Risk Management and the Board of Directors - An Indian Perspective

* S.K. Sachdeva and CS Bhagyashree Bardia

The corporate risk taking and the monitoring of risks have continued to remain front and centre in the minds of boards of directors, legislators and the media, fuelled by the powerful mix of continuing worldwide financial instability, ever-increasing regulation, anger and resentment at the alleged power of business including retrenchment, contraction, and changing dynamics. The reputational damage to companies and their boards that fail to properly manage risk is a major threat.

SEBI has issued SEBI (LODR) Regulations, 2015 which provides that top 100 listed entities, determined on the basis of market capitalisation, as at the end of the immediate previous financial year must constitute risk management committees to identify, evaluate and mitigate all risks associated with business, interest rates, currencies and other challenges companies face.The boards of these companies have to define the roles and responsibilities of the committee and may delegate monitoring and reviewing of the risk management plan to the panel.

Risk Oversight and Role of the Board

"Risk oversight" describes the role of the board of directors in the risk management process. The risk oversight process is the means by which the board determines that the company has in place a robust process for identifying, prioritizing, sourcing, managing and monitoring its critical risks and that that process is improved continuously as the business environment changes. By contrast, "risk management" is what management does, which includes appropriate oversight and monitoring to ensure policies are carried out and processes are executed in accordance with management's selected performance goals and risk tolerances.

Risks related to cyber security and IT oversight continues to be issues that merit ever-increasing attention and oversight. Online security breaches, theft of personal data, proprietary or commercially sensitive information and damage to IT infrastructure are omnipresent threats and can have a significant financial and reputational impact on companies.

Risk Challenges

Global business expansion, stricter regulatory environments, evolving use of integrated system by management, and resource and talent constraints are leaving companies with increased risk exposure. Board need to:

- Enhance insight into their business processes.
- Establish performance indicators to support a Control Framework and associated root cause analysis.
- Identify and analyze opportunities to manage control gaps.
- Manage risk through automation of analysis and enhanced work flow management.

Regular Control Monitoring

Visibility into business processes for compliance and governance, identification of process risks and control weaknesses, and closer alignment of business strategies to operations and resources are key objectives for major organisations. The challenge has been to monitor an integrated methodology and supporting infrastructure on an ongoing basis. It provides the platform for

- Independent testing of business transactions for errors, exceptions, and controls weaknesses.
- Process and cost effectiveness.
- Near real-time and regular monitoring of control effectiveness.
- Visualization for control status.

How Boards can handle Risks

The board cannot and should not be involved in actual day-to-day risk *management.* Directors should instead satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and risk appetite, that these policies and procedures are functioning as directed, and that necessary steps are taken to foster an enterprise-wide culture that supports appropriate risk awareness, behaviours and judgments about risk and that ensures that risk-taking beyond the company's determined risk appetite is recognized and appropriately escalated and timely addressed. The board should ensure that the senior executives are fully engaged in risk management and should also be aware of the type and magnitude of the company's principal risks.

The board can send a message to management and employees that comprehensive risk management is neither an impediment to the conduct of business nor a mere supplement to a firm's overall

compliance program, but is instead an integral component of strategy, culture and business operations.

The board and relevant committees should work with management to promote and actively cultivate a corporate culture and environment that understands and implements enterprise-wide risk management. Comprehensive risk management should not be viewed as a specialized corporate function, but instead should be treated as an integral, enterprise-wide component that affects how the company measures and rewards its success.

The board should formally undertake an annual review of the company's risk management system, including a review of board and committee-level risk oversight policies and procedures, a presentation of "best practices" to the extent relevant, tailored to focus on the industry or regulatory arena in which the company operates, and a review of other relevant issues such as those listed above.

Risk management should be tailored to the specific company, but, in general, an effective risk management system will

(1) adequately identify the material risks that the company faces in a timely manner;

(2) implement appropriate risk management strategies that are responsive to the company's risk profile, business strategies, specific material risk exposures and risk tolerance thresholds;

(3) integrate consideration of risk and risk management into strategy development and business decision-making throughout the company; and

(4) adequately transmit necessary information with respect to material risks to senior executives/the board/relevant committees.

Some of the important actions that Board/appropriate committees may consider as part of their risk management oversight include the following:

- review with management the company's risk appetite and risk tolerance,
- establish a clear framework for holding the CEO accountable for building and maintaining an effective risk appetite framework and providing the board with regular, periodic reports on the company's risk status;
- review with management the categories of risk the company faces, including any risk concentrations and risk interrelationships, as well as the likelihood of occurrence, the potential impact of those risks, mitigating measures and action plans to be employed if a given risk materializes;
- review with management the assumptions and analysis underpinning the determination of the company's principal risks and whether adequate procedures are in place to ensure that new or materially changed risks are properly and promptly identified, understood and accounted for in the actions of the company;
- review with committees and management the board's expectations as to each group's respective responsibilities for risk oversight and management of specific risks
- review the risk policies and procedures adopted by management,
- review management's implementation of its risk policies and procedures, to assess whether they are being followed and are effective;
- review with management the design of the company's risk management functions to assess whether they are appropriate given the company's size and scope of operations;
- review with management the primary elements comprising the company's risk culture,
- review with management the means by which the company's risk management strategy is communicated to all appropriate groups within the company
- review internal systems of formal and informal communication across divisions and control functions to encourage the prompt and coherent flow of risk-related information
- review reports from management, independent auditors, internal auditors, legal counsel, regulators and outside experts as considered appropriate regarding risks the company faces and the company's risk management function.

In addition to considering the foregoing measures, the board may also want to focus on identifying external pressures that can push a company to take excessive risks and consider how best to address those pressures.

Concluding Comments

The company's risk management structure should include an ongoing effort to assess and analyze the most likely areas of future risk for the company, including how the contours and interrelationships of existing risks may change and how the company's processes for anticipating future risks are developed. Anticipating future risks is a key element of avoiding or mitigating those risks before they escalate into crises. In reviewing risk management, the board or relevant committees should ask the company's executives to discuss the most likely sources of material future risks and how the company is addressing any significant potential vulnerability.

Of course, running a company is an exercise in managing risk in exchange for potential returns, and there can be danger in excessive risk aversion, just as there is danger in excessive risk-taking. But the assessment of risk, the accurate calculation of risk versus reward, and the prudent mitigation of risk should be incorporated into all business decision-making. ■

** S. K. Sachdeva and CS Bhagyashree Bardia are team members of Board Research & Advisory Division at IOD.*