RISK MANAGEMENT – IS MITIGATION ADEQUATE?
March 30, 2026

SUMMARY OF DISCUSSIONS

Background

Risk management has been, without argument, one of the major challenges that Boards are grappling with. The Risk Management Committee (RMC) that exists in most companies, is understood to be functioning sub-optimally, with the focus having been, for the most part, on operational risk. In recent times, and especially with the geopolitical situation having changed significantly, it is necessary for RMCs to examine the entire gamut of risks, and to put in place mitigation measures that will at least contain, if not eliminate, the negative impact of those risks. The fact that it is not a Committee mandated by statute, and has been created by regulation, places the RMC in an odd situation where, notwithstanding the importance of risk, it is not treated on par with some of the other committees. This is also reflected in the sub-optimal manner in which RMCs are constituted. The frequency of meetings is also not adequate given the size and the scope of the challenges involved. In this context, it is considered necessary for Chairs and members of RMCs to discuss the practices being followed in their companies, so that the combined experience of the participants can help to lay out a clear roadmap for RMCs and address all connected issues.

DISCUSSIONS

1. Role and Positioning of the Risk Management Committee (RMC)

- The Risk Management Committee (RMC)'s role has evolved significantly from being constituted to meet compliance requirements, to becoming a central pillar of the organisation's governance framework, with its role extending beyond reviewing policies, to providing strategic direction on how risks are identified, assessed, monitored and managed/ mitigated in practice.
- The effectiveness of the RMC lies not merely in the existence of risk frameworks or documentation, but in the depth and quality of its deliberations, its ability to challenge management assumptions, and its focus on evaluating whether mitigation measures are practical, implementable and aligned with the organisation's defined or implied risk appetite.
- The RMC should act as a strategic advisor to the Board, facilitating informed decision-making on risk-related matters. However, it should not be viewed as a substitute for the Board, in its responsibility towards risk management, as the ultimate accountability for risk management continues to rest with the Board.
- RMCs should avoid overburdening themselves with operational and strategic risks. Most large companies have management-level committees to consider them. RMCs should instead require managements to clearly articulate risk frameworks, including defining risk appetite, identifying risks and outlining mitigation plans, which the Committee can then evaluate, including by challenging any assumption.

2. Limitations of the Current RMC Framework

- RMC has been mandated only under SEBI LODR Regulations, 2015, and that too for companies of a certain size. This is a disadvantage since it is a Board appointed committee, and not a Board committee, as mandated under the Companies Act, 2013. All companies, irrespective of their size, face risks, and it is important that constitution of an RMC is not a response to a regulation, but because companies see value in the creation of the Committee.

- In practice, many RMCs are often either treated as compliance-driven bodies or, in adverse situations, as scapegoats when risks materialise, rather than being recognised as proactive enablers of effective risk governance.
- The ability of the RMC to function effectively is directly linked to its understanding of the business, as risk cannot be meaningfully assessed without a clear appreciation of the organisation's operations, value drivers and external dependencies. Capacity building of members is therefore important, but neglected. A number of RMCs are unable to understand the changes in the market, and the resultant emerging risk. This adversely impacts the quality of deliberations at RMC meetings. Reputation risk too is often not addressed by RMCs.
- Regulators, such as the Reserve Bank of India (RBI), have made considerable progress in the field of risk management, by anticipating the requirements of the financial sector, and ensuring that there is rigour in dealing with risks. RBI has also prescribed the formation of committees focused on Information Technology and cyber attacks.
- There is a need for SEBI to expand the mandate to constitute RMCs for companies beyond the top 1000 companies, so that companies start thinking in this direction. The mandate should also be expanded to include the systemically important companies.
- At present, the focus of the Regulator is only on the existence of the Committee, and not on the quality of agenda. There is a need to generate awareness that merely having a Committee is not sufficient.
- RMCs frequently do not get adequate time for meaningful deliberation, which restricts their ability to engage deeply with complex and evolving risks, thereby limiting the effectiveness of their oversight. Most RMCs meet only for the minimum number of meetings.
- While governance frameworks have evolved to provide detailed charters and expectations for the Board and the Audit Committee, similar clarity and depth is often lacking in the case of RMCs, resulting in ambiguity in their role and effectiveness. RMCs do not seem to have templates, like Audit Committees. There is a need for governance architecture to ensure that such templates exist. At the same time, there are some RMCs which are driven only by charters, and lists, and those do not adequately challenge management on risk management. This approach too is not correct.
- While in some Boards, it is considered important to have a common member between the Audit Committee and the RMC, this practice is not uniformly followed.
- Overly prescriptive regulations at times result in managements only responding to them, without thinking out of the box. There is a need for them to at times step back and capture real-world complexities, and anticipate or address risk scenario faced by organisations in a rapidly changing environment.
- Mid and small companies often do not have the bandwidth to move beyond business requirements, to consider the risks that they are facing.
- Regulations continue to play an important role in the formation of risk management frameworks, especially for organisations that adopt governance practices only when mandated. However, forward-looking companies must move beyond compliance, and focus on building robust, practical and forward-looking risk management frameworks. Managements that see value in risk management, often go beyond the minimum prescriptions of regulations.

3. Risk as an Integral Part of Business Strategy

- Risk and business are inherently interconnected. The ability to take informed and calibrated risks is fundamental to achieving growth, sustainability and long-term value creation. Risk management can be a strategic input to the Board. Risks can lead to opportunities.

- Traditional classifications of risks into financial, operational or strategic categories are becoming less relevant, as risks today are interconnected, systemic and capable of impacting multiple aspects of the organisation simultaneously.
- Important areas such as contract risk, which further have third parties, outsourcing risk and business continuity risks have gained prominence, particularly in the post-pandemic environment, highlighting the need for assessing the quantum of risk, and having a more integrated approach to risk management.
- Capital allocation decisions, including whether an organisation operates in growth mode or preservation mode, are intrinsically linked to risk considerations. However, such discussions are often not adequately addressed within the RMC framework. Till recently, most Boards considered this to be an agenda item only for companies in the financial sector.
- Risk discussions should be embedded into strategic decision-making processes, including capital allocation and business planning, rather than being treated as a separate or compliance-driven exercise.

4. The Evolving Risk Landscape: Geopolitical, Cyber and AI Risks

- Risk has moved decisively to centre stage, and is now omnipresent across all levels of an organisation, requiring continuous monitoring and proactive management, rather than periodic review and reactive responses.
- The current risk landscape is shaped by multiple overlapping and interdependent forces, which together increase the complexity, uncertainty and systemic nature of risks faced by organisations.

4A. Geopolitical Risks: Disruption Beyond Organisational Control

- Ongoing geopolitical conflicts and war-like situations have exposed significant vulnerabilities in global and Indian supply chains, leading to disruptions in sourcing, increased costs and uncertainty in business continuity.
- Organisations often underestimate the duration and impact of such events, initially assuming short-term disruptions, without fully assessing their long-term implications on operations and strategy.
- External factors such as trade restrictions, sanctions and shifting global alliances create risks that are beyond organisational control, but have a direct and material impact on business performance.
- De-globalisation trends and concentration of suppliers have increased systemic vulnerabilities, making organisations more susceptible to external shocks and disruptions. While companies may have some exposure to/ details of their suppliers, a deep dive into the suppliers of the suppliers, could reveal concentration of suppliers to a few worldwide becomes more apparent.
- A deeper examination of supply chains often reveals that multiple organisations depend on the same underlying sources, increasing concentration risk, to both the same supplier and to a few countries, and the resultant systemic exposure.
- Traditional planning frameworks are inadequate in such scenarios, requiring organisations to continuously recalibrate strategies in response to rapidly changing geopolitical conditions.

4B. Cyber Risk: From Operational Threat to Systemic Risk

- Cyber risk has evolved from being an IT-related concern to a systemic risk capable of disrupting entire business ecosystems, with potential implications extending beyond individual organisations.
- Threats to critical infrastructure, including undersea communication cables and internet connectivity, highlight the possibility of large-scale disruptions that can bring business operations to a standstill.
- Increasing digitalisation has resulted in organisations becoming heavily dependent on technology, with limited ability to operate effectively in its absence, thereby increasing their vulnerability.

- Cyber threats have evolved significantly, moving beyond ransomware attacks to broader risks that can impact entire networks, industries and economies. A number of companies have grappled with the "accounting entry" for payment for ransomware attacks.
- The consequences of cyber incidents extend beyond financial losses to include reputational damage, regulatory exposure and erosion of stakeholder trust.
- Cyber risk cannot be completely eliminated. Therefore, organisations must focus on building resilience, strengthening mitigation strategies and developing robust response mechanisms.
- Over time, cyber risks may become better understood. However, at present, they remain dynamic, evolving and difficult to quantify. Even now, most organisations do not completely appreciate cyber risks.

4C. Artificial Intelligence (AI) Risk: Complex Challenges

- The increasing use of AI has introduced a new and complex layer of risk, with implications across multiple functions and industries.
- AI-related risks include data misuse, lack of transparency, model bias and limited explainability, all of which create significant governance challenges.
- AI systems often rely on diverse and open data sources, increasing unpredictability and making outcomes difficult to control or validate.
- Even minor inputs can lead to disproportionate or unintended consequences, making these risks difficult to anticipate and manage.
- While AI offers significant opportunities in terms of efficiency and risk identification, it also raises concerns around data ownership, accountability and ethical use.
- The potential for generating manipulated or misleading outputs further complicates the risk landscape and requires heightened oversight.
- Regulatory frameworks in this area are still evolving and may not keep pace with technological advancements, creating gaps in governance and oversight.

4D. Interconnected Nature of Modern Risks

- Risks, including geopolitical, cyber and AI risks, are deeply interconnected and often amplify each other, creating a complex and systemic risk environment.
- Risks originating in one area can quickly cascade across geographies and sectors, making it difficult to isolate and manage them using traditional approaches.
- Static risk management frameworks, with only periodic reviews, are increasingly inadequate in addressing such dynamic and evolving risks.
- Organisations must therefore adopt continuous, adaptive and forward-looking approaches to risk management.

4E. Preparedness, Resilience and Value Chain Risks

- While awareness of risk management has increased post-pandemic, actual preparedness remains inconsistent across organisations.
- Learnings from crisis are often not institutionalised, leading to repeated vulnerabilities over time.
- Value chains are highly interconnected, and organisations must focus on building resilience by reducing dependencies and strengthening supply chains.
- Preparedness requires scenario planning, identification of key risks and development of structured response strategies.
- The focus should shift from predicting risks to building the capability to respond effectively when risks materialise.

5. Risk Appetite, Risk Identification and Risk Measurement

- Management is responsible for defining the risk appetite, identifying/ updating risk, categorising them based on the probability of their occurrence and resultant impact, and suggesting mitigation measures, while the RMC evaluates whether appropriate systems and frameworks are in place, and whether risks are being prioritised correctly and effectively.
- RMC often do not have clarity regarding the risk appetite, leading to ambiguity regarding the extent of risk the organisation is willing to accept.
- There is a need to establish clear mechanisms to define and measure risk appetite of the organisation and its tolerance levels, supported by reliable data and analysis. Risk should then be measured against this statement, and if management is found to be risk averse or not taking enough risks, there should be accountability.
- Risks should be identified and documented, even if they cannot be fully measured, as awareness itself is a critical first step towards preparedness. This list must periodically be revisited to understand if the probability of occurrence/ impact of the risk has undergone any change.
- Organisations should distinguish between operational risks, known and unknown risks, visible and non-visible risks, and ensure that each category receives appropriate attention. Unknown risks are the ones that deserve the most attention in today's world.
- Listing low-probability, but high-impact risks, is essential for building resilience and preparedness.
- Probability analysis, scenario planning and a rough action plan should be ready for all potential risks. This would include creation of SOPs for each risk, including what to do when it happens. Cost-benefit analysis of risks too should be conducted.
- Periodically updated heat maps must be prepared, and presented to the RMC.
- A number of companies have forgotten the lessons learnt from the pandemic. In sectors such as manufacturing sector, corporate planning and inventory management have to be done regularly, owing to changes in ground realities on a month-to-month basis.

6. Management as the First Line of Defence

- Management acts as the first line of defence and is responsible for identifying, assessing and managing risks at an operational level.
- It must design and implement practical mitigation strategies, and ensure that risks are addressed in a timely and effective manner.
- Management should continuously adapt business models in response to evolving risks, rather than relying on static approaches.
- There is increasing recognition among some managements of the value of the RMC, with organisations showing willingness to move beyond compliance-driven approaches.
- What is important is that the response of the company, in the event of a risk fructifying, should be decided. Measures for business continuity should be working at all times.

7. Ownership of Risk and Role of the Chief Risk Officer (CRO)

- There is often ambiguity regarding ownership of risk within organisations, particularly in determining whether responsibility lies with the CRO, the management, the business units or the RMC.
- The CRO plays a critical role in proactively identifying and flagging risks, including emerging and unknown risks, and ensuring that these are brought to the attention of the management and the RMC.
- The role of the CRO is not to solve all problems, but to anticipate risks and facilitate informed decision-making. For this, he/she has to work with business heads.

- Effective CROs bring a forward-looking perspective, supported by global awareness and access to relevant information. They have to visualise risks, and stay ahead of the curve.
- Lack of experienced CROs is a problem. There is a need to identify persons, who understand business and risks, and have the right aptitude, and appoint them as CROs. Unfortunately, most companies do not even have a dedicated CRO in position.
- While Internal Audit persons help in risk management, it is a sub-optimal solution.

8. Communication, SOPs and Crisis Management

- Not knowing what to do when there is a risk is a very common shortcoming of risk management frameworks today. Effective risk governance requires continuous flow of information, clear escalation mechanisms and strong communication channels.
- Clarity on escalation mechanisms is critical during crisis, including defining whom to approach and how decisions are to be communicated and implemented.
- Effective risk management requires strong vertical and horizontal communication across the organisation.
- Well-defined SOPs are essential to ensure structured and timely responses to risk events.
- Documentation alone is insufficient; the real value lies in execution, preparedness and response capability.

9. Board – RMC Engagement

- Risk management should be recognised as a shared responsibility across the Board, the RMC and the management, rather than being delegated entirely to the Committee, as such delegation can dilute accountability and weaken overall governance.
- In all forward-looking Boards, risk has become a systemic agenda item, since avoiding it has huge ramifications. “What if” has become an important dialogue among Board members.
- The RMC must act as a bridge between the Board and the management. It must decide what should go to the Board for discussions, such as strategic risks, which must be discussed at the Board level, with the operational risks being discussed at the RMC. Directors, who are not members of RMC, too should be involved in such discussions. In some Boards, the practice of the non-members of RMC attending RMC meetings as invitees exists.
- Policies relating to risk management must be approved at the Board level.
- Briefings on the proceedings of RMC meetings by the Chair of the RMC to the Board should be a structured and regular agenda item in Board meetings, ensuring that risk remains central to Board-level discussions. Enough time should be set aside for this.
- Boards often focus more on responding to crisis, rather than preparing for them, thereby highlighting the need for greater emphasis on preparedness and scenario planning.
- Informal discussions often provide deeper insights into risks. However, formal documentation remains critical for accountability and governance. Some Boards have informal discussions on risks at offsites, during non-formal meeting hours, to discuss the environment in which the business is operating. In some companies, the separate meeting of IDs is used for discussing risks, as it gives IDs a platform to have a freewheeling conversation, without a fixed agenda.
- Boards must ensure that managements also inform and educate key investors about the risks being faced by the organisation.

10. Realities of Risk Management

- Not all risks can be anticipated or mitigated. Organisations must accept a degree of uncertainty as inherent to business.

- Certain risks, particularly cyber and technology-related risks, cannot be completely eliminated and must be managed through resilience and preparedness.
- Risk management is a central aspect of business survival and long-term sustainability.
- The emphasis should therefore be on adaptability, responsiveness and continuous learning, rather than attempting to eliminate all risks.

EXCELLENCE ENABLERS

CORPORATE GOVERNANCE SPECIALISTS
ADDING VALUE, NOT TICKING BOXES
www.excellenceenablers.com

The views expressed in this report are the views of the participants at the roundtable and do not necessarily reflect the views of Excellence Enablers Private Limited.