scalable and flexible learning models. At the same time, these developments have introduced new challenges related to technological dependence, content differentiation, and maintaining quality across both traditional and digital formats.

The sector is increasingly shaped by an interconnected ecosystem involving educators, institutions, students, regulators, investors, and digital platforms. As educational products extend beyond institutional boundaries into platform-based and hybrid delivery modes, risk exposure has shifted from institution-level issues to system-wide challenges involving market alignment, operational sustainability, regulatory compliance, and stakeholder trust.

5.5.1.2 Key Risk Themes

The education sector is characterised by a multidimensional and interdependent risk landscape shaped by market dynamics, operational constraints, technological transformation, and regulatory complexity.

Demand-side uncertainty represents a primary risk driver. Changes in demographic profiles, socio-economic conditions, and labour market demands directly influence enrolment patterns and consumer preferences. Misalignment between educational offerings and market expectations can reduce demand viability and affect long-term sustainability. In addition, dependence on multiple stakeholders, including institutions, investors, and employers, complicates coordination and market positioning.

Operational and management risks are also significant. Inefficiencies in resource allocation, financial management, and internal processes can limit innovation capacity, constrain expansion, and affect service delivery. The interdependence between financial resources, human capital, and technological investment further amplifies these risks, as weaknesses in one area can affect overall organisational performance.

Quality and relevance risks remain central to sector performance. Gaps in curriculum design, instructional effectiveness, and alignment with industry requirements can directly affect employability outcomes, institutional credibility, and market competitiveness. As learning outcomes become increasingly linked to employment value, maintaining relevance becomes a critical determinant of sustainability.

Human capital risk plays a key role due to dependence on skilled educators, trainers, and content developers. Skill gaps, workforce attrition, and inadequate training can reduce instructional quality and innovation capacity. At the same time, resistance to technological change or insufficient capability development can slow digital transformation efforts.

Technology-related risks are increasingly prominent. Growing reliance on digital platforms introduces exposure to cybersecurity threats, data breaches, system failures, and data privacy concerns. The collection and use of large datasets for personalised learning and analytics further expand vulnerability to cyber incidents. In addition, intellectual property risks related to content creation and distribution—such as infringement and misuse—create legal and reputational exposure.

Emerging risks associated with AI introduce additional complexity. Issues such as algorithmic bias, lack of transparency, and governance challenges can affect learning outcomes, assessment fairness, and decision-making processes, particularly in automated or data-driven systems.

Regulatory and compliance risks are amplified by the sector's multi-layered governance structure. Institutions must comply with diverse regulatory frameworks across education, technology, and intellectual property domains. Frequent policy changes, accreditation requirements, and jurisdictional differences can increase compliance costs and operational uncertainty, particularly in collaborative or cross-border models.

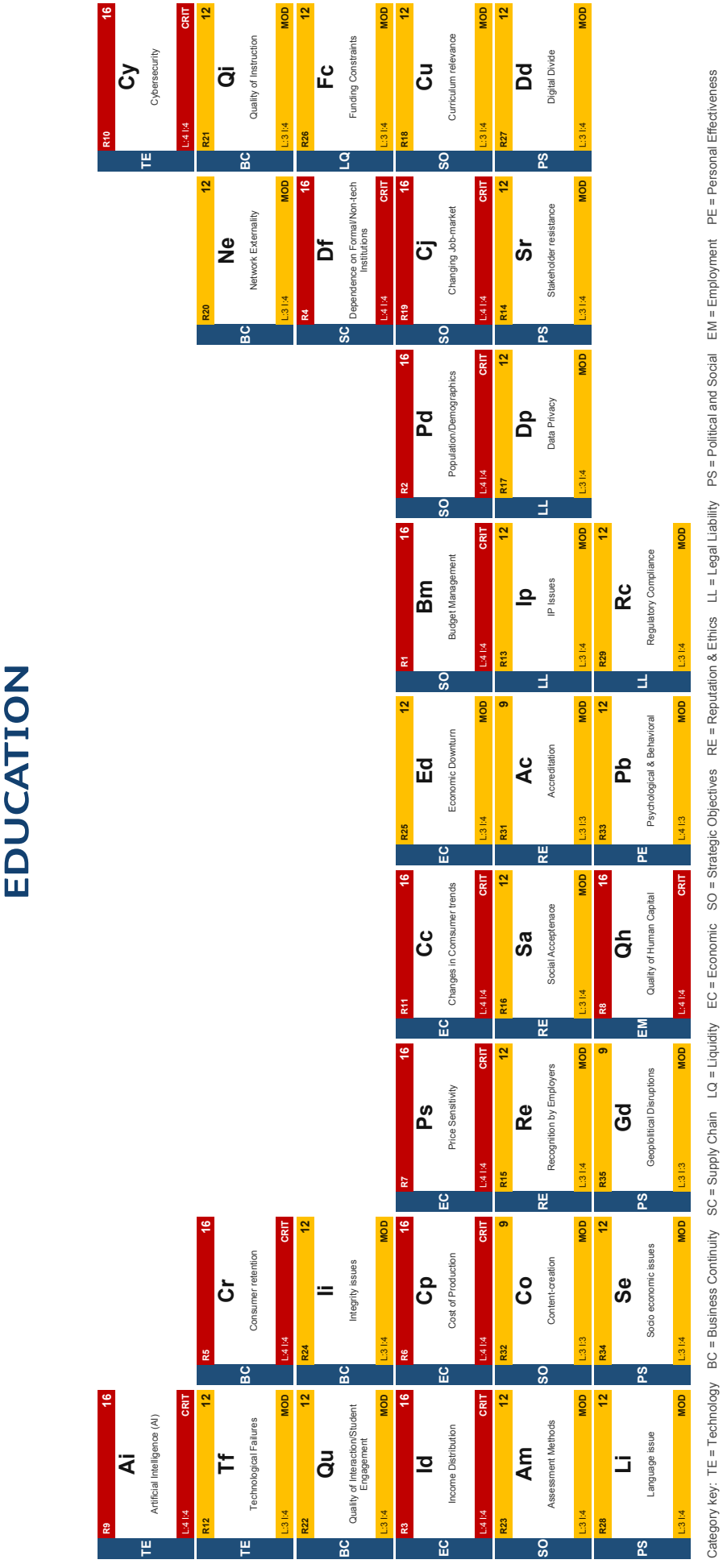
Macroeconomic and geopolitical factors also influence sector dynamics. Changes in economic conditions affect investment flows and demand for education services, while international regulatory requirements and recognition frameworks affect funding models, cross-border mobility, and international student flows.

Socio-political risks, including digital divide, language barriers, and unequal access to infrastructure, continue to constrain inclusivity and equitable service delivery. These challenges are particularly significant in technology-enabled education models, where disparities in access can widen existing gaps.

Reputational risk remains a critical cross-cutting theme. Academic integrity, quality of outcomes, and stakeholder trust directly influence demand, partnerships, and long-term institutional credibility. Failures in these areas can have immediate and widespread impact across both traditional and digital platforms.

The education sector's risk profile is defined by the interaction of learning delivery models, technological integration, regulatory oversight, financial sustainability, and stakeholder trust, where disruptions in one dimension can cascade across access, outcomes, and institutional credibility. Competitive advantage increasingly depends on the ability to adapt across pedagogical, technological, and operational dimensions while maintaining academic integrity, inclusivity, and resilience in an evolving and highly interconnected learning ecosystem.

5.5.1.3 The Periodic Risk Table



5.5.2 Mitigation Strategies

5.5.2.1 Prevention (Risk Avoidance and Reduction)

Prevention strategies in the education sector focus on reducing exposure to demand volatility, quality gaps, and technological risks by strengthening institutional design, improving operational efficiency, and enhancing stakeholder alignment.

A key area of prevention is academic quality and relevance, where institutions continuously update curricula through industry collaboration, real-world integration, and feedback-driven improvement. Faculty development programmes and structured competency mapping ensure that teaching quality remains consistent and aligned with learning outcomes.

Demand-related risks are mitigated through adaptive product design and pricing strategies, including segmentation-based offerings, flexible pricing models, and differentiated products to cater to diverse socio-economic groups. These strategies help address variations in income distribution and price sensitivity.

Operational and financial risks are managed through cost optimisation and resource efficiency, including the use of cloud-based systems, partnerships, and diversified revenue streams. These measures reduce dependency on single income sources and improve scalability.

Technology-related risks are mitigated through strong cybersecurity frameworks, including access controls, system monitoring, backup arrangements, and user awareness training. In addition, risks associated with AI systems are reduced through validation, monitoring, and human oversight mechanisms.

Institutions also address regulatory and stakeholder risks by maintaining compliance frameworks, engaging proactively with regulators, and building transparent relationships with stakeholders to reduce resistance and uncertainty.

Overall, prevention strategies are designed to embed resilience within academic, financial, and technological systems, reducing the likelihood of disruption.

5.5.2.2 Detection (Monitoring and Early Warning Systems)

Detection mechanisms in the education sector rely on continuous monitoring of academic, operational, and technological indicators to identify risks at an early stage.

Key Risk Indicators play a central role, including metrics such as student retention rate, course completion rate, academic performance indicators, and consumer sentiment indices, which provide insight into institutional performance and potential areas of concern.

Technology-related risks are monitored through system performance indicators, including uptime, incident frequency, and cybersecurity alerts. Continuous tracking of these metrics enables early detection of system vulnerabilities and operational disruptions.

Demand-related risks are monitored through enrolment trends, demographic data, and market demand forecasting, allowing institutions to adapt offerings in response to changing consumer behaviour.

Financial risks are identified through indicators such as cost -performance indices, funding stability, and revenue variance, providing visibility into financial health.

Regulatory risks are monitored through compliance trackers, audit findings, and policy updates, ensuring that institutions remain aligned with evolving regulatory requirements.

Overall, detection systems aim to provide real-time visibility and predictive insights, enabling proactive risk management.

5.5.2.3 Response (Incident and Crisis Management)

Response strategies focus on ensuring continuity of learning, protecting stakeholder interests, and minimising reputational impact during disruptions.

In the event of operational or technological failures, institutions deploy business continuity measures, including system backups, failover mechanisms, and alternative delivery modes such as online platforms.

Cyber incidents are managed through structured response protocols, including system isolation, recovery procedures, and communication with affected stakeholders to maintain trust.

Reputational risks are addressed through rapid communication and remediation mechanisms, including addressing complaints, managing public perception, and maintaining transparency with stakeholders.

Academic disruptions are managed through flexible delivery models, ensuring continuity of instruction and assessment through hybrid or remote learning systems.

Financial stress situations are addressed through cost controls, funding adjustments, and revenue diversification strategies.

Overall, response capability is defined by speed, adaptability, and proactive communication, ensuring minimal disruption and preservation of trust.

5.5.2.4 Resilience (Recovery and Adaptive Capability)

Resilience in the education sector is centred on adaptability to changing technological, economic, and societal conditions.

A key driver of resilience is digital transformation, enabling institutions to deliver education through scalable and flexible platforms. Hybrid learning models and digital infrastructure reduce dependence on physical systems and improve continuity.

Institutional resilience is strengthened through diversification of programmes, partnerships, and delivery models, allowing adaptation to changing demand patterns and labour market requirements.

Financial resilience is built through diversified revenue streams, efficient resource management, and long-term planning, enabling institutions to absorb economic shocks.

A critical aspect of resilience is continuous learning and improvement, where institutions analyse performance data, student feedback, and market trends to refine offerings and enhance effectiveness.

Resilience also involves addressing structural challenges such as the digital divide and socio-economic disparities, ensuring broader accessibility and inclusivity.

Overall, resilience enables institutions to operate as adaptive systems capable of evolving in response to dynamic conditions.

5.5.2.5 KRIs and Governance

Key Risk Indicators and governance frameworks are essential for ensuring effective risk management and strategic alignment in the education sector.

KRIs provide measurable insights into key risk areas, including academic performance, student retention, financial stability, system reliability, and stakeholder sentiment. These indicators are supported by diverse data sources such as institutional systems, surveys, and external data feeds.

Governance frameworks ensure that these indicators are monitored, reviewed, and acted upon through structured reporting systems, defined accountability, and leadership oversight.

Regular review cycles, ranging from real-time monitoring for critical systems to periodic evaluations for strategic risks, ensure continuous risk visibility.

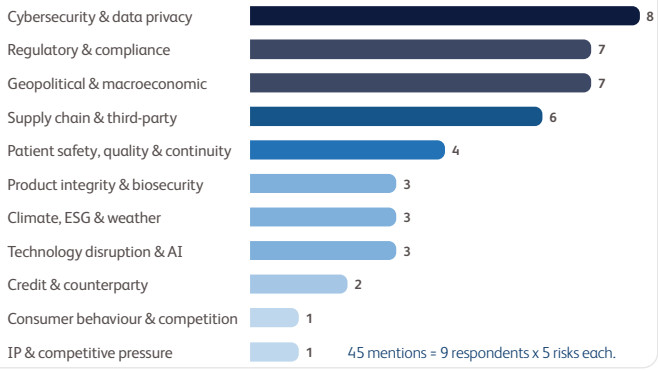
Integration of risk monitoring with decision-making processes enables institutions to respond proactively to emerging challenges and align operations with long-term objectives.

A key strength of governance lies in its ability to link data-driven insights with strategic action, ensuring that risk management supports both operational stability and long-term institutional success.

Hospitality, Tourism, Media, Retail, Healthcare-Pharma, Information Technology, Education, Food, Agriculture, & FMCG

9	100%	4.0/5	~6%
RESPONDENTS	SAY THEY ARE GROWING All 9 respondents	AVG RISK EXPOSURE 7 rate 4 . 1 rates 3 . 1 rates 5	MEDIAN RESOURCES TO RISK MGMT Range 2 to 12.5%

What keeps these industries up at night - top-five risk mentions



45 mentions = 9 respondents x 5 risks each.

Risk appetite - segment average by dimension

FINANCIAL	OPERATIONAL	REGULATORY	STRATEGIC
3.1/5	2.1/5	1.5/5	3.6/5
Moderate from 8 stated answers	Low from 7 stated answers	Very Low to Low from 8 stated answers	Moderate to Mod-High from 9 stated answers

A low score means the segment has little appetite for that type of risk-failures there are treated as unacceptable and are tightly controlled rather than taken on. A high score means the segment is willing to accept more of that risk in pursuit of growth, innovation and returns.

Crisis preparedness --- self-assessed, by segment

Pharma & ITES (post-pandemic)	Mod-High
Large listed FMCG	Mod-High
Hospital networks & organised agri	Moderate
Organised retail	Moderate
Smaller & unorganised players	Vulnerable

The risk outlook - what's rising now, what's coming next

RISING FASTEST . LAST 3 YEARS

- Cyber & digital fraud
- Climate unpredictability & extreme weather
- Regulatory & quality scrutiny
- Supply chain & API dependency
- Commodity & cost inflation
- Talent attrition

→

EMERGING . NEXT 3-5 YEARS

- AI governance
- Cyber & digital fraud
- Data privacy (DPDP)
- API & supply concentration
- Water stress & climate
- Residue, packaging & green claims rules
- Digital-first competition
- Specialist talent shortage
- Pricing & market access

Driven by: Rapid digitalisation & AI adoption across the value chain; Regulatory tightening -quality, residues, packaging, claims, data; Climate volatility & monsoon dependence; Concentrated global supply chains & third-party reliance.

How far ahead these industries plan

Now - 12 months	Operations, cyber, quality, inventory & crop-season risk
1 - 3 years	Consumer, regulatory, payer & workforce shifts
3 - 5 years	Climate, portfolio, digital transformation & capex
5 - 10 years +	R&D and patent cycles, water security & forestry

The dependency chain - what operations cannot run without

1. API, raw-material & ingredient suppliers
2. Cold-chain, logistics & import corridors
3. Cloud, HIS/EMR, payment & technology vendors
4. Monsoon cycles, rural incomes & dealer networks
5. Regulators - FSSAI, drug authorities, accreditation bodies
6. Skilled clinical, technical & seasonal workforce

6 of 9 report industry collaborations (IRM, FICCI, CII, ASCI, ISO cited), rated moderately effective-strongest on standards and awareness. Agriculture & food shows the weakest footprint: 2 of 4 report none.

From gaps to action

WHAT'S MISSING TODAY

- ✕ Specialist cyber & digital talent
- ✕ Fragmented risk, quality & farm-level data
- ✕ Supply-chain & third-party visibility
- ✕ Climate-risk modelling & forecasting
- ✕ Barrier: Fragmented, informal value chains & uneven partner maturity

WHAT WOULD CLOSE THE GAP

- ✓ Shared risk-intelligence platforms -counterfeits, cyber, shortages
- ✓ Common taxonomies, traceability & data standards
- ✓ Stronger board-level oversight & farmer insurance
- ✓ Sustained investment in analytics, cyber & continuity

Already in play: Quality management & pharmacovigilance, Dual sourcing & supplier audits, Cybersecurity & data-integrity controls, Weather analytics & agri-insurance.

The agenda - what these industries say they must do next

TOP COMPLIANCE PRIORITY
Keeping pace with regulatory change
then: Leveraging technology

MOST PRESSING SHARED CHALLENGE
Keeping pace with regulatory change
then: Improving data quality

#1 FOCUS NEXT 12-24 MONTHS
Accelerating digital transformation
6 of 9 review tolerance limits quarterly

What enables it (importance / 5): Maturity of risk & compliance functions **4.78**. Continuous risk assessment **4.78** Technology & data **4.67** Culture & values **4.56**. **Hardest rules to live with:** GMP, data integrity & pharmacovigilance; DPDP data- privacy & breach reporting; FSSAI labelling, claims & residue norms.

"Regulation defines quality, safety, data and claims standards end-to-end; analytics is moving from dashboards and forecasting to predictive, real-time monitoring, early warning and traceability."

5.6 Mining, Energy, Manufacturing, Infrastructure

About the researchers

Dr. Sri Kalyana Rama Jyosyula

Associate Professor
Department of Civil Engineering at
Mahindra University

Dr. Sri Kalyana Rama Jyosyula is an Associate Professor in the Department of Civil Engineering at Mahindra University and a Founding Director of Precastelite Confab Private Limited. His expertise includes smart and sustainable built environments, Enterprise Risk Management (ERM), construction project risk assessment, and infrastructure resilience. He is an IRM Level 1 certified professional. He serves on technical committees of the Bureau of Indian Standards (BIS) and the International Organisation for Standardisation (ISO) related to risk management and resilience. He has led numerous industry- and government-funded projects, consultancy assignments, and has authored several high-quality indexed journal papers, as well as holding multiple patents.

Rachapoodi Parimala

BBA (Digital Technologies) student at
Mahindra University IRM Level 1
certified professional

Rachapoodi Parimala is a BBA (Digital Technologies) student at Mahindra University, and is an IRM Level 1 Certified professional. She has contributed to sectoral risk analysis and research in the mining, energy, infrastructure, and manufacturing domains sectors.

5.6.1 Mining

5.6.1.1 Overview

The mining sector forms a foundational pillar of industrial development by supplying critical raw materials required for manufacturing, construction, power generation, and technological infrastructure. It encompasses the exploration, extraction, processing, and distribution of minerals such as coal, iron ore, base metals, precious minerals, and industrial aggregates, making it integral to economic growth and infrastructure expansion. Major tailings dam failures and commodity price downturns have highlighted the sector's exposure to high-impact, system-wide risks that extend beyond operational boundaries.

The sector is highly capital-intensive and operationally complex, with activities often concentrated in geographically fixed and resource-specific locations. Unlike more flexible industries, mining operations are tied to geological conditions, resulting in long asset lifecycles, extended payback periods, and significant upfront investment in heavy machinery, processing facilities, and tailings infrastructure. This creates heightened sensitivity to operational disruptions, commodity cycles, and regional infrastructure constraints.

In recent years, the industry has undergone structural transformation driven by advances in extraction technologies, increased automation, evolving global supply chains, and mounting pressure to comply with stringent environmental and sustainability standards. At the same time, mining operates within a rigorous regulatory framework focused on safety, environmental compliance, and land-use governance, alongside growing expectations from investors and stakeholders regarding ESG performance.

The risk landscape in mining is inherently multidisciplinary, spanning geotechnical uncertainty, asset integrity, operational safety, commodity market volatility, environmental sustainability, and community relations. These risks are deeply interconnected; failures in environmental management or community engagement can rapidly escalate into regulatory intervention, reputational damage, and financial constraint. As a result, mining operates as a tightly coupled system where operational viability, governance effectiveness, and socio-environmental alignment are closely linked.

> "I expect the sector to become cleaner, more digital, more decentralised and more interconnected. That is exciting, but it means risk will become more systemic."
>
> **— Power & Energy respondent,**
> when asked how the risk landscape will evolve over 5–10 years

5.6.1.2 Key Risk Themes

The mining sector faces a complex and interdependent risk landscape shaped by geotechnical vulnerability, operational hazards, environmental exposure, market volatility, and socio-political dynamics. These risks are structural in nature and often reinforce one another.

Geotechnical integrity and operational safety represent the most critical risk dimension. Mining operations involve inherently hazardous conditions, including underground excavation, slope stability management, and large-scale waste storage through tailings dams. These risks are characterised by low-frequency but extremely high-impact events, making early detection and continuous monitoring critical. Risks such as mine collapses, slope failures, equipment accidents, and occupational health hazards highlight the sector's exposure to catastrophic outcomes. Given the scale and nature of operations, even isolated failures can result in severe consequences, including loss of life, prolonged shutdowns, regulatory intervention, and substantial financial liabilities. Maintaining strong engineering controls, continuous monitoring, and a safety-first operational culture is therefore essential.

Commodity price cycles and financial resilience constitute another central risk theme. Mining organisations operate as price takers in global markets, exposing them to volatility driven by shifts in demand, trade dynamics, and macroeconomic conditions. Fluctuations in commodity prices, exchange rates, fuel costs, and energy inputs directly affect margins and project viability, particularly given the sector's high fixed cost base and long investment horizons. Downcycles can rapidly strain liquidity, making disciplined cost management, capital allocation, and financial resilience critical for sustaining operations.

Environmental risk has increased in both scope and strategic significance. Activities such as land disturbance, water contamination, air emissions, and waste generation create long-term ecological impact and regulatory exposure. Risks related to acid mine drainage, carbon emissions, water scarcity, and mine closure obligations are further amplified by tightening environmental regulations and rising ESG expectations. Non-compliance or inadequate environmental performance can result in penalties, litigation, capital withdrawal, and the potential stranding of assets.

Community relations and social licence to operate represent a critical and often decisive risk factor. Mining activities frequently intersect with local communities, leading to challenges related to land acquisition, displacement, resource competition, and environmental concerns. Where communities perceive that mining operations generate harm without equitable economic benefit, resistance can escalate into protests, legal disputes, or operational disruptions. Loss of social licence can effectively halt operations, regardless of technical or financial readiness, making transparent engagement, fair benefit-sharing mechanisms, and long-term trust essential to ensure continuity.

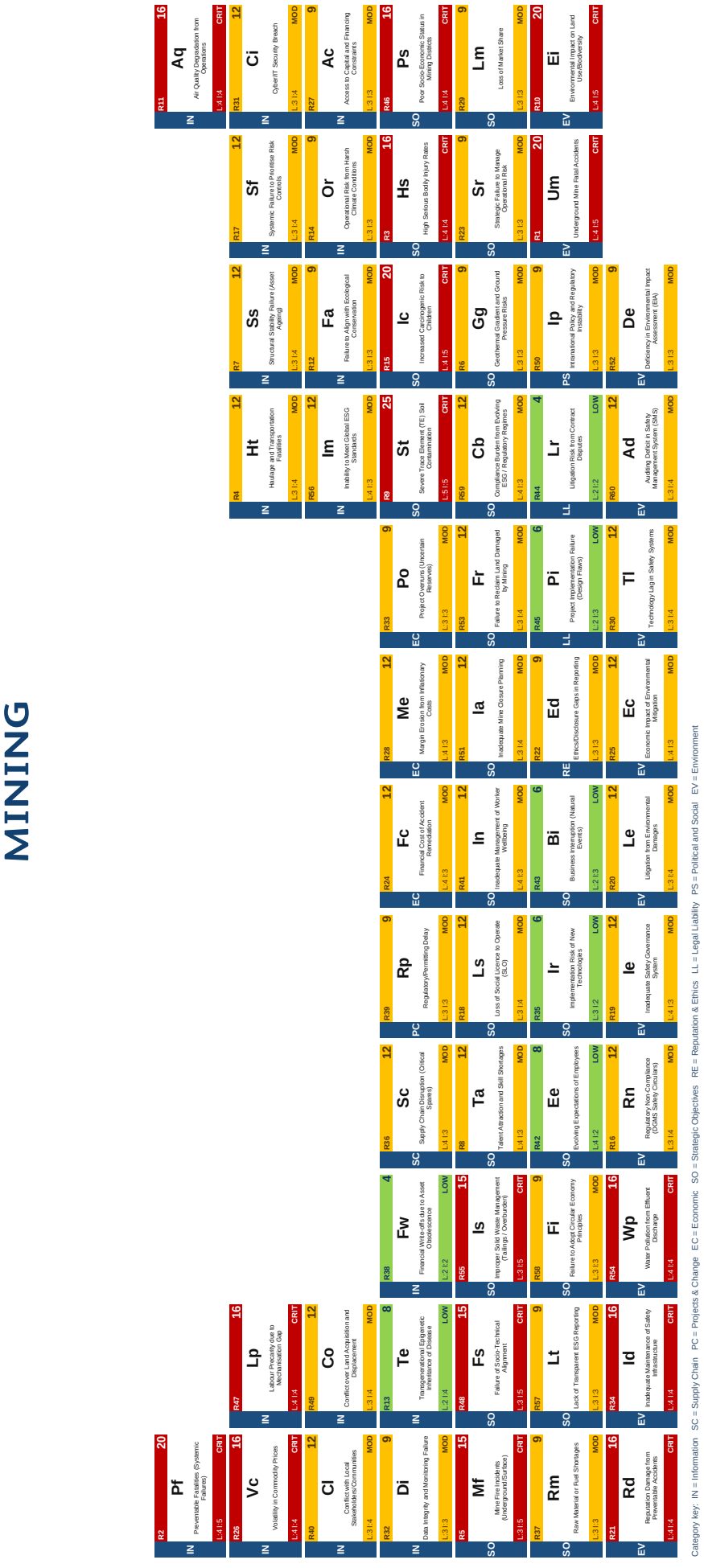
Logistical networks and infrastructure dependencies introduce additional operational vulnerabilities. Mining operations rely heavily on external infrastructure such as rail networks, ports, energy supply systems, and transport fleets to move bulk materials from remote locations. Disruptions in these systems—whether due to capacity constraints, infrastructure failure, or external shocks—can lead to inventory build-up, delayed shipments, and contractual penalties. Given the remote nature of many mining areas, supply chain resilience and infrastructure coordination are critical to maintaining output stability.

Technological and governance risks are also growing in importance. The adoption of automated systems, advanced monitoring technologies, and digital reporting frameworks is reshaping operations, but delayed implementation or inadequate integration can reduce efficiency and increase exposure to operational failure. At the same time, transparency in reporting, particularly in ESG and compliance domains, is becoming essential to maintain investor confidence and regulatory alignment.

The mining sector operates within a high-impact, resource-dependent system where geotechnical, financial, environmental, and socio-political risks are closely interlinked. Failures in any one area—such as a tailings breach, commodity price shock, or community conflict—can rapidly cascade into broader operational, regulatory, and financial consequences.

Managing risk in this sector demands alignment across technical, environmental, financial, and stakeholder dimensions, where organisations that effectively integrate these elements are better positioned to maintain operational stability and long-term value creation amid increasing complexity.

5.6.1.3 The Periodic Risk Table



5.6.2 Energy

5.6.2.1 Overview

The energy sector is a foundational driver of economic activity, supporting industrial systems, infrastructure, and everyday consumption. The sector underpins modern economic systems, functioning as critical infrastructure where supply continuity is essential and disruptions propagate rapidly across industries and public services. It encompasses a diverse mix of conventional energy sources such as thermal power and natural gas, alongside renewable systems including solar, wind, hydro, and emerging energy storage solutions. The sector is undergoing a significant structural transformation driven by decarbonisation imperatives, technological advancement, and evolving policy and regulatory frameworks.

This transition has created a dual-system environment in which legacy energy infrastructure coexists with rapidly expanding renewable and decentralised systems. As a result, the operating landscape has become increasingly complex, requiring energy providers to manage both long-term transition risks and short-term operational stability. High capital intensity, long asset lifecycles, and dependence on regulatory frameworks make the sector particularly sensitive to policy changes, financial conditions, and technological disruption.

Energy systems are characterised by their interconnected and critical nature, where supply continuity is essential and disruptions can have immediate cascading effects across industries, public services, and financial markets. The increasing integration of smart grids, digital monitoring systems, and automation technologies has improved efficiency but also expanded exposure to technological and cybersecurity risks. Consequently, the sector operates within a highly interdependent risk environment shaped by grid reliability, fuel availability, infrastructure resilience, and evolving sustainability expectations.

> "A major environmental incident — such as a tailings dam failure — represents the single most significant reputational risk for the global metals and mining industry."
>
> **— Metals & Mining respondent,**
> when asked about the biggest reputational threats

> "The automotive industry is significantly more prepared for major risk events today than it was five years ago — the pandemic, semiconductor shortages, cyber incidents and geo-political conflicts have fundamentally reshaped readiness."
>
> **— Automobile respondent,**
> when asked about crisis preparedness

5.6.2.2 Key Risk Themes

The energy sector risk landscape is driven by the interaction of transition dynamics, infrastructure dependencies, regulatory frameworks, and technological evolution. These risks are systemic and often amplify one another.

The transition toward low-carbon energy represents a central structural challenge. Traditional thermal assets face risks of obsolescence, reduced asset lifespans, and declining investor support due to decarbonisation policies and carbon-related regulations. Transition risk increasingly manifests through capital reallocation, where financing shifts away from carbon-intensive assets, while renewable energy systems introduce operational challenges associated with intermittency, resource variability, and integration into existing grid infrastructure. Balancing the stability of legacy systems with the expansion of clean energy capacity is therefore a key risk management priority.

Grid stability and system reliability constitute another critical risk dimension. The increasing share of weather-dependent energy sources such as solar and wind introduces variability that must be managed through advanced grid-balancing mechanisms, storage solutions, and transmission upgrades. Failure to modernise grid infrastructure can lead to supply disruptions, voltage instability, and large-scale outages, with significant economic and social consequences.

Regulatory and policy risk plays a decisive role in shaping sector outcomes. Energy providers operate under evolving frameworks governing tariffs, subsidies, emissions standards, and market access. Sudden changes in pricing mechanisms, incentive structures, or compliance requirements can materially affect project economics, investment decisions, and financial viability. The sector's dependence on policy direction further increases exposure to political and regulatory uncertainty.

Financial risks remain pronounced due to the sector's capital -intensive nature and long investment horizons. Exposure to interest rate fluctuations, delayed payments, funding constraints, and high upfront capital requirements can affect project viability and cash flow stability. Delayed payments and weak counterparty credit quality further introduce liquidity stress across the energy value chain, while uncertainty around long-term returns in the context of transition dynamics complicates capital allocation decisions.

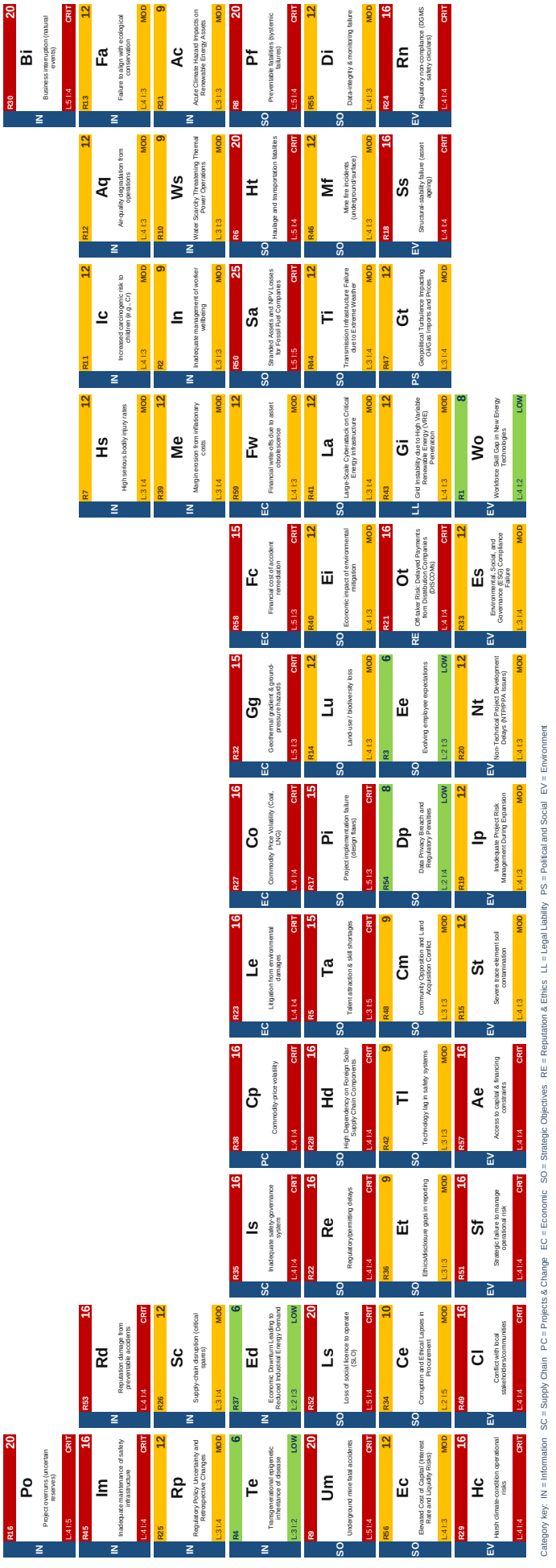
Technological and cybersecurity are increasing in importance as energy systems become more digitised. The integration of operational technology with digital control systems and smart grids expands the sector's cyber threat surface. Cyberattacks targeting critical infrastructure such as SCADA systems can disrupt generation and transmission networks, with potential implications for national security and economic stability.

Fuel supply security and resource variability also remain key concerns. Conventional energy systems face risks related to fuel supply disruptions, price volatility, and transportation constraints. For renewable generation, variability in natural resources such as sunlight, wind, and water availability introduces additional uncertainty in output and system planning.

Climate-related risks further compound sector exposure, both as a driver of transition and as a direct operational threat. Extreme weather events, including storms, floods, and heatwaves, can damage generation assets and transmission networks, disrupt supply, and increase maintenance costs. These risks necessitate investments in infrastructure resilience and climate-adaptive design.

The energy sector reflects a transition-driven system of interdependent risks, where technological change, regulatory shifts, environmental constraints, and financial dynamics interact to reshape risk profiles. Managing these interdependencies effectively is critical to balancing system reliability with long-term sustainability.

5.6.2.3 The Periodic Risk Table



5.6.3 Manufacturing

5.6.3.1 Overview

The manufacturing sector is a key driver of economic growth, employment, and global trade integration, spanning industries from heavy industrial production to advanced and high-technology manufacturing. It encompasses a wide range of activities including automotive production, machinery manufacturing, electronics, chemicals, textiles, and consumer goods, forming a core component of industrial value creation.

Manufacturing systems are deeply interconnected with global supply chains, making them highly sensitive to geopolitical developments, trade dynamics, and macroeconomic conditions. Manufacturing operates as a synchronised production system, where efficiency-driven models such as just-in-time create vulnerability to even minor disruptions, amplifying the impact of supply chain shocks. The sector is undergoing rapid transformation through the adoption of Industry 4.0 technologies, including industrial IoT, automation, robotics, AI, and advanced manufacturing techniques, enhancing efficiency and productivity while introducing new technological and operational complexities.

A defining characteristic of modern manufacturing is its reliance on synchronised, multi-tiered supply chains and lean inventory models. While these systems optimise efficiency, they also create vulnerability to disruptions, where delays or failures in a single component or supplier can halt entire production processes. As a result, manufacturing operates within a highly interconnected risk environment where operational continuity depends on both internal processes and external supply chain stability.

5.6.3.2 Key Risk Themes

Manufacturing risks are driven by supply chain interdependence, technological integration, operational execution, and market and regulatory dynamics.

Supply chain disruptions and input volatility represent one of the most significant risk dimensions. Dependence on global supplier networks, just-in-time inventory systems, and concentrated sourcing exposes manufacturers to risks arising from geopolitical tensions, logistics delays, trade restrictions, and raw material shortages. Limited visibility beyond Tier-1 suppliers further increases exposure to hidden dependencies within the supply chain, allowing even minor disruptions to cascade across production lines and lead to delays, increased costs, and revenue loss. Strengthening supplier diversification and end-to-end supply chain visibility has therefore become a strategic priority.

Technological risks are increasingly prominent with the integration of Industry 4.0 systems. The use of interconnected industrial IoT platforms, robotics, and cloud-based manufacturing systems introduces vulnerabilities related to cybersecurity, system outages, and technology integration failures. Cyberattacks or software disruptions can halt production, damage equipment, and compromise sensitive intellectual property, highlighting the need for robust digital security frameworks.

Product quality and liability risks remain critical, particularly in industries where defects can have significant financial, legal, and safety consequences. Failures in quality control, component integrity, or process consistency can lead to recalls, litigation, and reputational damage. Ensuring end-to-end traceability and stringent quality assurance is essential to mitigate these risks.

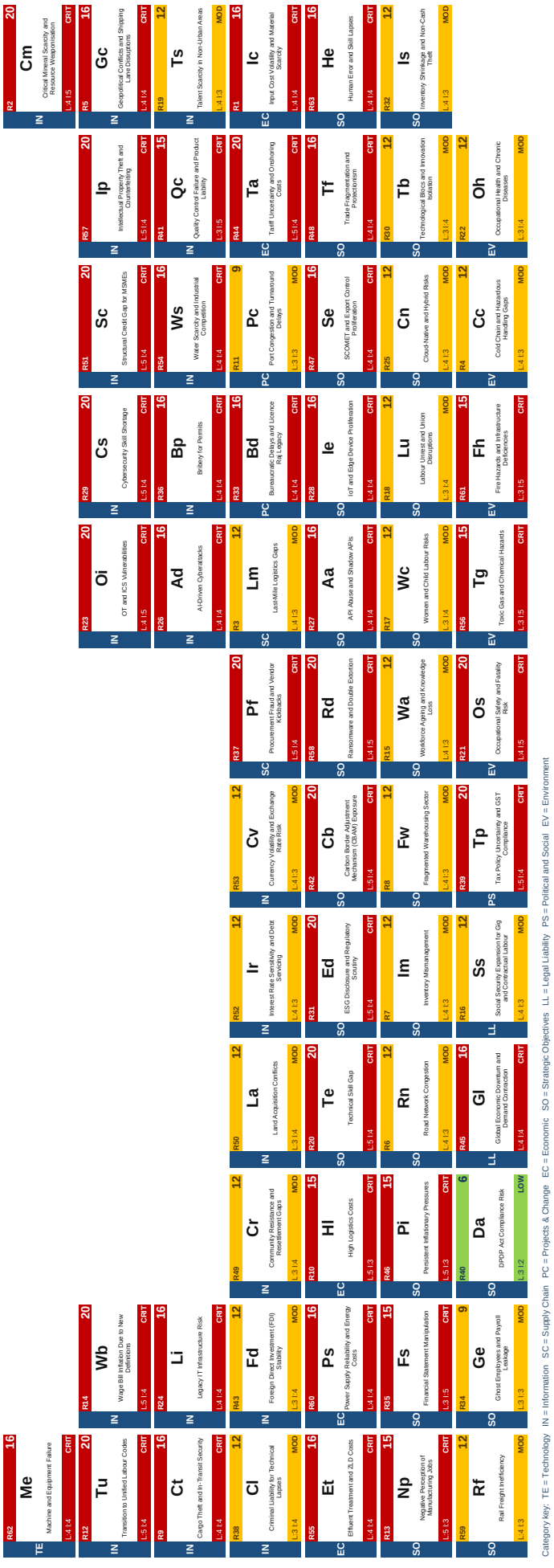
Workforce capability and labour dynamics also influence sector performance. The shift toward automation and advanced manufacturing technologies has increased demand for specialised technical skills, while traditional workforce structures face challenges related to attrition, skill gaps, and adaptation to new systems. Maintaining a skilled and adaptable workforce is critical to sustaining productivity and operational efficiency.

Environmental and regulatory compliance risks are becoming more significant as governments and stakeholders impose stricter standards on emissions, waste management, and sustainability practices. Non-compliance can result in financial penalties, operational restrictions, and reputational damage, while increasing focus on carbon accountability is reshaping cost structures and investment priorities.

Financial risks linked to capital investment, demand fluctuations, and global economic conditions further affect sector stability. Manufacturing performance is closely tied to economic cycles, making it vulnerable to changes in consumer demand, export markets, and currency movements.

Overall, manufacturing operates as a globally interconnected production system where operational efficiency, technological resilience, supply chain robustness, and regulatory compliance are closely linked. Effective risk management requires balancing lean operational models with structural resilience, supported by digital integration, workforce development, and supply chain diversification.

5.6.3.3 The Periodic Risk Table



5.6.4 Infrastructure

5.6.4.1 Overview

The infrastructure sector encompasses large-scale physical systems that enable economic activity and societal functioning, including transportation networks, energy systems, urban development, and public utilities. It forms the backbone of economic growth by supporting mobility, trade, urbanisation, and service delivery across sectors.

Infrastructure development is characterised by high capital intensity, long project lifecycles, and complex stakeholder ecosystems involving governments, private investors, contractors, and regulatory bodies. Projects often operate through multi-layered contractual and financing structures, including public-private partnerships, and are subject to extensive regulatory oversight and socio-environmental considerations. Large infrastructure projects frequently experience delays and cost overruns due to land acquisition challenges and regulatory complexities, highlighting the sector's inherent execution risks.

A defining feature of the sector is its long-term, illiquid asset profile, which exposes projects to compounded risks during both construction and operational phases. Infrastructure assets are also closely tied to geographic and environmental conditions, making them sensitive to land acquisition challenges, regulatory approvals, and changing political and economic priorities.

With increasing adoption of digital technologies, including smart infrastructure systems, data-driven monitoring, and climate -resilient engineering, the sector is evolving to improve efficiency and sustainability. However, these advancements also introduce new forms of systemic and technological risk.

5.6.4.2 Key Risk Themes

Infrastructure risks arise from project complexity, financial exposure, regulatory uncertainty, and environmental and operational dependencies, with strong interconnections across these dimensions.

Project execution risk remains the most critical challenge. Large-scale infrastructure projects are inherently complex and frequently face delays due to land acquisition issues, permitting challenges, design changes, and coordination difficulties among stakeholders. These delays often result in cost overruns and extended time-lines, increasing financial pressure and affecting project viability.

Financial risks are significant due to the capital-intensive nature of infrastructure investments. Projects are highly sensitive to changes in interest rates, inflation, funding availability, and cost escalation. Delays during construction can increase financing costs, particularly interest during construction, placing additional strain on project economics.

Land acquisition and regulatory approvals represent another major risk area. Securing land titles, managing community displacement concerns, and obtaining environmental clearances can be time-consuming and contentious processes. Legal disputes, policy changes, and political resistance can stall projects, locking capital and delaying returns.

Demand and revenue risk affects projects dependent on user-based income models, such as toll roads, airports, and ports. Variability in traffic volumes, economic conditions, and competing infrastructure can lead to lower-than-expected utilisation, affecting revenue generation and debt servicing capacity.

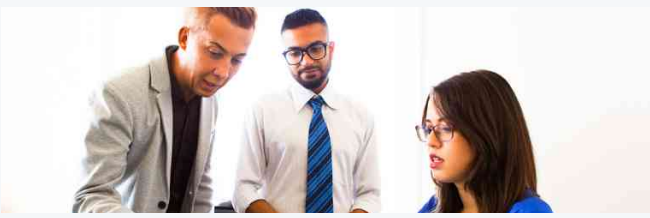
Asset lifecycle and maintenance risks are also significant. Infrastructure assets require continuous maintenance and monitoring to ensure safety and longevity. Failure to maintain assets adequately can lead to deterioration, service disruptions, and, in extreme cases, structural failure with significant financial and legal consequences.

Climate and environmental risks are increasingly material. Infrastructure systems are directly exposed to extreme weather events, including floods, heatwaves, and storms, which can damage assets and disrupt services. Changing environmental conditions require the incorporation of climate-resilient design and long-term adaptation strategies.

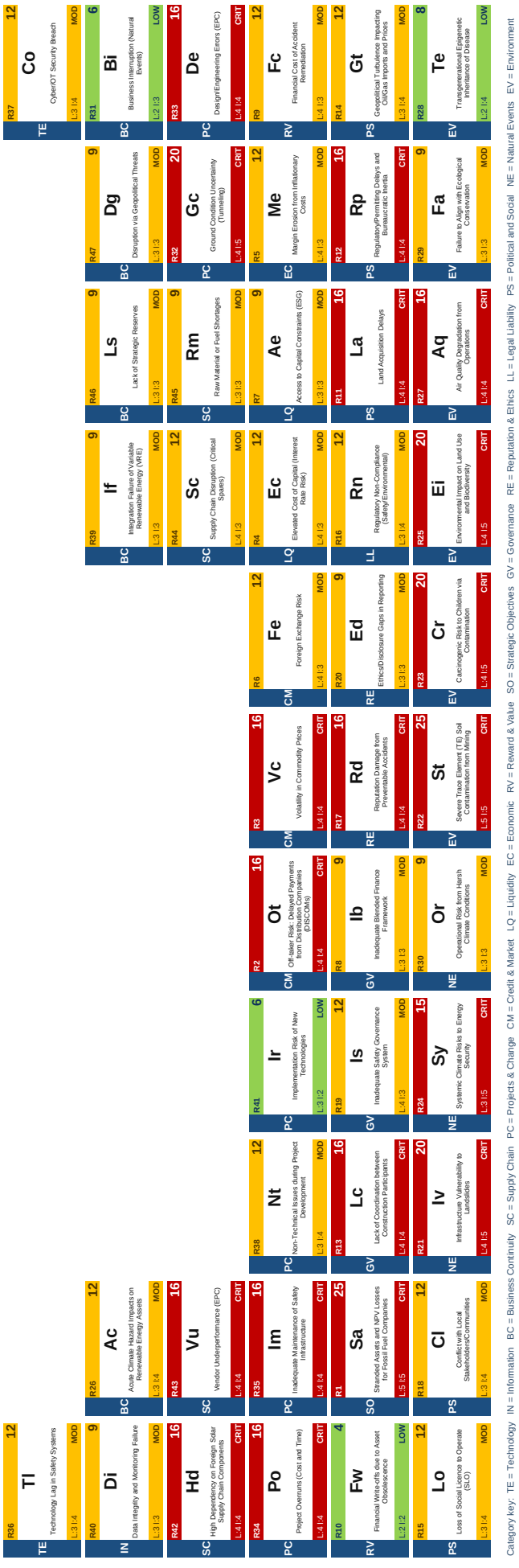
Technological risks are emerging with the integration of smart systems and digital infrastructure. Increased reliance on smart systems introduces risks related to data integrity, system failure, and cyber vulnerabilities, which can disrupt operations and affect service delivery, particularly in critical infrastructure networks.

Infrastructure delivery takes place within a highly interconnected ecosystem, where execution efficiency, financing structures, regulatory alignment, and environmental factors collectively shape project outcomes. Long-term success depends on effective coordination and embedding resilience across both design and operations.

> "Low for safety and compliance; moderate for market and technology bets; selective for growth capex."
>
> **— Integrated Power Utility respondent,**
> when asked about the industry's risk appetite



5.6.4.3 The Periodic Risk Table



5.6.5 Mitigation Strategies

5.6.5.1 Prevention (Risk Avoidance and Reduction)

Prevention strategies across the mining, energy, manufacturing, and infrastructure sectors are focused on reducing exposure to high-impact operational, environmental, and financial risks through system-level controls and resilient design. Given the inherent risk intensity of these industries, prevention is anchored in strengthening safety systems, stabilising supply chains, and integrating sustainability into core operations.

A primary priority is occupational safety and operational risk reduction, particularly in environments involving hazardous processes and heavy equipment. Organisations are increasingly adopting zero-harm frameworks that integrate engineering safeguards, preventive maintenance, structured training, and emergency preparedness. This reflects a shift from compliance-driven safety toward a deeply embedded safety culture within operations.

Supply chain resilience is another critical pillar. Multi-sourcing strategies, inventory buffers, and robust logistics planning reduce dependence on single suppliers and enable continuity during disruptions. This is particularly important in industries reliant on critical raw materials or complex project supply chains.

Financial risk prevention is addressed through stabilisation mechanisms such as hedging, long-term procurement contracts, and flexible sourcing arrangements. These approaches help manage commodity price volatility and protect margins in uncertain market conditions.

Environmental risk mitigation is central to prevention, given the significant footprint of these sectors. Organisations implement environmental management systems, pollution control technologies, and biodiversity protection measures to reduce ecological impact and ensure regulatory compliance. These initiatives also support long-term sustainability and investor expectations.

Preventive strategies further extend to managing regulatory and socio-political risks through early stakeholder engagement. Incorporating regulatory timelines into project planning and maintaining transparent communication with communities and authorities reduces the likelihood of delays, disputes, and operational disruptions.

Overall, prevention focuses on embedding resilience at the source, reducing exposure before risks materialise into operational or financial disruption.

5.6.5.2 Detection (Monitoring and Early Warning Systems)

Detection mechanisms are critical in identifying emerging risks early, particularly in sectors where disruptions can escalate rapidly and have large-scale consequences. Effective detection relies on continuous monitoring systems, integrated data flows, and well -defined Key Risk Indicators.

Operational safety risks are monitored through indicators such as lost-time injury rates and high-severity incident frequencies. Continuous tracking enables early identification of unsafe conditions and systemic weaknesses, allowing timely intervention.

Supply chain risks are assessed using metrics such as supplier performance, delivery reliability, and inventory levels. Indicators including on-time delivery rates and critical stock coverage provide early warnings of potential disruption, enabling proactive mitigation.

Financial and market risks are tracked through indicators such as input cost trends, hedging effectiveness, and liquidity metrics. These provide real-time visibility into exposure to market volatility and financing constraints.

Environmental risk detection is supported by continuous monitoring of emissions, water usage, and environmental compliance indicators. Early identification of deviations ensures corrective action before regulatory breaches or operational impact occurs.

Technology-related risks, particularly cybersecurity, are monitored through advanced systems that track network activity, vulnerabilities, and patch compliance. These frameworks ensure early identification of threats across both IT and operational technology environments.

The strength of detection lies in its ability to bridge data and action, reducing the time between risk emergence and organisational response.

5.6.5.3 Response (Incident and Crisis Management)

Response strategies are designed to manage high-impact events effectively, particularly those related to safety incidents, operational breakdowns, and environmental disruptions. Given the scale and complexity of these sectors, response frameworks must be structured, coordinated, and operationally robust.

In safety and operational contexts, response focuses on rapid containment, emergency management, and restoration of normal operations. Defined protocols, trained response teams, and tested emergency systems ensure that incidents are addressed efficiently and impact is minimised.

Supply chain disruptions are managed through contingency mechanisms such as alternate sourcing, logistics rerouting, and utilisation of buffer inventories. These actions enable continuity in production and project execution despite external constraints.

Financial response frameworks provide stability during disruptions through access to credit facilities, liquidity buffers, and risk transfer mechanisms such as insurance. These reduce the financial impact of operational or market shocks.

Environmental incidents require coordinated containment, remediation, and regulatory engagement. Effective response minimises ecological damage while maintaining compliance and stakeholder confidence.

Technology and cybersecurity incidents are addressed through structured response protocols involving system isolation, recovery processes, and forensic investigation. Preparedness is reinforced through regular testing and simulation of high-risk scenarios.

Stakeholder communication remains a critical component, particularly in managing reputational and socio-political risks. Transparent and timely engagement with regulators, communities, and investors helps preserve trust and mitigate long-term impact.

Response effectiveness is ultimately defined by speed, coordination, and execution discipline, ensuring that disruptions are contained before escalating into systemic failure.

5.6.5.4 Resilience (Recovery and Adaptive Capability)

Resilience reflects the organisation's ability to recover from disruption while adapting to evolving risk conditions. In capital-intensive sectors, resilience is closely tied to system robustness, financial flexibility, and adaptive operational capability.

Structural resilience is achieved through infrastructure hardening, redundancy, and diversification. Backup systems, alternative supply arrangements, and resilient asset design ensure continuity in the face of disruptions such as extreme weather events or infrastructure failures.

Recovery capability is strengthened through well-defined processes for restoring operations, supported by regular validation of systems and response mechanisms. This ensures that recovery timelines are achievable under real conditions.

Financial resilience is critical in managing volatility and uncertainty. Access to capital, liquidity buffers, and flexible cost structures enable organisations to absorb shocks and sustain operations during downturns.

Operational adaptability allows organisations to adjust production levels, reallocate resources, and revise project timelines in response to changing conditions. This flexibility is essential in managing supply chain disruptions, regulatory delays, and demand fluctuations.

Continuous learning plays a central role in resilience. Post-incident analysis identifies underlying weaknesses and informs improvements in preventive and detection systems, creating a reinforcing feedback loop that strengthens long-term capability.

Resilience also depends on maintaining strong relationships with communities and regulators. Sustaining social licence to operate and aligning with evolving ESG expectations reduce exposure to socio-political risks.

Resilience therefore extends beyond recovery, enabling organisations to adapt, stabilise, and sustain performance in a dynamic risk environment.

5.6.5.5 KRIs and Governance

Key Risk Indicators and governance frameworks underpin effective risk management by translating complex operational, financial, and environmental exposures into measurable signals.

KRIs are embedded across organisational systems, covering safety performance, supply chain reliability, financial stability, environmental compliance, and cybersecurity posture. These indicators draw on multiple data sources to provide comprehensive visibility into risk conditions.

Structured monitoring processes ensure consistent evaluation. Critical risks are tracked in real time, while strategic indicators are reviewed periodically to support long-term planning.

Governance frameworks ensure that monitoring results in action. Clear accountability structures, escalation protocols, and integration with leadership decision-making enable timely and informed responses.

Board-level oversight, particularly in areas such as ESG, financial exposure, and operational risk, ensures alignment between risk management and organisational strategy.

Effective governance maintains a dynamic risk view, linking monitoring, analysis, and strategic decision-making. This enables organisations to respond proactively to emerging risks while sustaining operational resilience and long-term value creation.

5.7 Oil & Gas Industry

About the researchers

Dr. Shivdasini S. Amin

Head of the Global Centre for Enterprise Risk Management at Mahindra University

Dr. Shivdasini S. Amin is a distinguished academic leader, Professor, and Master Certified Coach (MCC-ICF), ACTC with over 25 years of experience spanning higher education, leadership development, organisational behaviour, and enterprise risk management. She currently serves as the Head of the Global Centre for Enterprise Risk Management at Mahindra University, where she drives research, industry partnerships, and academic innovation. She is also the head of the department of humanities and social sciences at Mahindra University. She is recognised among the world's most influential coaching leaders, she has coached senior executives, mentored doctoral scholars, and led transformative initiatives across academia and industry. Her work is guided by a deep commitment to developing human potential, fostering institutional excellence, and creating meaningful impact through leadership, learning, and research.

Akshaya Buri

Bachelor of Business Administration (BBA) degree from Mahindra University
IRM level 1 certified professional

Akshaya Buri is a student of Bachelor of Business Administration (BBA) degree from Mahindra University, and is currently affiliated with D.E. Shaw. She is an IRM level 1 certified professional, and her interests include enterprise risk management, business strategy, and industry research. She contributed to the development of risk registers and mitigation frameworks for the Oil & Gas, Hospitality, Tourism, Retail, and Media sectors, with a focus on identifying emerging risks and evaluating their potential impact on the Indian business environment.

5.7.1 Oil & Gas

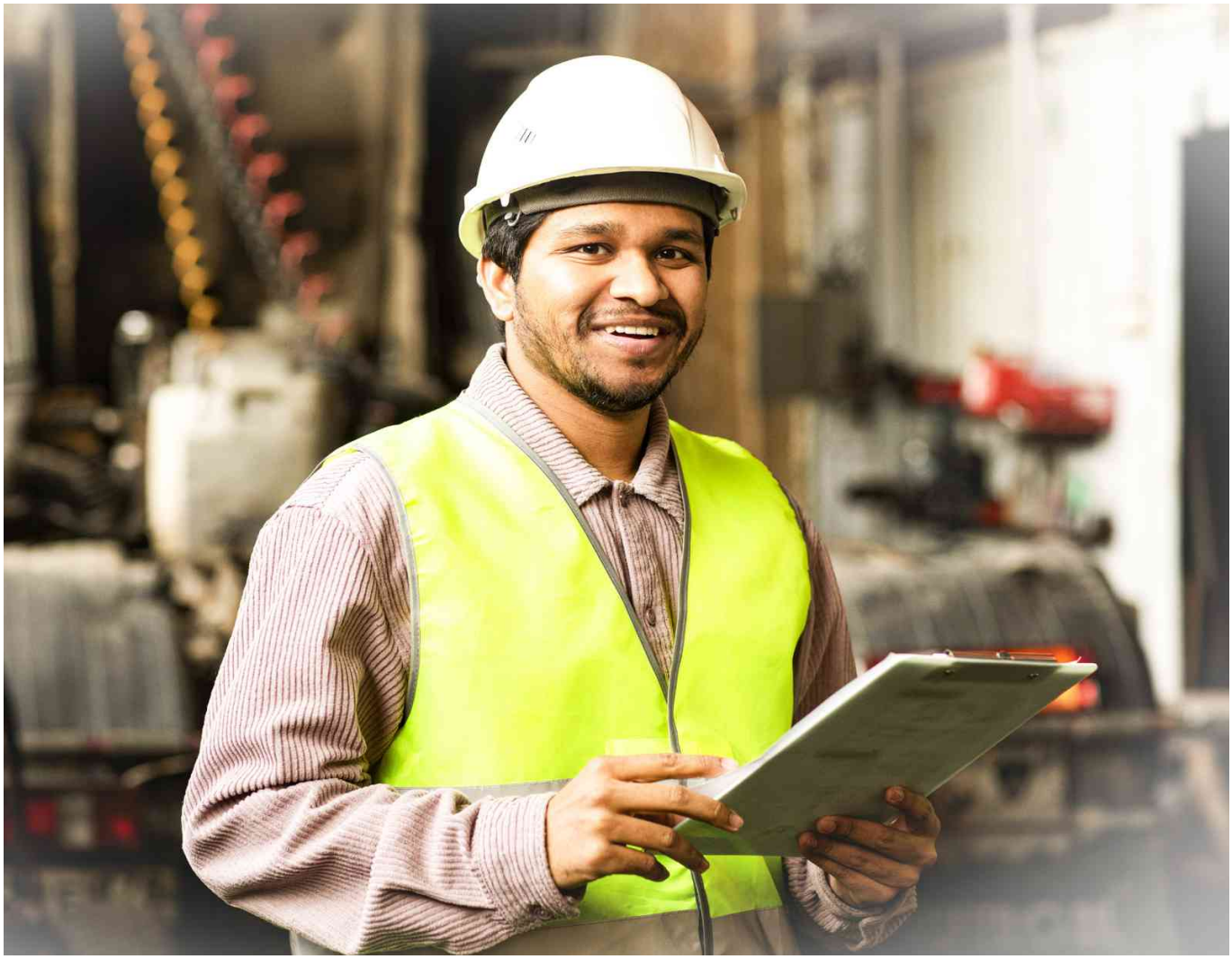
5.7.1.1 Overview

The oil and gas sector remains a cornerstone of global and national energy systems, playing a critical role in supporting economic activity, industrial production, and energy security. It underpins key value chains including transportation, manufacturing, power generation, petrochemicals, fertilisers, and aviation, making it central to both economic growth and infrastructure stability. In India, the sector is particularly significant given the country's position as one of the world's largest energy consumers and its substantial dependence on imported crude oil and natural gas.

The sector encompasses upstream exploration and production, midstream transportation and storage, LNG import infrastructure, and downstream refining, petrochemical processing, and fuel distribution. It operates through a highly interconnected network of pipelines, refineries, storage facilities, ports, and transmission systems. Episodes of global oil price volatility and supply disruptions have highlighted the sector's exposure to geopolitical and market -driven shocks, where disruptions at any stage—exploration, transport, refining, or distribution—can rapidly propagate across the value chain and into broader economic activity.

The industry is characterised by high capital intensity, technological complexity, and geographic dispersion, with operations spanning both offshore and onshore environments. It is also undergoing significant transformation driven by energy transition policies, decarbonisation commitments, renewable energy expansion, and increasing investor focus on environmental, social, and governance (ESG) performance. At the same time, the growing digitisation of operations—including SCADA systems, advanced monitoring tools, and integrated digital infrastructure—has enhanced efficiency while introducing new technology-related risks.

The sector operates within a highly dynamic and externally influenced environment shaped by global commodity markets, geopolitical developments, supply chain interdependencies, foreign exchange movements, and regulatory interventions. As a result, risk exposure extends beyond traditional operational concerns to include the interaction of energy security, environmental sustainability, infrastructure resilience, technological dependence, and public trust. A defining characteristic of the sector is the interdependent nature of these risks, where developments in one domain often produce cascading effects across multiple dimensions of performance.



5.7.1.2 Key Risk Themes

The oil and gas sector faces a complex and multidimensional risk landscape shaped by geopolitical exposure, operational hazards, environmental pressures, technological dependence, and structural transition dynamics. These risks are highly inter-connected and often self-reinforcing.

One of the most critical risk dimensions relates to **energy security and import dependency**. The sector's reliance on imported crude oil and LNG exposes it to geopolitical instability, global commodity price volatility, foreign exchange fluctuations, and supply chain disruptions. Events such as conflicts, sanctions, or shipping constraints in key producing regions can rapidly affect input availability and pricing, with downstream implications for inflation, trade balances, and economic stability. Limited domestic substitution capacity further amplifies this exposure, making energy security a foundational strategic concern.

Process safety, operational integrity, and catastrophic event risk remain central to the sector. Activities involving refining, transportation, and storage of hydrocarbons carry inherent hazards, where incidents such as refinery fires, explosions, pipeline failures, or equipment breakdowns can lead to significant loss of life, environmental damage, and prolonged operational disruption. Ageing infrastructure, inadequate maintenance practices, and workforce safety challenges further increase the probability of such events. The asymmetry between relatively low probability and extremely high impact makes these risks particularly critical.

Climate transition and stranded asset risks are becoming increasingly significant. The global shift toward decarbonisation, combined with stricter emissions regulations, ESG compliance requirements, and investor expectations, is reshaping the sector's long-term outlook. Traditional hydrocarbon assets face the **risk of declining valuations, reduced economic lifespans, and constrained financing.** Organisations must balance the need to maintain current energy supply with the imperative to adapt business models and capital allocation strategies to align with evolving sustainability priorities.

Infrastructure resilience and business continuity represent another key risk area. The sector depends on a complex network of physical infrastructure that is increasingly exposed to climate-related disruptions such as floods, cyclones, and extreme weather events, as well as risks related to ageing assets and mechanical failures. The linear and interconnected nature of pipeline and transport networks creates single-point-of-failure risks, where disruptions in pipelines, refineries, storage facilities, or transport systems can interrupt supply chains and affect multiple downstream sectors. Strengthening both physical asset resilience and integrated business continuity planning is therefore essential.

Environmental and community-related risks are also rising in importance. Issues such as air pollution, water contamination, biodiversity impacts, waste management, and land-use conflicts can result in regulatory penalties, litigation, and reputational damage. In addition, community opposition, particularly in environmentally sensitive or densely populated areas, can delay or prevent project execution. Public perception and stakeholder expectations increasingly influence project approvals, operational continuity, and social licence to operate.

Technological risks are expanding as the sector adopts digital systems and integrated operational technologies. Cybersecurity threats targeting critical infrastructure, including SCADA systems, pipeline controls, and refinery operations, pose significant risks to operational continuity and safety. Failures in digital monitoring systems, data integrity issues, and implementation challenges in digital transformation programmes further increase exposure. Given the critical nature of energy infrastructure, such risks also carry broader national security implications.

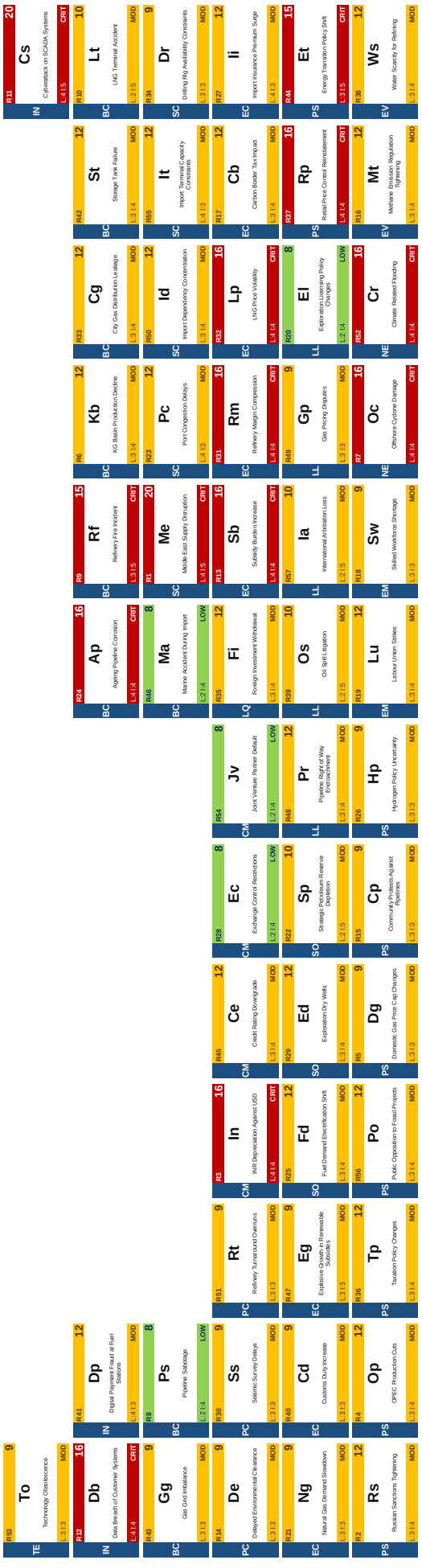
Regulatory, governance, and compliance risks remain a defining feature of the sector. Oil and gas operations are subject to extensive regulatory oversight across environmental, safety, financial, and operational domains. Risks related to regulatory changes, environmental litigation, disclosure requirements, permitting delays, and governance failures can significantly affect operational flexibility and investment decisions. Increasing scrutiny from regulators, investors, and civil society further heightens the importance of transparent governance and strong internal controls.

Financial risks continue to play a central role, driven by volatility in crude oil and LNG prices, currency fluctuations, refining margin compression, and subsidy or pricing interventions. These factors create uncertainty in revenue streams and profitability, complicating long-term financial planning and capital allocation.

The oil and gas sector operates within a highly interconnected risk environment where geopolitical developments, operational failures, environmental pressures, technological disruptions, and regulatory actions interact closely. Disruptions—such as supply shocks, infrastructure failures, or regulatory interventions—can rapidly propagate across energy markets, industrial production, and broader economic systems.

Sustained performance depends on how effectively organisations align operational safety, energy security, infrastructure resilience, environmental stewardship, digital security, and financial discipline while maintaining stakeholder trust during both short-term disruptions and long-term transition pressures.

5.7.1.3 The Periodic Risk Table



5.7.2 Mitigation Strategies

5.7.2.1 Prevention (Risk Avoidance and Reduction)

Prevention strategies in the oil and gas sector are designed to reduce exposure to high-impact risks by strengthening operational systems, diversifying supply sources, and embedding financial and environmental controls into core processes.

A key focus area is supply chain resilience, particularly in mitigating geopolitical risks. Organisations diversify crude sourcing across regions, maintain strategic inventory buffers, and establish flexible logistics arrangements to reduce dependency on specific supply routes. These measures help ensure continuity of operations even during disruptions in global energy markets.

Operational risk prevention is driven by asset integrity and maintenance systems, including predictive maintenance, inspection protocols, and real-time monitoring. Advanced techniques such as thermographic inspections, intelligent pipeline monitoring, and structural integrity assessments help identify potential failures before they escalate into incidents.

Environmental risk mitigation is achieved through implementation of sustainability and compliance controls, including emission monitoring, water recycling systems, and infrastructure upgrades to withstand climate-related risks. Preventive measures also include methane leak detection systems and low-emission technologies to meet regulatory requirements.

Financial risks are mitigated through hedging strategies, long-term supply agreements, and pricing models that reduce exposure to volatility in crude prices, LNG markets, and currency fluctuations. Treasury controls and exposure limits further support financial stability.

Technological risk prevention focuses on cybersecurity and system architecture, including segregation of operational and enterprise systems, access controls, and continuous monitoring. These measures reduce the likelihood of cyber intrusions and system manipulation.

Overall, prevention strategies aim to build structural robustness across operations, supply chains, and financial systems, reducing the likelihood of major disruptions.

5.7.2.2 Detection (Monitoring and Early Warning Systems)

Detection mechanisms in the oil and gas sector rely on real-time monitoring systems and clearly defined metrics to identify emerging risks at an early stage. Given the scale and complexity of operations, early warning systems are critical in preventing escalation of risks into large-scale disruptions.

Operational risks are tracked through indicators such as equipment performance, inspection results, and incident trends, enabling early detection of potential failures. Metrics such as equipment vibration levels, corrosion rates, and inspection anomalies help identify underlying issues.

Supply chain risks are monitored through indicators such as inventory levels, shipping delays, and market price movements. Tracking metrics such as crude inventory coverage and freight disruptions provides early signals of supply stress.

Financial risks are detected through monitoring of price trends, exchange rate movements, and margin indicators. Metrics such as refining margins, hedge coverage levels, and exposure limits provide insight into financial vulnerability.

Environmental risks are monitored through data from weather systems, emission tracking, and compliance reporting. Indicators such as rainfall intensity, emission levels, and regulatory alerts enable proactive management of environmental exposure.

Cyber and technological risks are detected through continuous monitoring systems such as SIEM dashboards and intrusion detection tools. Metrics such as unauthorised access attempts and system anomalies provide early warning of potential cyber incidents.

Overall, detection systems are designed to provide continuous visibility across operational, financial, and environmental domains, enabling timely intervention.

5.7.2.3 Response (Incident and Crisis Management)

Response strategies in the oil and gas sector focus on rapid containment, operational continuity, and mitigation of financial and environmental impact. Given the potential scale of disruptions, response mechanisms must be highly structured and coordinated.

Operational incidents such as fires, spills, or equipment failures are managed through emergency response protocols, including shutdown procedures, containment systems, and trained response teams. Rapid response is critical in limiting damage and ensuring safety.

Supply disruptions are addressed through activation of contingency arrangements, including alternative sourcing, re-routing of shipments, and utilisation of strategic reserves. These actions help maintain supply continuity during disruptions.

Financial response mechanisms include utilisation of insurance coverage, hedging instruments, and liquidity buffers to manage the economic impact of disruptions.

Environmental incidents are managed through coordinated response measures, including containment, remediation, and

regulatory reporting. Effective response helps reduce environmental damage and legal exposure.

Cyber incidents are addressed through incident response plans, including system isolation, recovery protocols, and forensic investigation, ensuring minimal disruption to critical operations.

Stakeholder communication, particularly with regulators, partners, and customers, plays a key role in maintaining trust and managing the reputational impact of incidents.

5.7.2.4 Resilience (Recovery and Adaptive Capability)

Resilience in the oil and gas sector is built through the ability to recover from disruptions while adapting to evolving risk conditions, particularly in the context of energy transition and geopolitical volatility.

Structural resilience is achieved through diversified supply chains, redundant infrastructure, and robust asset design, ensuring continuity even in adverse conditions such as extreme weather or supply shocks.

Financial resilience is supported by effective capital management, hedging strategies, and access to credit, enabling organisations to absorb market volatility and maintain operations.

Operational flexibility plays a critical role, allowing organisations to adjust production levels, optimise refining configurations, and reallocate resources based on market conditions and disruptions.

A key dimension of resilience is strategic adaptation, particularly in response to energy transition. Investments in alternative energy, petrochemicals, and low-carbon technologies enable organisations to adapt to changing demand patterns and regulatory expectations.

Learning and continuous improvement, through post-incident analysis and system enhancements, further strengthen resilience over time.

5.7.2.5 KRIs and Governance

Key Risk Indicators and governance frameworks are central to effective risk management in the oil and gas sector, providing structured oversight and enabling proactive decision-making.

KRIs are used to monitor a wide range of risk factors, including operational performance, supply chain stability, financial exposure, environmental compliance, and cybersecurity. These indicators are supported by multiple data sources, including operational systems, market intelligence platforms, and regulatory feeds.

Defined review frequencies ensure continuous monitoring of critical metrics, with high-risk areas such as safety and cybersecurity tracked in real time, while financial and strategic metrics are reviewed periodically.

Governance structures ensure that risk insights are translated into action through clear accountability, escalation mechanisms, and integration with organisational decision-making processes. Board-level oversight, particularly in areas such as ESG and financial risk, ensures alignment with long-term strategy.

Effective governance enables a dynamic and forward-looking approach, where monitoring, analysis, and decision-making are continuously integrated, allowing organisations to manage risk proactively in a complex and evolving environment.

Infrastructure, Manufacturing, Energy, Mining, & Oil & Gas

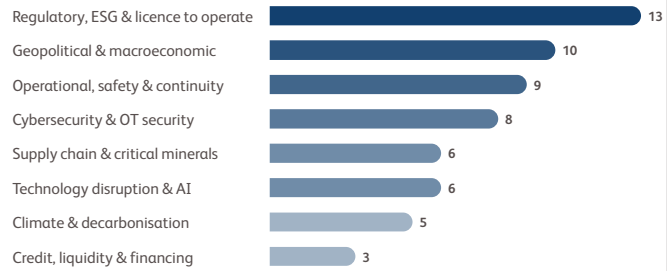
12
RESPONDENTS

83%
SAY THEY ARE GROWING
Power and one Real Estate respondent report Stable

3.8/5
AVG RISK EXPOSURE
8 rate 4 . 3 rate 3 . 1 rates 5

~5%
MEDIAN RESOURCES TO RISK MGMT
Range 0.9-12.5%

What keeps these industries up at night - top-five risk mentions



60 mentions = 12 respondents × 5 risks each

Risk appetite - segment average by dimension

FINANCIAL	OPERATIONAL	REGULATORY	STRATEGIC
3.1/5	2.1/5	2.0/5	3.7/5
Moderate	Low	Low	Mod-High
from 10 stated answers	from 8 stated answers	from 10 stated answers	from 10 stated answers

A low score means the segment has little appetite for that type of risk-failures there are treated as unacceptable and are tightly controlled rather than taken on. A high score means the segment is willing to accept more of that risk in pursuit of growth, innovation and returns.

Crisis preparedness self—assessed, by segment

Large corporates-event-driven crises	High
Power & utilities (grid, outages)	Mod-High
Mid-size infra & contractors	Moderate
Systemic, long-horizon risks	Maturing

The risk outlook - what's rising now, what's coming next

RISING FASTEST . LAST 3 YEARS

- Cyber-physical / OT exposure
- Climate as an immediate operating issue
- Supply chains, semiconductors & critical minerals
- Geopolitics & trade restrictions
- Regulatory & ESG pressure

EMERGING . NEXT 3-5 YEARS

- Decarbonisation & carbon pricing
- Storage economics & grid flexibility
- Cyber-physical OT attacks
- Critical minerals & battery supply
- Technical talent attrition
- Social licence to operate
- Trade restrictions & protectionism
- Climate adaptation & water stress
- Software-defined vehicle risk

Driven by: Energy transition & decarbonisation pressure; Geopolitics, trade & critical-mineral concentration; Rapid digitalisation of operations & OT; Regulatory & ESG intensification.

How far ahead these industries plan

0 - 2 years	Safety, outages, commodity prices, cyber events
3-5 years	Most actionable board window — regulation, transition, execution
5-15 years +	Climate, resource depletion & social licence

The dependency chain - what operations cannot run without

1. Power, fuel & water supply
2. Rail, ports & logistics corridors
3. Permits, approvals & community consent
4. Critical-mineral & equipment suppliers
5. Contractors & EPC partners
6. Telecom, cloud & OT technology vendors

11 of 12 report collaborations, but effectiveness diverges sharply - from "very good" to "negligible"; strongest on safety and ESG standards, weakest on emerging long-horizon risks.

From gaps to action

WHAT'S MISSING TODAY

- ✕ Skilled technical & project-risk talent
- ✕ Integrated real-time data & early warning
- ✕ Cyber-OT expertise
- ✕ Climate modelling & scenario planning
- ✕ Barrier: Fragmented vendors & uneven maturity

WHAT WOULD CLOSE THE GAP

- ✓ Faster approvals & clearer long-term policy signals
- ✓ Shared data standards & threat intelligence
- ✓ Storage, grid & climate-resilient capex
- ✓ Skilled project, safety & cyber-OT talent
- ✓ Industry-government resilience forums

Already in play: Predictive asset management, Supplier & geographic diversification, Cyber-OT hardening, Climate-resilient design.

The agenda - what these industries say they must do next

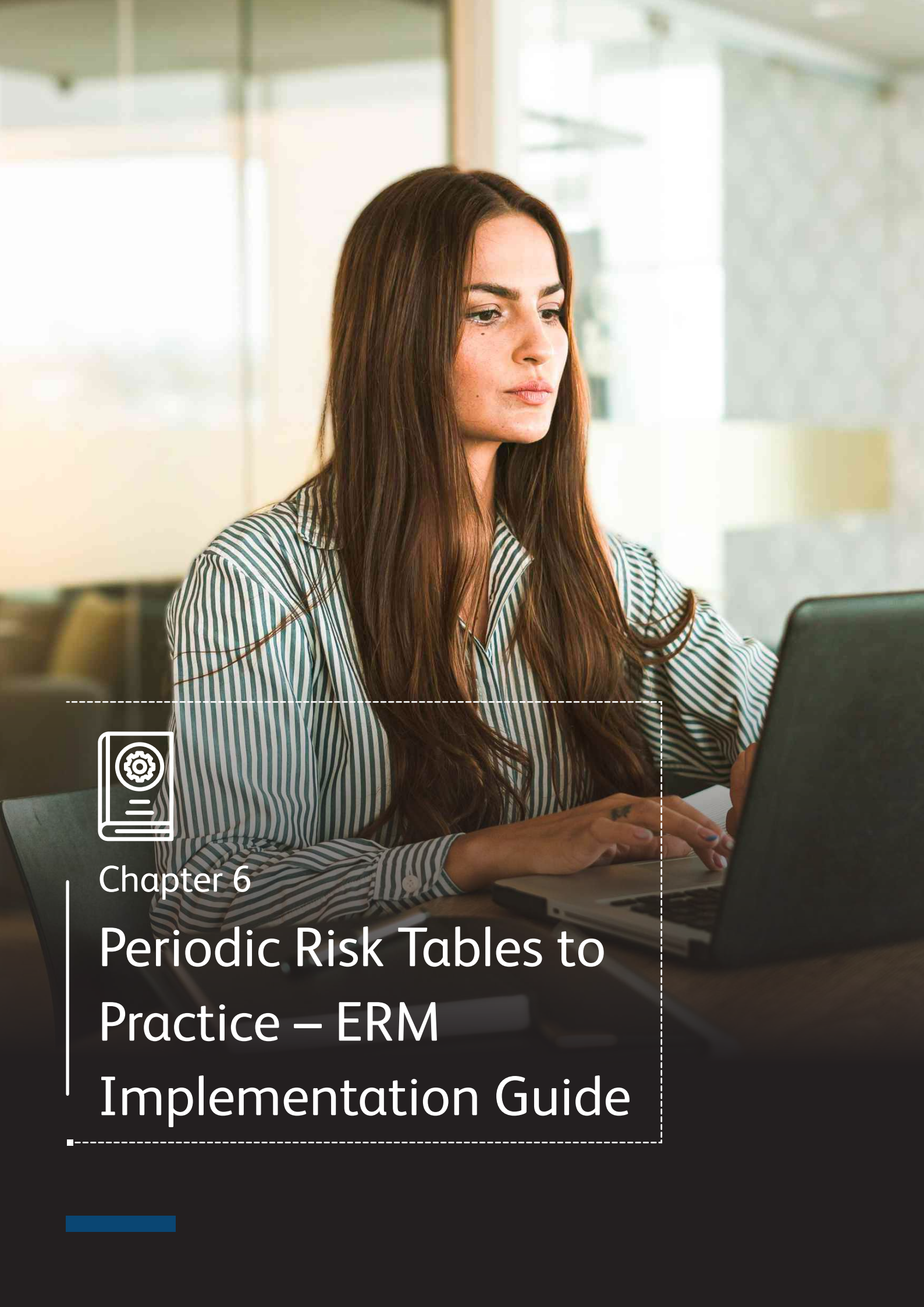
TOP COMPLIANCE PRIORITY
Keeping pace with regulatory change
then: Active board oversight

MOST PRESSING SHARED CHALLENGE
Strengthening third-party oversight
then: Strengthening governance & culture

#1 FOCUS NEXT 12-24 MONTHS
Accelerating digital transformation
8 of 12 review tolerance limits quarterly

What enables it (importance / 5): Maturity of risk & compliance functions **4.75**. Culture & values **4.75** Continuous risk assessment **4.67** Technology & data **4.42**. **Hardest rules to live with:** Environmental approvals & mine closure; Carbon tax, CBAM & emissions norms; Land, RERA & right-of-way approvals.

"Policy is both enabler and constraint - tariffs, approvals, carbon rules and grid codes shape returns; analytics is shifting from dashboards and SCADA to predictive, AI-assisted risk operations."



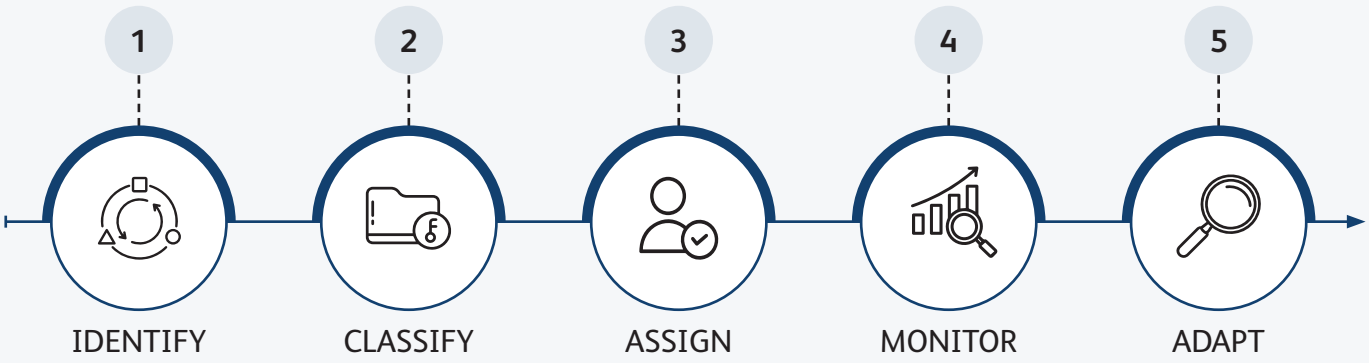
Chapter 6

Periodic Risk Tables to Practice – ERM Implementation Guide

6.1 Embedding Risk Tables in ERM Frameworks

Embedding the Periodic Risk Table (PRT) within an Enterprise Risk Management framework requires a shift from static documentation to a continuously evolving risk management system. Rather than treating risk identification as a one-time exercise, organisations must position the PRT as an active reference point that informs operational, financial, and strategic decision-making.

This is operationalised through a continuous risk lifecycle:



This ensures that risks are systematically recognised, structured, owned, tracked, and dynamically updated over time.

This integration begins by aligning PRT risk categories with existing ERM components, including risk registers, control frameworks, and reporting systems. Each risk is mapped to business units and assigned clear ownership, ensuring accountability is embedded within operational processes rather than centralised within compliance functions.

The strength of the PRT lies in its structured taxonomy, which enables organisations to move beyond fragmented risk identification toward a holistic understanding of interdependencies. By organising risks around underlying drivers—such as technological, environmental, economic, and governance factors—organisations can identify patterns and anticipate emerging exposures.

Embedding the PRT into core processes, including budgeting, strategic planning, and performance management, ensures that risk considerations are integrated into everyday decision-making. This transforms risk management from a compliance activity into a core element of organisational strategy.

6.2 Risk Appetite & Threshold Setting

Risk appetite provides the link between strategic objectives and acceptable risk exposure. The PRT enhances this process by enabling structured, measurable, and consistent definition of risk tolerance across categories.

Organisations can translate risk appetite into quantifiable thresholds linked to Key Risk Indicators, allowing real-time monitoring. Clear bands can be established for acceptable exposure, warning levels, and breach thresholds, ensuring consistency and clarity in decision-making across functions. Examples of such metrics include financial indicators such as Value-at-Risk (VaR) and liquidity ratios to monitor exposure relative to defined appetite levels.

This can be operationalised through a threshold framework, where each risk is continuously monitored across defined zones:

- Green Zone – within appetite
- Amber Zone – early warning
- Red Zone – breach requiring escalation

Risk appetite must remain dynamic. External conditions—such as regulatory changes, economic cycles, or technological disruption—can alter risk capacity. The PRT supports periodic recalibration of thresholds, ensuring alignment with evolving business strategy.

In this way, risk appetite evolves from a static policy into a continuously monitored and actively managed framework.

6.3 Scenario Analysis & Stress Testing

Scenario analysis and stress testing extend the PRT by enabling organisations to examine how risks behave under adverse conditions and how multiple risks interact simultaneously.

Using the PRT structure, organisations can identify key risk drivers and construct scenarios reflecting realistic stress conditions—from isolated events such as cyber incidents to systemic disruptions involving economic downturns and regulatory tightening. This can be further strengthened through reverse stress testing, which starts from a defined failure outcome and works backward to identify the conditions and risk combinations that could trigger such an event.

Stress testing quantifies resilience under these conditions, assessing whether controls, financial buffers, and response mechanisms are sufficient. Importantly, the PRT enables modelling of multi-risk chain reactions—for example, a cyber incident leading to operational disruption, followed by reputational damage and regulatory scrutiny —highlighting how interconnected risks can escalate across domains. These insights help identify vulnerabilities and inform investment, mitigation priorities, and contingency planning.

This approach shifts risk management from reactive response to proactive preparedness, enabling organisations to anticipate and manage complex, multi-risk scenarios.

6.4 Heatmaps vs Periodic Risk Tables

Traditional risk heatmaps provide a simplified view of risk based on likelihood and impact, making them effective for communication and prioritisation. However, they are limited in capturing interdependencies and systemic relationships.

The PRT offers a more structured and analytical perspective by organising risks based on their source, characteristics, and linkages. It enables deeper insight into how risks influence one another across operational, financial, and strategic dimensions.

In practice, both tools are complementary. Heatmaps support executive communication, while the PRT enables deeper analysis and strategic planning. Together, they balance simplicity with analytical depth.

6.5 Building Dashboards & Digital Risk Registers

Effective implementation of the PRT requires digital enablement to support real-time monitoring and data-driven decision-making.

Risk dashboards provide visibility into Key Risk Indicators, trends, and threshold breaches. This is supported by a layered digital architecture comprising data, analytics, and visualisation, where risk information is collected, processed, and presented in an actionable format. By integrating data from internal systems, such as finance, operations, and HR, with external data sources, organisations can maintain a continuously updated view of risk exposure.

Digital risk registers serve as structured repositories capturing risk ownership, controls, and mitigation status. Unlike static registers, these systems are dynamic and integrated with real-time data.

Advanced implementations leverage predictive analytics and automation to identify emerging risks early. At the analytics layer, modelling and predictive tools enable early warning signals, while the visualisation layer translates complex risk data into intuitive dashboards for decision-makers. This transforms risk management into a continuous, forward-looking capability, enhancing organisational responsiveness and resilience.

6.6 Governance: Roles of Board, CRO & Risk Committees

Effective governance is critical to embedding the PRT within organisational processes.

The Board provides strategic oversight, defines risk appetite, and ensures alignment between risk exposure and long-term objectives. Its role is to maintain visibility over key risks and ensure integration into decision-making at the highest level.

The Chief Risk Officer operationalises the framework, maintaining the PRT, ensuring consistency across functions, and translating risk insights into actionable guidance for leadership.

Risk committees provide cross-functional coordination, reviewing risk reports, monitoring indicators, and evaluating mitigation strategies. Threshold breaches automatically trigger reporting to the risk committee, with predefined response timelines to ensure timely escalation and coordinated action. Their role is to ensure an integrated and timely response across organisational units.

Together, these structures establish accountability, alignment, and continuous oversight.

6.7 Implementation of the Toolkit

6.7.1 Purpose of the Toolkit

The purpose of the PRT Implementation Toolkit is to translate the conceptual framework into a structured, operational system embedded within organisational processes.

It enables organisations to move from risk identification to execution by linking ownership, controls, monitoring, and continuous improvement. This addresses a key limitation of traditional ERM systems, where risks are documented but not actively managed.

6.7.2 Step-by-Step Implementation Framework

Implementation begins with structuring risks using the PRT, mapping them to specific organisational contexts, business models, and operational realities.

The next step is assigning ownership, embedding accountability within business units rather than central compliance functions.

Risks are then translated into measurable constructs through Key Risk Indicators and thresholds, enabling data-driven monitoring and decision-making.

Mitigation strategies are designed based on risk severity and nature, ensuring appropriate balance between prevention and response, with attention to cost-effectiveness.

The framework is then integrated into digital systems to enable real-time monitoring, automated alerts, and seamless reporting.

Finally, continuous review and feedback loops ensure that the system evolves with changing business and external conditions.

6.7.3 Integration into Governance Framework

Effective implementation requires alignment with governance structures at all levels.

Risk ownership must align with organisational hierarchy, ensuring risks are managed where decisions are made. Clear reporting and escalation mechanisms ensure timely communication of risk exposure.

Integration with existing processes—such as audit, compliance, and strategic planning—ensures that risk management is embedded in key decisions rather than treated as a standalone activity.

This transforms the PRT into a central tool for organisational oversight and accountability.

6.7.4 Technology & Data Enablement

Technology is fundamental to operationalising the PRT, enabling scale, integration, and real-time insight.

Integrated data systems connect internal and external data sources, ensuring accurate and timely inputs for KRIs. Visual dashboards allow stakeholders to monitor trends and identify anomalies efficiently.

Advanced organisations incorporate automation and predictive analytics to identify emerging risks, enabling early intervention.

Strong data governance ensures the reliability and integrity of information, which is critical for effective risk management.

6.7.5 Output of the Toolkit

- The PRT toolkit generates a set of structured outputs that strengthen decision-making.
- These include dynamic risk registers, real-time dashboards, clearly defined risk appetite frameworks, and scenario-based insights into organisational resilience.
- Collectively, these outputs enable organisations to move beyond documentation toward actionable, data-driven risk management.

6.7.6 Key Success Factors

Successful implementation depends on several critical factors.

Leadership alignment ensures that risk management is embedded within strategic priorities. Integration into business processes ensures that the framework is actively used rather than passively maintained.

Data quality and system reliability underpin effectiveness, requiring strong governance and accountability.

Equally important is the establishment of clear ownership structures and a risk-aware culture. Employees must actively engage with risk identification and management.

When these elements are in place, the PRT becomes a dynamic capability that supports resilience, adaptability, and long-term value creation.

Chapter 7

Case Studies

Overview

The distance between a well-designed ERM framework and genuinely resilient organisations is not measured in policy documents or risk registers. It is measured in decisions, behaviours, and the lived experience of risk practitioners across industries. This chapter bridges that gap by grounding enterprise risk management principles in India-specific sector realities, exploring the strategic value of the Periodic Risk Table as a governance and communication tool, and distilling the most consequential lessons and good practices that separate organisations where ERM is a genuine performance lever from those where it exists as a compliance artefact.

About the researcher

Prof. Swanand Kopardekar

Faculty Chair - Enterprise Risk Management with IRM India Affiliate

Prof. Swanand Kopardekar works as Faculty Chair - Enterprise Risk Management with IRM India Affiliate. He has a rich experience of 26 years and has worked in the BFSI sector, Mobility Services, Education and Realty Sector

A seasoned Enterprise Risk Management (ERM) professional with experience in designing, implementing, and strengthening risk management frameworks across the BFSI and real estate sectors. He possesses deep expertise in integrating risk management with strategic decision-making, process improvement, and operational excellence to enhance organisational resilience.

He is also recognised for developing and delivering high-impact ERM, governance and compliance training programs, while building organisational capability through knowledge management, customised learning solutions, and best-practice sharing. He is adept at designing risk management frameworks, policies, and business process improvement initiatives aligned with organisational objectives.

7.1 India-Specific Sector Case Studies

The methodological basis for these case studies, including their composite construction, masking approach, and review process, is set out in Section 3.13.

Case Study A

Pharmaceutical and Life Sciences: API Supply Chain Concentration Risk

Sector: Pharmaceuticals / Life Sciences

Background: A listed Indian pharmaceutical company with significant exports to regulated markets in the US and EU had built its competitive advantage on cost-efficient Active Pharmaceutical Ingredient (API) procurement, with over 70 % of key APIs sourced from a concentrated cluster of Chinese suppliers. The strategy delivered strong margins through an extended period of stable global trade — and embedded a significant concentration risk that remained unquantified.

The Risk Challenge: When India imposed export restrictions on certain antibiotics in early 2020 —a response to domestic availability pressures — the company simultaneously faced API price volatility, US FDA drug shortage alerts for amoxicillin and penicillin (an 18 percentage-point increase in reported shortages), and disrupted Red Sea shipping lanes that extended lead times by 12 days on Europe-to-Asia lanes. The three risk events arrived simultaneously, exposing the inadequacy of single-tier supplier mapping.

The Response: The company initiated a formal supply chain risk programme anchored on four disciplines: multi-tier supplier mapping down to raw material sourcing, strategic API inventory buffering calibrated at 90 days for critical molecules, an alternative supplier qualification programme targeting Indian and European API manufacturers, and integration of logistics risk (shipping route vulnerability) into the enterprise risk register. A cross-functional Supply Chain Risk Committee was established with representation from procurement, regulatory affairs, finance, and the CRO's office.

Outcome and Lesson: As supply chain risk researchers confirm, "as much as 85 % of supply disruptions originate with sub-tier suppliers, where many businesses don't have visibility". This company's experience validated that finding precisely. The pivotal insight is that **visibility without actionability is ineffective** — a lesson reinforced by a senior VP at a global biopharma: "We learned that visibility without actionability is useless." Pharma risk management must connect upstream supplier intelligence directly to procurement decision authority.

Case Study B

Fast-Moving Consumer Goods (FMCG): ESG and Reputational Risk Integration

Sector: FMCG / Consumer Products

Background: A leading Indian FMCG conglomerate operating across food, personal care, and home products segments was confronted with an emerging ESG compliance imperative following SEBI's Business Responsibility and Sustainability Reporting (BRSR) framework expansion, which mandated disclosure of supply chain sustainability practices for top-listed companies. The company's existing risk framework had no formal mechanism for ESG risk identification or escalation.

The Risk Challenge: The risk was not merely regulatory — it was reputational and strategic. Consumer research commissioned by the company's marketing team revealed that approximately 60 % of urban Indian consumers under 35 expressed preference for brands with credible sustainability credentials, while investor relations reported growing questions from ESG-oriented institutional investors about supply chain labour practices and carbon intensity in manufacturing operations.

The Response: The company embedded ESG risk as a formal category within its COSO ERM-aligned framework, designating ESG Risk Owners at the business unit level (Risk Champions), supported by a centrally maintained ESG Risk Register. BRSR disclosures were mapped against material risk categories. Supply chain audits were extended to tier-2 agricultural suppliers. The Board's Risk Management Committee took on formal responsibility for reviewing ESG risk trends semi-annually alongside financial and operational risks.

Outcome and Lesson: SEBI's ESG and BRSR requirements are now a governance reality for India's listed companies. The early movers in ESG risk integration — those who treated BRSR compliance as the floor rather than the ceiling — gained measurable benefits in investor dialogue quality and brand positioning. The core lesson: **ESG risk is simultaneously a regulatory, reputational, strategic, and financial risk, and must be governed across all four dimensions, not managed as a standalone sustainability report.**

Case Study C

Information Technology and Business Process Management: Operational Resilience During a Platform Outage

Sector: IT Services / BPM

Background: A large Indian IT services firm delivering critical application management, cloud operations, and data processing services to global banking and insurance clients experienced a third-party platform outage triggered by a software update failure from a major cloud infrastructure provider. The outage lasted approximately nine hours, affecting client SLA commitments across three geographies.

The Risk Challenge: The firm's Business Continuity Plan (BCP) had been designed around individual client engagements — not for a scenario where a shared infrastructure dependency simultaneously disrupted multiple delivery teams serving multiple clients. The cascading nature of the outage exposed a BCP architecture that was insufficiently networked. Regulatory notifications to client banks were delayed beyond contractually agreed timelines.

The Response: Post-incident, the firm redesigned its operational risk governance around a Technology Concentration Risk framework. Cloud provider dependency was quantified at the portfolio level — not just the project level. Multi-cloud fallback capabilities were negotiated into platform contracts. A 24/7 Operational Resilience Watch was established, with defined escalation protocols that could activate cross-client crisis response within 30 minutes of a trigger event. The CRO's office gained visibility into real-time infrastructure health dashboards shared by key platform providers.

Outcome and Lesson: This case illustrates the argument that **technology risk is a horizontal risk driver:** it cuts across all client engagements, all geographies, and all risk categories simultaneously. The firm's experience mirrors a broader sector finding — that ERM must integrate third-party and fourth party risk assessment mapped against critical operational dependencies, not just internal control frameworks.

Case Study D

Infrastructure and Renewables: Geopolitical Supply Concentration and Energy Transition Risk

Sector: Power / Renewable Energy / Infrastructure

Background: An infrastructure development company executing large-scale renewable energy projects across multiple Indian states identified a dependency risk that had been largely invisible in its risk framework: a significant proportion of solar panel components — including polysilicon and solar cells — were sourced through supply chains concentrated in China. With India's commitment to achieving 500 GW of non-fossil fuel energy capacity by 2030, where solar energy is expected to contribute a significant portion, the risk was strategic in nature.

The Risk Challenge: China's imposition of rare earth and critical material export restrictions — broadened through 2024 and 2025 to encompass 12 of 17 rare earth elements — created price volatility and lead-time uncertainty for solar components. Although China expanded the controls in October 2025 by adding five additional element, the Chinese Ministry of Commerce suspended most of these October measures for one year beginning 10 November 2025, with the suspension remaining in effect until 10 November 2026. Simultaneously, India's domestic PLI (Production-Linked Incentive) scheme for solar manufacturing created a policy window for supply chain localisation — but the window required capital commitment decisions with long lead times, which the company's existing risk framework was not equipped to support.

The Response: The company integrated geopolitical supply risk as a standalone risk category in its strategic risk register, alongside climate risk and execution risk. A Supply Chain Resilience Scorecard was developed for key component categories, measuring concentration risk (single-source percentage), geographic diversity, and alternative supplier readiness time. The Scenario Planning team modelled three supply disruption scenarios — mild, moderate, and severe — and used the outputs to guide procurement contract structuring and capital allocation.

Outcome and Lesson: India's infrastructure ambitions create a direct intersection between geopolitical risk and strategic execution risk. Morgan Stanley projects India's infrastructure investment to rise from 5.3 % of GDP in FY24 to 6.5 % by FY29 — a scaling trajectory that amplifies supply concentration risk proportionally. **Geopolitical risk must be integrated into infrastructure project risk registers at the strategic design stage, not as a reactive disclosure after procurement decisions are made.**

7.2 The Periodic Risk Table: Applications Across Governance Roles

Concept and Rationale

The Periodic Risk Table is a structured visual intelligence tool—modelled on Mendeleev's periodic table—that classifies risk elements within a specific sector into discrete, navigable categories. Unlike conventional risk registers that present risks as linear lists, the Periodic Risk Table illustrates risk as an ecosystem. This approach enables the recognition of systemic connections, cluster vulnerabilities, and patterns of interaction, surfacing the relative weight of different risk families within a sector.

As applied in IRM India's sector-specific frameworks, the Periodic Risk Table is designed not as a technical document for risk specialists but as a governance communication and decision-support instrument for diverse stakeholders — from board directors to process owners — each with distinct risk responsibilities and decision contexts. The table also functions as a training and risk culture tool, creating a shared vocabulary for risk across functions and hierarchies.

The following section articulates how different governance stakeholders can derive distinct, role-calibrated value from the Periodic Risk Table.

For the Board of Directors

Primary Application: Strategic Risk Oversight and Horizon Scanning

The board's risk oversight responsibility operates at the level of strategy, enterprise resilience, and stakeholder accountability, rather than at the operational level of individual risk events. The Periodic Risk Table supports the board by providing a sector-level map of the risk terrain, enabling directors to ask more penetrating questions, such as:

- Which risk families are structurally most significant in this sector?
- Where do we have genuine exposure concentration?
- Which emerging risk elements are not yet on the management risk register but appear on the sector periodic table?

According to the NC State 2025 State of Risk Oversight report, 61 % of executives report rising risk complexity, yet only 32 % rate their risk oversight as mature or robust. Furthermore, only 11 % believe their Enterprise Risk Management (ERM) processes offer a strategic advantage.

The Periodic Risk Table addresses this gap by translating the complex risk landscape into a structured, visual format. This allows directors to engage with risk at a strategic level without requiring technical expertise.

Specific use cases for the Board:

- Annual strategy reviews: map strategic assumptions against relevant risk elements on the sector periodic table to identify unaddressed exposures
- Board risk appetite calibration: use the periodic table to ground risk appetite discussions in the actual composition of sector risk, not abstract tolerance statements
- Horizon scanning: identify risk elements at the frontier of the periodic table (emerging risks) that are not yet reflected in the management risk register
- Peer governance comparison: assess whether the organisation's risk register covers the full spectrum of elements present in the sector table

For the Chief Risk Officer (CRO)

Primary Application: ERM Architecture, Risk Portfolio Management, and Risk Intelligence

The CRO derives strategic value from the Periodic Risk Table as a risk architecture reference — a structured catalogue that ensures the ERM framework is comprehensive (covering all relevant risk families for the sector), coherent (organising related risks into logical groupings), and current (incorporating emerging risk elements as they crystallise from theoretical to material). It prevents the common ERM failure mode of framework incompleteness — where risks not on the periodic table are not registered, not owned, and not managed.

As ERM research confirms, "the CRO role is critical in times of stress, but effectiveness depends on CEO and board support, culture, and incentives". The Periodic Risk Table supports CRO effectiveness by providing a common reference framework that facilitates constructive dialogue with the Board and the CEO — moving ERM reporting from descriptive risk listing to analytical risk portfolio management.

Specific use cases for the CRO:

- Framework design and gap analysis: benchmark the current enterprise risk register against the sector periodic table to identify coverage gaps
- Risk interconnection mapping: use the periodic table's groupings to develop risk interconnection matrices that reveal cascade pathways between risk families
- Risk appetite calibration: structure the risk appetite statement around the periodic table's risk families rather than generic categorical tolerances
- Emerging risk integration: use the periodic table as a structured onboarding path for new risk categories (AI risk, climate transition risk, geopolitical supply risk) as they enter the sector landscape

For the Risk Management Committee (RMC)

Primary Application: Portfolio Risk Review, Risk Aggregation, and Escalation Governance

The Risk Management Committee (RMC) maintains an enterprise -wide view to ensure that risks identified at the functional and business unit levels aggregate into a coherent portfolio for organisational governance. The Periodic Risk Table serves as an aggregation scaffold for the RMC, providing a structured reference to determine if escalated risks cover the full landscape of material risk elements within the sector, or if certain risk families are being systematically under-reported.

A critical and recurring ERM failure is that "boards receive information, not insight — reports may focus on listing risks rather than explaining their interconnections, trends, and potential impact on strategy". The Periodic Risk Table counters this by providing the RMC with a structured basis for cross-risk trend analysis: comparing this quarter's risk heat map against the full periodic table reveals not only which risks are hot but which elements of the landscape are conspicuously absent — a possible signal of under-reporting or emerging blind spots.

Specific use cases for the RMC:

- Quarterly portfolio review: use the periodic table as a check-list reference to assess coverage completeness across all risk families
- Escalation protocol design: define escalation triggers by risk family and element, rather than by generic severity thresholds alone
- Cross-functional risk correlation: identify when risk events reported by different business units belong to the same periodic table cluster — signalling a systemic risk rather than isolated incidents
- Annual framework refresh: use the periodic table to structure the annual ERM framework review, ensuring new elements are incorporated and obsolete ones are retired

For Risk Champions

Primary Application: Functional Risk Identification, Training, and Risk Culture Building

Risk Champions — embedded within business functions as the front line of the risk culture — derive the most immediate practical value from the Periodic Risk Table as a risk identification guide and training scaffold. The periodic table gives Risk Champions a structured taxonomy for their function's risk landscape: it translates the abstract language of ERM frameworks into a concrete, sector-specific vocabulary of risk types that functional teams can recognise and articulate.

Risk capability gaps are one of the most consequential sources of ERM failure — "risk registers are filled with vague statements; impact and likelihood are scored inconsistently; emerging risks are misunderstood or ignored". The Periodic Risk Table mitigates this by providing a shared reference point that anchors risk identification workshops, self-assessments, and risk escalation discussions in a common language.

Specific use cases for Risk Champions:

- Risk identification workshops: use sector periodic table elements as structured prompts for bottom-up risk identification at the function or process level
- New joiner onboarding: introduce the periodic table as a risk literacy tool for new employees entering risk-relevant roles
- Risk culture initiatives: display the sector periodic table visibly within the function as a daily reminder of the organisation's risk landscape
- Emerging risk early warning: Risk Champions with front-line exposure are often the first to observe signals of risks that are not yet on the formal register — the periodic table provides a framework for naming and escalating these observations

For Process Owners

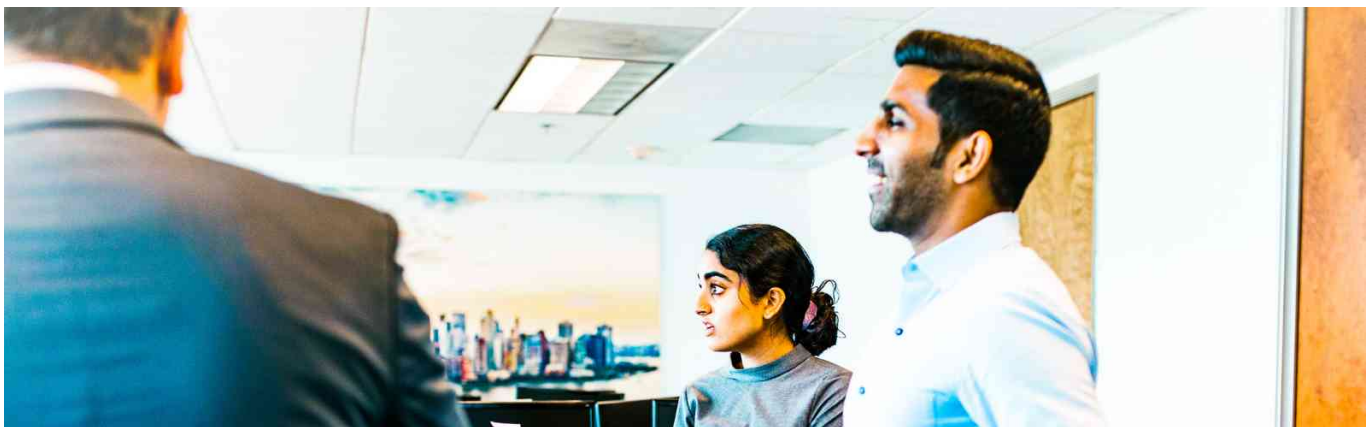
Primary Application: Process-Level Risk Assessment and Control Design

The Periodic Risk Table serves as a process risk scanning tool for Process Owners, who hold direct accountability for the efficiency, compliance, and resilience of operational workflows. It enables them to systematically identify relevant risk elements and evaluate the adequacy of existing controls.

This tool is particularly valuable for operational leaders who manage material risk exposure but may lack formal risk training. By converting expert ERM framework knowledge into an accessible, visual format, the periodic table allows non-specialist Process Owners to engage meaningfully with risk management.

Specific use cases for Process Owners:

- Process risk mapping: cross-reference process activities against relevant periodic table elements to identify unmitigated exposures
- Control effectiveness review: assess whether existing controls address the risk elements most material to the process, rather than solely the risks that have historically occurred
- Change management risk assessment: when processes are redesigned or digitised, use the periodic table to scan for newly introduced risk elements
- Incident investigation: when control failures occur, use the periodic table's taxonomy to classify the event and identify related risk elements that may be implicated



For the CEO and Other CXOs

Primary Application: Strategic Decision-Making, Capital Allocation, and Opportunity-Risk Calibration

The CEO and senior CXOs require risk intelligence that is directly connected to strategy execution, rather than reports that catalogue threats without linking them to key decisions. The Periodic Risk Table serves the CEO by providing a strategic landscape that contextualises the risk portfolio within the broader universe of material sector risks. This enables critical oversight: Are we investing disproportionately in visible risks while underpreparing for less familiar ones? Are our strategic bets exposed to risk elements underrepresented in our current framework?

McKinsey's board-level ERM research identifies a foundational principle that applies equally to the CEO: "risk should be seen not as an obstacle to performance, but as a variable to be actively managed in service of strategic objectives". The Periodic Risk Table operationalises this principle by making the full portfolio of risk elements legible — enabling strategic conversations about where to accept risk, where to mitigate, and where risk concentration is inconsistent with the organisation's strategic intent.

Specific use cases for CEO and CXOs:

- Strategic planning integration: use the sector periodic table to stress-test strategic plans against the full risk landscape, not just the risks already in the register
- M&A and investment decisions: assess whether target organisations or new markets introduce risk elements not currently covered in the acquirer's ERM framework
- Innovation and growth risk calibration: identify which risk elements are associated with proposed new business models or digital transformation initiatives
- Stakeholder communication: use the periodic table to frame risk disclosures to investors, regulators, and boards in structured, sector-contextualised terms rather than generic risk categories

7.3 Lessons Learned and Good Practices

The following lessons are drawn from the convergence of sector case study evidence, the 2025 NC State State of Risk Oversight report findings, IRM India's practitioner experience, and the global ERM research base. They represent the most consequential differentiators between organisations where ERM generates strategic value and those where it generates compliance documentation.

Lesson 1: ERM Frameworks Without Risk Culture Are Compliance Theatre

Perhaps the single most replicated finding across global and India-specific ERM research is that framework design is not the binding constraint on ERM effectiveness. The binding constraint is culture. As IRM India's own analysis confirms: "A strong ERM framework cannot compensate for a weak risk culture. If people fear consequences for escalation or believe that raising risks is unwelcome, the framework will remain ineffective, regardless of its design".

The pattern is consistent: organisations that experienced significant risk failures — despite having formally documented ERM frameworks — were characterised by cultures in which early warning signals were filtered by middle management, risk ownership was nominal rather than accountable, and performance incentives rewarded results over risk discipline. The corollary is equally important: organisations with strong risk cultures — where raising risks is encouraged, escalation is expected, and uncomfortable truths are welcomed — outperform on resilience even when their formal frameworks are less sophisticated.

Good Practice: Embed risk culture indicators — escalation rates, near-miss reporting volumes, risk-adjusted performance metrics — into leadership assessments and performance frameworks. Culture is behaviourally measurable; measure it.

Lesson 2: Risk Registers Are Not Risk Management

A risk register is a record, while risk management is a process. Confusing the two is a persistent dysfunction in ERM implementation. Risk registers created annually for regulatory or audit purposes often exist only to satisfy reporting requirements rather than to guide decisions. When operational and strategic decisions proceed independently of documented risk assessments, the ERM framework serves a documentation function instead of a governance function.

The NC State 2025 ERM report's finding is stark: only 30% of organisations integrate risk exposure into capital allocation decisions, and only 27% say their ERM process helps manage reputation-impacting risks. These figures suggest that for the majority of organisations, ERM and decision-making remain structurally decoupled.

Good Practice: Apply the "decision test" to every risk report and risk register entry: "Does this information change a question we ask, a decision we make, or an action management takes?" If the answer is consistently no, the risk process needs redesign — not more documentation.

Lesson 3: Risk Ownership Must Be Real, Not Nominal

Clear, accountable, and empowered risk ownership is a structural prerequisite for effective Enterprise Risk Management (ERM). When risk ownership is assigned without authority, budget, or performance accountability, it remains symbolic and fails to produce meaningful monitoring or mitigation.

The India-specific pattern is particularly instructive: across several sectors, the most critical governance change has been elevating risk ownership from a transactional operational function to a senior, empowered role with direct escalation access to the CRO and the Board.

Research on ERM governance consistently finds that companies with dedicated, senior risk leadership and clear risk ownership structures outperform peers on risk-adjusted performance metrics.

Good Practice: Map every material risk on the enterprise risk register to a specific, named owner with defined authority, budget allocation, and performance metrics tied to risk management outcomes. Ownership without authority is accountability without enablement.

Lesson 4: Boards Need Insight, Not Information Volume

Board risk oversight is often undermined by information quality rather than quantity. While risk dashboards, heat maps, and extensive risk registers generate significant volume, they frequently lack the clarity boards require for meaningful oversight. Management teams often escalate risk information in formats that prioritise thoroughness over decision-making utility.

A board-level ERM governance principle derived from Moody's practice and McKinsey research holds that board risk oversight is most effective when "risk discussions move from compliance demonstrations to strategic conversations about risk-adjusted opportunities and emerging threats".

Good Practice: Structure board risk reporting around three questions: (1) What is the current state of the risk landscape, and how has it changed? (2) Which risks require a board-level decision or escalation? (3) What emerging risks are approaching the threshold of materiality? Supplement heat maps with narrative analysis that explains interconnections, trends, and strategic implications.

Lesson 5: Risk Appetite Statements Must Be Decision-Ready

Risk appetite statements are among the most universally present but least operationally effective elements of formal ERM frameworks. The NC State 2025 report notes that 65 % of public companies have a formal risk appetite statement — but the critical question is not whether one exists but whether it changes decisions. Phrases such as "moderate risk appetite" or "low tolerance for compliance breaches" are analytically meaningless in real-world trade-off situations unless they are translated into specific, quantified thresholds, escalation triggers, and decision limits.

Good Practice: Translate risk appetite statements into operational parameters: maximum acceptable loss thresholds by risk category, escalation triggers that are automatically activated when KRIs breach defined levels, and explicit guidance on which risk categories are in-appetite, at the boundary, and out-of-appetite for the current strategic period. The test of a usable risk appetite statement is whether a business unit manager can apply it in a real-time decision without consulting the CRO.

Lesson 6: Emerging Risks Require a Different Methodology

Conventional ERM methodology is calibrated for known risks with measurable probability and impact distributions. Emerging risks — AI governance failures, geopolitical supply disruptions, climate physical impacts, novel cyber threats — do not behave like known risks. They are characterised by high uncertainty, potentially nonlinear impact trajectories, and limited historical data. Applying probability-impact matrices designed for known risks to emerging risks produces systematically misleading assessments: risks that are genuinely dangerous are rated low-probability and receive insufficient attention.

Good Practice: Maintain a parallel Emerging Risk Register, reviewed quarterly, that uses scenario-based assessment rather than probability-impact scoring. Criteria for inclusion in the Emerging Risk Register should be: novelty (not yet in the mainstream register), potential materiality (could be significant if it crystallises), and rate of evolution (is the risk environment changing faster than the review cycle). Assign horizon-scanning responsibility to Risk Champions and senior Risk Owners.

Lesson 7: Third-Party Risk Is First-Party Exposure

A consistent finding across the banking, IT services, healthcare, and pharmaceutical sector cases in this chapter is that the most consequential risk events originated not within the organisation but within its external ecosystem — suppliers, technology platforms, regulators, and government scheme administrators. Yet most ERM frameworks allocate disproportionately greater governance attention to internal risks than to third-party exposures.

Financial services research confirms that "third-party risk management must include contractual incident notification requirements and continuous monitoring of vendor security posture". This principle generalises: third-party risk is not a vendor management function — it is an enterprise risk function, with the same governance requirements as internal strategic and operational risk.

Good Practice: Map the top 20 third-party dependencies (by impact of failure) in the enterprise, assign risk owners to each, establish minimum contractual risk standards, and include third-party resilience indicators in the Board's quarterly risk report. The question should not be "what are our internal risks?" but "where does our operational continuity depend on someone else's risk management?"

Lesson 8: ERM Must Connect to Performance, or It Will Lose to Performance

The most structural barrier to ERM effectiveness in high-growth organisations is the separation of risk management from performance management. When success is measured and rewarded exclusively on growth, revenue, and cost metrics — and risk discipline is treated as a supporting function — the organisational incentive structure consistently favours speed over caution, volume over quality, and short-term performance over long-term resilience. Risk frameworks that cannot influence these incentives will always operate at the margin of strategic decision-making.

The 2025 NC State report identifies "competing priorities and resource constraints" as the top barrier cited by 41 % of executives as obstacles to advancing risk management. The underlying dynamic is not resource scarcity — it is incentive misalignment.

Good Practice: Incorporate risk-adjusted performance metrics into leadership evaluation frameworks at all levels above first-line management. Define risk management KPIs — escalation quality, KRI breach rates, audit finding closure rates, third-party risk scores — and include them in balanced scorecard frameworks alongside financial KPIs. Risk management becomes strategically influential when performance frameworks make it count.

Lesson 9: Technology Is an Enabler, Not a Substitute for Judgement

The rapid proliferation of GRC (Governance, Risk, and Compliance) technology platforms, AI-powered risk dashboards, and real-time monitoring tools has created a temptation to equate ERM maturity with technology sophistication. This is a category error. Technology enables better risk data, faster reporting, and more comprehensive monitoring — but it does not replace the human judgement, cultural norms, and governance structures that determine whether risk information is acted upon. The organisations that derive the greatest value from risk technology are those that have first invested in the governance architecture and risk culture that can absorb and use the information technology produces.

Good Practice: Before investing in ERM technology upgrades, assess whether the existing governance structures are capable of acting on better risk information. The sequence that generates maximum value is: governance clarity - cultural readiness - technology enablement. Investing in technology before resolving governance and culture gaps produces sophisticated data that nobody acts on.

Lesson 10: India-Specific Risk Context Requires India-Specific Risk Intelligence

While global ERM frameworks like COSO and ISO 31000 provide sound structural principles, they were not designed for India's specific regulatory architecture and market dynamics. India's risk landscape is defined by several distinguishing characteristics: the regulatory pace of bodies like SEBI, RBI, and IRDAI; the heavy enterprise dependency on government schemes such as PMJAY, PLI, and PM Gati Shakti; the unique supply chain dynamics within the pharmaceutical and IT export sectors; and the growing criticality of the nation's digital infrastructure.

India's 2025 risk management landscape "will reflect a balance of global best practices and localised strategies," with SEBI's BRSR framework setting governance standards that are in some respects ahead of global norms, while also reflecting India-specific priorities in areas from infrastructure resilience to digital financial inclusion.

Good Practice: Complement global ERM frameworks with India -specific risk intelligence — sector regulatory watch programmes, domestic supply chain resilience assessments, and risk culture calibration tools designed for India's organisational and institutional context. The IRM India Affiliate's work in developing sector -specific Periodic Risk Tables, educational programmes, and India -contextualised risk governance tools represents precisely this localisation imperative.this localisation imperative.

Synthesis

The case studies and lessons in this chapter demonstrate that the **value of an ERM framework is measured by its use rather than its design**. Leading Indian organisations across banking, pharmaceuticals, FMCG, IT services, healthcare, and infrastructure have shown that ERM becomes a performance asset when it is anchored in accountability, integrated into decision-making, and communicated through tools like the Periodic Risk Table. Furthermore, success is sustained by a culture that rewards surfacing risk rather than suppressing it.

The gap between ERM as documentation and ERM as governance is, ultimately, a leadership choice. This chapter's lessons and good practices are the building blocks of that choice.

Chapter 8

Future of ERM in India

8.1 AI-Driven Risk Sensing

The future of Enterprise Risk Management in India is likely to be fundamentally shaped by the increasing integration of AI into organisational systems, transforming how risks are identified, monitored, and managed. Traditional risk management approaches have relied heavily on periodic assessments and historical data, often limiting their effectiveness in rapidly changing environments. In contrast, AI-driven risk sensing introduces a continuous, real-time capability to detect emerging vulnerabilities by analysing patterns across large and diverse datasets.

With the expansion of digital ecosystems across sectors such as banking, education, energy, and manufacturing, organisations are generating vast volumes of operational, financial, and behavioural data. AI systems can process these datasets to identify anomalies, predict disruptions, and generate early warning signals that were previously difficult to detect. For instance, subtle shifts in consumer behaviour, irregularities in system performance, or deviations in supply chain patterns can be flagged before they escalate into major risks.

However, the adoption of AI-driven risk sensing also introduces new layers of complexity. Organisations must navigate concerns related to algorithmic bias, data privacy, model governance, and over-reliance on automated decision-making. As a result, the future of ERM in this domain will require a balanced approach that combines technological sophistication with strong governance, ensuring that human oversight remains integral to risk evaluation and response.

8.2 Climate & Biodiversity Risks

Climate change and biodiversity loss are emerging as some of the most significant systemic risks facing Indian organisations, with implications that extend far beyond environmental concerns into operational, financial, and strategic domains. The increasing frequency of extreme weather events, coupled with long-term ecological degradation, is creating a risk environment that is both unpredictable and difficult to quantify.

For sectors such as agriculture, energy, infrastructure, and manufacturing, climate-related disruptions are already affecting production cycles, supply chains, and asset stability. Floods, droughts, and heatwaves can lead to operational shutdowns, resource shortages, and increased costs, while biodiversity loss impacts ecosystem services that underpin economic activities.

These risks are further compounded by regulatory pressures and evolving stakeholder expectations around sustainability and ESG performance.

In this context, ERM frameworks in India must evolve to incorporate environmental risks not as isolated categories but as systemic factors that influence multiple dimensions of organisational performance. The Periodic Risk Table provides a useful structure for integrating these risks by positioning them alongside traditional operational and financial risks, highlighting their interdependencies and cumulative impact.

Looking ahead, organisations will need to move beyond compliance -driven approaches to adopt proactive strategies that include climate scenario analysis, sustainable resource management, and investment in resilient infrastructure. The ability to integrate environmental considerations into core business strategy will become a key differentiator in long-term competitiveness.

8.3 India's Regulatory Trajectory

India's regulatory landscape is undergoing significant transformation, with increasing emphasis on transparency, accountability, and alignment with global standards. Developments in areas such as data protection, ESG disclosures, financial reporting, and sector-specific compliance are reshaping how organisations approach risk management.

Regulations such as evolving data protection frameworks, stricter environmental norms, and enhanced corporate governance requirements are expanding the scope of compliance risk. At the same time, regulators are placing greater emphasis on risk-based approaches, requiring organisations to demonstrate not only compliance but also the robustness of their internal risk management systems.

This evolving regulatory trajectory presents both challenges and opportunities. On one hand, organisations must navigate increasing complexity, higher compliance costs, and the need for continuous monitoring of regulatory changes. On the other hand, stronger regulatory frameworks can enhance market stability, improve investor confidence, and encourage the adoption of more sophisticated risk management practices.

In the future, ERM systems in India will need to be more agile and integrated, enabling organisations to respond quickly to regulatory changes while maintaining alignment with strategic objectives. The use of structured tools such as the Periodic Risk Table can support this transition by providing a consistent framework for identifying, categorising, and tracking regulatory risks across sectors.

8.4 The 2030 Risk Horizon

Looking toward the 2030 horizon, the risk landscape in India is expected to become increasingly complex, interconnected, and dynamic. The convergence of technological innovation, environmental challenges, geopolitical shifts, and socio-economic transformation will create a multi-layered risk environment where traditional boundaries between risk categories become increasingly blurred.

Technological advancements, including AI, automation, and digital platforms, will continue to reshape industries, creating both opportunities and vulnerabilities. Cybersecurity threats, data governance challenges, and technology-driven disruptions will remain central to risk management agendas. At the same time, climate change, resource constraints, and sustainability pressures will intensify, requiring organisations to rethink long-term strategies and investment decisions.

Geopolitical uncertainties and global trade dynamics will also influence risk exposure, particularly for sectors that rely on international supply chains and capital flows. Domestically, demographic shifts, urbanisation, and changing consumer behaviour will continue to redefine demand patterns and operational challenges.

In this evolving environment, the future of ERM in India will depend on the ability of organisations to adopt integrated, forward-looking, and adaptive risk management frameworks. The Periodic Risk Table, as developed in this study, provides a foundation for achieving this by enabling a structured and holistic view of risks, capturing their interconnections and evolution over time.

Ultimately, the organisations that succeed will be those that move beyond reactive risk management and develop the capability to anticipate change, respond effectively, and continuously adapt. The future of ERM, therefore, lies not only in managing risks but in building resilient, agile, and strategically aligned organisations capable of thriving in uncertainty.

Appendices

Appendix A: Glossary

A.1 Risk Category Codes (IRM Risk Wheel)

Every element in the Periodic Risk Tables carries one of the eighteen category codes below, drawn from the IRM Risk Wheel (see Section 3.4 and Figure 3.1).

Code	Category	Definition
SO	Strategic Objectives	Risks to the formulation and achievement of the organisation's strategy and business model.
GV	Governance	Risks arising from board effectiveness, oversight structures, decision rights, and organisational culture.
RE	Reputation & Ethics	Risks to reputation, stakeholder trust, and ethical conduct.
LL	Legal Liability	Risks of litigation, contractual liability, and legal or regulatory enforcement.
PS	Political and Social	Risks from political developments, public policy, social attitudes, and societal expectations.
EC	Economic	Risks arising from macroeconomic conditions such as growth, inflation, and demand cycles.
CM	Credit & Market	Risks from credit exposure and from movements in market prices, interest rates, and currencies.
LQ	Liquidity	Risks to the availability of cash and funding to meet obligations as they fall due.
RV	Reward & Value	Risks in remuneration, incentive structures, and the creation and distribution of value.
TE	Technology	Risks from the adoption, performance, failure, and obsolescence of technology.
IN	Information	Risks to the confidentiality, integrity, and availability of information and data, including cyber risk.
BC	Business Continuity	Risks of disruption to critical operations and to the organisation's ability to recover.
SC	Supply Chain	Risks in supplier networks, sourcing, and logistics.
PC	Projects & Change	Risks in the delivery of projects, programmes, and organisational change.
EM	Employment	Risks in workforce availability, capability, retention, and labour relations.
PE	Personal Effectiveness	Risks arising from individual capability, conduct, and performance.
NE	Natural Events	Risks from natural hazards and catastrophic physical events.
EV	Environment	Risks relating to the natural environment, including climate change and resource stewardship.

A.2 Abbreviations

The following abbreviations are used in the body of the report and on the Periodic Risk Tables themselves:

Abbreviation	Expansion
AGR	Adjusted Gross Revenue
AI	Artificial Intelligence
API (pharmaceuticals)	Active Pharmaceutical Ingredient
API (technology)	Application Programming Interface
ARPU	Average Revenue Per User
ATC	Air Traffic Control
ATF	Aviation Turbine Fuel
ATM	Automated Teller Machine
BANI	Brittle, Anxious, Non-linear, Incomprehensible
BCP	Business Continuity Plan
BFSI	Banking, Financial Services and Insurance
BPO	Business Process Outsourcing
BRSR	Business Responsibility and Sustainability Report
BSNL	Bharat Sanchar Nigam Limited
CBAM	Carbon Border Adjustment Mechanism
CBS	Core Banking System
CDN	Content Delivery Network
CEO	Chief Executive Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRO	Chief Risk Officer
CX	Customer Experience
DBT	Direct Benefit Transfer
DBU	Digital Banking Unit
DGCA	Directorate General of Civil Aviation
DGMS	Directorate General of Mines Safety
DISCOM	Distribution Company (electricity)
DPDP	Digital Personal Data Protection (Act)
DR	Disaster Recovery
EIA	Environmental Impact Assessment
EPC	Engineering, Procurement and Construction
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
ESG	Environmental, Social and Governance

Abbreviation	Expansion
ESOP	Employee Stock Ownership Plan
F&B	Food and Beverage
FDI	Foreign Direct Investment
FMCG	Fast-Moving Consumer Goods
FPI	Foreign Portfolio Investment
FSSAI	Food Safety and Standards Authority of India
FX	Foreign Exchange
GIFT	Gujarat International Finance Tec-City
GLOF	Glacial Lake Outburst Flood
GMP	Good Manufacturing Practice
GNSS	Global Navigation Satellite System
GST	Goods and Services Tax
GTF	Geared Turbofan
HQLA	High-Quality Liquid Assets
HRO	High Reliability Organisation
ICAO	International Civil Aviation Organization
ICE	Internal Combustion Engine
ICS	Industrial Control System
INR	Indian Rupee
IP	Intellectual Property
IP-1	Infrastructure Provider Category-I (telecom licence)
IRDAI	Insurance Regulatory and Development Authority of India
IRM	Institute of Risk Management
ISO	International Organization for Standardization
ITeS	IT-enabled Services
KG Basin	Krishna–Godavari Basin
KRI	Key Risk Indicator
KYC	Know Your Customer
LAF	Liquidity Adjustment Facility
LEO (government and public services)	Law Enforcement Organisation
LEO (telecom and satellite services)	Low Earth Orbit
LIMS	Laboratory Information Management System

Abbreviation	Expansion
LNG	Liquefied Natural Gas
M&A	Mergers and Acquisitions
MCA	Ministry of Corporate Affairs
MD	Managing Director
MICE	Meetings, Incentives, Conferences and Exhibitions
MIP	Minimum Import Price
MRO	Maintenance, Repair and Overhaul
MSME	Micro, Small and Medium Enterprises
MTM	Mark-to-Market
NABARD	National Bank for Agriculture and Rural Development
NBFC	Non-Banking Financial Company
NCIIPC	National Critical Information Infrastructure Protection Centre
NPCI	National Payments Corporation of India
NPV	Net Present Value
NSQ	Not of Standard Quality (drugs)
NTP	Notice to Proceed
OEM	Original Equipment Manufacturer
OPEC	Organization of the Petroleum Exporting Countries
OT	Operational Technology
PII	Personally Identifiable Information
PIL	Public Interest Litigation
PLI	Production Linked Incentive
PMO	Project Management Office
POS	Point of Sale
PPA	Power Purchase Agreement
PR	Public Relations
PRT	Periodic Risk Tables
PSU	Public Sector Undertaking
PUMO	Polarised, Unthinkable, Metamorphic, Overheated
QMS	Quality Management System
R&D	Research and Development
RAN	Radio Access Network
RBI	Reserve Bank of India

Abbreviation	Expansion
RMC	Risk Management Committee
ROI	Return on Investment
RTI	Right to Information
RUPT	Rapid, Unpredictable, Paradoxical, Tangled
SaaS	Software as a Service
SAF	Sustainable Aviation Fuel
SARFAESI	Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002
SCADA	Supervisory Control and Data Acquisition
SCOMET	Special Chemicals, Organisms, Materials, Equipment and Technologies (export-control list)
SEBI	Securities and Exchange Board of India
SLA	Service Level Agreement
SLO	Social Licence to Operate
SME	Small and Medium-sized Enterprise
SMS	Safety Management System
SPOF	Single Point of Failure
SRO	Self-Regulatory Organisation
TUNA	Turbulent, Uncertain, Novel, Ambiguous
UDAN	Ude Desh ka Aam Nagrik (regional connectivity scheme)
UPI	Unified Payments Interface
USD	United States Dollar
USOF	Universal Service Obligation Fund
VaR	Value at Risk
VRE	Variable Renewable Energy
VUCA	Volatility, Uncertainty, Complexity, Ambiguity
WEF	World Economic Forum
ZLD	Zero Liquid Discharge

Appendix B: Likelihood and Impact Scoring Matrices

Each risk element was scored on sector-calibrated five-point likelihood and impact scales. The rubrics below define, for each sector, how each point on the two scales was interpreted, reflecting the sector-specific calibration described in Sections 3.5 and 3.6. Composite scores are the product of the likelihood and impact scores (range 1–25) and resolve to three bands: Low (8 or below, green), Moderate (9–14, amber), and Critical (15 and above, red).

B.1 Aviation

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Context
1	Rare	Not seen in Indian Aviation in 15+ years.	< 2 %	Requires a "Black Swan" chain of failures.
2	Unlikely	Occurred 1-2 times in the last decade.	2 % – 15 %	Usually caught by standard safety buffers.
3	Possible	Occurs once every 1-2 years.	16 % – 40 %	E.g., technical groundings, seasonal disruptions.
4	Likely	Multiple times a year across the fleet.	41 % – 70 %	Linked to rapid expansion or high-cycle operations.
5	Almost Certain	Persistent/Daily occurrence.	> 70 %	E.g., minor technical delays, bird strikes in specific zones.

Impact

Score	Safety & Human Life	Regulatory (DGCA/BCAS/ICAO)	Financial (Shareholders/Leasing)	Trust & Ecosystem
1	No injury.	Minor audit observation.	< 0.5 % EBITDA impact.	Minor delay.
2	Minor discomfort; no safety risk.	Small fine; procedural correction.	0.5 % - 1 % EBITDA impact.	Localised dissatisfaction.
3	Minor injury/ Localised hazard.	Significant fine; temporary tail grounding.	1-5 % EBITDA hit; credit rating watch.	Mass cancellations; social media crisis.
4	Serious injury/ Serious incident.	Operational suspension; systemic audit.	> 5 % EBITDA hit; major liquidity stress.	Significant loss of market share.
5	Hull Loss/Fatality/ Catastrophic Event.	AOC Revocation/ National Security Breach.	Bankruptcy/Lease default/ Total capital loss.	Total brand collapse; loss of trust in airspace.

B.2 Financial Services

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Systemic Vulnerability
1	Rare	Not seen in Indian FS in 10+ years.	< 5 %	Requires a "Black Swan" event or total collapse of multiple high-level controls.
2	Unlikely	Occurred 1-2 times in the last decade.	5 % – 20 %	Requires a rare combination of external shocks and internal oversight failure.
3	Possible	Occurs every 2-3 years.	21 % – 50 %	Likely if current internal controls remain static while the market evolves.
4	Likely	Multiple times a year across the industry.	51 % – 80 %	High due to 2026 market volatility, rapid tech shifts, or talent churn.
5	Almost Certain	Persistent or ongoing; monthly/weekly.	> 80 %	Risk is inherent to the current business model or infrastructure.

Impact

Score	Financial (Shareholders)	Regulatory (Regulators)	Operational (Ecosystem)	Trust (Customers)
1	< 0.1 % Net Profit hit.	Minor observation in RBI/ SEBI audit.	Isolated internal glitch; no downtime.	Negligible complaints.
2	0.1 % –1 % P&L hit; No threat to CRAR.	Small fine; mandated process update.	1-hour outage for non-critical services.	Localised churn/ Social media mention.
3	1 % –5 % P&L hit; share price dip.	Formal warning; public disclosure.	UPI/Payment rail outage > 2 hours.	"Trending" social media dissatisfaction.
4	> 5 % P&L hit; Rating downgrade.	PCA (Prompt Corrective Action) level.	Data breach involving PII.	Mass withdrawal; loss of Institutional Trust.
5	Total Capital Erosion; Insolvency.	Licence Revocation; Criminal proceedings.	Systemic contagion; failure of "Too Big To Fail."	Nationwide panic; complete brand collapse.

B.3 Government and Public Services

Likelihood

Score	Level	Historical Frequency / Industry Precedent	Statistical Probability
1	Rare	Not seen in Indian governance in 10+ years.	< 2 %
2	Unlikely	Occurred 1–2 times in the last decade.	2 % – 15 %
3	Possible	Known to occur every 1–2 years.	16 % – 40 %
4	Likely	Routine challenge seen multiple times a year.	41 % – 70 %
5	Almost Certain	Persistent or ongoing systemic issue.	> 70 %

Impact

Score	Citizen Delivery & Social Welfare	Oversight & Legal (CAG/CVC/DPDP)	Fiscal & Economic (Sovereign)	Trust & Reputation (Global/National)
1	Minor delay in non-essential services; no impact on welfare.	Minor audit observation; no further action required.	< 0.1 % budget deviation; negligible fiscal impact.	Localised grievance; no media or political traction.
2	Brief interruption in a specific district-level scheme.	Internal inquiry initiated; minor compliance breach.	0.1 % – 0.5 % Ministry budget deviation.	Small social media mention; localised dissatisfaction.
3	Regional outage of DBT or essential services (e.g., Health/Ration).	Stricture by Parliament Committee; major fine under DPDP Act.	0.5 % – 1 % Ministry budget hit; delay in Gati Shakti milestones.	Significant national media backlash; loss of "Digital India" trust.
4	Widespread service failure affecting multiple states/sectors.	Systemic corruption probe; suspension of senior leadership.	> 1 % budget hit; threat to sector-wide public investment.	Large-scale social unrest; international criticism of governance.
5	National Mission Failure (e.g., National Health Stack collapse).	Presidential Reference; Constitutional Crisis; Licence Revocation.	Sovereign Credit Downgrade; National Fiscal/Insolvency Crisis.	Permanent loss of Sovereign Trust; Global divestment; Security Breach.

B.4 Telecom

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Context
1	Rare	Not seen in Indian Telecom in 10+ years.	< 2 %	Requires a "Black Swan" event (e.g., subsea cable cut).
2	Unlikely	Occurred 1-2 times in the last decade.	2 % – 15 %	Usually managed by automated failovers.
3	Possible	Occurs every 1-2 years.	16 % – 40 %	E.g., localised monsoon outages, interference.
4	Likely	Multiple times a year across the network.	41 % – 70 %	E.g., fibre cuts from construction, cyber-intrusions.
5	Almost Certain	Persistent/Daily occurrence.	> 70 %	E.g., retail complaints, localised tower congestion.

Impact

Score	Service & Infrastructure	Regulatory & Security (DoT/TRAI)	Financial (Shareholders/ARPU)	Trust & Data
1	Negligible latency.	Minor compliance filing error.	< 0.5 % EBITDA impact.	Minor UX glitch.
2	Brief localised outage (< 1 hour).	Administrative warning.	0.5 % - 1 % EBITDA impact.	Minor social media traction.
3	Regional outage > 4 hours; DPI impact.	Significant penalty under DPDP Act.	1-5 % EBITDA hit; B2B segment churn.	Data leak (limited users); brand dip.
4	Multi-state service disruption.	Severe DPDP penalties; licence warning.	> 5 % EBITDA hit; debt covenant breach.	Large-scale data exposure; enterprise loss.
5	National Blackout/ 5G backbone failure.	Spectrum Licence Revocation/ Security Breach.	Debt default/Bankruptcy/ Total cap loss.	Mass PII Data Breach; permanent loss of trust.

B.5 Food Security

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Food System Context
1	Rare	Not seen across major supply chains for 10+ years	< 5 %	Needs a rare mix of climate, trade, and safety failures.
2	Unlikely	Seen in one market, commodity, or route	5 %–20 %	Limited to a supplier corridor, product class, or jurisdiction.
3	Possible	Occurs every 2–3 years	21 %–50 %	Triggered by commodity spikes, regulatory change, or transport strain.
4	Likely	Repeats across food networks every year	51 %–80 %	Driven by climate shocks, trade friction, urban demand, and digital exposure.
5	Almost Certain	Structural and recurring	> 80 %	Built into food systems: climate, regulation, land pressure, and cyber reliance.

Impact

Score	Sourcing / Price / Margin	Food Safety / Regulation	Production / Cold Chain / Trade	Consumer Trust / Availability
1	< 0.5 % cost or margin hit	Minor compliance note	Small delay or local handling issue	No real consumer effect
2	0.5 %–1 % cost or margin hit	Small correction	Short interruption in one lane or market	Local dissatisfaction
3	1 %–5 % cost or margin hit	Warning / recall of limited scope	Route delay, contamination risk, or customs friction	Noticeable availability or trust hit
4	> 5 % cost or margin hit	Major recall / regulatory action	Multi-market disruption or supply breakdown	Strong consumer concern; retailer pressure
5	Supply shock / business stress	Licence, ban, or severe legal exposure	Trade-system or cold-chain failure at scale	Severe trust loss; prolonged shortage

B.6 Fast Moving Consumer Goods

Likelihood

Score	Level	Historical Frequency	Statistical Probability	FMCG Operating Context
1	Rare	Not seen in mature national networks for 10+ years	< 5 %	Needs an extreme failure across plants, warehouses, and route-to-market.
2	Unlikely	Seen in one brand, plant, or region	5 %–20 %	Limited to a single SKU, vendor, or channel.
3	Possible	Occurs every 2–3 years	21 %–50 %	Triggered by demand swings, supplier misses, or customs delays.
4	Likely	Repeats across the sector each year	51 %–80 %	Driven by warehouse strain, price volatility, distributor issues, and consumer downtrading.
5	Almost Certain	Persistent and structural	> 80 %	Built into FMCG: thin margins, channel dependence, high-volume logistics, and fast demand shifts.

Impact

Score	Revenue / Gross Margin	Plant / Warehouse / Distributor Network	Shelf Availability / Fill Rate	Consumer / Retailer Confidence
1	< 0.5 % revenue or margin hit	Minor process issue	Single-SKU disruption	Limited retailer complaint
2	0.5 %–1 % revenue or margin hit	Short production or dispatch delay	Local stockout	Small channel friction
3	1 %–5 % revenue or margin hit	Batch loss, customs delay, or supplier miss	Category-level availability issue	Retailer pushback; consumer switching
4	> 5 % revenue or margin hit	Warehouse, plant, or supply chain disruption	Multi-region stockout or expiry losses	Material shelf loss; market share pressure
5	Margin collapse / working-capital stress	Network breakdown or major compliance event	Severe service failure across channels	Lasting brand damage; trade confidence loss

B.7 Agriculture

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Farm / Agri System Context
1	Rare	Not seen in stable belts for 10+ years	< 5 %	Needs an extreme compound shock across weather, pests, and water.
2	Unlikely	Seen in one crop, district, or season	5 %–20 %	Localised to a farm type, region, or input chain.
3	Possible	Occurs every 2–3 seasons	21 %–50 %	Triggered by rainfall swings, input spikes, or market slippage.
4	Likely	Repeats across the sector every year	51 %–80 %	Driven by climate variability, pest pressure, water stress, and cost volatility.
5	Almost Certain	Structural and recurring	> 80 %	Built into agriculture: weather, biology, price swings, and infrastructure gaps.

Impact

Score	Yield / Farmer Income	Crop Health / Livestock Health	Storage / Transport / Market Access	Food Supply / Rural Stability
1	< 0.5 % income hit	Minor field loss	Localised storage or routing issue	No material supply effect
2	0.5 %–1 % income hit	Limited pest or input issue	Short post-harvest delay	Small local price impact
3	1 %–5 % income hit	Meaningful crop / herd losses	Market access friction or spoilage	Noticeable supply reduction
4	> 5 % income hit	Major yield loss / livestock mortality	Storage, transport, or irrigation breakdown	Regional shortage; strong farmer distress
5	Season-wide income shock / viability stress	Widespread crop failure or disease outbreak	Distribution collapse or severe water loss	Food security pressure; recovery takes seasons

B.8 Healthcare & Pharma

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Pharma Context
1	Rare	Not seen in regulated plants or portfolios for 10+ years	< 5 %	Needs an extreme shock across API supply, quality, and approvals.
2	Unlikely	Seen in one plant, molecule, or market	5 %–20 %	Limited to a single site, batch, or product line.
3	Possible	Occurs every 2–3 years	21 %–50 %	Triggered by GMP lapses, pricing pressure, or pipeline delays.
4	Likely	Repeats across the sector each year	51 %–80 %	Driven by API dependence, compliance load, patent expiry, and R&D pressure.
5	Almost Certain	Structural and recurring	> 80 %	Built into the model: generics competition, quality risk, and supply fragility.

Impact

Score	Revenue / Margin / Pipeline	GMP / Regulator / Patient Safety	Manufacturing / Cold Chain / Supply	Brand / Market Access
1	< 0.5 % EBITDA hit	Minor observation	Isolated documentation or handling issue	Limited commercial impact
2	0.5 %–1 % EBITDA hit	Small warning / correction	Single-batch or short-chain disruption	Localised customer or doctor concern
3	1 %–5 % EBITDA hit	Inspection finding / import or export delay	Batch rejection, cold-chain lapse, or plant slowdown	Noticeable market access or trust hit
4	> 5 % EBITDA hit	Recall, warning letter, or major compliance action	Plant shutdown, prolonged shortage, or API break	Strong reputational damage; channel loss
5	Revenue shock / licence stress	Licence suspension / criminal or civil action	Multi-site disruption or patient safety event	Severe trust collapse; long recovery

B.9 Information Technology

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Tech Context
1	Rare	Not seen in mature environments for 10+ years	< 5 %	Needs multiple control failures plus a major attacker or platform fault.
2	Unlikely	Seen only in weakly controlled environments	5 %–20 %	Limited to one app, tenant, team, or vendor.
3	Possible	Occurs every 2–3 years	21 %–50 %	Triggered by misconfigurations, access errors, patch gaps, or supplier exposure.
4	Likely	Repeats across the sector each year	51 %–80 %	Driven by always-on attack surface, cloud dependence, and human error.
5	Almost Certain	Persistent and structural	> 80 %	Built into modern tech stacks: identity theft, ransomware, cloud reliance, and change risk.

Impact

Score	Data / IP / Regulated Records	Security / Service Continuity	Platform / Cloud / DevOps	Customer / Regulator Trust
1	< 0.5 % revenue or cost hit	Minor alert, no outage	Single system or low-criticality tool affected	Local complaint; no external scrutiny
2	0.5 %–1 % revenue or cost hit	Short interruption or limited exposure	One app, tenant, or pipe-line disrupted	Limited customer concern
3	1 %–5 % revenue or cost hit	Material incident / contained breach	Major service degradation, delayed releases, or vendor issue	Notifiable incident; trust hit
4	> 5 % revenue or cost hit	Ransomware, major breach, or prolonged outage	Core environment or cloud dependency impaired	Significant customer churn; regulatory action
5	Business shutdown / capital stress	Catastrophic breach or systemic compromise	Identity, production, and recovery environment all affected	Severe legal exposure; lasting brand damage

B.10 Hospitality

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Hotel / Resort Context
1	Rare	Not seen across major hotel chains for 10+ years	< 5 %	Needs an extreme demand shock plus OTAs, staffing, and cost pressure at once.
2	Unlikely	Seen only in isolated properties or cities	5 %–20 %	Limited to one asset, one season, or one operating issue.
3	Possible	Occurs every 2–3 years in the sector	21 %–50 %	Triggered by seasonality, service lapse, or rate pressure.
4	Likely	Repeats across the industry each year	51 %–80 %	Driven by OTA dependence, wage inflation, debt load, and demand swings.
5	Almost Certain	Structural and recurring	> 80 %	Built into the model: fixed assets, staffing churn, and peak-season concentration.

Impact

Score	GOP / EBITDA	Hotel Licence / Food Safety / Labour	Property Operations	Guest Trust / RevPAR
1	< 0.5 % EBITDA hit	Minor inspection note	Single outlet / minor housekeeping issue	Few complaints; no booking impact
2	0.5 %–1 % EBITDA hit	Small fine / correction	Short service delay or room-block issue	Localised dissatisfaction
3	1 %–5 % EBITDA hit	Notice / closure of one unit / wage violation action	Banquet, F&B, or room inventory disruption	Noticeable review damage; repeat-booking pressure
4	> 5 % EBITDA hit	Regulatory action / forced remediation	Property-wide disruption, food incident, or staff shortage	RevPAR hit; brand damage; cancellations rise
5	Liquidity stress / default risk	Licence suspension / severe legal exposure	Hotel shutdown, debt stress, or major accident	Trust collapse; mass cancellations; long recovery

B.11 Tourism

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Destination Context
1	Rare	Not seen in key circuits for 10+ years	< 5 %	Needs an exceptional shock across source markets, access, and seasonality.
2	Unlikely	Seen in one destination or one season	5 %–20 %	Localised to a circuit, route, or visitor segment.
3	Possible	Occurs every 2–3 years	21 %–50 %	Triggered by weather, policy, health, or access issues.
4	Likely	Repeats across major circuits each year	51 %–80 %	Driven by monsoons, connectivity gaps, source-market dependence, and crowding.
5	Almost Certain	Persistent structural exposure	> 80 %	Built into tourism: seasonality, climate sensitivity, and access constraints.

Impact

Score	Tourism Receipts / Occupancy	Visa / Entry / Local Permits	Access / Circuit Operations	Destination Appeal / Word of Mouth
1	< 0.5 % receipts hit	Minor portal or permit issue	Single-route delay	Limited complaint volume
2	0.5 %–1 % receipts hit	Small process correction	Short disruption to one circuit	Localised dissatisfaction
3	1 %–5 % receipts hit	Advisory / temporary policy friction	Itinerary disruption or partial access loss	Review decline; booking slowdown
4	> 5 % receipts hit	Major policy change / visa friction	Route closure, season loss, or access restriction	Material demand drop; cancellations spike
5	Severe revenue shock / circuit collapse	Entry suspension / compliance shutdown	Destination isolation or prolonged closure	Brand collapse for the circuit; trust loss

B.12 Retail

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Retail Context
1	Rare	Not seen in organised retail for 10+ years	< 5 %	Needs a black-swan shock across demand, supply, and pricing.
2	Unlikely	Seen only in one format or geography	5 %–20 %	Isolated execution or competitive pressure; usually containable.
3	Possible	Occurs every 2–3 years in the sector	21 %–50 %	Triggered by category shifts, markdown cycles, or channel mix changes.
4	Likely	Repeats across the industry each year	51 %–80 %	Driven by price wars, cost inflation, and omnichannel friction.
5	Almost Certain	Persistent / structural	> 80 %	Built into modern retail: discounting, platform dependence, and demand volatility.

Impact

Score	Gross Margin / EBITDA	Retail Regulation / Compliance	Store, DC & Fulfilment	Brand / Loyalty
1	< 0.5 % EBITDA hit	Minor audit note	Single-store or single-SKU disruption	Local complaint; no lasting damage
2	0.5 %–1 % EBITDA hit	Small fine / process correction	Limited stockout or short logistics delay	Localised dissatisfaction
3	1 %–5 % EBITDA hit	Notice / enquiry / compliance action	Category-level stock imbalance or channel disruption	Social backlash; moderate churn
4	> 5 % EBITDA hit	Major investigation / forced remediation	Network-wide markdowns, store closures, or fulfilment stress	Material brand damage; market share loss
5	Margin collapse / capital stress	Licence / approval risk	Operating model breakdown across stores, supply chain, and online	Boycott, trust collapse, or severe brand impairment

B.13 Media

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Media Context
1	Rare	Not seen in major Indian media in 10+ years	< 5 %	Needs an extreme shock across audience, ad market, and regulation.
2	Unlikely	Seen in a single format or outlet type	5 %–20 %	Limited to niche platform, language market, or channel.
3	Possible	Happens every 2–3 years	21 %–50 %	Triggered by ad-cycle swings, platform policy shifts, or content changes.
4	Likely	Recurs across TV / digital / OTT each year	51 %–80 %	Driven by audience fragmentation, creator migration, and monetisation pressure.
5	Almost Certain	Persistent structural pressure	> 80 %	Core to the business model: platform dependency, ad volatility, and audience churn.

Impact

Score	Ad & Subscription P&L	Content / Broadcast / IT Rules	Platform, Production & Distribution	Audience / Advertiser Trust
1	< 0.1 % P&L hit	Minor compliance observation	Localised upload / playout / feed issue	Negligible audience impact
2	0.1 %–1 % P&L hit	Small fine / correction	Short outage or limited content delay	Local churn; minor advertiser concern
3	1 %–5 % P&L hit	Warning / public disclosure / takedown	Platform or feed disruption >24 hours	Noticeable audience drop; advertiser caution
4	> 5 % P&L hit	Major action / content restriction	Distribution or production disruption across a key channel	Material audience loss; ad pullback
5	Revenue model stress / capital erosion	Licence / broadcast / legal action	Collapse of distribution or monetisation pathway	Trust breakdown; mass audience or advertiser exit

B.14 Education

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Education Context
1	Rare	Not seen in stable institutions for 10+ years	< 5 %	Needs a major shock across enrolment, staffing, funding, and delivery.
2	Unlikely	Seen in one campus, programme, or intake cycle	5 %–20 %	Limited to a single course, cohort, or delivery channel.
3	Possible	Occurs every 2–3 academic cycles	21 %–50 %	Triggered by fee pressure, demand shifts, or faculty constraints.
4	Likely	Repeats across the sector each year	51 %–80 %	Driven by budget stress, enrolment volatility, and talent shortages.
5	Almost Certain	Structural and recurring	> 80 %	Built into education: retention pressure, demand swings, and human-capital dependence.

Impact

Score	Tuition / Funding / Cash Flow	Accreditation / Delivery / Compliance	Faculty / Student Services	Learner Outcomes / Reputation
1	< 0.5 % revenue or budget hit	Minor admin issue	Small timetable or service delay	Limited student complaint
2	0.5 %–1 % revenue or budget hit	Local compliance correction	One programme or unit affected	Localised dissatisfaction
3	1 %–5 % revenue or budget hit	Notice / audit finding / course disruption	Faculty gap or service downgrade	Enrolment softness; reputation dent
4	> 5 % revenue or budget hit	Accreditation risk / regulatory action	Major staffing, delivery, or cost failure	Student churn; brand damage
5	Funding stress / operating viability risk	Registration / approval risk	System-wide breakdown in teaching or support	Trust collapse; long-term enrolment loss

B.15 Mining

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Mine Site Context
1	Rare	Not seen in well-controlled operations for 10+ years	< 5 %	Needs a rare combination of ground, equipment, and control failures.
2	Unlikely	Seen in one pit, shaft, or processing unit	5 %–20 %	Localised to a site, machine, or operating condition.
3	Possible	Occurs every 2–3 years	21 %–50 %	Triggered by haulage, maintenance, ventilation, or environmental stress.
4	Likely	Repeats across the industry each year	51 %–80 %	Driven by underground exposure, ageing assets, labour gaps, and environmental load.
5	Almost Certain	Persistent and structural	> 80 %	Built into mining: high hazard work, deep operations, and long-tail environmental risk.

Impact

Score	Fatality / Injury / Lost Time	Mine Safety / Statutory Compliance	Plant / Haulage / Tailings / Ground Control	Land, Water & Biodiversity
1	Minor first-aid case	Routine inspection note	Single-equipment delay	Minimal site disturbance
2	Recordable injury	Small corrective action	Local stoppage or contained defect	Limited remediation needed
3	Serious injury / material lost time	Formal notice / enforced fix	Shaft, haulage, or fire-related disruption	Noticeable site impact; cleanup required
4	Fatality / multiple serious injuries	Major regulatory action / suspension	Production halt, structural failure, or fire	Significant contamination or habitat damage
5	Multiple fatalities / shutdown risk	Licence suspension / prosecution	Mine-wide collapse, tailings failure, or long outage	Severe ecological damage; long remediation tail

B.16 Energy

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Energy Context
1	Rare	Not seen in stable asset fleets for 10+ years	< 5 %	Needs a major compound failure across people, plant, and compliance.
2	Unlikely	Seen in one plant, field, or project	5 %–20 %	Limited to a single unit, crew, or site.
3	Possible	Occurs every 2–3 years	21 %–50 %	Triggered by skills gaps, maintenance misses, or asset stress.
4	Likely	Repeats across the sector each year	51 %–80 %	Driven by ageing infrastructure, specialist skill shortages, and remote operations.
5	Almost Certain	Structural and recurring	> 80 %	Built into energy systems: outages, safety exposure, and transition complexity.

Impact

Score	Revenue / EBITDA / Capex	Safety / Grid / Regulatory	Generation / Asset Uptime	Reliability / Reputation
1	< 0.5 % EBITDA hit	Minor compliance note	Small unit or non-critical outage	No material market reaction
2	0.5 %–1 % EBITDA hit	Small corrective action	Short outage or project delay	Local concern
3	1 %–5 % EBITDA hit	Formal inquiry / permit issue	Meaningful downtime or commissioning slippage	Stakeholder pressure rises
4	> 5 % EBITDA hit	Major safety or regulatory action	Plant, field, or network disruption	Material reliability damage
5	Capital stress / shutdown risk	Licence, grid, or safety suspension	System-wide outage or major incident	Severe trust loss; long recovery

B.17 Manufacturing

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Manufacturing Context
1	Rare	Not seen in stable plants for 10+ years	< 5 %	Needs a rare mix of input shock, logistics failure, and shopfloor disruption.
2	Unlikely	Seen in one plant or product line	5 %–20 %	Limited to a single SKU, supplier, route, or warehouse node.
3	Possible	Occurs every 2–3 years	21 %–50 %	Triggered by input spikes, inventory errors, or transport bottlenecks.
4	Likely	Repeats across the sector each year	51 %–80 %	Driven by commodity volatility, lane congestion, theft, and fragile supply chains.
5	Almost Certain	Structural and recurring	> 80 %	Built into manufacturing: raw material swings, logistics gaps, and working-capital pressure.

Impact

Score	EBITDA / Working Capital	Plant / Line / Warehouse	Supply Chain / Freight	Customer / Margin / Continuity
1	< 0.5 % EBITDA hit	Minor line interruption	Single-load or single-bay issue	No meaningful customer impact
2	0.5 %–1 % EBITDA hit	Short stoppage or limited rework	Local dispatch or storage delay	Minor delivery or fill-rate miss
3	1 %–5 % EBITDA hit	Batch loss, inventory imbal-ance, or partial line halt	Route disruption, cold-chain loss, or cargo theft	Margin pressure; service slippage
4	> 5 % EBITDA hit	Plant slowdown, severe short-age, or major material spike	Multi-node logistics failure	Material customer loss; cash strain
5	Liquidity stress / shutdown risk	Factory shutdown or pro-longed input shortage	Supply-chain collapse across critical lanes	Severe market loss; survival risk

B.18 Infrastructure

Likelihood

Score	Level	Historical Frequency	Statistical Probability	Infrastructure Context
1	Rare	Not seen in active projects for 10+ years	< 5 %	Needs a rare combination of policy, funding, and execution failure.
2	Unlikely	Seen in one project or asset class	5 %–20 %	Limited to a single SPV, counterparty, or corridor.
3	Possible	Occurs every 2–3 years	21 %–50 %	Triggered by cost inflation, funding stress, or payment delays.
4	Likely	Repeats across the sector each year	51 %–80 %	Driven by DISCOM stress, commodity swings, financing costs, and execution risk.
5	Almost Certain	Structural and recurring	> 80 %	Built into infrastructure: long-dated capital, policy exposure, and cash-flow fragility.

Impact

Score	Project IRR / DSCR / NPV	EPC / O&M / Off-taker	Commissioning / Asset Uptime	Lender / Investor Confidence
1	< 0.5 % valuation hit	Minor contract or site issue	Short delay with no critical path impact	No material confidence impact
2	0.5 %–1 % valuation hit	Small correction or notice	Limited delay in one package	Mild lender concern
3	1 %–5 % valuation hit	Payment slippage, change order, or cost overrun	Milestone delay or partial outage	Higher funding cost; tighter covenants
4	> 5 % valuation hit	DISCOM stress, refinancing pressure, or major cost escalation	Commissioning delay, outage, or asset impairment	Sponsor and lender stress rises
5	NPV impairment / default risk	Off-taker failure, licence issue, or project distress	Shutdown, stranded asset, or major remediation	Funding freeze; survival risk

B.19 Oil & Gas

Likelihood

Score	Level	Historical Frequency	Statistical Probability	India Oil & Gas Context
1	Rare	Not seen in major import / production chains for 10+ years	< 5 %	Needs a rare combination of geopolitical, operational, and logistics failures.
2	Unlikely	Seen in one basin, terminal, or shipment corridor	5 %–20 %	Limited to a single asset, cargo, or pipeline.
3	Possible	Occurs every 2–3 years	21 %–50 %	Triggered by sanctions, weather, equipment failure, or price shocks.
4	Likely	Repeats across the sector each year	51 %–80 %	Driven by import dependence, FX moves, ageing assets, and cyclone exposure.
5	Almost Certain	Persistent structural exposure	> 80 %	Embedded in the business: geopolitics, price volatility, and asset reliability risk.

Impact

Score	Upstream / Refining Margin	DG / PSU / Safety Compliance	Production / Import Logistics	Public Safety / Market Confidence
1	< 0.5 % EBITDA hit	Minor audit observation	Short supply delay or unit trip	Minimal market reaction
2	0.5 %–1 % EBITDA hit	Small fine / process correction	One cargo delay or minor pipeline issue	Localised concern
3	1 %–5 % EBITDA hit	Formal inquiry / regulatory notice	Basin decline, terminal outage, or shipping disruption	Price pressure; stakeholder concern
4	> 5 % EBITDA hit	Major sanction / licence pressure	Refinery fire, cyclone damage, or import interruption	Fuel shortages; strong market and public reaction
5	Capital erosion / shutdown risk	Licence suspension / criminal proceedings	Major platform, refinery, or terminal failure	Severe safety event; systemic confidence shock

Appendix C: Bibliography & References

Abugri, C., & Colley, V. (2026). Bias, fairness, and explainability in AI-driven credit scoring: A critical review of algorithmic governance in financial risk assessment. *Journal of Economics Intelligence and Technology, 2(1)*.

Agriculture Institute. (2025). *Agriculture risks, types & mitigation strategies.* https://agriculture.institute/agripreneurship/agriculture-risks-types-mitigation-strategies/

Agriculture Policy Team. (2025). *Farm practices & management: Risk management.* U.S. Department of Agriculture, Economic Research Service. https://www.ers.usda.gov/topics/farm-practices-management/risk-management/

Aircraft Fleet Recycling Association. (2026). *Best management practice for management of used aircraft parts and assemblies.*

Airports Council International. (2024). *Airport economics report & key performance indicators.*

Airports Council International, International Air Transport Association, & Worldwide Airport Coordinators Group. (2024). *Worldwide Airport Slot Guidelines.*

Akbas, M. Ç. (2024). Measuring the impact of enterprise risk management on performance, value, and risk indicators of Borsa Istanbul XBANK companies with data mining prediction models. *Humanities and Social Sciences Communications*, 11(1), Article 1350. https://doi.org/10.1057/s41599-024-03871-z

Almulla, M. M. (2024). Food security is a collective effort—Here's what we need to do. *World Economic Forum*. https://www.weforum.org/

Andersen, T. J., & Young, P. C. (2023). Enhancing public sector enterprise risk management through interactive information processing. *Frontiers in Research Metrics and Analytics, 8,* Article 1239447. https://doi.org/10.3389/frma.2023.1239447

Anthem, P. (2025). Food security—*What it means and why it matters.* World Food Programme. https://www.wfp.org/

Ashna, Jo, A. A., & Ramamurthy, L. (2023). *EdTech: Examining experiences, challenges and future directions.* Centre for Public Policy Research.

Aviation Working Group. (2026). *Cape Town Convention compliance index: Methodology*.

Bamber, G. J., Gittell, J. H., Kochan, T. A., & von Nordenflycht, A. (2009). *Up in the air: How airlines can improve performance by engaging their employees. Cornell University Press.*

Bank of England. (2025). *The Bank of England's climate-related financial disclosure 2025*. https://www.bankofengland.co.uk/climate-change/the-bank-of-englands-climate-related-financial-disclosure-2025

Basel Committee on Banking Supervision. (2015). *Corporate governance principles for banks.* Bank for International Settlements.

Beyond compliance: The hidden threats and opportunities in ERM. (n.d.). [Post]. LinkedIn. https://www.linkedin.com/pulse/beyond-compliance-hidden-threats-opportunities-erm-mark-e-s--jbcoe

Birthal, P. S., Hazrana, J., & Negi, D. S. (2021). Effectiveness of farmers' risk management strategies in smallholder agriculture: Evidence from India. *Climatic Change, 169*, Article 30. https://doi.org/10.1007/s10584-021-03271-1

Bisht, I. S., Rana, J. C., & Ahlawat, S. P. (2020). The future of smallholder farming in India: Some sustainability considerations. *Sustainability*, 12(9), 3751. https://doi.org/10.3390/su12093751

Board of Governors of the Federal Reserve System. (2023). *Review of the Federal Reserve's supervision and regulation of Silicon Valley Bank*.

Borenstein, S., & Rose, N. L. (2014). How airline markets work—or do they? Regulatory reform in the airline industry. In N. L. Rose (Ed.), *Economic regulation and its reform: What have we learned?* (pp. 63–135). University of Chicago Press.

Bureau of Indian Standards. (2018). IS 15700:2018—*Quality management systems: Requirements for service organizations.*

Bureau of Industry and Security. (2024). *Export administration regulations* (15 C.F.R. Parts 730–774). U.S. Department of Commerce.

Burke, T. (2025). *Critical infrastructure annual risk review highlights changing risk landscape* [Media release]. Department of Home Affairs, Australian Government. https://minister.homeaffairs.gov.au/TonyBurke/Pages/critical-infrastructure-annual-risk-review-highlights-changing-risk-landscape.aspx

CA Global. (2025). *COSO and WBCSD guidance on integrating ESG risks into ERM* [Post]. LinkedIn. https://www.linkedin.com/posts/caglobal_coso-wbcsd-esg-guidance-activity-7368847718665940992-FrxA

CAE Inc. (2024). *Aviation talent forecast*.

Capitol Technology University. (2025). *Emerging threats to critical infrastructure: AI-driven cybersecurity trends 2025*. https://www.captechu.edu/blog/ai-driven-cybersecurity-trends-2025

Carnegie Endowment for International Peace. (2025, September). *Mapping India's cybersecurity administration in 2025*. https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025

Centre for Economic Policy Research. (n.d.). *Geopolitical risk and supply chain diversification*. VoxEU. https://cepr.org/voxeu/columns/geopolitical-risk-and-supply-chain-diversification

Chand, R. (2022). *Agriculture challenges and policies for the 21st century* (NABARD Research and Policy Series No. 6/2022). National Bank for Agriculture and Rural Development.

Chang, X., Song, Z., & Zhou, T. (2025). Geopolitical risk and global supply chain resilience. *Finance Research Letters, 86*, Article 108551. https://doi.org/10.1016/j.frl.2025.108551

Chauhan, S. (2025). Seed Bill 2025 built for corporates, not cultivators, farmers warn. *Down To Earth*. https://www.downtoearth.org.in/

Cheftel, J. C. (2011). Emerging risks related to food technology. In *Advances in food protection: Focus on food safety and defense* (pp. 223–254). Springer. https://doi.org/10.1007/978-94-007-1100-6_13

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. COSO.

Committee of Sponsoring Organizations of the Treadway Commission, & World Business Council for Sustainable Development. (2018). *Applying enterprise risk management to environmental, social and governance-related risks*. COSO.

Competition Commission of India, & Indian Council for Research on International Economic Relations. (2021). *Market study on the telecom sector in India*.

Comptroller and Auditor General of India. (2023). Report No. 16 of 2023: *(Union Government (Compliance Audit)*.

Conde, J., et al. (2024). Applying digital twins for the management of information in turnaround event operations in commercial airports. *arXiv*. https://arxiv.org/abs/2408.14291

CRISIL Ratings. (2021). *CRISIL ratings criteria for mobile telephony services*.

CrossCountry Consulting. (n.d.). *Integrating ESG compliance into enterprise risk management for long-term value*. https://www.crosscountry-consulting.com/insights/blog/integrating-esg-compliance-into-enterprise-risk-management-for-long-term-value/

Cyber and Infrastructure Security Centre. (2025). 2025 *critical infrastructure annual risk review*. Department of Home Affairs, Australian Government. https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-annual-risk-review-2025.pdf

Dabur India Ltd. (n.d.). *Financial results and reports*. https://www.dabur.com/investor-relations/financial-results-reports/

Dash, P. (n.d.). *Towards a critical infrastructure protection programme for India*. Foundation for Integrated National Security. https://finsindia.org/towards-a-critical-infrastructure-protection-programme-for-india-dr-padmalochan-dash.html

David, R. P. (2025). *EdTech industry report 2025: Key data & innovation insights*. StartUs Insights. https://www.startus-insights.com/

Dekker, S. (2019). *Foundations of safety science: A century of understanding accidents.* Routledge.

Deloitte. (2023). *Technology, media, and telecommunications predictions 2023*. Deloitte Insights.

Department of Telecommunications. (2022). *The Indian Telegraph Right of Way (Amendment) Rules, 2022*. Government of India.

Department of Telecommunications. (2024). *Annual report 2024–25*. Ministry of Communications, Government of India.

Dheya Research Team. (2026). *India education to employment gap: Why 53% of graduates are unemployed and what fixes it*. https://www.dheya.com/

Diligent. (n.d.). *Improving board oversight of ERM* [Video]. https://www.diligent.com/resources/videos/improving-oversight-erm

Dobruszkes, F., Dehon, C., & Givoni, M. (2014). Does European high-speed rail affect the current level of air services? An EU-wide analysis. *Transportation Research Part A: Policy and Practice, 69, 461–475*.

Duong, T. T., Brewer, T., Luck, J., & Zander, K. (2019). A global review of farmers' perceptions of agricultural risks and risk management strategies. *Agriculture*, 9(1), 10. https://doi.org/10.3390/agriculture9010010

Dwivedi, P., Ramesh, G., Lakhotia, R., Gupta, M., Awasthi, J., Sinha, A., & Chakraborti, A. (2026). *India skills report 2026*. Confederation of Indian Industry Centre of Excellence for Skills.

Elitecon International. (n.d.). *Market assessment reports.* https://eliteconinternational.com/

Emami Ltd. (n.d.). *Investor relations.* https://www.emamiltd.in/investor-relations/

Enterprise Risk Management Initiative, & AICPA & CIMA. (2025). 2025 *the state of risk oversight: An overview of enterprise risk management practices* (16th ed.). North Carolina State University. https://erm.ncsu.edu/resource-center/2025-the-state-of-risk-oversight-an-overview-of-enterprise-risk-management-practices-16th-edition/

EUROCONTROL. (2024). *Adapting aviation to a changing climate: Effects and impacts of climate change for aviation.*

European Securities and Markets Authority. (2024). *Final report on greenwashing* (ESMA36-287652198-2699).

European Union Aviation Safety Agency. (2023). *Safety Information Bulletin: Global Navigation Satellite System outage and spoofing* (SIB No. 2022-02R2).

Ewing, L.-A. (2021). Rethinking higher education post COVID-19. In J. Lee & S. H. Han (Eds.), *The future of service post-COVID-19 pandemic* (Vol. 1). Springer.

EY. (n.d.). *How to expand future-ready healthcare in India.* https://www.ey.com/en_in/insights/health/how-to-expand-future-ready-healthcare-in-india

Farmonaut. (2025). *Current agriculture issues 2025 India: 9 urgent fixes.* https://farmonaut.com/

Financial Stability Board. (2018). *Supplementary guidance to the FSB principles and standards on sound compensation practices.*

Financial Stability Board. (2019). *Third-party dependencies in cloud services: Considerations on financial stability implications.*

Financial Stability Board. (2025). *FSB roadmap for addressing financial risks from climate change: 2025 progress report.* https://www.fsb.org/uploads/P140725-2.pdf

Flyvbjerg, B. (2014). What you should know about megaprojects and why: An overview. *Project Management Journal, 45(2),* 6–19.

Flyvbjerg, B., & Budzier, A. (2011). Why your IT project may be riskier than you think. *Harvard Business Review, 89(9),* 23–25.

Food and Agriculture Organization of the United Nations. (2026). *GIEWS country brief: India.* https://www.fao.org/giews/

Food and Agriculture Organization of the United Nations, International Fund for Agricultural Development, United Nations Children's Fund, World Food Programme, & World Health Organization. (2025). *The state of food security and nutrition in the world 2025: Addressing high food price inflation for food security and nutrition*. FAO. https://doi.org/10.4060/cd6008en

Food Logistics. (n.d.). *Risk & compliance*. https://www.foodlogistics.com/risk-compliance/

Food Safety and Standards Authority of India. (2006). *Food Safety and Standards Act, 2006*.

Food Safety and Standards Authority of India. (2011). *Food Safety and Standards (Licensing and Registration of Food Businesses) Regulations, 2011* (as amended through 2023).

Foundation for Integrated National Security. (n.d.). *Towards institutionalising India's critical infrastructure protection programme.* https://finsindia.org/towards-institutionalising-india-critical-infrastructure-protection-programme.html

From contagion to containment: A review of systemic financial risk and regulatory governance. (n.d.). Virtus Interpress. https://virtusinterpress.org/From-contagion-to-containment-A-review-of-systemic-financial-risk-and-regulatory-governance.html

Frontiers. (n.d.). *Frontiers in Sustainable Food Systems*. https://www.frontiersin.org/journals/sustainable-food-systems

Gambhir, A., Albert, M. J., Doe, S. S. P., Donges, J. F., Farajalla, N., Giatti, L. L., Gundimeda, H., Hendel-Blackford, S., Homer-Dixon, T., Hoyer, D., Adan, S., Jacome-Polit, D., Kemp, L., Korowicz, D., Kovacic, Z., Kwakkel, J., Laybourn, L., Lempert, R., Mahamoud, A., … Richardson, R. (2025). A systemic risk assessment methodological framework for the global polycrisis. Nature Communications, 16, Article 7382. https://doi.org/10.1038/s41467-025-62029-w

Gerbec, M., Čaleta, D., Modic, J., Giunta, G., & Durante, N. G. (2025). Cross-CI assessment of risks and cascading effects in the ATLANTIS project. *Applied Sciences, 15*(19), Article 10374. https://doi.org/10.3390/app151910374

Gour, A. (2025). *State of India's environment 2025: A grim warning for climate, health, and development*. Climate Fact Checks.

Gourdel, R., Monasterolo, I., Dunz, N., Mazzocchetti, A., & Parisi, L. (2022). *The double materiality of climate physical and transition risks in the euro area* (ECB Working Paper No. 2665). European Central Bank.

Government of India. (2025a). *Annual report 2024–25*. Protection of Plant Varieties and Farmers' Rights Authority.

Government of India. (2025b). *Economic Survey 2024–25*. Ministry of Finance.

Government of India. (2025c). *One nation, one license, one payment: Balancing AI innovation and copyright. Part I: Working paper on generative AI and copyright*. Ministry of Commerce and Industry.

Government of India. (2026). *Economic Survey 2025–26*. Ministry of Finance.

Goyal, A., Nathani, N., Prabhala, P., Breman, T., Agarwal, A., & Goswami, D. (2025). *Value creation in Indian agriculture. McKinsey & Company*.

Grant Thornton Bharat. (n.d.). *BFSI and fintech: Road ahead in the digital era.* https://www.grantthornton.in/insights/thought-leadership/bfsi-and-fintech-road-ahead-in-the-digital-era/

GSMA. (2022a). *2G and 3G network sunsetting.*

GSMA. (2022b). *The Internet value chain 2022.*

Hardaker, J. B., Lien, G., Anderson, J. R., & Huirne, R. B. M. (2015). *Coping with risk in agriculture: Applied decision analysis* (3rd ed.). CABI.

Hindustan Unilever Limited. (2025). *Integrated annual report 2024–25*.

ICICI Lombard. (2024). *FMCG sector risk index 2024*. https://www.icicilombard.com/docs/default-source/ciri/2024/fmcg-sector.pdf

ICICI Lombard General Insurance Company Limited. (2022). *FMCG sector risk report 2022* (Corporate India Risk Index).

ICICI Lombard General Insurance Company Limited. (2023). *Agriculture sector risk report 2023* (Corporate India Risk Index).

India Brand Equity Foundation. (n.d.-a). *FMCG industry*. https://www.ibef.org/industry/fmcg

India Brand Equity Foundation. (n.d.-b). *Infrastructure development in India: Market size, investments and government initiatives*. https://www.ibef.org/industry/infrastructure-sector-india

India Brand Equity Foundation. (2025). *FMCG infographic*: May 2025.

India Code. (2023). *The Digital Personal Data Protection Act,* 2023 (Act No. 22 of 2023). Ministry of Law and Justice.

Indian Council for Research on International Economic Relations. (2018). *The anatomy of an internet blackout: Measuring the economic impact of internet shutdowns in India.*

Indian Institute of Science. (2025). *Policy brief: Vulnerability of agriculture households.*

Industrial Cyber. (2025). *NERC 2025 RISC report finds cybersecurity, supply chain and critical infrastructure interdependencies among top reliability risks*. https://industrialcyber.co/reports/nerc-2025-risc-report-finds-cybersecurity-supply-chain-critical-infrastructure-interdependencies-among-top-reliability-risks/

Institute of Risk Management. (2002). *A risk management standard.*

Institute of Risk Management India Affiliate. (n.d.). *Enterprise risk management standards and regulations: Navigating from compliance to culture*. https://www.theirmindia.org/blog/enterprise-risk-management-standards-and-regulations-navigating-from-compliance-to-culture/

Institute of Risk Management India Affiliate. (2023a). *Enhancing sustainability: Top 30 risks faced by the education sector.*

Institute of Risk Management India Affiliate. (2023b). *Navigating the shelves: Top 30 risks in the FMCG sector.*

Institute of Risk Management India Affiliate. (2023c). *Weathering the storm: Top 30 risks in the agriculture sector.*

International Air Transport Association. (2024a). *Airport Handling Manual (AHM).*

International Air Transport Association. (2024b). *Standard Ground Handling Agreement (SGHA).*

International Air Transport Association. (2025). *Global air cargo market analysis: Post-pandemic cyclicality.*

International Civil Aviation Organization, International Air Transport Association, & International Federation of Air Line Pilots' Associations. (2015). *Fatigue management guide for airline operators (2nd ed.).*

International Energy Agency. (2023). *India gas market report: Outlook to 2030.*

International Finance Corporation. (n.d.). *IFC handbook on agro supply chains.*

International Labour Organization. (2019). Working on a warmer planet: *The impact of heat stress on labour productivity.*

International Labour Organization. (2024). *Global employment trends for youth 2024.*

International Monetary Fund. (2023). *Global financial stability report: Safeguarding financial stability amid high inflation.*

International Organization of Securities Commissions. (2023). *Supervisory practices to address greenwashing* (Final Report FR12/23).

International Science Council. (2022, March 10). *Systemic risk briefing note highlights complexity of interconnected risks.* https://council.science/news/systemic-risk-briefing-note/

Iyer, K. C., & Thomas, N. (2021). An econometric analysis of domestic air traffic demand in regional airports: Evidence from India. *Journal of Air Transport Management*, 94, 102070.

Jain, A., Jhunjhunwala, G., Khalid, W., Wusqa, U. T., & Gupta, S. (2025). ***Building a green economy for Viksit Bharat: New opportunities for jobs, growth and sustainability in India.*** Council on Energy, Environment and Water.

The Japan Times. (2025, October 11). ***The world's chip supply chain is bracing for fallout from China's rare earth controls.*** https://www.japantimes.co.jp/business/2025/10/11/economy/china-chips-rare-earths-focus/

Jencap Group. (2023). ***The seven most common risks in agribusiness.*** https://jencapgroup.com/insights/agriculture/the-seven-most-common-risks-in-agribusiness/

Kapur, D., & Vaishnav, M. (Eds.). (2018). ***Costs of democracy: Political finance in India.*** Oxford University Press.

Keizer, J. A., & Halman, J. I. M. (2009). Risks in major innovation projects: ***A multiple case study within one of the world's leading fast-moving consumer goods companies. International Journal of Technology Management,*** 48(4), 499–517.

Khatri, P., Kumar, P., Shakya, K. S., Kirlas, M. C., & Tiwari, K. K. (2024). Understanding the intertwined nature of rising multiple risks in modern agriculture and food systems. ***Environment, Development and Sustainability***, 26(9), 24107–24150. https://doi.org/10.1007/s10668-023-03638-7

Kochar, J. (2025). 2025 and beyond: ***Redefining risk management and internal controls*** [Post]. LinkedIn. https://www.linkedin.com/pulse/2025-beyond-redefining-risk-management-internal-controls-jatin-kochar-ob4yc

Komljenovic, J., Hansen, M., Sellar, S., & Birch, K. (2024). ***EdTech in higher education: Empirical findings from the project "Universities and Unicorns: Building digital assets in the higher education industry.***" Centre for Global Higher Education, University of Oxford.

KPMG. (n.d.). ***Consumer and retail.*** https://kpmg.com/in/en/home/industries/consumer-and-retail.html

KPMG. (2019). ***Imagine a new connected world: Intelligent. Immersive. Inventive.***

KPMG. (2025). ***The Indian FMCG sector: Q1 FY26.***

Kumar, G. A. (n.d.). ***Risks in agriculture: Types of challenges that farmers face.*** Wikifarmer. https://wikifarmer.com/

Kumar, R., & Badika, A. (2026). India's generative AI moment: Copyright law at regulatory crossroads. Bar & Bench.

Kumar, S., Mishra, A. K., Pramanik, S., Mamidanna, S., & Whitbread, A. (2020). Climate risk, vulnerability and resilience: Supporting livelihoods of smallholders in semiarid India. ***Land Use Policy***, 97, 104729. https://doi.org/10.1016/j.landusepol.2020.104729

Kumar, V. (2026). Online higher education boom: NEP 2020, UGC regulations, trends, and future outlook. ***Careers360***. https://www.careers360.com/

Maersk. (2025, February 28). ***Navigating 2025's geopolitical supply chain landscape.*** https://www.maersk.com/insights/resilience/2025/02/28/geopolitical-supply-chain-landscape

Marginson, S. (2004). Don't leave me hanging on the Anglophone: The potential for online distance higher education in the Asia-Pacific region. ***Higher Education Quarterly***, 58(2–3), 74–113. https://doi.org/10.1111/j.1468-2273.2004.00263.x

Marginson, S. (2006). Dynamics of national and global competition in higher education. ***Higher Education, 52***, 1–39. https://doi.org/10.1007/s10734-004-7649-x

Marico Limited. (2025). Future-ready, agile, resilient: ***Annual report 2024–25.***

MarketsandMarkets. (n.d.). ***Enterprise risk management (ERM) market: Global forecast to 2030.*** https://www.marketsandmarkets.com/Market-Reports/enterprise-risk-management-market-113046879.html

Marsh. (n.d.). *From risks to resilience: Technology transformation in healthcare*. https://www.marsh.com/en/industries/healthcare/insights/from-risks-to-resilience.html

Marsh. (2024). *Fielding challenges: The top risks facing today's agribusinesses.*

Maslach, C., & Leiter, M. P. (2016). Understanding the burnout experience: Recent research and its implications. *World Psychiatry, 15*(2), 103–111.

Mastering ERM and strategy governance: Board-level takeaways. (n.d.). [Post]. LinkedIn. https://www.linkedin.com/pulse/mastering-erm-strategy-governance-board-level-im-taking-bin-himd-lw78f

McKinsey & Company. (n.d.). *A board perspective on enterprise risk management* (McKinsey Working Papers on Risk No. 18). https://www.mckinsey.com/client_service/risk/working_papers

McKinsey & Company. (2025). *Value creation in Indian agriculture.*

McKinsey & Company. (2026). *The great unbundling of Indian e-commerce: MSMEs and the direct-to-consumer revolution.*

Ministry of Electronics and Information Technology. (2023a). *India Stack and Digital Public Infrastructure: Framework for scalable inclusion.*

Ministry of Electronics and Information Technology. (2023b). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (as amended in 2023).

Ministry of Law and Justice. (2023). *The Telecommunications Act, 2023.*

Ministry of Statistics and Programme Implementation. (2024). *Flash report on central sector projects.*

Ministry of Tourism. (2025). *India tourism data compendium 2025* (66th ed.). Government of India.

Mishra, A. K., Kumar, A., Joshi, P. K., & D'Souza, A. (2018). Production risks, risk preferences, and contract farming: Impact on food security in India. *Applied Economic Perspectives and Policy*, 40(3), 353–378.

Moreira, J. C. R. (2025). Risk management in education: A systematic literature review of the last five years. *Revista de Gestão Social e Ambiental,* 19(1). https://doi.org/10.24857/rgsa.v19n1-127

Morris, M. (2025, July). *Critical infrastructure cybersecurity landscape (July 27–28, 2025)* [Post]. LinkedIn. https://www.linkedin.com/pulse/critical-infrastructure-cybersecurity-landscape-july-morris-cciso-fjdoc

Mothi Prasanna, S., & Thennavan, B. (2023). Complete case analysis: *PepsiCo Corporation v. Gujarat Farmers. Journal of Emerging Technologies and Innovative Research,* 10(12).

Narain, S., & Mahapatra, R. (Eds.). (2025). *State of India's environment in figures 2025. Centre for Science and Environment.*

National Institute of Standards and Technology. (n.d.). *AI risk management framework*. U.S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework

National Institute of Standards and Technology. (2023). *Post-quantum cryptography standardization.*

National Institute of Standards and Technology. (2024). *Adversarial machine learning: A taxonomy and terminology of attacks and mitigations* (NIST AI 100-2e2023). U.S. Department of Commerce.

Neeti Niyaman. (2025). *ESG compliance in India 2025: SEBI BRSR and CSR rules.* https://neetiniyaman.com/esg-compliance-india-regulations-reporting/

Nestlé India Limited. (2025). *Annual report 2024–25.*

Nishith Desai Associates. (2018). *EdTech platform held liable for hosting infringing content. Lexology.*

Nishith Desai Associates. (2024, June). *Advancing ESG: India's new disclosure frameworks by RBI and SEBI*. https://www.nishithdesai.com/fileadmin/user_upload/Html/Hotline/Yes_Governance_Matters_June0424-M.html

NITI Aayog. (n.d.). *Goal 2: End hunger, achieve food security and improved nutrition and promote sustainable agriculture*.

NITI Aayog. (2026). *Scenarios towards Viksit Bharat and net zero: Agriculture* (Vol. 6).

Occupational Safety and Health Administration. (2021). *Communication tower erection and maintenance safety*.

Oil Industry Safety Directorate. (2025). *OISD Standard 116 (Revision): Fire protection facilities for petroleum refineries and oil/gas processing plants*.

Oliver Wyman. (2026). *Global fleet and MRO market forecast 2026–2036*.

Open Risk. (n.d.). *The periodic table of risk elements*. Open Risk Management. https://www.openriskmanagement.com/the-periodic-table-of-risk-elements/

Organisation for Economic Co-operation and Development. (n.d.). *Supply chain interdependencies*. https://www.oecd.org/en/topics/sub-issues/supply-chain-interdependencies.html

Organisation for Economic Co-operation and Development. (2025). Ensuring the resilience of critical infrastructure. *In Government at a glance 2025*. OECD Publishing. https://www.oecd.org/en/publications/2025/06/government-at-a-glance-2025_70e14c6c.html

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology.

Pathak, B. K. (2022a). Economic implications of MOOCs in higher education: An Indian perspective. *WEA Commentaries, 12(1),* 7–9.

Pathak, B. K. (2022b). Economic realities of virtual higher education in a post-pandemic India. *Shiksha Vimarsha*, 35–44.

Pescaroli, G., & Alexander, D. (2017). Cross-sectoral and multi-risk approach to cascading disasters. *In Words into action guidelines: National disaster risk assessment* (pp. 23–31). United Nations Office for Disaster Risk Reduction. https://www.preventionweb.net/files/52828_ccrosssectoralmultirisk.pdf

pharmaphorum. (n.d.). *Ensuring compliance, strengthening resilience: Strategies for pharma supply chains*. https://pharmaphorum.com/market-access/ensuring-compliance-strengthening-resilience-strategies-pharma-supply-chains

Polycrisis. (2026). *Global risk forecast 2026*. https://polycrisis.org/resource/global-risk-forecast-2026/

Polycrisis and systemic risk: Assessment, governance and response. (n.d.). Deutsche Nationalbibliothek. https://d-nb.info/1372622829/34

Pooja, S. P. (2025). Climate change and the triple threat: Water scarcity, agriculture decline, and food insecurity in India. *Indian Journal of Legal Review*, 5(12).

Press Information Bureau. (2025). *India launches first Digital Threat Report 2024 to support cybersecurity in the banking, financial services and insurance (BFSI) sector* [Press release]. Government of India. https://pib.gov.in/PressReleseDetailm.aspx?PRID=2119801

Procter & Gamble. (n.d.). *Investor relations*. https://www.pginvestor.com/

Protection of Plant Varieties and Farmers' Rights Authority. (2025). *Annual report 2024–25*.

Renuka. (2026, May 25). How is India particularly vulnerable to heat-related stress on its food system? The Indian Express.

Research Institute for Sustainability. (n.d.). *Advancing systemic risk assessment for complex, interdependent systems*. RIFS Potsdam. https://publications.rifs-potsdam.de/rest/items/item_6005307_2/component/file_6005308/content

Reserve Bank of India. (2024). *State finances: A study of budgets of 2023–24*.

Reserve Bank of India. (2026). *Annual report 2025–26*.

Resilience in critical infrastructures: Conceptual frameworks addressing convergence of communication, energy, finance and health-care systems. (2025). *International Journal of Multidisciplinary Research and Growth Evaluation*. https://www.multiresearchjournal.com/arclist/list-2025.5.5/id-5023

Resilient telecommunications infrastructure. (n.d.). *World Bank Group*.

Reuters. (2025, October 9). *China expands rare earths restrictions, targets defence and chips*. https://www.reuters.com/world/china/china-tightens-rare-earth-export-controls-2025-10-09/

Revealing sustainable insights: Power BI enhanced bibliometric analysis of ESG initiatives and climate-related financial risks. (n.d.). *Journal of International Commercial Law and Technology*. https://jiclt.com/article/revealing-sustainable-insights-power-bi-enhanced-bibliometric-analysis-of-esg-initiatives-and-climate-related-financial-risks-249/

Risk & Insurance. (2021). *Seven critical risks facing the agriculture industry*.

Risk Management Association of India. (n.d.-a). *Healthcare risk management in India explained.* https://rmaindia.org/healthcare-risk-management-in-india-explained/

Risk Management Association of India. (n.d.-b). *How to integrate ESG risks into the enterprise's overall risk management*. https://rmaindia.org/how-to-integrate-esg-risks-into-the-enterprises-overall-risk-management/

Risk Management Association of India. (n.d.-c). *Why organizations fail despite having ERM frameworks.* https://rmaindia.org/why-organizations-fail-despite-having-erm-frameworks/

Romanosky, S., & Petrun Sayers, E. L. (2024). Enterprise risk management: How do firms integrate cyber risk? *Management Research Review*, 47(1), 1–17. https://doi.org/10.1108/MRR-10-2021-0774

Saheed Bhagat Singh College. (2025). *EdTech industry report: Growth, challenges and trends.*

Saint Akadiri, S., & Ozkan, O. (2025). Cross-quantile interdependence among future energy, metaverse, artificial intelligence, fintech, space, cyber security, and digital assets. *Energy & Environment*. Advance online publication. https://doi.org/10.1177/0958305X251349475

Schneider, L., & La Hoz Theuer, S. (2019). Environmental integrity of international carbon market mechanisms under the Paris Agreement. *Climate Policy*, 19(3), 386–400.

Scott, M. (2025). Understanding critical infrastructure as systems and networks [Technical paper]. https://ihsonline.org/Portals/0/Tech%20Papers/2025/Scott_Understanding_Critical_Infrastructure_as_Systems_and_Networks.pdf

Shah, S. Q. A., Lai, F.-W., Shad, M. K., Hamad, S., & Ellili, N. O. D. (2025). Exploring the effect of enterprise risk management for ESG risks towards green growth. *International Journal of Productivity and Performance Management*, 74(1), 224–249. https://doi.org/10.1108/IJPPM-10-2023-0582

Sharma, S. K., & Pathak, S. L. (2024). *Urbanization, population and environment. Springer*. https://doi.org/10.1007/978-981-97-6020-6

Shukla, S., Abraham, S., & Parekh, S. (2025). *How can India scale climate-resilient agriculture practices and climate-smart farming*? Council on Energy, Environment and Water.

SiliconExpert. (2025). *China's new rare earth export controls: Impact on global supply chains* [Post]. LinkedIn. https://www.linkedin.com/posts/siliconexpert_compliancemanagement-supplychainrisk-rareearths-activity-7387140835152347138-9qLe

Singh, B., & Yadav, J. P. (2022). Sustainable agriculture development through organic farming in India. *ECS Transactions*, 107(1), 14919–14929. https://doi.org/10.1149/10701.14919ecst

Singh, R. B., Paroda, R. S., & Dadlani, M. (2022). Science, technology and innovation. In R. Chand, P. Joshi, & S. Khadka (Eds.), *Indian agriculture towards 2030*. Springer. https://doi.org/10.1007/978-981-19-0763-0_8

Singh, S. K., & Beillard, M. J. (2024). *Grain and feed annual: India* (GAIN Report No. IN2024-0016). U.S. Department of Agriculture Foreign Agricultural Service.

Smart Compliance. (2021). *How agribusiness owners can bolster risk management efforts*. https://smartcompliance.co/

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7), 1880–1903.

Soni, R., Gupta, R., Agarwal, P., & Mishra, R. (2022). Organic farming: A sustainable agricultural practice. *Vantage: Journal of Thematic Analysis*, 3(1), 21–44.

S&P Global Mobility. (2025, May). *Critical minerals shortages: A looming threat to the EV industry*. https://www.spglobal.com/automotive-insights/en/blogs/2025/05/critical-minerals-shortages-looming-threat-ev-industry

Srinivasan, N. (2025). *State of India's livelihoods 2025*. ACCESS Development Services.

Supply Chain Wizard. (2025). *Redefining resilience: Lessons from 2024 fuelling pharma supply chain strategy in 2025*. https://supplychainwizard.com/redefining-resilience-lessons-from-2024-fueling-pharma-supply-chain-strategy-in-2025/

Supreme Court of India. (2019). *Union of India v. Association of Unified Telecom Service Providers of India.*

Tata Consumer Products Limited. (n.d.). *Annual reports.*

Telecom Regulatory Authority of India. (2017). *Recommendations on approach towards sustainable telecommunications.*

Telecom Regulatory Authority of India. (2023). *Consultation paper on assignment of spectrum for space-based communication services.*

Telecom Sector Skill Council. (2023). *Telecom talent in the 5G era: Demand–supply gap report 2023–24*.

TeleGeography. (2023). *The future of submarine cable maintenance.*

Tiwari, R., Chand, K., Bhatt, A., Anjum, B., & Thirunavukkarasu, K. (2021). Agriculture 5.0 in India. In S. Khan, K. Thirunavukkarasu, A. AlDmour, & S. S. Shreem (Eds.), *A step towards Society 5.0* (pp. 156–175). CRC Press.

Total Assure. (2025). *AI cybersecurity statistics in 2025: Comprehensive data on threats and defences*. https://totalassure.com/blog/ai-cybersecurity-stats

Towards resilient sustainability: An adaptive model of risk management integration in sustainability accounting for high-risk industries. (n.d.). *RSF Conference Series: Business, Management and Social Sciences.* https://proceeding.researchsynergypress.com/index.php/rsfconferenceseries1/article/view/939

TradeVerifyd. (2025). *5 geopolitical trends that could disrupt your supply chain in 2025*. https://tradeverifyd.com/resources/5-geopolitical-trends-that-could-disrupt-your-supply-chain-in-2025

TrustCloud. (n.d.). *ISO 31000 vs COSO ERM: Enterprise risk frameworks compared*. https://www.trustcloud.ai/risk-management/iso-31000-vs-coso-erm-frameworks-navigating-the-risk-landscape/

Tucker, R. B. (2025, November 25). Polycrisis: What's next for humanity in the age of acceleration? *Forbes*. https://www.forbes.com/sites/robertbtucker/2025/11/25/polycrisis-whats-next-for-humanity-in-the-age-of-acceleration/

Understanding ransomware through the lens of disaster risk: Implications for cybersecurity and economic stability. (n.d.). *International Journal of Disaster Risk Management.* https://internationaljournalofdisasterriskmanagement.com/index.php/Vol1/article/view/104

Unicommerce. (n.d.). Resources and warehouse management insights.

United Nations Conference on Trade and Development. (2024). *Enhancing supply chain resilience amid rising global risks.* https://unctad.org/news/enhancing-supply-chain-resilience-amid-rising-global-risks

United Nations Office for Disaster Risk Reduction. (n.d.). *Scoping study on compound, cascading and systemic risks in the Asia-Pacific region*. https://www.undrr.org/media/79226/download

United Nations Office for Disaster Risk Reduction. (2022). *Global assessment report on disaster risk reduction 2022: Our world at risk.*

Varuna Group. (2025). What is FMCG logistics? Top seven FMCG challenges and how to overcome them. https://varuna.net/

Vassilev, A., Oprea, A., Fordyce, A., & Anderson, H. (2024). A*dversarial machine learning: A taxonomy and terminology of attacks and mitigations* (NIST AI 100-2e2023). National Institute of Standards and Technology.

Vectra AI. (n.d.). *Financial services cybersecurity explained: Threats and defenses.* https://www.vectra.ai/topics/financial-services-cybersecurity

Verma, D. (2025). From unicorns to uncertainty: A critical review of Indian EdTech failures. *Inspira: Journal of Commerce, Economics & Computer Science, 11(2), 63–68.*

Watson Farley & Williams. (2023). *Aviation in India transformed: A guide for international aircraft financiers on investing in India's unprecedented expansion.*

World Bank. (2020). *Resilient tourism: Competitiveness in the face of disasters.*

World Bank. (2022). *Financing India's urban infrastructure needs: Constraints to commercial financing and prospects for policy action.*

World Bank. (2023). *Private participation in infrastructure: Transport and aviation.*

World Bank Group. (2024a). *Annual report fiscal year 2024: Food Systems 2030.*

World Bank Group. (2024b). *Digital public infrastructure and development: A World Bank Group approach.*

World Economic Forum. (2021). *Clean skies for tomorrow: Sustainable aviation fuels as a pathway to net-zero aviation.*

World Economic Forum. (2024). *Global food security trends and predictions 2024.*

World Economic Forum. (2025a, January). *3 surprising findings in the Global Risks Report 2025.* https://www.weforum.org/stories/2025/01/3-surprising-findings-global-risks-report-2025/

World Economic Forum. (2025b). *The future of jobs report 2025.*

World Economic Forum. (2025c). *The global risks report 2025* (20th ed.). https://www.weforum.org/publications/global-risks-report-2025/

World Economic Forum. (2026). The global risks report 2026 (21st ed.). https://www.weforum.org/publications/series/global-risks-report/

World Health Organization. (2020). *5G mobile networks and health.*

XcalData. (n.d.). *XcalData portal.*

XcalData. (2026, February). *Indian FMCG sector analysis.*

Disclaimer

This Report has been prepared jointly by **KPMG in India, Mahindra University**, and the **Institute of Risk Management (IRM) India Affiliate** (collectively referred to as "**Parties**") for general informational and educational purposes. The analyses, observations, data, methodologies, frameworks and recommendations presented herein are derived from information obtained from publicly available sources and other sources considered reliable at the time of publication. The contents of this Report are intended to encourage awareness and informed discussion on the subject matter covered and should not be construed as definitive guidance or recommendations for any particular situation without appropriate independent review, validation and professional assessment. Nothing contained in this Whitepaper constitutes legal, financial, regulatory, technical or other professional advice, nor should it be interpreted as creating any contractual obligation or relationship.

Although reasonable care has been exercised in the preparation of this Report, the Parties do not warrant or guarantee the accuracy, completeness, adequacy or reliability of the information contained herein. The Parties accept no responsibility for any errors, omissions or consequences arising from the use of, or reliance upon, the contents of this Report. References to information, opinions or materials originating from third parties are provided for convenience only and should not be regarded as an endorsement of their accuracy, completeness or reliability. Readers are solely responsible for evaluating the suitability of the information for their own purposes and are encouraged to seek independent professional advice based on their specific circumstances.

All intellectual property rights in any materials, content, data, frameworks, methodologies or other contributions provided by each Party (**"Contributed Material"**) and incorporated into this Report shall remain the sole and exclusive property of the respective contributing Party. The content of this Report comprises proprietary materials contributed by IRM India Affiliate, Mahindra University and KPMG in India, and the publication of such Contributed Material does not operate as an assignment, transfer or waiver of any intellectual property rights, nor does it grant any licence or right of use except as expressly agreed in writing between the Parties. Except with the prior written consent of the relevant intellectual property owner or as otherwise permitted by applicable law, no part of this Report or any Contributed Material may be reproduced, copied, adapted, published, transmitted, distributed or communicated to any third party in any form or by any means.

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

The IRM logo displayed above belongs to the Institute of Risk Management (IRM) and is used by IRM India Affiliate under authorisation. IRM India Affiliate is the official trade name of Gleco International Private Limited (as per GST registration).

The Mahindra University logo displayed above belongs to the Mahindra University and is used by Mahindra University under authorisation.


irm
Developing risk professionals
KPMG
Mahindra™
University
Global Thinkers. Engaged Leaders.
Knowledge Partner