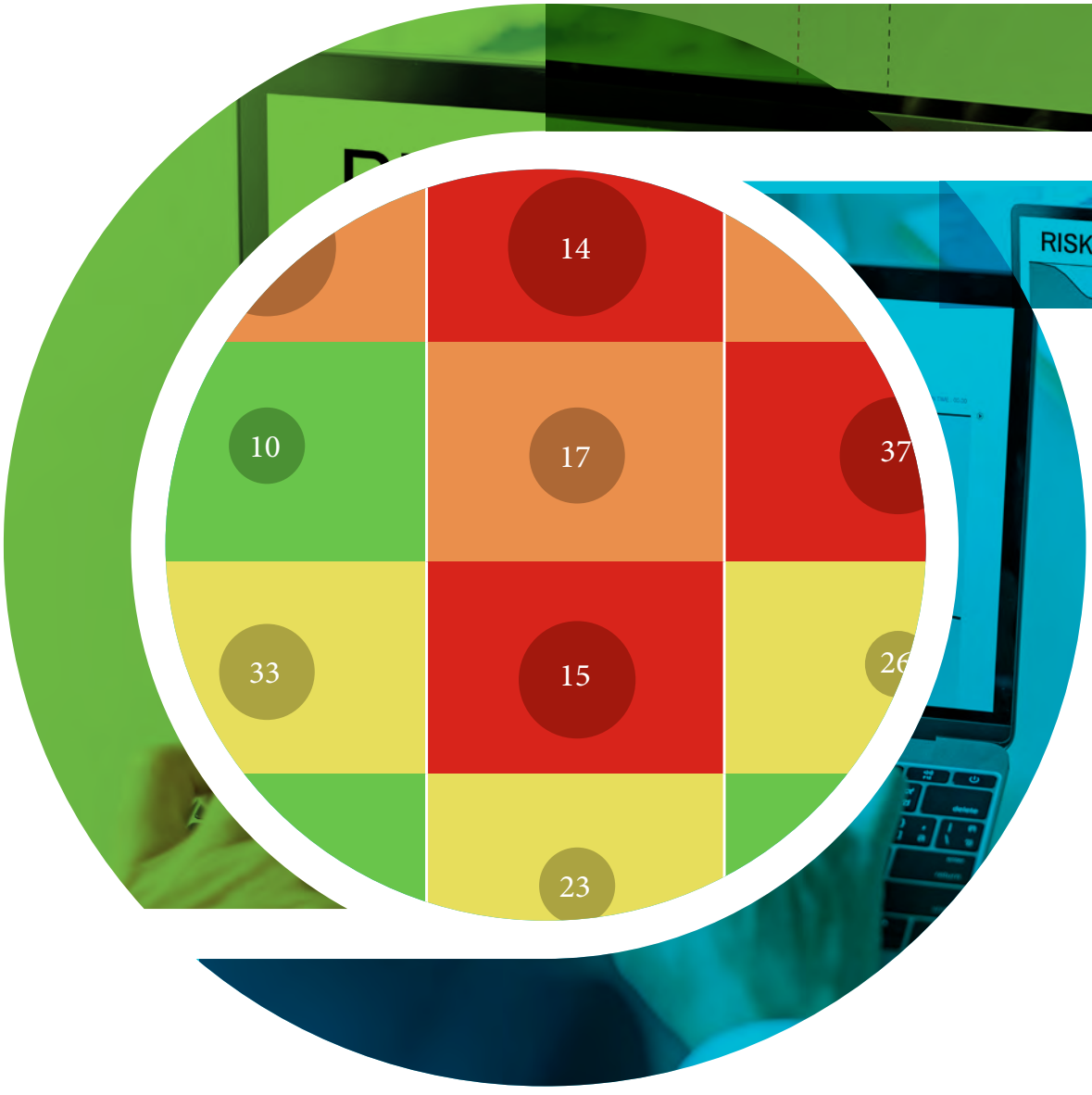
MODEL RISK CODE

Enabling ▪ Faster ▪ Bolder ▪ Risk-intelligent Decisions



November, 2022

GRMI GLOBAL RISK MANAGEMENT INSTITUTE

FICCI

CONTENTS

PREFACE

The 'FICCI-GRMI Risk Code' is a practical playbook with best practices and guidelines around risk management, covering two key aspects: Key Principles of Risk Management ('What') and Implementation of Risk Management ('How').

The Risk Code also covers how risk management is nuanced for MSMEs and for new-age companies which include internet-based companies and start-ups as defined by the Department for Promotion of Industry and Internal Trade. The Risk Code would provide a seamless linkage with other governance and business frameworks operating within the organisation.

The Risk Code applies to entities including, but not limited to, listed companies, public unlisted companies, private companies, start-ups, not-for-profit organisations, societies, and trusts. The target audience of the Risk Code includes:

a. All those engaged in managing risk for their organisation including the Board, Risk Management Committee, CEO, CXOs, Business Unit/Operating Heads, CROs, and business managers.

b. All stakeholders who are directly involved in an organisation's business operations or are interested in the organisation's business, or can influence it including, but not limited to, Employees, Vendors, Customers, Lenders, Government, Regulators, Shareholders, Financial institutions, Community, Rating agencies, and Industry associations.

It is a practical playbook with best practices and guidelines around risk management.

The Risk Code broadly covers the following chapters and each chapter is further classified into various sub-chapters, as necessary.

RELEVANCE OF THE RISK CODE

Why it is imperative for organisations to adopt the Risk Code.

PRINCIPLES OF THE RISK CODE

Covers the key principles around which the Risk Code is structured for adoption by organisations. The seven principlesrevolve around Strategy and Leadership, Risk-embracing Culture, Ownership and Empowerment, Resources and Structure, Communication & Reporting, Governance and Oversight and Risk Data & information Repository.

IMPLEMENTATION GUIDELINES

Provides implementation guidance around the seven principles and is a playbook for the Board of Directors, Risk Management Committee, CEO, and CXOs.

INDUSTRY/SECTORAL VIEW

• Expansion of Risk Management Committee applicability beyond the top 1000 organisations in terms of market capitalisation currently mandated as per SEBI's Listing Obligations and Disclosure Requirement Regulations, 2015, as amended.

• Dynamic regulatory framework, the expansive role of the Risk Management Committee under the new regulations, coupled with an objective to report any forensic reviews.

• Risk management implementation for MSMEs and new-age companies, which include internet-based companies and start-ups as defined by the Department for Promotion of Industry and Internal Trade.

FOREWORD FICCI

ARUN CHAWLA
Director General,
FICCI

We are pleased to present the pioneering work on risk management–Model Risk Code, a practical playbook for the Indian industry with effective enablers for the implementation of risk management practices so that organisations can take bolder, faster, risk-intelligent business decisions.

The Risk Code is intended for listed companies, public unlisted companies, private companies, start-ups, not-for-profit organisations, societies, trusts, as well as MSMEs and start-ups, for which the implementation of risk management practices is nuanced due to their dynamic nature of business, varying maturity levels, and risk appetite. The Risk Code would be especially useful for the sectors witnessing multi-dimensional disruption across technological, demographic, financial, and other external aspects.

Against the background of an evolving spectrum of risks, be it industry-specific risks, strategic, ESG, operational, reporting, competition, people, reputational, compliance, physical security, data privacy, or business continuity risks, there is general consensus that being 'risk intelligent' offers competitive advantage to organisations; however, not having robust risk management practices often leads to an existential crisis. Underscoring the value that can be derived through the implementation of risk management practices, FICCI and Global Risk Management Institute had collaborated to develop a 'Model' Risk Code for Indian industry that guides business for effectively managing risks in all segments of business.

We are grateful to Mr M Damodaran, Chairperson, Excellence Enablers and former Chairman, SEBI, for his leadership to the Task Force on Risk and esteemed members of the Task Force for their guidance in developing the Code. We would also like to place on record our appreciation for the comprehensive work undertaken in formulating the Code by our partner, Global Risk Management Institute, and its Industry Interaction Council comprising Prof. Madhu Vij, Visiting Faculty at IIM Raipur & IIM Jammu; Mr. Mukesh Butani, Founding & Managing Partner, BMR Legal; Prof. Rajan Saxena, Former Vice-Chancellor of SVKM's NMIMS; Mr. Richard Rekhy, Board Member, KPMG Dubai; and Ms. Ritu Chawla Kochhar, India Head, Spencer Stuart.

We hope that the Code would guide businesses to develop effective enablers for the practical implementation and benefit from making risk-intelligent decisions for not only dealing with risks but also optimising risks.

FOREWORD CHAIRMAN, RISK TASKFORCE

M DAMODARAN

Chairperson, Excellence Enablers
and Former Chairman, Securities and
Exchange Board of India (SEBI)

It gives me great pleasure in bringing to you the Model Risk Code ("MRC") for corporates. This is a practical playbook with best practices and guidelines relating to risk management. The MRC is intended to equip corporates with an enabling tool to implement robust risk management practices.

This initiative is very critical in this day and age. There is a clear recognition that the corporate universe has not attached adequate importance to risk for several years. Events such as COVID-19 pandemic and the recent geopolitical tensions have further exposed the vulnerability of the corporate sector, which has borne the brunt of several factors, including supply chain risk, demand risk, third-party risks, BCP risk, and the challenges arising out of virtual operations. Boards as well as individual Directors have their tasks cut out in driving a risk culture, as also to create a climate for risk appreciation, awareness, and the implementation of sound practices. The Model Risk Code empowers the corporates to embrace risk management practices and reap its benefits.

With the SEBI LODR Regulations, 2015, as amended, providing for the setting up of Risk Management Committees ("RMC"), risk management as a subject, was brought centrestage. However, the constitution of the RMC in some corporates has been a half-hearted exercise, in terms of composition, time commitment, and the rigour of meetings. Most importantly, the understanding, categorization, and mapping of risks, probability and impact of risks and looking at risk management mechanisms, remained a tick box exercise. While the SEBI Regulations apply only to the top 1000 corporates by market capitalisation, the Model Risk Code does pave the way for appreciation that there is significant merit even for other corporates to voluntarily set up appropriate risk management systems. This coupled with good governance practices will pave the way for a safer corporate universe.

I am hopeful that the Model Risk Code initiative will nudge all stakeholders to drive better adoption of risk management practices, and to take forward the governance and sustainable value creation agenda.

I wish to thank the Federation of Indian Chambers of Commerce & Industry ("FICCI"), Global Risk Management Institute ("GRMI"), and specially the eminent members of the Risk Taskforce for giving shape to this important initiative. I am confident that the MRC will not only drive a risk intelligent Indian corporate universe, but will also set a benchmark for governments, industry associations and corporates globally.

FOREWORD GRMI

SUBHASHIS NATH

Founder & CEO of GRMI, and Founder of Axis Risk Consulting, now Genpact Enterprise Risk Consulting LLP

The world has turned on its head over the last five decades. While Milton Friedman's landmark shareholder-first doctrine suggested that social responsibility of business was to generate profits, the 2022 Edelman Trust Barometer which surveyed 36,000 respondents across 28 countries, found 81% of respondents wanting chief executives to not just speak about social and political issues, but also take the lead in terms of being part of the solution and not just the problem. This is what puts a tremendous responsibility on businesses to be resilient, agile and future ready. The fundamental purpose of Model Risk Code is to enable businesses to be resilient, agile and future ready. In order to get there, businesses need to have risk embedded in the organisation's DNA fuelled by a significant top-down driven change management journey.

Risk management needs to be appreciated as an essential enabler for faster, bolder and better informed decision making, as against the traditional outlook of Risk function in an organization being the roadblock for decision making. This needs value creation and preservation through risk management to be celebrated and shared across the organisation by leadership. ESG is a great area where companies are clearly experiencing the positive value creation by exploiting risk through innovation and agility as compared to competitors. Launching eco-friendly products such as insect-based pet food and biodegradable shoes are well known examples by now. Unilever in 2019 reported that sustainable brands grew 69% faster than the rest of the business and delivered 75% of the company's overall growth. All these go to show the value of effective risk management. While risk around climate and environment were talked about for long, companies have shown how effectively responding to these risks through innovation, agility, approaches such as fail fast, and incredible clarity of purpose from leadership, can deliver significant value creation.

It is also critical that leadership appreciates that effective risk management is about being prepared for non business as usual situations, which require leaders to learn the science of scenario planning on an ongoing basis to be prepared to deal with the risk of known unknows and unknown unknowns, and at the least be ready with responses for non business as usual scenarios.

The couple of other aspects that organizations need to address would be around the positioning and empowerment of the Risk Management organization and its leader, as well having complete clarity about risk management not being synonymous with the internal audit function and this again requires clarity and adequate communication right from the Board and the CEO of the organisation.

At GRMI, we are humbled to have been able to publish the Model Risk Code under the guidance of an incredibly illustrious Risk Task Force comprising Board members, business leaders, CROs, regulator and academia, and in collaboration with FICCI. We look forward to publishing Guidance Notes around areas of interest that we have heard from many of the large corporations and senior leaders, as part of the industry consultation phase in the coming year. At GRMI we remain committed to our "purpose" of providing enablers to building a more resilient, agile, future ready India Inc, which can then be a benchmark for others to look up to and emulate.

MESSAGES

GRMI'S INDUSTRY INTERACTION COUNCIL

PROF. MADHU VIJ - Former Senior Finance Professor FMS Delhi & visiting faculty at IIM Raipur & IIM Jammu

The importance of managing risk in the context of continued technological advancements has become a priority for all organisations. Risk management has become a core factor for business competitiveness and sustainability. I am happy that GRMI along with FICCI has taken on a thought leadership role in developing a model risk code document that will help companies create an ecosystem to build resilience and drive value in organisations.

MUKESH BUTANI - Founding and Managing Partner, BMR Legal Consulting LLP

Risk as a subject has and continues to undergo monumental changes due to influx of regulatory oversight and evolution of new business models. The Model Risk Code (MRC), first of its kind, is meant to serve as a definitive guide to business heads, regulators, students, and academicians. Penned by experts under the pupilage of business leaders, CFO's, CRO's, academicians, regulators, and experienced professionals, it's an outcome of team's efforts resonating their practical insights and experiences.

PROF. RAJAN SAXENA - Former Vice-Chancellor of the SVKM's NMIMS

Given the business complexities in the last decade, risk management has emerged as a highly specialised domain. This triggered GRMI and FICCI to set up a Risk Taskforce under the leadership of Mr. M Damodaran and develop a Model Risk Code (MRC) for the industry. The MRC will sensitise top management and guide the industry in managing their risks effectively should firms choose to implement it. The MRC is much like and yet different from Corporate Governance Code. It will be a significant contribution by two great institutions, GRMI and FICCI.

RICHARD REKHY - Current Board Member, KPMG Dubai

Today companies which want to grow at a fast pace need to have strong risk processes to help them achieve sustainable and profitable growth. To this end it is important that we develop a risk code which is a common language and framework. This is akin to the Corporate Governance Code which was brought in many years back and after many iterations became a Corporate Governance framework for the Indian Corporates. I can see the Model Risk Code (MRC) taking a similar trajectory. This is a start of journey which over a period of times can be embedded into regulation for all corporates.

RITU CHAWLA KOCHHAR - India Head, Spencer Stuart

The risks modern organisations face have grown more complex, fuelled by the rapid pace of globalization. A Model Risk Code (MRC) is a need of the hour and will help equip managements and boards with a holistic framework and proactive approach to managing risks in a comprehensive and consistent manner.

PROFILE

RISK TASKFORCE MEMBERS

M DAMODARAN

Chairperson, Excellence Enablers and Former Chairman, Securities and Exchange Board of India (SEBI)

SUBHASHIS NATH

Founder & CEO of GRMI, and Founder of Axis Risk Consulting, now Genpact Enterprise Risk Consulting LLP

SIDHARTH BIRLA

Past President, FICCI & Chairman, Xpro India Limited

SUBHRAKANT PANDA

Vice President, FICCI and Managing Director, Indian Metals & Ferro Alloys Ltd.

PROF. MADHU VIJ

Academic Council Chair and President at GRMI, Former Senior Finance Professor at FMS Delhi and visiting faculty at IIM Raipur & IIM Jammu

MUKESH BUTANI

Founding and Managing Partner, BMR Legal Consulting LLP

PROF. RAJAN SAXENA

Former Vice-Chancellor of the SVKM's NMIMS

RICHARD REKHY

Former CEO of KPMG India, current Board Member of KPMG Dubai

JENITHA JOHN

FORMER IIA GLOBAL CHAIRPERSON

NAWSHIR MIRZA

Former Senior Partner at E&Y LLP (India)

P. DWARAKANATH

Former Non-Executive Chairman, GSK

PR RAMESH

Former Deloitte India, Chairman

PROFILE

RISK TASKFORCE MEMBERS

PROF. PAUL L. WALKER

James J. Schiro / Zurich
Chair in ERM at
St. John's University

RICHARD EVANS

Former Chief Risk Officer, Citibank

RITU CHAWLA KOCHHAR

India Head, Spencer Stuart

SATYAVATI BERERA

Chief Operating Officer, PwC India

SHARDUL SHROFF

Executive Chairman, Shardul Amarchand Mangaldas & Co

SUNIL MEHTA

Non-Executive Chairman, Yes Bank

JAYANT PALAN

Co-Founder & Director, Global Risk Management Institute

NG SHANKAR

Former Group Executive President – Corporate Audit, Aditya Birla Group

PROF. VINAY DUTTA

Former Senior Professor, Fore School of Management

EXECUTIVE SUMMARY

The risk and opportunity landscape for organisations and its impact is getting wider and more unpredictable as the business environment becomes more complex and dynamic. The spectrum of risks is ever evolving, including industry-specific risks, strategic, ESG, operational, reporting, competition, people, reputational, compliance, physical security, data privacy, and business continuity risks among others. While being 'risk intelligent' may offer novel opportunities and a significant competitive advantage for organisations, not having robust risk management practices may lead to an existential crisis.

The Board should reinforce the need for robust risk management practices that are core to sustainable value creation for the organisation. It should demonstrate its commitment to investing in the requisite resources for robust risk management processes including people, technology, external partners, time, attention, training, and communication. The Board should reward the executive management's ability to anticipate and respond profitably to market opportunities as well as prepare for potentially large adverse risk events. There are three key enablers for executive management.

Firstly, the organisation should promote a culture of 'fail fast' and celebrate such early-stage failures. Early-stage failures have a lower impact which in turn allows organisations to promote creativity, and innovation, and a culture that offers a chance for course correction.

Secondly, risk considerations in decision making must be embedded into the DNA of the organisation. Embedding risk considerations and defining responsibilities for various parts of the risk management process should be part of the KRA definition and taking risk-intelligent decisions should be incentivised by the operating plan.

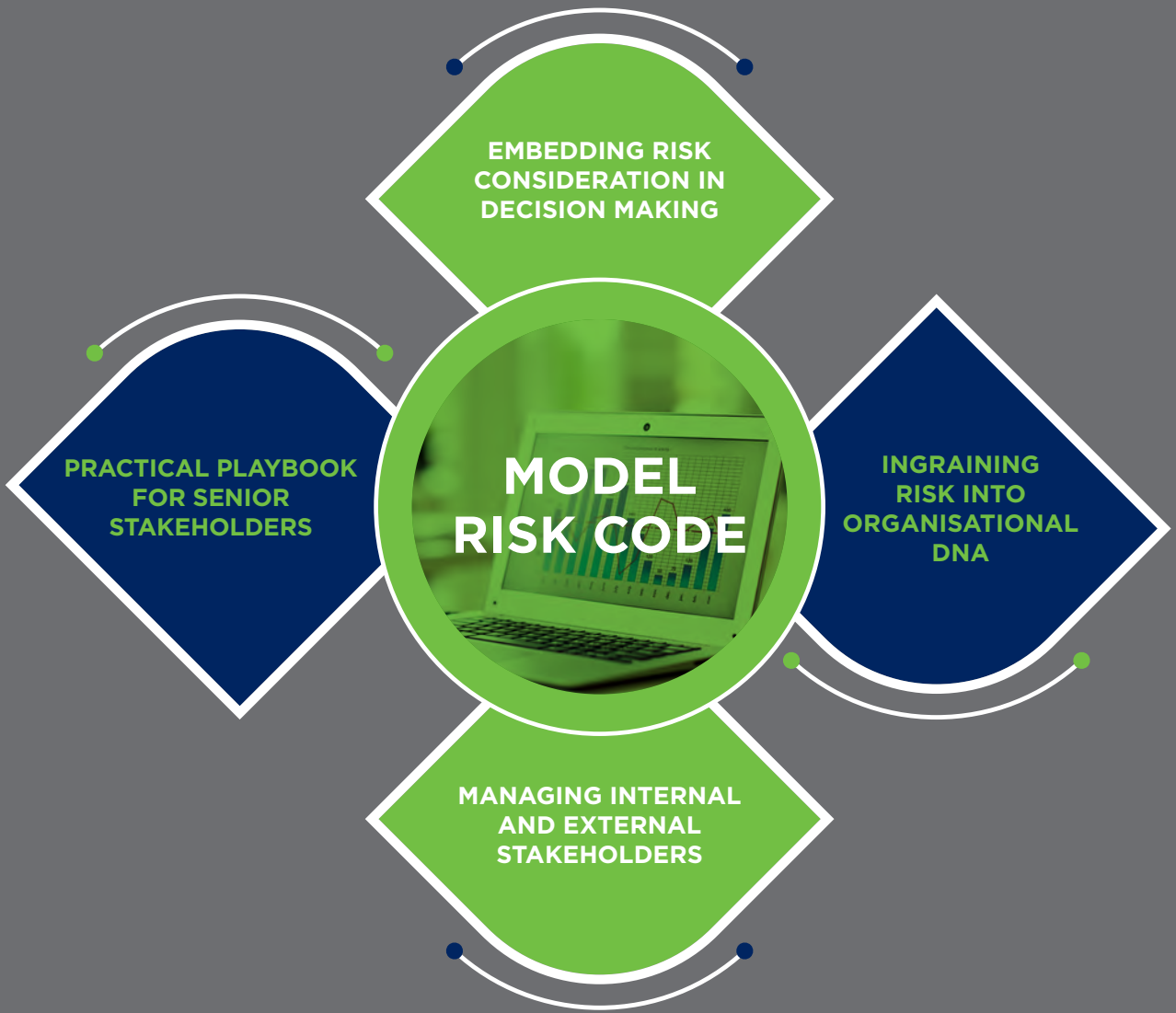
Thirdly, the organisation should consider and evaluate scenarios beyond the Business-as-Usual activities. It should use the 'what-if' approach to scenario building which will allow managers to brainstorm and prepare for specific downside events and plan for the unexpected even if they seem hypothetical now.

To implement risk management in practice, there should be joint accountability across organisational levels and functions with three clear lines of responsibility and accountability — Risk Ownership, Risk Management and Combined Assurance (internal & external auditor).

Organisations should perform a thorough and periodic evaluation of the nature and extent of risks to which the company is exposed and address the full spectrum of risks. Organisations may identify risks through brainstorming with employees from diverse functions, risk identification workshops, internal risk identification questionnaires, analysis of past loss incidents, industry benchmarking, scenario analysis, or stress tests. However, organisations should also continue to get better at interpreting noise in internal and external environments that may affect the strategy and business objectives of the organisation. The noise may eventually be turned into a data signal, and the data signal may eventually emerge as a risk factor that impacts the business model of the organisation.

EXECUTIVE SUMMARY

ENABLING . FASTER . BOLDER . RISK-INTELLIGENT DECISIONS



The Board and senior executive management should define the amount of capital and/or existing assets it is willing to put at risk to achieve future growth and earnings. If appropriately defined, risk appetite can be leveraged as a tool for forward planning, encouraging managed risk-taking, performance management, and for mitigating threats. There should be a robust mechanism to trigger alarm bells if risk impact is exceeding the defined risk appetite.

The consequence of risks may be measured over three key parameters — the quantum of the adverse consequence, the probability that the adverse consequence will occur, and the velocity at which the consequence will hit the business. Organisations can move towards attaining precision of consequence and probability measurement by capturing, preserving, analysing, and extrapolating historical incidents or risk events.

Organisations should be very watchful of systemic risks breeding in their operating setup. Small failures or seemingly insignificant individual risk events that cause losses may be 'early warning signals' that, if not detected and addressed in time, may lead to catastrophic failures.

Depending on the nature and impact of risks, the organisation needs to select an appropriate risk response – Treat, Tolerate, Transfer, or Terminate. Timely and appropriate risk response processes can reduce the inherent risk levels to lesser and possibly acceptable risk levels.

Significant risk factors also emanate from internal and external stakeholders and the organisation needs to have a defined stakeholder framework to communicate and engage with stakeholders to address those risks. The stakeholders should include employees, customers, vendors, third parties, lenders, regulators, shareholders, the government, and the community. The framework should include understanding how each stakeholder impacts the organisation, frequency and mode of engagement, reporting, and feedback close looping.

On a day-to-day basis, organisations are generating huge amounts of data, and leveraging such data is key to measuring risk exposures and strengthening the capability of the risk management function. The risk data needs to be retrieved accurately, aggregated, synthesised, and communicated appropriately. The Board should also define the scope and frequency of risk reports it expects to receive from the executive management around risk events and risk appetite breaches. Organisations should also use heat maps to report significant risk factors and risk responses to the BOD and BOD-level RMC every quarter and seek specific guidance, as required.

Irrespective of the SEBI LODR regulations, 2015, as amended around BOD-level RMC, which applies only to the top 1000 companies by market capitalisation, there is significant merit for organisations to voluntarily embrace the regulation. Depending on the organisation's size, scale, complexity, and availability of resources, it may choose to have a BOD-level RMC and/or an Operating-level RMC and/or a CRO in place to reap the benefits of having an independent committee to oversee risk management practices.

Risk factors such as the COVID-19 pandemic have exposed the vulnerability of the Indian MSME sector as it has borne the brunt of factors such as supply chain risk, demand risk, third-party risks, BCP risk, and challenges of remote ways of working. Knowing how to deal with risk will enable the transition of these organisations into the league of risk-intelligent enterprises of the future. Even for start-ups and new-age companies, it is a great opportunity to embrace risk management.

MODEL RISK CODE IN A PAGE

PRINCIPLES

- Strategy and Leadership
- Risk-embracing Culture
- Ownership and Empowerment
- Resources and Structure
- Communication and Reporting
- Governance and Monitoring
- Risk Data and Information Repository

PRACTICES

- Cultivating the risk versus reward culture
- Integrating risk/reward considerations into decision making
- Using the 'what-if' element for scenario building
- Identifying/communicating early warning signals
- Dealing with 'unknown unknowns' (risks) and certain mega global risk factors
- Best practices on the Identification, categorisation and mapping of risks
- Managing the organisation's strategic risks
- Define people and models for quantification measurement/limits of risks against risk appetite
- Guidelines for measurement of risks
- Implementing robust risk response systems and processes
- Practices around managing risk data
- Measuring and reporting of actual outcome/ loss vis-à-vis the defined risk models
- Reporting of risks to the BOD and BOD-level RMC
- Key implementation challenges and best practices to address

PRACTICAL PLAYBOOK

- Members of Board of Directors
- BOD-level RMC
- CEO
- CXOs/Business Unit Heads/Operating-level RMC

ROADMAP

MODEL RISK CODE JOURNEY

Setting up FICCI-GRMI Risk Taskforce-Q2, 2021 *

Industry feedback on draft Model Risk Code (MRC)-Q3, 2022

MRC release on November 24, 2022

Formation of FICCI-GRMI Risk COE-Q1, 2023

Socialise with MCA to push for voluntary adoption-Q2, 2023, to Q4, 2023

Release of MRC guidance notes-Q3,2023, to Q1, 2024

Drive increased adoption by corporates, share learnings to global corporates/ industry bodies

*Quarter definition is basis calender year

USERS AND APPLICABILITY

The following users of the Risk Code have been identified-those who are directly involved in the Risk Management Process:

• **Oversight body** : BOD, supported by a Board-appointed RMC wherever applicable.

• **Executive management** : including CRO & all other 'CXOs', 'CXO-1' executives, and others as applicable. The definition of the executive layer would vary from organisation to organisation.

• **Operating management** : responsible for risk management implementation, including individual business unit/operating heads and Operating-level Risk Management Committee.

Industry applicability : The Principles chapter of the Risk Code is industry agnostic, however, the Implementation guidelines to be subsequently released will cover customised guidelines for different industries - Manufacturing, Retail/FMCG, Services, Hospitality, Telecom, E-commerce, Banking, Financial Services, Insurance, Education, Healthcare, start-ups/new-age organisations.

Users of the Model Risk Code (MRC) include Oversight body, Executive Management and Operating Management.

ABBREVIATIONS

1	BAU	Business As Usual
2	BOD	Board of Directors
3	BCP	Business Continuity Planning
4	CEO	Chief Executive Officer
5	COSO	Committee of Sponsoring Organisations of the Treadway Commission
6	CRO	Chief Risk Officer
7	ESG	Environmental, Social, and Governance
8	FICCI	Federation of Indian Chambers of Commerce & Industry
9	FIRM	Financial, Infrastructure, Reputational, Marketplace
10	FS	Financial Services
11	GRMI	Global Risk Management Institute
12	ISO	International Organisation for Standardisation
13	IT	Information Technology
14	KPI	Key Performance Indicators
15	KRA	Key Responsibility Areas
16	KRI	Key Risk Indicators
17	LODR	Listing Obligations and Disclosure Requirement Regulations
18	MD	Managing Director
19	MSME	Micro, Small, and Medium Enterprises
20	P & L	Profit and Loss
21	PESTLE	Political, Economic, Social, Technological, Legal, Environmental
22	RMC	Risk Management Committee
23	SEBI	Securities and Exchange Board of India
24	4T	Four Treatments of Risk

GLOSSARY

1	Assurance	is a positive declaration intended to give confidence or comfort.
2	Combined assurance	involves combining risk management efforts across the three lines (Risk ownership, Risk Management, and Combined Assurance) to enable a holistic approach towards risk management, an effective control environment, and uniform risk reporting.
3	Dynamic environment	includes risks that can emerge, change, or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges, and responds to those changes and events in an appropriate and timely manner (as defined under 2018 ISO 31000).
4	Heat map	is a two-dimensional data visualisation technique that shows the magnitude of a phenomenon by using colour variations and giving obvious visual cues to the reader about how the phenomenon varies or is clustered.
5	Inherent risk	refers to the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or consequence.
6	Key Risk Indicator	is a metric for measuring the likelihood that the combined probability and consequence of an event will exceed the organisation's risk appetite.
7	Managed risk	is knowing the facts and having information about the event and the resources available to cope with it.
8	Residual risk	refers to the risk to an entity that is remaining after management's response to the risk.
9	Rewarded risk	represents the subset of risk factors associated with aspects such as new products, markets, acquisitions, and business model which impact future growth and have the potential for value creation.
10	Risk	is the uncertainty that a future event, behaviour, or decision may adversely (or favourably) impact the achievement of an organisation's objectives. Therefore, it also signifies the opportunity to create and preserve value for the organisation.
11	Risk data	comprises quantitative and qualitative data collated and managed by the business which allows measuring and monitoring of risk factors.
12	Risk capacity	refers to how much capital erosion or loss a business can bear beyond which an organisation may not be able to financially sustain or be a going concern.

GLOSSARY

13	Risk tolerence	the willingness or propensity to take risks. To explain, two businesses with same degree of capital buffers and financial sustainability may have different propensities to take on risks.
14	Risk appetite	refers to the types and quantum of risk that an organisation is willing to take to deal with a particular decision/event in pursuit of its objectives. It is defined with reference to the risk capacity and risk tolerance of the organisation.
15	Risk data aggregation	involves defining, gathering and processing risk data.
16	Risk-intelligent decision making	refers to decisions that have been made after considering applicable risk factors that may impact the decision's outcome. However, the risk landscape of all organisations continues to be dynamic (and not static) and hence requires a continuous monitoring of risks.
17	Risk management maturity	as it moves from 'ad hoc' to a more systematic and integrated approach, where risk management is part of the culture and a way of doing business.
18	Risk velocity	is the measure of the speed at which an exposure can impact an organisation. It is the time that passes between the point of occurrence of an event and the point at which the organisation first feels its impact. Risks with high velocity may include, but are not limited to, BCP risk, system outage risk, foreign exchange fluctuation, and customer pricing.
19	Stakeholder	refers to anyone who is impacted by the organisation's risk management practices and who in turn can impact the organisation. These include the following: • Stakeholders who are directly involved in the organisation's business operations – employees, vendors, customers. • Stakeholders who are interested in the organisation's business – lenders, shareholders, financial institutions, regulators. • Stakeholders influencing the organisation's business–government, community, rating agencies, industry associations, competitors, minority groups such as proxy firms.
20	Unmanaged risk	means not having the facts and information about the event, or the resources to cope with it.
21	Unrewarded risk	is the subset of risk factors such as the integrity of financial statements and compliance with regulations that do not have incremental premium or value-adding potential attached to them but can detract from value.

1.0 RELEVANCE OF RISK CODE

1.1 HOW FICCI-GRMI RISK CODE IS INTENDED TO BE AN ENABLER FOR ORGANISATIONS

The risk and opportunity landscape for organisations and its impact is getting wider and unpredictable with a rise in global issues such as pandemics, geopolitical disruptions, income disparity, carbon emissions, resource constraints, systemic financial failures, and climate change. This has also led to a significant focus on aspects of ESG, BCP, resilience, supply chains, and third-party risk management, and it has become imperative for organisations to address them. These aspects, if addressed and integrated into the strategy and business operations, may bring in significant competitive advantage and are a huge opportunity for organisations. But if not addressed, they may lead to an existential crisis.

The pursuit of any opportunity in business always involves risk, and companies make money by exploiting good risk-reward opportunities that are properly managed. Organisations that are most effective and efficient in managing risks of both existing assets and for future growth will, in the long run, outperform those that are less so. Clearly, a sound system of risk management is not meant to eliminate risk but rather optimise risk-taking in a way that the company understands the risk-reward trade-off and takes decisions that maximise rewards while taking managed risks.

It is necessary for organisations to manage the full spectrum of risks, adequately assess and address risk from all perspectives, have a holistic view of the risks facing it, and systematically and intelligently anticipate and drive an integrated response to potentially significant risks. This must be ingrained in the DNA of the organisation to allow long-term value creation and preservation. For an organisation, becoming 'risk intelligent' is no longer about just gaining a competitive advantage but about sustenance. A lack of effective and efficient risk management processes may put a question mark on the sustenance of the organisation.

The FICCI-GRMI Risk Code is intended to equip organisations with the practical implementation of risk principles to strengthen the risk management process, and empower them with a sound risk management system. Adoption of the Risk Code will help organisations:

1.1.1 Avoid critical failures by identifying significant or poorly understood risks being taken.

1.1.2 Take difficult decisions in a structured and risk-intelligent way to maximise the probability of success and minimise the probability of significant losses.

1.1.3 Prevent fraud events and mitigate risks posed by fraud events.

1.1.4 Have structured processes to gauge the signs of systemic risks and implement measures to prevent significant adverse events or systemic failures.

1.1.5 Operate more efficiently day to day, by optimising the use of capital and other resources.

1.1.6 Preserve value by operating within the regulatory framework and avoiding financial penalties and reputational repercussions due to non-compliance.

1.1.7 Create value through better, forward-looking risk-based decision making within the ESG framework. While investors and external agencies are considering ESG as a key evaluation parameter, it is imperative that if the organisation's products or services are not in line with ESG norms, its role in the ecosystem is eliminated in due course.

1.1.8 Enhance the organisation's ability to adapt to disruptions by being more resilient and ensuring the continuity of business operations.

1.1.9 Safeguard the organisation's people, assets and capital to protect the interests of the shareholders and other stakeholders.

1.1.10 Identify new innovation possibilities through by foreseeing emerging risk factors when fully understood via strategic disruption or opportunity workshops.

1.1.11 Increase the likelihood of successful innovation by incorporating risk-reward assessments into the new product or business process.

1.1.12 Preserve market capitalisation as investors, lenders, and creditors expect robust risk management practices and will penalise an organisation's market capitalisation if it fails to manage risk well.

1.1.13 Minimise the cost of capital since credit rating agencies include risk management as one of the evaluation criteria so that organisations that are deficient in their risk management practices may have to bear a higher cost of capital.

1.1.14 Proactively address political and economic risks for regulated industries/service segments more prone to situations such as changes in policy.

1.2 RMC BEYOND THE TOP 1000 COMPANIES BY MARKET CAP AS PER SEBI'S LODR

1.2.1 Between 2015 and 2021, as larger companies started embracing the RMC requirement, SEBI expanded the regulations around the applicability and role of RMC from the top 100 listed companies to the top 1000 companies by market capitalisation. Given the success of the RMC regulation and the current realisation that risk management has a critical role to play in an organisation's sustainable growth due to events such as the COVID-19 pandemic and the ongoing geopolitical crisis, the regulation may potentially be expanded to a larger subset of listed companies over the next few years.

1.2.2 However, irrespective of the regulation, there is significant merit for organisations to voluntarily embrace SEBI's regulation around RMC. While voluntary adoption will keep organisations prepared in the event SEBI were to expand the RMC applicability mandate, more importantly, they will be able to reap the benefits of having a dedicated risk management think tank.

1.2.3 The BOD should eventually decide whether to voluntarily establish a separate RMC and should consider factors including but not limited to:

1.2.3.1 The size and composition of the Board.

1.2.3.2 The scale, diversity, and complexity of the company's operations.

1.2.3.3 The nature of the significant risks that the company faces.

1.3 RISK MANAGEMENT FOR MSMEs AND NEW-AGE ORGANISATIONS (LISTED & UNLISTED)

1.3.1 The key dilemma in the case of MSMEs and new-age organisations will continue to be the perceived conflict between innovation, the need to operate at speed, and risk management, and therefore the need for prioritisation of resources between business and risk management.

1.3.2 For effective adoption of the Risk Code by MSMEs and new-age organisations, it would be essential to see the direct correlation of value preservation through effectively managing risks. Return on capital employed, which should be a key measure for all MSMEs and new-age organisations, has a positive correlation for organisations that manage or exploit risk well, and a negative correlation for organisations that are unable to manage risks effectively, and hence face value destruction.

1.3.3 Risk factors such as the COVID-19 pandemic have beyond doubt exposed the vulnerability of the MSME sector to significant changes in the internal and external environment. The MSMEs have borne the brunt of factors such as supply chain risk, demand risk, third-party risks, BCP risk, and challenges of remote ways of operations. Additionally, with the accent of disruptive business models cutting across industries, current business models of MSMEs are being challenged and they may be forced to course correct.

1.3.4 Understanding and appreciating how risk management can bring about the desired change, having a risk-ingrained mindset and adopting practical risk management guidelines within the constraints of available resources may be a saviour for MSMEs.

1.3.5 New-age organisations which include start-ups as defined by the Department for Promotion of Industry and Internal Trade and internet-based companies are more vulnerable to internal and external environmental risks because they must deal with resource constraints to be able to establish end-to end processes vis-à-vis traditional or legacy organisations.

1.3.6 However, as the size of the business expands, the challenges and opportunities become numerous and complex. The ever-changing profile of new-age/budding enterprises makes them more vulnerable to uncertainties and consequent risks.

1.3.7 Knowing the ways to deal with risk will probably be fundamental to the transition of new-age/budding enterprises into the league of risk-intelligent enterprises of the future. Developing a risk management culture will differentiate such organisations by helping them make the right decisions to survive and thrive in the long run.

1.3.8 It is a great opportunity for the new-age organisations to embrace risk management practices at an early stage to reap its benefits and retain their competitive advantage.

2.0 PRINCIPLES

2.1 STRATEGY AND LEADERSHIP-SUPPORT RISK REWARD-BASED DECISION MAKING BY ESTABLISHING A CLEAR BUSINESS AND RISK STRATEGY AS WELL AS EFFECTIVE BUSINESS AND RISK MANAGEMENT LEADERSHIP

2.1.1 Given how the risk landscape of organisations is getting more and more complex and considering the significant adverse impact, the Board should acknowledge and reinforce that robust risk management practices are core to sustainable value creation for organisations. They are no longer optional or only a compliance requirement but rather a prerequisite for capital preservation and future growth and competitiveness.

2.1.2 The Board should intervene if a 'person in power' including majority shareholders in an organisation circumvents or overrides processes in place, because this maybe a major risk facing the organisation.

2.1.3 The Board should prevent the possibility of management over-riding when making critical decisions despite the company having robust systems and processes.

2.1.4 The role of independent directors as part of the Board is extremely critical as they bring in an external independent lens, accountability, and authority to question on behalf of concerned stakeholders and drive robust governance practices.

2.1.5 The Board should encourage the management to do a high/medium/low categorisation of the risks faced by the organisation to allow prioritisation and reporting of such risks to the Board and Board-level RMC. The Board should communicate with the stakeholders (lenders, shareholders, financial institutions, regulators) about the top risks faced by the organisation and actions being taken to address those risks, including confirming that the organisation's risk management processes are functioning effectively.

2.1.6 The Board should encourage the executive management to have a defined ESG roadmap, set ESG goals, identify measurable ESG metrics, and authorise or endorse specific actions to achieve the defined goals.

2.1.7 The Board should incentivise the executive management to be 'risk intelligent', i.e., reward their ability to anticipate and respond profitably to market opportunities and prepare for potentially large adverse risk events or business disruption.

2.1.8 The Board and Risk Management Committee should lead by example by discussing risk events and scenarios, both opportunities and problems, during meetings.

2.1.9 The Board should set the tone by driving the risk-aware culture across the organisation and demonstrate its commitment to investing in the requisite resources for robust risk management staff and processes.

2.1.10 The Board should declare and demonstrate its commitment to supporting robust risk management processes, including endorsing the risk policies and framework and defining clear lines of accountability for risk-taking and risk monitoring.

2.1.11 The Board should mandate the executive management to set up a vision/roadmap of actions to increase the effectiveness of risk management throughout the organisation and move up on the risk management maturity curve.

2.1.12 The Board should lend support and transition the risk management agenda from Compliance – Type control ('tick the box') to a Business Enabling control ('faster, bolder, risk-intelligent decisions').

2.1.13 The Board should question if the organisation is demonstrating a risk-averse behaviour and, in turn, foregoing rewards, or intelligently taking appropriate and rewarded risks.

2.1.14 The Board should define the amount of capital and/or existing assets the organisation is willing to put at risk to achieve future growth and earnings.

2.1.15 The Board and executive management should use and position the dedicated risk management function to aggregate and integrate all the risks across all divisions and functions within a larger organisation. The risk management function must cut across all organisational lines (functional/business unit/ divisions) to identify the correlation of risks for the Board and executive management to assess and decide on potential risk-altering strategies.

2.2 RISK-EMBRACING CULTURE-RISK-INGRAINED MINDSET IS FOSTERED AND ALLOWED TO PERCOLATE ACROSS THE ORGANISATION TO ENHANCE PERFORMANCE

2.2.1 The Board should set the tone by laying down its belief that risk management is not is not just about avoiding risks but more importantly about exploiting risks to create business value and competitive advantage for the organisation.

2.2.2 The Board should emphasise how embedding risk considerations into decision making is key to taking 'managed risks' vis-à-vis 'unmanaged risks', which is what differentiates a risk-intelligent enterprise and drives organisational success.

2.2.3 The Board and executive management should encourage and reward the timely and transparent flow of information about problems or adverse events without fear of being penalised, to promote both lesson-learning from mistakes and faster damage control.

2.2.4 Risk management infused into the organisational culture would ensure that strategy and decision making would evolve out of a risk-intelligent process rather than the decisions being risk-averse or leading to unmanaged risks which can be 'value destructive' for organisations.

2.2.5 The organisation's culture should encourage innovation, entrepreneurship, and acceptance of failures, and not be averse to taking calculated risks for growth.

2.2.6 There needs to be a clear communication of the scope of freedom to act, while staying within the risk appetite of the organisation, exercise judgement, make mistakes, and learn from them, but not be penalised.

2.2.7 The reward philosophy of the organisation should encourage the desired employee behaviour by aligning it with the risk management strategy and risk appetite of the organisation, with measurable risk management

principles and policy compliance as part of compensation and performance management system.

2.3 OWNERSHIP & EMPOWERMENT- RESPONSIBILITIES AND AUTHORITY ARE CLEARLY ARTICULATED TO TAKE EMPOWERED DECISIONS AND SUPPORTING ACTIONS

2.3.1 The responsibilities for various parts of the risk management process should be clearly defined and articulated as part of the KRA and operating plan of the organisation, including:

2.3.1.1 Continuously monitoring the internal and external environment to identify emerging risk factors.

2.3.1.2 Embedding risk-reward considerations into business decision making.

2.3.1.3 Integrating and coordinating risk measurement and reporting across the organisation.

2.3.1.4 Escalating signals of risk appetite breaches or significant losses arising from specific risk events.

2.3.2 There should be joint accountability for risk management across organisational levels and functions with three clear lines of responsibility and accountability as under:

2.3.2.1 Risk ownership (first line) - by the businesses who is empowered to take risk decisions within the approved risk appetite, and to report on the risk parameters according to risk policy standards.

2.3.2.2 Risk management (second line) - by the independent risk management function that assists executive management and the Board with the firmwide aggregation and assessment of risk and are empowered to change risk appetite; it monitors the first line and ensures risks and controls are managed effectively. The second line includes a risk management function to monitor the implementation of effective risk management and assist in reporting risk-related information, a compliance function to monitor compliance with applicable laws and regulations, and a controllership function to monitor financial risks and reporting issues.

2.3.2.3 Independent and combined assurance - by internal auditors and statutory auditors who enjoy a high level of organisational independence and provide assurance of first and second-line activities. It independently tests and provides assurance (to executive management, the Board, and other concerned stakeholders) of the effectiveness and integrity of the risk management framework and the operating risk practices.

2.3.3 Clear ownership and cross-functional collaboration are extremely critical for effective risk management. While the primary responsibility for risks may be assigned to a single individual for greater accountability, overall responsibility around risk management may be shared across organisational levels and functions. The individual with primary responsibility should also have the authority to call for collaboration across various parts of the organisation in managing risks irrespective of reporting lines.

2.4 RESOURCES & STRUCTURE - ALLOCATION OF RISK RESOURCES ARE ADEQUATE, AND THE RISK STRUCTURE IS APPROPRIATE AND COMMENSURATE WITH THE SIZE AND COMPLEXITY OF THE ORGANISATION

2.4.1 Allocation of adequate resources, the definition of appropriate risk appetite, and setting a risk management structure commensurate with the size and complexity of the organisation are essential to ensure that the organisation has robust risk management practices.

2.4.2 The upfront investment is not only limited to the financial cost but also to time commitment, attention, training, and communication with both internal and external stakeholders. The resources required for the design and implementation of risk management processes should include, but are not limited to, the following:

The upfront investment is not limited to the financial cost but also to time commitment, attention, training, and communication with both internal and external stakeholders.

2.4.2.1 People – ensure that all three lines (Risk Ownership, Risk Management and Combined Assurance) of the organisation that are most involved with risk management tasks are staffed with people who have the right skill sets and experience. Build a pipeline of talented and trained people who can be part of the succession plan for future risk management teams.

2.4.2.2 Technology resources – allocate sufficient finance to develop and maintain risk measurement, reporting, and control systems.

2.4.2.3 External partners – use external consulting or technology resources to aid the development of permanent internal risk management practices.

2.4.3 Depending upon their size, scale, complexity, and availability of resources, organisations may choose to have an RMC to reap the benefits of having an independent committee to oversee risk management practices, integrating risk considerations in decision making and eventually, implemented in substance, creating a competitive advantage for the organisation. The RMCs, both at the Board-level and the Operating-level, should also assess the risk information that has been reported, and the actual profit or loss that was recorded in relation to the risk levels, especially that which resulted from any significant risk events. Currently, the SEBI's LODR regulations, 2015 as amended, mandate only the top 1000 listed companies in terms of market capitalisation to have an RMC in place, while it is optional for the companies that do not fall within the mandate.

The role of the Audit Committee includes overseeing financial reporting controls, internal controls, providing independent assurance on processes and controls (design and operating effectiveness) as reviewed and reported to them by the internal audit function, and overseeing risk assessment for internal audit scoping exercise. However, the RMC has a partnering role with the Strategy or equivalent function in terms of future-proofing the organisation with a forward-looking approach. Its role includes ingraining risk considerations in decision making and partnering on broader aspects of business strategy, new products, new markets, mergers and acquisitions, technology, and business resilience. The RMC should be a more proactive leg of the risk management ecosystem which focuses on embedding risk culture into the DNA of the organisation. This would also allow the internal auditors to focus more on value creation projects and initiatives as a robust second line will require lesser time and effort investment in routine assurance activities.

Appointed by	BOD
Strength	At least three members
Chair	An Independent Director from the members of the BOD
Composition	2/3 members should be Independent Directors
Invitees	MD, CEO, CXO, business unit heads, and an external risk domain expert as necessary
Frequency of meetings	Once a quarter

While there is no mandate to have an Operating-level RMC, organisations should have an Operating-level RMC to support the BOD-level RMC and to oversee and ensure the effective implementation of risk management. The Operating-level RMC may be at a business unit level, geographical level, or a functional level.

Appointed by	MD and Executive Management
Strength	At least five members
Chair	Business unit head/region head/functional head depending on the organisation structure
Composition	Mix of business unit heads, region heads and functional heads
Invitees	General Managers or Managers or equivalent from functions and business units based on the meeting agenda
Frequency of meetings	On a need basis, subject to once a month at minimum

2.4.4 While the ultimate responsibility for risk management is with the Board and Board-appointed RMC, the implementation responsibility around risk management within an organisation resides with the CEO and all other CXOs. The scale, diversity, and complexity of a company's operations will determine the need for a Chief Risk Officer (CRO) to be responsible for the second line of risk management oversight and policy implementation.

2.4.4.1 In the absence of a CRO in an organisation, it is recommended that a nominee from the RMC, who may be a CXO, will play the role of a CRO, however, ensuring that the individual does not have any business targets and the roles are not conflicting.

2.4.4.2 In organisations where there is a CRO, the functional reporting of the CRO may be to the Board-level RMC, while the administrative reporting could be to the CEO/MD.

2.4.4.3 However, in cases where the CRO does not report to the Board-level RMC, he/she should have access to the Board-level RMC whom they can meet independently.

2.4.4.4 For a CRO's role to be effective, a CRO would be expected to have adequate prior experience to bring in the required business/ functional perspectives of the company/industry leading practices. The CRO should mandatorily be an invitee to all critical leadership meetings be it marketing, technology, operations, finance, or others and may be empowered to have access to requisite organisational data. The CRO should not have any business targets that could conflict with his risk management role and should ideally not have any additional responsibilities. However, if he/she must have another role, that should not conflict with his/her primary role as a CRO.

2.4.4.5 The CRO and the risk management function should operate autonomously and independently and should not have any pre-conceived notions.

2.4.4.6 The CRO or equivalent designate should ensure that the aggregate risk appetite of individual business units is within the risk capacity of the organisation. The CRO should also make an independent assessment and report the actual circumstances and impact, including the P&L impact of any risk appetite being exceeded.

2.5 COMMUNICATION AND REPORTING - EFFECTIVE, CONTEXTUAL, AND PERIODIC COMMUNICATION IS ESTABLISHED WITH INTERNAL AND EXTERNAL STAKEHOLDERS

2.5.1 Establishing external communication and reporting mechanisms of risk information provides a continuous way to keep affected stakeholders informed of the organisation's efforts and commitment towards effective risk management processes.

2.5.2 Effective internal communication helps to ensure that the organisation's risk engagement remains strong. Internal communication is also critical to promoting and defining the risk management function's role as an 'enabler' rather than a 'detractor' for the business and promoting its role in creating sustainable business value and driving operational excellence.

2.5.3 The risk information communicated should not only focus on socialising the impact of risk events, but also on the velocity of the risk events so that the concerned stakeholders are aware of the limited response time in case of high-velocity risk events, and risk responses are chosen appropriately.

2.5.4 Communication protocols and information standards, including who in the organisation is responsible for gathering and reporting any risk information and the periodicity of communication, should be defined by the CRO or the equivalent designate in agreement with the CEO and Board.

2.5.5 External communication can build confidence in the organisation as well as meet regulatory requirements around risk disclosures. At the same time, the sensitivity of information should be considered when making external disclosures.

2.5.6 Organisations should have a defined stakeholder engagement framework to bring in a transparent and open interaction environment between the organisation and its stakeholders and enable the exchange of information, feedback, and consultation on requisite issues.

2.6 GOVERNANCE AND MONITORING - A MECHANISM IS ESTABLISHED TO ENSURE THE CORRECT DESIGN AND IMPLEMENTATION OF ROBUST RISK MANAGEMENT SYSTEMS AND PROCESSES

2.6.1 The Board has ultimate responsibility for approving the strategy of the company in a manner that addresses stakeholder expectations and does not expose the company to an unacceptable level of risk. Hence, the Board, including the independent directors who bring in an independent external perspective is responsible for the governance of the risks and for setting the tone and direction for the company in the way risks are being managed and reported. The Board should establish a separate Board RMC and appoint a CRO if required (refer to provision 2.4.4).

2.6.1.1 Determining the risk appetite – The Board should approve the company's risk appetite as determined by the executive management including the nature and extent of the significant risks that the Board is willing to take in achieving its objectives.

2.6.1.2 Ensuring right design and implementation – The Board and Board RMC should hold the executive management accountable for ensuring that all three lines of risk management responsibility are operating effectively with sufficient human and technological resources so that they can implement the agreed risk management framework, including:

2.6.1.3 Articulating and communicating risk responsibilities and authority.

2.6.1.4 Communicating with internal and external stakeholders around risk management information and major risk events.

2.6.1.5 Reporting on actual changes, or model possible changes, in the internal or external environment to be able to anticipate and track emerging risks.

2.6.1.6 Ensuring that the risk response and reporting systems are working effectively to bring down the inherent risk to residual levels.

2.6.1.7 Ensuring periodic benchmarking with industry best practices of risk management is conducted by Board-level RMC with support from business.

2.6.1.8 Demonstrating how management has embedded risk-reward considerations into business decision making.

2.6.1.9 Determining the availability of adequate resources for effective risk management implementation.

2.6.1.10 Presenting robust human resource succession plans to ensure that there is adequate depth in the required risk management staff in all three lines of responsibility within the organisation.

2.6.2 Risk reporting – The Board should define the scope and frequency of risk reports it expects to receive from the executive management. The frequency may be monthly, quarterly, or semi-annually and shall include, but may not be limited to:

2.6.2.1 All risk appetite breaches, and the steps to rectify them.

2.6.2.2 The current risk profile of the whole organisation, as well as of its parts if it has multiple business lines, and any concerning concentrations and/or correlations of risks.

2.6.2.3 The largest risks, defined by potential downside loss amounts, of the organisation.

2.6.2.4 Significant risk factors, old and new or emerging, that the organisation is dealing with, along with the risk response measures it is taking.

2.6.2.5 Notable actual risk events that caused tangible or intangible losses to the company since the last risk report to the Board, how the actual losses compared to what was forecast or modelled as the expected loss, and what lessons have been learnt and actions taken.

2.6.2.6 Any significant risks that the executive management is choosing to accept as they expect a favourable outcome or to retain competitive advantage while ensuring that reporting is such that the confidentiality of sensitive information, if any, is maintained.

The Board, in turn, if it so believes, should report to the stakeholders (lenders, shareholders, financial institutions, regulators) that its risk management processes are reviewed, benchmarked, and audited.

2.6.3 Progress across the risk management maturity curve – The organisation should have the risk management maturity model and parameters defined to gauge where it currently stands on the maturity curve, and the roadmap it chooses to adopt to move up the curve. It also needs to ensure (annually or semi-annually) that the processes, systems, and measures it is embracing are not just addressing risks in the short term (fit for purpose) but will benefit the sustainable growth of the organisation (fit for future).

2.7 RISK DATA AND INFORMATION REPOSITORY - A ROBUST MECHANISM IS ESTABLISHED AROUND RISK INFORMATION TO ENSURE THE INTEGRITY, AVAILABILITY, AND REPORTING OF RISK DATA

2.7.1 Positive and negative events generate data including P & L data that help organisations learn and measure KRI metrics and enable risk-based decision making. The executive management should compare data to risk estimates to generate meaningful information such as risk-reward comparisons from actual events and ‘near misses’, which can then be used for future risk-based assessment and decision making.

2.7.2 The CRO and/or the ‘second line’ risk management function should define, and state in risk policy, the required risk information, and the format of the data from each risk-generating business line.

2.7.3 Each business line (the ‘first line’) is responsible for assigning appropriate resources

to generate and report all required risk data with the time frequency that is necessary and agreed upon (which may be daily or even real-time in certain instances) to the CRO and the risk management function.

2.7.4 Each business line is responsible for reporting any risk appetite breaches to the CRO immediately.

2.7.5 The 'second line' risk management function is responsible for managing risks due to factors such as data privacy and data security. It is also responsible for aggregating the risk data across the organisation and reporting any concerns and data deficiencies, as well as regular risk reports, to the executive management and to Board-level RMC.

"With increasing complexities in business operations, dynamic regulatory environment, and increasing onus on board members, the risk management function is only becoming more and more sought after."

3.0 LEADING PRACTICES AROUND RISK MANAGEMENT

3.1 CULTIVATING A RISK CULTURE

3.1.1 Risk considerations should be embedded into the decision-making process thereby enabling risk-intelligent decision making and encouraging 'rewarded risk'-taking behaviour. Innovation is also more likely to be successful in such organisations as they provide an environment for being risk intelligent and creative.

3.1.2 While organisations should reward success, they should permit failure and view the cost of failures as part of an investment into innovation. They should promote a culture of 'fail fast' and celebrate such early-stage failures as they have a lower cost impact, which in turn allows organisations to promote creativity and innovation. Such failures should be celebrated also because they offer a chance for course correction and add to learning and improvement.

3.1.3 There should be a culture that encourages innovation and accepts some failures; the key is for employees to be 'risk intelligent' rather than 'risk ignorant'. It is about encouraging employees to take more risks, but about not being risk-averse or curbing entrepreneurial thinking while they innovate, and to encourage them to consider the risk versus reward trade-off. Risk-taking should be with reference to the organisation's risk appetite.

3.1.4 To cultivate the risk/reward culture, organisations may include creative ways including:

3.1.4.1 Setting up an office environment to encourage creativity in certain ways including the use of post-it ballots, visual thinking, creativity boot camps, and storyboards.

3.1.4.2 Allocating time for employees to ideate, brainstorm, or participate in workshops.

3.1.4.3 Encouraging games around risk simulation, and scenario analysis.

3.1.5 Organisations can even assess the risk culture by conducting employee surveys and asking questions about openness to take risks and make mistakes. Such surveys can also bring out customised ways for organisations to cultivate the desired culture. An annual assessment of the risk culture may provide insights into the organisation to course correct if required and adopt the requisite measures to cultivate the desired culture.

3.1.6 There should be an explicit whistle-blower mechanism to encourage openness and frank whistleblowing with a strong anti-retaliation assurance.

3.1.7 Customised risk/reward training is to be included in the personal development plans of all the managerial groups to equip them with the skill sets to make good risk-based decisions.

3.1.8 Risk management culture should be embedded across the supply chain ecosystem including vendors, dealers, and third parties. For example, there may be risk factors such as raw material shortage, quality, fire safety, financial reporting, or attrition for which organisations may share their practices with vendors, dealers, and third parties for them to incorporate.

There may be a dedicated team in the supply chain department that is responsible for upgrading the supplier's and dealer's excellence by replicating the organisation's practices for the vendors, dealers, and third parties.

3.2 INTEGRATING RISK/REWARD CONSIDERATIONS INTO DECISION MAKING

3.2.1 The risk/reward considerations should become an integral part of business decision making including strategic decisions, mergers and acquisitions, joint ventures, health and safety processes, project management, outsourcing decisions, change management, and market expansion, and even ongoing activities such as role definitions, monthly/ quarterly strategy review, annual operating plans, budget exercises (including budgeting for risk management), performance management, and KRA definition.

3.2.2 It is important to include risk parameters, both quantifiable (where possible) and qualitative, in the performance review criteria and process of all employees, in whichever role they operate including but not limited to cash flow management, brand management, people management, debt management, customer management, and IT security.

3.3 USING THE 'WHAT-IF' ELEMENT FOR SCENARIO BUILDING

3.3.1 The value from implementing risk management practices accrues only when organisations are able to consider and evaluate scenarios beyond the Business-as-Usual. Organisations should use the 'what-if' approach to scenario building which will allow managers to brainstorm and prepare for specific downside events, even if they seem hypothetical at the moment. They need to ask questions such as:

a. What if one of our biggest customers has a decline in business or leaves us for a competitor or some other reason?

b. What if there is a significant rise in our key input prices?

c. What if there is a sudden increase in consumer demand?

d. What if there is a calamity in the geography of my key supplier?

e. What if our central server room catches fire or my key IT system is hacked?

f. What if there is a significant adverse change in the political landscape, either local, national, or international?

The Board, the RMC, the CEO, and CXOs should ask questions about such possible scenarios relevant to their businesses to trigger brainstorming and preparedness for such events if they were to occur.

3.4 IDENTIFYING AND COMMUNICATING EARLY WARNING SIGNALS OF EMERGING AND/OR CHANGING RISKS

The risk management strategy must address the full spectrum of risks, which should include industry-specific risks, strategic, ESG, carbon footprint, operational, reporting, competition, people, reputational, environmental, social, compliance, physical security, data privacy, and business continuity risks among others. Given that a company's objectives, its organisational structure, and the environment in which it operates are continually evolving, the risks it faces are continually changing. A sound system of risk management, therefore, depends on a thorough and periodic evaluation of the nature

and extent of risks to which the company is exposed.

3.4.1 Organisations should get better at anticipating (and possibly measuring) change, interpreting change, adapting, and innovating. Change may not just be about a newly emerging risk, but also about the cause and effect of a known and/or current risk. Changes either in the internal or external environment may substantially affect the strategy and business objectives of the organisation.

3.4.2 In an era of machine-learning, artificial intelligence and big data, the amount of data available to an organisation is going up exponentially and it needs to leverage internal and external data to cut down the noise (information and metrics) that impacts the business.

3.4.3 The noise (information and metrics) can include, but is not limited to, social, consumer behaviour, technological, environmental, economic, and political changes. The internal environment may include changes in leadership, personnel, rapid growth, sudden contraction, or changes in innovation. The external environment may include changes to regulations, the geo-political landscape, changes in government policy, economic factors, or market behaviour. The noise (information and metrics) may eventually be turned into a data signal, and the data signal may eventually emerge as a risk factor that impacts the business model of the organisation. The organisation may then respond to the risk factors by adjusting the business model, mission, and vision statements of the organisation.

3.4.4 There are various approaches that organisations may adopt to try and understand the changes, data signals, and emerging risks. However, the key is to identify these changes on a timely basis and link them back to how they could impact the business model and strategy of the organisation, and then make an appropriate and measured response to manage the risk.

3.4.5 Structured models may be used to gauge the changes including PESTLE, FIRM scorecard, or British Standard 31100 (Strategic, Project, Financial, Operational). Organisations must examine data or and other informational resources from globally reliable sources including industry, governments, and consulting firms. These resources may be used to identify trends and subsequent implications for the organisation. For example, political trends may include an anti-incumbency wave, social trends may include change in population growth rates or demographics, and technology trends may include digital disruption or innovation in a particular industry.

3.4.6 To identify early warning signals, organisations may:

3.4.6.1 Identify trends by analysing what data series and signals investors and industry analysts are currently using in their models.

3.4.6.2 Study emerging risk reports or resources published by other organisations, consulting firms, public policy experts, and economic or political experts and review applicability for themselves.

3.4.6.3 Leverage artificial intelligence and machine learning to scan social media content and news feeds to identify upcoming trends.

3.4.6.4 Do in-depth disruption workshops where executives get together to imagine the unknowns and possible black swan events. These can help uncover the impact on the assumptions being made about the future and see how their innovation and business strategy need to stay agile to respond to those potential events.

3.4.7 Organisations should be very watchful of systemic risks breeding in their operating setup. They should not ignore small failures or seemingly insignificant risk events that cause losses, as they may be 'early warning signals' that, if not detected and addressed on time, may lead to catastrophic failures. Hence, losses arising from such small systemic failures or insignificant risk events should be monitored continously and compared to expected losses, while thoroughly investigating large, unexpected losses.

3.5 DEALING WITH 'UNKNOWN UNKNOWNS' (RISKS) AND CERTAIN MEGA GLOBAL RISK FACTORS

3.5.1 While some of the broader risks within the general categorisations such as natural disasters, a pandemic, geopolitical disruptions, cybersecurity threats, governmental policy on data localisation and technology failures are acknowledged and perhaps even quantified, there remains an 'unknown unknown' dimension to risks which may emanate from any risk category. To take some examples, the nature of COVID-19 and how different governments would respond, the wider geopolitical consequences of individual crisis events, the global inflationary trends and interest rate policy or the ransomware attacks and the magnitude of their impact. The 'unknown unknown' dimension can have a disproportionate adverse impact; it may also throw open significant business opportunities if the organisation's risk management processes are agile enough to derive a competitive advantage in such situations.

3.5.2 These are low-probability and high-consequence risk factors occurring very infrequently but driven by factors beyond the control of an organisation. However, the low probability of such an event occurring is less relevant if the risk has a disproportionate and extremely large impact. These risk factors must be addressed or else they may pose an existential threat to the organisation. Readiness for dealing with such risks would require:

3.5.2.1 Being prepared to deal with such events by doing scenario analysis exercises and having already laid out and tested processes to deal with an abrupt impact on supply chains, people, IT systems, and clients across various geographies, potentially simultaneously.

3.5.2.3 Having organisation-wide accurate communication coordinates of stakeholders across the value chain to adequately respond to unknown events.

3.6 BEST PRACTICES ON THE IDENTIFICATION, CATEGORISATION, AND MAPPING OF RISKS

3.6.1 Organisations may leverage one or more of the following techniques to identify risks:

3.6.1.1 Brainstorming with employees from diverse departments, functions, and levels in risk identification workshops.

3.6.1.2 Internal risk identification questionnaires.

3.6.1.3 Analysis of past loss incidents, especially those that were higher than predicted loss forecasts.

3.6.1.4 External industry benchmarking.

3.6.1.5 Scenario analyses.

3.6.1.6 Quantifiable stress tests.

3.6.2 The risk management function should

facilitate the preparation of a robust risk library and updating of the library annually. The risk description should be very clear and be measured using a common risk metric in which to express the magnitude of the risk, rather than using multiple (and perhaps overly technical) risk languages. Wherever possible, similar risks must be categorised and aggregated together so that organisations get a holistic view of the impact, which helps determine mitigation strategies.

3.6.3 Senior management should always consider how different risks might correlate together, either positively (creating greater impacts) or negatively (providing potential offsets).

3.6.4 Once identified and assessed, the risk factors should be communicated to the concerned business stakeholders in a timely manner and discussed with them to come up with a coordinated risk response.

3.7 MANAGING THE ORGANISATION'S STRATEGIC RISKS

3.7.1 For an organisation to understand and address its strategic risks, the risk management process and the strategic planning process must go together. The risk management function should be functioning in close coordination with the strategy group of the organisation, and this may be an emerging best practice being embraced. A disjointed approach will contribute to failure and could potentially disrupt the achievement of the organisation's goals.

3.7.2 While the risk management function should continuously scan the environment to assess changes and risk signals and their impact on the company's business model, the strategic plan must be developed in tandem with the risk assessment and should be agile to address the strategic risk factors.

3.8 DEFINE PEOPLE AND MODELS FOR QUANTIFICATION/MEASUREMENT OF RISKS AGAINST RISK APPETITE

3.8.1 A simple way is to measure the maximum impact an event can have on the objectives whether it is in terms of capital erosion, reputation loss, loss of life, data breach, or compliance breach, and then match it against the risk capacity of the organisation.

3.8.2 The senior executive management should develop the risk appetite statement aided by the actual and hypothetical scenarios and stress testing of data. They should be advised by the CRO and independent risk management staff and supported by a cross-functional team with different risk propensity. This enables discussion and dissent, ultimately helping to arrive at a risk appetite statement that is aligned with the culture and intent of the whole organisation.

3.8.3 The risk appetite statement definition should have taken the historical and forecasted company, industry, and external agency data (where applicable/available) into consideration.

3.8.4 The risk appetite statement should be used for capital allocation, preparing business plans and budgets, considering possible new business opportunities as well as for possible exits from existing businesses and evaluating mergers and acquisitions.

3.8.5 The defined risk appetite must be within the risk capacity of the organisation so that a buffer exists, and the size of the buffer should depend on its propensity to take risks and the scenario analyses of worst-case events.

3.8.6 Unless the stakeholders understand the capacity of the organisation to sustain a loss, any business decision taken can expose the organisation to the risk of not meeting its objectives. Innovation and entrepreneurship cannot be successfully undertaken unless there is a clear understanding of the risk appetite and performance is measured against the risk appetite metrics. If appropriately defined, risk appetite can be leveraged as a tool for forward planning, encouraging managed risk-taking, performance management, and mitigating threats. Depending on the quantum of risk from a business decision, risk appetite either prevents or prompts an organisation's decisions, including product portfolio expansion, territorial expansion, or new acquisitions.

3.8.7 The risk appetite statement should consider and reflect the following:

3.8.7.1 Measure of loss that the organisation is willing to accept in terms of parameters including but not limited to earnings (in total and per share), revenue, loss of capital, and market capitalisation.

3.8.7.2 A forward-looking approach and consideration of various scenarios.

3.8.7.3 Significant risks the organisation is willing to take as part of growth strategy.

3.8.7.4 Attitude towards compliance, health, and safety.

3.8.7.5 The propensity of the organisation to take risks.

3.8.7.6 The ability of the key risk-takers and managers to adapt and react quickly to changes in events and risks.

3.8.7.7 Learnings from past audits or business failures, if any.

3.8.7.8 Nature of the business, size and scale, and geographical diversity of operations.

3.8.7.9 Stakeholder sensitivity, credit rating, and shareholder expectations.

3.8.7.10 Complexity of supply chains and regulatory oversight on the business.

3.8.8 There should be a robust mechanism to trigger alarm bells if risk impact is exceeding the defined risk appetite. It may require immediate course correction in terms of additional capital and/or resources to address the risk, and measures to prevent such risk events in the future.

3.9 GUIDELINES FOR MEASUREMENT OF RISKS

3.9.1 Risks may be measured over three key parameters:

3.9.1.1 The size of the adverse consequence.

3.9.1.2 The probability that the adverse consequence will occur.

3.9.1.3 The velocity at which the consequence will hit the business.

3.9.2 To measure risks, organisations need to create a risk scale to measure the consequence and probability of risks — the scale being customised according to the risk tolerance of the organisation. While the risk scale is a quantitative measure, the quantitative impact of every risk factor may not be readily available

with precision, so best estimates of the consequence and probability should be made by a multi-member team.

3.9.3 Organisations can move towards attaining precision of consequence and probability measurement by capturing, preserving, analysing, and extrapolating historical incidents or risk events, whether observed within the organisation or from competitors in the same or similar industries. For key risk areas, organisations may consider maintaining risk event logs with aggregated visibility at an organisational level for better quantification of impact and assessment of likelihood.

3.9.4 Risk measurement may be a combination of qualitative and quantitative techniques as certain risk factors such as reputation or non-compliance with applicable laws and regulations may not lend themselves to numerical measurement but may still have tolerance limits defined by the Board. Hence, qualitative measurement allows relative prioritisation and treatment of such risks.

3.9.5 Measurement of risk velocity can be based on an appropriate judgement of the risk management function in coordination with the concerned department or function to which the business activity pertains.

3.10 IMPLEMENTING ROBUST RISK RESPONSE SYSTEMS AND PROCESSES

3.10.1 Timely risk response processes can reduce the inherent risk levels to lower and possibly acceptable risk levels. The internal audit team of the organisation, be it an in-house team or an outsourced one, would be responsible for assuring that the chosen risk responses are operating effectively to reduce inherent risks to acceptable residual levels, and hence have a critical role to play in the overall risk management ecosystem. Organisations may choose an appropriate risk response from the below '4Ts of risk response':

3.10.1.1 Tolerate – choose to accept the risk as it is if it is within acceptable levels and the cost of reducing or hedging it is higher than the expected benefits.

3.10.1.2 Treat – implement controls to reduce either the consequence, probability, or both, thereby reducing the residual risk to an acceptable level.

3.10.1.3 Transfer – transfer the risk to a third party, for example, by taking insurance, using derivatives, outsourcing, or sharing the risk with a joint venture partner. However, organisations must consider that all these options themselves entail risk, especially counterparty risk.

3.10.1.4 Terminate – avoid the risk by choosing not to continue the activity that is giving rise to the risk. This may be by exiting the risk entirely or hedging it until a full exit can be achieved.

3.10.2 Questions organisations may ask while choosing an appropriate risk response include:

3.10.2.1 Will the benefits of executing the risk response outweigh its costs?

3.10.2.2 Do we have offsets of the risk somewhere else in the organisation (that can come from the negative correlation of certain businesses)?

3.10.2.3 If the risk response is to reduce or transfer some or all the risk, would that reduce the competitive advantage that the organisation has today, and would that reduction cause further losses elsewhere in the organisation?

3.11 PRACTICES FOR MANAGING RISK DATA

Leveraging organisational data is key to measuring risk exposures, strengthening the capability of the risk management function to make judgements, identifying problems ahead of time, and allowing better strategic decision making. However, the risk data needs to be retrieved accurately, aggregated, synthesised, and communicated appropriately to leverage the risk data effectively. So, there is a need to have a robust risk data management framework.

3.11.1 Risk data aggregation should be a joint responsibility of the risk management function and the business team. While the risk management function is responsible for defining the required risk data, the business is responsible for providing the desired quality of data in the requisite format.

3.11.2 The risk management function should have a defined inventory and classification of risk data required along with the desired reporting frequency.

3.11.3 The risk management function should define standard data templates for the business to capture / retrieve and provide data. The taxonomies for data fields and formats should be standardised across the organisation to bring consistency and clarity.

3.11.4 The organisation should have a strong data governance framework including robust IT controls and an appropriate BCP plan to ensure the accuracy, integrity, and availability of risk data. The IT system controls should prevent unauthorised alteration or manipulation of data.

3.11.5 The IT architecture should allow data to be extracted on an automated basis to minimise the probability of errors. Only where professional judgements are required should human intervention be allowed.

3.11.6 The IT architecture should be flexible to allow the customisation of data extraction formats and facilitate the provision of additional data parameters if they need to be captured to measure or assess emerging risks.

3.11.7 Both the business team and risk management function should monitor the accuracy of data on a continuously. A predefined list of validation rules should be run on the data to check for accuracy and completeness. An appropriate escalation procedure and corrective action plan should be defined to rectify any errors in the data.

3.11.8 The business team should make data available to the risk management function on a timely basis as per a predefined frequency to allow timely risk reporting.

3.11.9 The circulation of risk data and risk reports should be limited as appropriate to ensure integrity and confidentiality.

3.11.10 The risk management function should ensure that the risk reports are accurate, complete, and easy to understand, allowing the Board, RMC, or executive management to take appropriate decisions.

3.12 MEASURING AND REPORTING OF ACTUAL OUTCOME/LOSS VIS-À-VIS THE DEFINED RISK MODELS

3.12.1 Once the risk responses are agreed upon, the risk management function may periodically

review the actual progress made in implementing them. There is a need for assurance that risk mitigants implemented are operating effectively to keep inherent risk at an acceptable level.

3.12.2 Implementation of the risk responses may be a critical performance measure and be one of the KPIs of the department and business unit head concerned.

3.12.3 After the implementation of risk responses, the risk management function must periodically re-measure the risk to obtain assurance that the risk has been reduced to the desired residual levels.

3.12.4 If there are any seemingly minor adverse incidents or risk events that occur, there should be a defined incident management process to capture and record these. Such minor incidents, if not appropriately captured and acted upon, may lead to serious consequences including a crisis-like situation.

3.12.5 Businesses are responsible for keeping an ongoing record of all material losses that they have experienced, and these should be compared to the predicted expectation of loss for such incidents. Risk management should review these records and work with the business to resize the risk estimates if actual losses exceed expected losses.

3.13 REPORTING OF RISKS TO THE BOD AND BOD-LEVEL RMC

Organisations may use heat maps to report significant risk factors to the BOD and BOD-level RMC on a quarterly basis. The reporting should cover the following:

3.13.1 Significant risks the executive management and/or the CRO and Operating-level RMC believe need the attention of the BOD and BOD-level RMC. These may be in terms of potential adverse consequences of the risk or a new opportunity/ enhancement of an existing opportunity that the risk might be offering.

3.13.2 Proposed risk response or actual implementation of risk response to address the risk and showcase how the inherent risk level is reducing to residual levels to bring it down within the defined risk limits.

3.13.3 Specific guidance required from the BOD and BOD-level RMC concerning the reported risks, opportunities, and addressal plan.

3.14 KEY IMPLEMENTATION CHALLENGES AND BEST PRACTICES

3.14.1 Dealing with criticism and dispelling the common image–the overall risk management culture should dispel any image of being a hindrance to implementing new ideas; it should rather change the perception to risk/reward management being an enabler to bolder, faster, and risk-intelligent business decisions.

3.14.2 Managing risk data – given the quantum of risk data that organisations generate, it becomes a significant operational challenge to appropriately manage the data and convert it to useful information. The data sets may be getting pulled out from disparate sources, unstructured, and in inconsistent formats, which limits the ready usability/reliability of the data in the received state. The resultant information derived from such data may also not be useful. Therefore, organisations need to clearly articulate the requisite risk information and accordingly dedicate appropriate resources to structure the data formats and then curate it into meaningful information. The resources should be adequate

to develop the information reports, perform testing and rollout, and train the risk and control owners on the reporting process.

3.14.3 Focus limited to BAU–as organisations continue to invest efforts in BAU, the considerations of scenarios beyond the BAU take a backseat. This is where the scenario building of potential risk events fails and eventually, risk management doesn't get implemented in substance. Organisations need to continuously ask 'what if' and consider scenarios beyond the BAU to be able to appropriately identify and address risk events. Most large risk event blow-ups can historically be sourced to non-BAU scenarios.

"Organisations need to clearly articulate the requisite risk information and accordingly dedicate appropriate resources to structure the data formats and then curate it into meaningful information."

4.0 RISK MANAGEMENT PLAYBOOK

4.1 PLAYBOOK FOR THE BOD

4.1.1 ROLE DEFINITION FROM A RISK MANAGEMENT PERSPECTIVE

4.1.1.1 Approving the risk appetite of the organisation.

4.1.1.2 Setting the tone at the top and instilling the right culture across the company.

4.1.1.3 Developing and sustaining the culture and behaviour to support effective risk management and reinforcing doing the right thing naturally – instilling risk culture in the DNA of the organisation.

4.1.1.4 Monitoring the implementation of a robust framework to identify, measure, periodically communicate, and engage with stakeholders.

4.1.1.5 Ensuring that strategic planning and risk management processes are in sync with each other as the strategic planning process must be agile enough to address emerging risk factors.

4.1.1.6 Monitoring the company's exposure to risk and the key risks that could undermine its strategy, reputation, or long-term viability.

4.1.1.7 Ensuring that executive management has put in place action plans to mitigate the risks identified as decided – 4T execution.

4.1.1.8 Providing oversight of the risk management system and reviewing its adequacy and effectiveness at least annually.

4.1.2 KEY DECISION FACTORS FROM A RISK MANAGEMENT PERSPECTIVE

4.1.2.1 Determining whether setting up an RMC is required (for organisations that are not mandated as per SEBI's LODR regulations, 2015 as amended) depending on the size and composition of the Board, size and scale of the company's operations, and the risk landscape of the company.

4.1.2.2 Determining if members of the RMC are independent of the management unless a member is consciously appointed when deemed necessary.

4.1.2.3 Determining if the diversity of background and skill set of RMC members is appropriate.

4.1.2.4 Defining the role of the Remuneration Committee in linking risk management with remuneration as risk awareness and management should be one of the key parameters of evaluation for CXOs.

4.1.2.5 Ascertaining whether a CRO is required depending on the scale, diversity, and complexity of the company's operations.

4.1.2.6 Deciding if the reporting hierarchy of the CRO is appropriate:

a. In organisations where there is a CRO, the functional reporting of the CRO may be to Board-level RMC, while the administrative reporting could be to the CEO/MD.

However, in cases where the CRO does not report to the Board-level RMC, he/she should have access to the Board-level RMC whom they can meet independently.

b. The CRO should not have any business targets that could conflict with his/her risk management roleand should ideally not have any additional responsibilities. However, if he/she must have another role, that should not conflict with his or her primary role as a CRO.

4.1.2.7 Determining the adequacy of resources and availability of requisite experience to manage risks.

4.1.2.8 Periodicity and nature of training in the risk management domain to the Board members including independent directors both as an induction programme and on an ongoing basis.

4.1.3 QUESTIONS TO ASK THE BOD-LEVEL RMC AT BOARD MEETINGS

4.1.3.1 Can the management demonstrate a systematic and disciplined process for risk identification, assessment, and prioritisation; risk response; and risk monitoring and reporting?

4.1.3.2 Is the risk information adequate and appropriate to allow risk-based decision making?

4.1.3.3 Is there a common risk taxonomy across the organisation?

4.1.3.4 Has management invested time in analysing internal and external environmental changes which may impact the organisation's business model and resultant threats and opportunities?

4.1.3.5 Is management doing enough to deal with such internal and external environmental changes?

4.1.3.6 Is there a culture of innovation in the organisation to deal with disruptions in the business environment and to stay ahead of the competition?

4.1.3.7 Is the strategic risk information being shared on a timely basis for the BOD to extend meaningful help to the executive management rather than being rushed into decisions?

4.1.3.8 Are there any unlikely but high-consequence threats that might sink the business?

4.1.3.9 Is there a top-down message to allow employees to think out of the box, take risks, and make mistakes to allow the organisation to stay ahead of the curve?

4.1.3.10 Are the roles and KRAs of the RMC, CEO, and CXOs clearly defined in terms of risk management?

4.1.3.11 Are business decisions proposed after considering pertinent risk parameters–applying a 360 degree risk lens?

4.1.3.12 Should executive members of the RMC have voting rights in the decision making of the RMC?

4.1.3.13 How does the executive management get assurance around the reduction of inherent risk levels to residual risk levels?

4.1.3.14 Are there established channels of communication for individuals to report suspected breaches of laws and regulations or other improprieties?

4.2 PLAYBOOK FOR BOD-LEVEL RMC

4.2.1 Role definition from a risk management perspective

4.2.1.1 Ensuring that roles and KRAs of CXOs and business unit heads are clearly defined in terms of risk management.

4.2.1.2 Annual scanning of the environment to gauge the impact on the company's risk profile.

4.2.1.3 Promptly bringing to the attention of the Board any significant changes to the existing risk landscape or any emerging risk factors that have come to its notice.

4.2.1.4 Advising the Board on strategic decisions from the perspective of their impact on the risk tolerance of the company.

4.2.1.5 Advising the Board on the company's risk exposure, risk tolerance, and mitigation strategy.

4.2.1.6 Reviewing the robustness of the organisation's BCP processes.

4.2.1.7 Working with the executive management to prepare an ESG roadmap and monitoring follow - through on it.

4.2.1.8 Checking if adequate and appropriate risk information is reported to the Board on a timely basis to drive adequate prioritisation.

4.2.1.9 Reviewing the company's risk assessment process, including the parameters used and the methodology adopted.

4.2.1.10 Reviewing the company's capability to identify and manage new risk types.

4.2.1.11 Reviewing the company's procedures including the whistle-blower mechanism for detecting frauds and illegal transactions.

4.2.1.12 Periodic training in the risk management domain to the members of the RMC both as an induction programme and on an ongoing basis.

4.2.1.13 Monitoring residual versus inherent risk levels for identified risks and reviewing acceptability of exposure.

4.2.1.14 Ensuring that risk ownership continues to stay with the respective departments and not assumed to be with the CRO.

4.2.2 KEY DECISION FACTORS FROM A RISK MANAGEMENT PERSPECTIVE

4.2.2.1 Need for independent external advice where appropriate on strategic decisions.

4.2.2.2 Applying risk weights to performance measurement of CXOs and business unit heads as input for the Remuneration Committee.

4.2.2.3 Deciding whether the executive management takes into consideration the correlation between risk factors.

4.2.3 QUESTIONS TO ASK CEO, THE CXOS/ BUSINESS UNIT HEADS/OPERATING-LEVEL RMC AT RMC MEETINGS

4.2.3.1 Is the velocity of risk understood, assessed, and considered in firming up risk response strategies?

4.2.3.2 Are strategic/key business decisions proposed after considering pertinent risk parameters?

4.2.3.3 Are the CXOs and business unit heads responsive towards risk findings?

4.2.3.4 Are the results of the risk identification workshops feeding into the internal audit plan?

4.2.3.5 Are proposed actions to fix material breaches adequate and monitored for timely implementation?

4.2.3.6 Does the company's whistle-blower mechanism ensure anonymity and include anti-retaliation measures?

4.2.3.7 Is the risk management function independent of departments and business units?

4.2.3.8 Is the risk identification exercise exhaustive enough to, include significant risks including but not limited to operations, people, ESG, market, credit, liquidity, technological, cyber, legal, health and safety, environmental, or reputation?

4.2.3.9 Is there a mechanism to identify emerging risks periodically?

4.2.3.10 Is there a mechanism to assess emerging risks and re-assess known risks periodically?

4.2.3.11 Are risk tolerance limits clearly articulated for various risk categories?

4.2.3.12 Are authority, responsibility, and accountability clearly defined such that decisions are made, and actions taken by the appropriate people?

4.2.3.13 Has the inherent risk level of identified key risks reduced to desired residual levels for them to accept the exposure?

4.3 PLAYBOOK FOR THE CEO

4.3.1 Role definition from a risk management perspective

4.3.1.1 Driving an appropriate tone at the top and setting the direction for the executive management including the CXOs and business unit heads in terms of attitude towards risk management.

4.3.1.2 Driving a risk culture by creating a positive perception and communicating the relevance and value derivation from risk management practices till they become a part of the DNA of the organisation, and then continue to sustain the ingrained culture.

4.3.1.3 Drive effective designing and implementation of the risk management systems and processes.

4.3.1.4 Evaluating the effectiveness of the risk management systems and processes.

4.3.1.5 Identifying the risks relevant to the business of the company.

4.3.1.6 Identifying changes to the existing risk landscape or any emerging risk factors and promptly bringing them to the attention of the Board-level RMC, only if significant.

4.3.1.7 Ensuring that adequate and appropriate risk information is reported to the Board-level RMC on a timely basis to drive adequate prioritisation.

4.3.1.8 Ensuring the quality, adequacy, and timeliness of the information that goes to the Board.

4.3.1.9 Ensuring that risk management processes are not only limited to 'unrewarded risks', but also encompass the 'rewarded risk' which brings in levers for value creation.

4.3.1.10 Ensuring inherent risk levels have been reduced to desired residual levels for the exposure to stay within the organisation's risk appetite/capacity.

4.3.2 Key decision factors from a risk management perspective

4.3.2.1 Whether the organisation will benefit by taking a particular risk, given how it is being managed.

4.3.2.2 The right balance between mitigating the downside of risks to an acceptable level while still taking advantage of opportunities.

4.3.2.3 The risk-reward trade-off, i.e., the costs of managing risk vis-à-vis the benefit obtained by managing the related risks.

4.3.3 Questions to ask to the CXOs/Business Unit Heads/Operating-level RMC at periodic business update meetings

4.3.3.1 Are decisions proposed after considering pertinent risk parameters including evaluating non-BAU scenarios?

4.3.3.2 How are the CXOs and business unit heads nurturing a culture of innovation?

4.3.3.3 Are the risk factors identified by the CXOs and Operating-level RMC exhaustive?

4.3.3.4 What is the quantum of risk exposure if a particular risk is not mitigated?

4.3.3.5 Is an ongoing evaluation of the competitive landscape of the organisation is being done including potential threats posed by newer entrants or by players from completely different industries?

4.4 PLAYBOOK FOR CXOS/BUSINESS UNIT HEADS/OPERATING-LEVEL RMC

4.4.1 Role definition from a risk management perspective

4.4.1.1 Assuming and managing risks and taking ownership of the assumed risks.

4.4.1.2 Designing, implementing, and monitoring the risk management and internal control systems.

4.4.1.3 Identifying the risks relevant to the business of the company.

4.4.1.4 Identifying changes to the existing risk landscape or any emerging risk factors and promptly bringing them to the attention of the CEO and Board-level RMC, only if significant.

4.4.1.5 Ensuring that an exhaustive set of risk factors have been identified for consideration of appropriate risk response.

4.4.1.6 Ensuring that adequate and appropriate risk information is reported to the CEO and Board-level RMC on a timely basis to drive adequate prioritisation.

4.4.2 Key decision factors from a risk management perspective

4.4.2.1 The right balance between mitigating the downside of risks to an acceptable level while still taking advantage of opportunities.

It Is necessary for organisations to manage the full spectrum of risks, adequately assess and address risk from all perspectives.

4.4.2.2 Whether the appropriate individual or team member has been assigned the responsibility to manage specific risks.

4.4.2.3 Whether the cost of risk response is greater than the anticipated benefit.

4.4.2.4 Whether there is a lack of willingness to address risks, implement agreed risk responses, and how is one addressing them.

4.4.3 Questions to ask operating leaders at periodic operating review meetings

4.4.3.1 Is the team competent enough to apply risk considerations to business decisions?

4.4.3.2 Are business decisions proposed after considering pertinent risk parameters, and considering non-BAU scenarios?

4.4.3.3 Is there an indoctrination of risk thinking at an operational level?

4.4.3.4 Is the correlation and functional inter-dependencies of various risk exposures considered while one addresses a particular risk and its related response?

4.4.3.5 Are the relative movement of consequence and likelihood of risk basis the chosen risk response and the residual risk within the risk appetite of the organisation?

5.0 STAKEHOLDER MANAGEMENT

5.1 Various risk factors emanate from internal and external stakeholders and the organisation needs to have a defined framework to communicate and engage with stakeholders to address those risks. While the internal stakeholders include the employees, the external stakeholders include customers, vendors, third parties, lenders, regulators, shareholders, and the community. The framework should include but not be limited to:

5.1.1 Identification of relevant stakeholders and understanding how they impact the organisation.

5.1.2 Mode of communication with stakeholders.

5.1.3 Frequency of engagement.

5.1.4 Communication/Reporting to be made to stakeholders.

5.1.5 Process to take and incorporate feedback from stakeholders.

5.2 Below are indicative modes of engagement with different stakeholders of an organisation to address specific risk parameters. The modes of engagement below are recommended practices, however, based on the specifics of the organisation.

Stakeholders	Indicative risks	Engagement mode
Customers	Changing preferences and trends, product safety issues, or recalls	Consumer research, social listening workshops, emails, press release
Vendors	Supply disruptions, non-compliance by vendors	Vendor conferences, workshops, emails, press release
Employees	Capability, diversity, equality, inclusion	Meeting with the union, coffee with HR, appraisal discussions, workshops, emails
Government	Changing regulations and compliance	Industry associations, meetings, press release
Investors	ESG activism	Investor conferences/workshops/emails
Community	Local activism, unrest	CSR

5.3 Nature and frequency of communication around risk management to internal and external stakeholders but are not limited to the following. These are recommended practices, however, may vary based on the specifics of the organisation. The organisation would always ensure that it does not disclose financial challenges or distress or any other information which is detrimental to the interests of the company.

Information	Communicated to	Frequency
Status and success of risk management efforts	Employees, vendors, customers, lenders, government, regulators, shareholders, community	Half-yearly or as determined by the organisation
Key risk factors as it impacts them (both threats and opportunities) the organisation is dealing with, and actions being taken to address or leverage them	Employees, vendors, customers, lenders	Quarterly or as determined by the organisation
Socialising role of risk management function	Employees	Half-yearly or as determined by the organisation
Role of employees in identifying and managing risks, measuring performance, and alignment with compensation	Employees (as required)	Half-yearly or as determined by the organisation
Major change in internal/ external environment impacting external stakeholders	Employees, vendors, customers, lenders	Real-time, as and when required
Major change in internal/ external environment impacting internal stakeholders	Employees	Real-time, as and when required
Responding to the concerns and expectations of stakeholders	Employees, vendors, customers, lenders, government, regulators, shareholders, community	Real-time, as and when required
Communicating and discussing unaddressed or emerging risk factors bottom-up	As per the defined escalation procedure – business managers, risk committees	Real-time, as and when required
Disclosures to meet regulatory requirements	Shareholders, regulators, government	As prescribed under existing regulation
Disclosure and transparency regarding voluntary conformance to the FICCI-GRMI Risk Code	Employees, vendors, customers, lenders, government, regulators, shareholders, community	Annually or as determined by the organisation

ACKNOWLEDGEMENT

FICCI, GRMI and the Risk Taskforce members sincerely thank all the senior leaders, professionals, and practitioners from leading organisations for making time to participate in the Model Risk Code feedback and stress testing process and providing some incredibly insightful and qualitative perspectives to enrich the Model Risk Code output. GRMI looks forward to continuing to engage with the industry to further enrich the Model Risk Code initiative as it moves into its next leg of the journey.

Mr. Ajay Seth	Former CFO, Maruti Suzuki India
Mr. Ajay Singh	CFO India and Region Finance Director - South Asia at Hitachi Energy
Mr. Anil Mathews	CRO, Hindalco Industries Limited
Mr. Anil Verma	Executive Director & President of Godrej & Boyce Mfg. Co. Ltd.
Mr. Ankush Jain	CFO, Dabur India Limited
Mr. Ashok Jain	Vice President Finance & Co Secretary at Dabur India Limited
Mr. Chaitanya Adapa	Head, udaanCapital
Mr. Girraj Kumar Bansal	Head - Internal Audit - Dabur India Limited
Mr. James Durkan	Former SVP and Controller – Asia, Middle East and North Africa sector, PepsiCo
Mr. Mahaveer Jain	Vice President and Head – Internal Audit, Diageo
Mr. Murali Ganesan	Executive VP, Finance at ITC
Mr. N Kumar	Vice Chairman, Sanmar Group
Ms. Neha Puri	VP Finance, ReNew Power Private Limited
Ms. Nidhi Seksaria	CRO, Mahindra & Mahindra
Mr. Poovanna Ammatanda	Head Legal - South Asia, Hitachi Energy, General Counsel & Company Secretary, Hitachi Energy India Ltd.
Mr. R Govindan	EVP Corporate Finance and CRO, L&T Limited
Mr. Rajesh Daga	Chief Internal Audit & Risk Management, TATA Power
Ms. Samita Shah	Vice President - CF, Treasury & Risk Management, Tata Steel
Mr. Sandeep Deshpande	CFO, Jyoti International Foods Pvt. Ltd.
Mr. Shantanu Ghosh	Former Global Business Leader - Enterprise Solutions, Genpact
Mr. Simon Britsch	CFO, Bayer South Asia
Mr. Sivaram Subramoniam	Head of Internal Audit, Titan Company Ltd
Mr. Supratim Dutta	Executive Director & Chief Financial Officer, ITC
Mr. Suresh Krishnan	Managing Director and CEO at Paradeep Phosphates Limited
Mr. Vimal Agarwal	CFO, Mahindra Lifespaces Limited
Mr. Vineet Jain	CFO, Medtronic India
Mr. Vishal Agrawal	Chief Enterprise Risk Management, Tata Steel

In case of any feedback on the Model Risk Code or if you want us to connect with you to provide any clarifications on the draft Risk Code, kindly please feel free to reach out to us on at the email ID riskcode@grm.institute.

FICCI ADDRESS
Federation of Indian Chambers of Commerce & Industry
Federation House
Tansen Marg, New Delhi 110001

WWW.FICCI.IN

GRMI REGISTERED OFFICE AND CAMPUS ADDRESS
Risk Educators Pvt. Ltd., Global Risk Management Institute
Plot No. 88, Sector – 44, Gurgaon - 122 003
Haryana I Tel: 0124 6510126

connect@grm.institute I riskcode@grm.institute

WWW.GRM.INSTITUTE

GRMI GLOBAL RISK MANAGEMENT INSTITUTE FICCI

FICCI - GRMI Risk Code Initiative