

India Risk Code *(draft)*

Date: July 1st, 2022



Draft is being distributed only for the purposes of feedback and comments

Table of Contents

No.	Chapter	Page Nos.
	Preface	3
	Executive Summary	4
	Users and Applicability	6
	Abbreviations	6
	Glossary	7
1.0	Relevance of the Risk Code	8
1.1	How FICCI-GRMI Risk Code is intended to be an enabler for organizations	8
1.2	RMC beyond Top 1000 Companies by Market Cap as per SEBI's LODR	9
1.3	Risk Management for MSMEs and New-age Organisations (listed & unlisted)	10
2.0	Principles	11
2.1	Strategy & Leadership	12
2.2	Risk-embracing Culture	12
2.3	Ownership & Empowerment	12
2.4	Resources & Structure	12
2.5	Communication & Reporting	13
2.6	Governance & Monitoring	14
2.7	Risk Data & Information Repository	15
3.0	Leading Practices around Risk Management	16
4.0	Risk Management Playbook	23
5.0	Stakeholder Management	28
6.0	RMC Applicability Beyond Top 1000 Companies Mandated as per SEBI's LODR Regulations, 2015 as amended	29
7.0	Risk Management for MSMEs and New-age Organisations (listed & unlisted)	30

Draft is being distributed only for the purposes of feedback and comments

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 include:

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

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

a. Relevance of the Risk Code – Why it is imperative for organisations to adopt the Risk Code
b. Principles of the Risk Code – Covers the key principles around which the Risk Code is structured for adoption by organisations. The seven principles revolve around Strategy & Leadership, Risk Embracing Culture, Ownership & Empowerment, Resources & Structure, Communication & Reporting, Governance & Oversight and Risk Data & Information Repository
c. Implementation Guidelines – Provides implementation guidance around the seven principles and is a playbook for the Board of Directors, Risk Management Committee, CEO, and CXOs
d. 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, expansive role of 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.

Draft is being distributed only for the purposes of feedback and comments

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 the 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 have to 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 at the moment.

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 and 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, external 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.

The Board and senior executive management should define the amount of capital and / or existing assets it is willing to put at risk in order 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 in the event that risk impact is exceeding the defined risk limits.

The impact 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 its operating setup. Small failures or seemingly insignificant individual risk events that cause losses may be 'early warning signals' which, 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. Implementation of the risk responses may be a critical performance measure and be one of the KPIs of the concerned business unit.

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 in order 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 limit breaches. Organisations should also use heat maps to report significant risk factors and risk responses to the BOD and BOD-level RMC on a quarterly basis and seek specific guidance, as required.

Irrespective of the SEBI LODR regulations, 2015, as amended around BOD-level RMC, which applies only to 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 practices at an early stage in order to take advantage of their potential and retain a competitive edge.

Users and Applicability

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

a. Oversight body –BOD, supported by a Board-appointed RMC wherever applicable.
b. Executive management – including CRO and all other 'CXOs', 'CXO-1' executives, and others as applicable. The definition of the executive layer would vary from organisation to organisation
c. 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.

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 & 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 & 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 - 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. Decisions – includes decisions around assuming risks, risk appetite, and various risk treatment options
4. Dual hatting – refers to a situation wherein an individual is assigned two distinct responsibilities, be it in terms of the assigned roles or across different functions / business units
5. Dynamic environment – risks 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)
6. Heat map – 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
7. Inherent risk – the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or consequence
8. Key Risk Indicator – a metric for measuring the likelihood that the combined probability and consequence of an event will exceed the organization's risk appetite
9. Managed risk – knowing the facts and having information about the event and the resources available to cope with it
10. Residual risk – the risk to an entity that is remaining after management's response to the risk
11. 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
12. Risk – 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
13. Risk data – quantitative and qualitative data collated and managed by the business which allows measuring and monitoring of risk factors
14. Risk capacity – refers to how much capital an organisation needs to sustain itself if it was impacted by a risk event
15. Risk tolerance – the willingness or propensity to take risks
16. Risk Appetite – refers to the types and quantum of risk that an organisation is willing to take in pursuit of its objectives. It is a combination of risk capacity and risk tolerance
17. Risk data aggregation -– defining, gathering and processing risk data
18. Risk-intelligent decision making – decisions that have been made after consideration of applicable risk factors which may impact the outcome of the decision. However, the risk landscape of all

organizations continues to be dynamic (and not static) and hence requires a continuous monitoring of risks

19. Risk limit – a numerical threshold defined in relation with specific risk exposures
20. 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
21. Risk velocity – 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
22. Stakeholder – 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
23. Unmanaged risk – not having the facts and information about the event, or the resources to cope with it
24. Unrewarded risk – 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 the Risk Code

1.1 How FICCI-GRMI Risk Code is intended to be an enabler for organizations

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 has to 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. 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 to 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 in order 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 with 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 organization's ability to adapt to disruptions by being more resilient and ensuring continuity of business operations
1.1.9 Safeguard the organisation's people, assets and capital in the interests of the shareholders and other stakeholders
1.1.10 Identify new innovation possibilities through foreseeing of emerging risk factors when fully understood via strategic disruption or opportunity workshops
1.1.11 Increase the likelihood of innovation being successful by incorporating risk-reward assessments into the new product or new 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 addressing political and economic risks for regulated industries / service segments more prone to situations such as change in policy

1.2 RMC beyond 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 top 100 listed companies to 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 COVID-19 pandemic and the ongoing geo-political 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 take a decision of 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 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 COVID-19 pandemic have beyond doubt exposed the vulnerability of the MSME sector towards significant changes in the internal and external environment. The MSMEs have borne the most severe 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 environment risks because they have to 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 in order to reap its benefits and retain their competitive advantage.

2.0 Principles

2.1 Strategy & 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 the 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 in the event that a 'person in power' including majority shareholders in an organization circumvents or overrides processes in place, because this maybe a major risk facing the organization.

2.1.3 The Board should prevent the possibility of management over-rides at the time of making critical decisions in spite of the company having robust systems and processes in place.

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 categorization of the risks faced by the organization to allow prioritization and reporting of such risks to the Board and Board level RMC. The Board should communicate with the stakeholders (lenders, shareholders, financial institutions, regulators) regarding the top risks faced by the organization and actions being taken to address those risks, including confirming that the organization'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 in investing in the requisite resources for robust risk management staff and processes.

2.1.10 The Board should declare and demonstrate its commitment to support 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, balanced, risk-intelligent decisions').

2.1.13 The Board should question if the organisation is showcasing 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 in order 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 of the risks across all divisions within a larger organisation. The risk management function must cut across all organisational lines to identify the correlation of risks for the Board and executive management to assess and decide upon 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 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 emphasize 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, in order 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, accept 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, exercise judgment, 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 for which the businesses subject to operational RMCs should be responsible

2.3.1.4 Escalating signals of risk limit 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 are empowered to take risk decisions up to approved risk limits, 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 limits or grant temporary limit excesses; it monitors the first line and ensures risks and controls are managed effectively. The second line includes a risk management function to monitor 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 (third line) - 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 primary responsibility of 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 structure commensurate with the size and complexity of the organisation are essential in order to ensure that the organisation has robust risk management practices.

2.4.2 The upfront investment is not limited to the financial cost but also 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:

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, organizations 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, if implemented in substance, creating a competitive advantage for the organisation. The RMCs, both at Board level and at 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 mandates 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.

While the Audit Committee would provide oversight on controls and assurance process as defined are operating effectively, the RMC should have a broader focus on areas including business strategy, new products, new markets, and mergers & acquisitions. The RMC should be a proactive leg of the risk management ecosystem which focuses on embedding risk culture into the DNA of the organization. This would also allow the internal auditors to focus more on value creation projects and initiatives as the robust second line will require lower time and effort investment.

2.4.3.1 Composition and Operating Model of BOD-level RMC

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 operating-level RMC within the organisation, organisations should have an operating-level RMC to support the BOD-level RMC and to oversee and ensure effective implementation of risk management. The Operating level RMC may be at a Business Unit level, Geographical level or a functional level.

2.4.3.2 Composition and Operating Model of Operating-level RMC

Appointed by	MD and Executive Management
Strength	At least five members
Chair	Business unit head / region head/ functional head depending on the organization structure
Composition	Mix of business unit heads, region head 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 full-time Chief Risk Officer (CRO) to operate across the whole

organisation and 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.

2.4.4.2 In organisations where there is a Chief Risk Officer, the CRO shall report to the Board-level RMC.

2.4.4.3 If the CRO also reports to the MD/CEO, the Board-level RMC and the CRO shall meet at least quarterly on a one-to-one basis, without the presence of the MD/CEO.

2.4.4.4 The CRO should not be required to report to any of the business unit heads, should not have any business profitability targets, and should not have any additional responsibilities under 'dual hatting'.

2.4.4.5 The CRO and the risk management function should operate in an autonomous and independent manner and should not have any pre-conceived notions.

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

2.5 Communication & Reporting - Effective, contextual, and periodic communication is established with internal & 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, 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 exchange of information, feedback, and consultation on requisite issues.

2.6 Governance & 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, or nominate an existing CXO to play the role of a CRO as necessary to assist it in carrying out its responsibility of overseeing the company's risk management systems and processes which broadly includes the following:

2.6.1.1 Determining the risk appetite – The Board should determine the company's risk appetite including the nature and extent of the significant risks which 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 to 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 limit breaches, and the steps taken to rectify them

2.6.2.2 The current risk profile of the whole organisation, as well as of its component 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 & Information Repository - A robust mechanism is established around risk information to ensure 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 not just its usage of risk limits, but also any risk limit breaches to the CRO immediately.

2.7.5 The 'second line' risk management function is responsible for managing risks due to factors such as localization of data and theft / leakage. 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 the Board RMC.

3.0 Leading Practices around Risk Management

3.1 Cultivating the risk versus reward 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 also give permission to fail 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 of 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 not 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.

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 use of post-it ballots, visual thinking, creativity boot camps, storyboards

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

3.1.4.3 Encourage games around risk, simulation, and scenario analysis

3.1.5 Organisations can even assess the risk culture by doing employee surveys and asking questions about openness to take risks and make mistakes. Such surveys can also bring out customised ways for the 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 overt 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 imbibed across the supply chain ecosystem including vendors, dealers and third parties. For example, there may be risk factors like raw material shortage, quality, fire safety, financial reporting or attrition for which organizations may share their practices with the vendors, dealers and third parties for them to incorporate. There may be a dedicated team in supply chain department which is responsible for upgrading the supplier's and dealer's excellence by replicating the organization's practices on 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 like 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 management 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, 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 has to 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 new 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 organization 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, change 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 making adjustments to 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 have to 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, 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 unimaginable 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 change in response to those events.

3.4.7 Organisations should be very watchful of systemic risks breeding in its operating setup. They should not ignore small failures or seemingly insignificant risk events that cause losses, as they may be 'early warning signals' which, if not detected and addressed on time, may lead to catastrophic failures. Hence, losses arising from such small failures or insignificant risk events should be monitored on a continuous basis 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 localization and technology failures are acknowledged and perhaps even quantified, there remains an 'unknown unknown' dimension to risks which may emanate from every broad risk category. To take some examples, the particular nature of COVID-19 and how different governments would respond, the wider geo-political 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 risk is identified, understood, and addressed on time.

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. Addressing these risk factors should be based on the pillars:

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

3.5.2.2 Being prepared with appropriate capital buffers to absorb immediate cash flow issues and interim financial losses; the capital buffers should be stress-tested to evaluate if they are adequate

3.5.2.3 Having an organisation-wide integration of IT and financial systems which would help companies respond to unknown risk 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 preparation of a robust risk library and updating of the library on an annual basis. The risk description should be very clear and find a common risk metric in which to express the magnitude of the risk, rather than using multiple (and perhaps overly technical) risk language. 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 have to go together. The risk management responsibility should ideally be positioned within 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 has to be developed in tandem with the risk assessment and should be agile and adaptive so as to address the strategic risk factors.

3.8 Define people and models for quantification/measurement/limits 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 the same against the risk capacity of the organisation.

3.8.2 The Board and 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 which is aligned to 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 has to 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 for mitigating threats. Depending on the quantum of risk from a business decision, risk appetite either prevents or provokes 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 Risk limits are defined for individual business units, functions, and risk categories based on the overall risk appetite of the organisation. The internal risk management function/ CRO should propose the different risk limits for Board approval, taking into consideration performance and risk versus return, as well as the correlation effects that currently exist, and might exist under stressed conditions, between different business units. Thus, the sum of business limits may exceed the aggregate risk appetite limit of the total organisation if risk limit usage and risk correlations mean that the aggregate risk appetite will not be exceeded. Otherwise, some significant amount of risk capital may be left permanently unutilized.

3.8.9 There should be a robust mechanism to trigger alarm bells in the event that risk impact is exceeding the defined risk limits. 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 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 limits 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 Organizations 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.

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, the qualitative measurement allows relative prioritisation and treatment of such risks.

3.9.5 Measurement of risk velocity can be based on an appropriate judgment 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 smaller and possibly acceptable risk levels. The internal audit team of the organization, be it an in-house team or an outsourced one, would be responsible to provide assurance that the chosen risk responses are ensuring that inherent risks are being reduced 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 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 out 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

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

3.10.1.6 Will the benefits from executing the risk response outweigh its costs?

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

3.10.1.8 If the risk response is to reduce or transfer some or all of 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 around managing risk data

Leveraging organisational data is key to measuring risk exposures, strengthening the capability of the risk management function to make judgments, 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 in order 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 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 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 in order 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 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 continuous basis. 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 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 which the executive management and / or the CRO and Operating level RMC believe needs the attention of the BOD and BOD level RMC. These may be in terms of potential adverse consequence of the risk or a new opportunity / enhancement of 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 with respect to the reported risks, opportunities, and addressal plan.

3.14 Key implementation challenges and best practices to address

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 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 takes 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.

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 organization

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

4.1.1.5 Ensuring that the strategic planning and the risk management process are in sync with each other as the strategic planning process has to 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 their adequacy and effectiveness at least on an annual basis

4.1.2 Considerations to make

4.1.2.1 Determining whether or not setting up an RMC is required (for organisations which 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 Deciding if members of the RMC are independent of the management unless the member is consciously appointed when deemed necessary

4.1.2.3 Ensuring diversity of background and skill set of RMC members

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 case the organisation has a CRO, the CRO shall report to the Board-appointed RMC. In case the CRO is reporting directly to the MD or the CEO, the RMC shall meet with the CRO on a one-on-one basis without the presence of the MD & CEO at least on a quarterly basis.
b. The CRO should not be required to report to any of the business unit heads, have any business targets, or have any additional responsibilities under 'dual hatting'

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

4.1.2.8 Periodic 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 Right to challenge / Questions to ask

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 stay ahead of 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 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 in order 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 (considerations)?

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

4.1.3.13 How does the executive management get assurance around 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

4.2.2 Considerations to make

4.2.2.1 Taking 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 interaction and correlation between risk factors

4.2.2.4 Wherever a CRO is appointed, ensuring that risk ownership continues to stay with the respective departments and not with the CRO

4.2.3 Right to challenge / Questions to ask

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 there any material breaches of risk limits by departments?

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

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

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

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

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

4.2.3.9 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?

4.2.3.10 Is there a mechanism to identify emerging risks on a periodic basis?

4.2.3.11 Is there a mechanism to assess emerging risks and re-assess known risks on a periodic basis?

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

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

4.2.3.14 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

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

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 actually brings in levers for value creation

4.3.1.10 Ensuring inherent risk levels have been reduced to desired residual levels for the Board to accept the exposure

4.3.2 Considerations to make

4.3.2.1 Quantum of risk exposure if a particular risk is not mitigated

4.3.2.2 Benefit to the organisation by taking a particular risk, provided it is managed appropriately

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

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

4.3.2.5 Whether 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

4.3.3 Right to challenge / Questions to ask

4.3.3.1 Are decisions proposed after considering pertinent risk parameters?

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

4.3.3.3 Are CXOs and business unit heads challenging the status quo and striving towards more effective and efficient ways of working?

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

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

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 Considerations to make

4.4.2.1 Achieve the right balance between mitigating the downside of risks to an acceptable level whilst still taking advantage of opportunities

4.4.2.2 Whether the correlation of various risk exposures is considered while one addresses a particular risk

4.4.2.3 How consequence and likelihood are moving basis the chosen risk response

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

4.4.2.5 Whether the cost of risk response is greater than the anticipated benefit

4.4.2.6 Consideration of functional inter-dependencies while evaluating risk and corresponding risk responses

4.4.2.7 Whether there is a lack of willingness to address risks and implement agreed risk responses

4.4.3 Questions to ask

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?

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

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, the government, shareholders, the government, and the community. The framework should be including but not 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:

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 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 may be including but not limited to:

Information	Communicated to	Frequency
Status and success of risk management efforts	Employees, vendors, customers, lenders, government, regulators, shareholders, community	Bi-annually / Annually
Key risk factors (both threats and opportunities) the organisation is dealing with and actions being taken to address or leverage them	Employees, vendors, customers, lenders	Quarterly
Socialising role of risk management function	Employees	Semi-annually / Annually
Role of employees in identifying and managing risks, measuring performance, and alignment with compensation	Employees (as required)	Semi-annually / Annually
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 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 bottoms-up	As per 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

---

We would be grateful to receive your feedback on the draft Risk Code. Please send your inputs to risk.taskforce@ficci.com or riskcode@grm.institute

We would be happy to reach out to you in case you wish to speak to us, kindly drop us a message on the above email ids.

FICCI **GRMI**