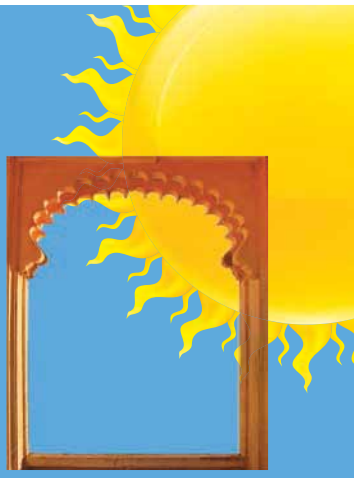
NSE

Quarterly Briefing

NSE Centre for Excellence in Corporate Governance

July 2016 | No. 14



# Risk Management and the Board of Directors in Indian Firms

Chief Contributor: Afra Afsharipour [1]

## Executive Summary


- Enterprise Risk Management ("ERM") is a systematic and holistic approach for firms to address all their risks, whether operational, strategic or financial.
- Although not involved in the everyday management of risk, the board of directors plays an important oversight role in ERM by guiding and reviewing the company's risk policy and ensuring that an effective risk management system is in place.
- Like elsewhere in the world, India's regulatory structure provides that the board must play a central role in risk management.
- Corporate India has become much more engaged with ERM, although there is room for improvement.
- Enhancing the board's risk management role can help address the many complex areas of risk faced by Indian firms.


[1] Professor of Law, UC Davis School of Law

## 1. Introduction

Risk management, also known as Enterprise Risk Management ("ERM"), is a systematic and holistic approach for firms to address all their risks, whether operational, strategic or financial, comprehensively. ERM focuses on identifying risks, developing and monitoring a risk management system and reacting to risk events, when they occur. As ERM is a firm-wide effort to manage all the firm's risks, involvement by the company's board of directors and senior management is imperative. In India, both the Companies Act, 2013 and the Listing Guidelines view risk management practices as one of the fundamental functions of the board of directors.

## 2. Evolution of an ERM framework globally

Beginning in the mid-1980s, the Committee of Sponsoring Organizations of the Treadway Commission (COSO), initially formed in part to study fraudulent financial reporting, began to articulate a risk management framework. [3] In 2004, following several corporate governance scandals around the world, COSO issued a detailed report defining ERM as "… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." [4] The COSO approach presents eight interrelated components of ERM:

- internal environment (the tone of the organization),
- setting objectives,
- event identification,
- risk assessment,
- risk response,
- control activities,
- information and communications, and
- monitoring.

## 3. The importance of effective risk management

The significance of ERM can be seen in the value it creates when effectively implemented and the value it destroys when there are shortcomings in leadership and implementation.

*Value creation.* ERM is a critical component of value creation. To create value successfully, ERM must play a central role in every substantive business decision. Effective ERM can enable a company to manage potential future events that create uncertainty, and respond to uncertainty in a manner that reduces the likelihood of downside surprises. ERM can also help a company improve the quality of risk taking and thereby, give the company a competitive advantage.

*Avoiding value destruction.* A company cannot preserve its value if its ERM is below standard. This role of preserving corporate value is far more visible when ERM fails than when it succeeds. Failures in risk management have contributed to some of the most significant scandals and losses suffered by companies. Recent significant failures include environmental disasters (e.g. BP), financial fraud (e.g. Enron, WorldCom, Satyam), foreign bribery (e.g. Siemens) and massive trading losses (e.g. JP Morgan). According to the OECD, these risk management failures were often "facilitated by corporate governance failures, where boards did not fully appreciate the risks that the companies were taking (if they were not engaging in reckless risk-taking themselves), and/or deficient risk management systems." [5]

[3]COSO is a joint initiative of five private sector organizations that provides thought leadership through the development of frameworks and guidance on critical aspects of organizational governance, including enterprise risk management.

[4]Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2004), Integrated Framework, www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf.

[5]OECD, Risk Management and Corporate Governance (2014), http://www.oecd.org/daf/ca/risk-management-corporate-governance.pdf

***Case Study: BP's deep water oil spill***

On April 20, 2010, an explosion at BP's offshore oil drilling rig caused by a blowout resulted in the death of 11 people and ignited a fireball that continued for 36 hours until the rig sank. This left the well gushing at the seabed for 87 days, resulting in the largest oil spill in U.S. waters and devastating the economy and coastline in the Gulf of Mexico Region.

BP itself suffered considerably as a result of the spill; criminal and civil settlements to date have cost the company tens of billions of dollars. The accident was not a first for BP which only 5 years previously had sustained a deadly explosion at a Texas refinery. Several investigative reports generated after the 2005 explosion identified significant risk issues including lack of uniform safety culture, lack of effective early warning systems, lack of effective education and training, and inadequate senior management oversight. By the time the deep water horizon spill occurred 5 years later, BP's board and senior management had still not created systems for addressing many of these issues, according to BP's own accident report in 2010. The failure of the BP Board to implement an effective ERM system, even 5 years after its ERM weaknesses were exposed by the 2005 explosion, demonstrates the Board's shortcomings. BP's ERM failure proved to be disastrous not only for BP, but also for the environment.

## 4. Corporate governance and risk management: the role of the Board

Corporate governance and effective ERM go hand in hand. While directors are not involved in the everyday management of risk, the board plays an important oversight role in ERM by guiding and reviewing the company's risk policy and ensuring that an effective risk management system is in place. The enhanced communication between board and business units that underlies ERM can facilitate and strengthen the board's role in both decision-making and monitoring. Particularly since the onset of the global financial crisis in 2008, ERM has come to the forefront of board discussions. Recognizing that risk management failures can severely impact the board's reputation, shareholder advisory groups in some jurisdictions, such as the US, include risk oversight as a criteria for voting recommendations regarding board members. Further, board members may also be subject to liability for failure to monitor risks. US courts have found that directors can be liable where there is "sustained or systemic failure of the board to exercise oversight such as an utter failure to attempt to assure [that] a reasonable information and reporting system exists."

## 5. Overview of India's regulatory framework for risk management

Similar to international standards, India's regulatory framework recognizes the board's central role in ERM. Experts in India have addressed this role since the early 2000s. For example, the 2003 report of the Narayana Murthy Committee included an extensive discussion of risk management, stating that "it is important for corporate Boards to be fully aware of the risks facing the business" and that shareholders must "know about the process by which companies manage their business risks". [6] More recently, the regulatory structure has also attended to the board's role in risk management.

*The Companies Act, 2013.* The Companies Act, 2013 acknowledges the need for risk management and requires that the board develop and implement a risk management policy, and identify risks which may threaten the company's existence. The Act does not specifically require a separate risk management committee nor does it include guidance to boards about how to develop effective risk management systems.

The Act includes several references to risk management, including:

- Under Section 134(3)(n): The board's report must include a statement indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the board may threaten the existence of the company.
- Under Section 177(4)(vii): As part of its responsibilities, the audit committee must evaluate internal financial controls and risk management systems.

[6]N.R. Narayana Murthy et al., Report of the SEBI Committee on Corporate Governance, Securities and Exchange Board of India, 2003, available at http://www.sebi.gov.in/commreport/corpgov.pdf.

- Schedule IV to the Act (Code for Independent Directors): Independent directors must "[bring] independent judgment to bear on the Board's deliberations especially on issues of strategy, performance, risk management"…and must "satisfy themselves…that financial controls and the systems of risk management are robust and defensible."

*SEBI's Listing Regulations (2015).* Under the Listing Regulations, one of the board's key functions is to review and guide the company's risk policy and ensure that appropriate risk management systems are in place. The company must have procedures to inform the board about the assessment and mitigation of risk, so that the board can fulfill its responsibility for framing, implementing and monitoring the company's risk management plan.

The listing regulations also require that the top 100 listed companies, determined by market capitalization as of the end of the immediate previous financial year, must have a board-level Risk Management Committee. The board must define the roles and responsibilities of the Committee and may delegate to it monitoring and reviewing of the risk management plan. The Committee's chair and a majority of its members must be board members, although senior executives of the company may also serve as members of the Committee.

## 6. Challenges facing Boards of Directors in developing ERM

Over the past several years, corporate India has become much more engaged with and sensitized to ERM. Leading companies have formed risk management and compliance teams that are integrated within the firm and that provide valuable information to the board. Nevertheless, there is room for improvement. For example, a December 2014 report by Grant Thornton found that only 24 of the top 100 Indian companies had at the time formed risk management committees on their boards.

Indian boards face significant challenges in designing and implementing an effective ERM system, including:

- *Effectively linking risk and strategy:* Integrating risk management into the overall corporate strategy is a challenge for many India firms. The challenge is to have an ERM system that encompasses a process capable of being applied in strategy setting across the enterprise. "Effective risk management is not about eliminating risk taking, which is a fundamental driving force in business and entrepreneurship." [7] In other words, taking appropriate risk needs to be at the heart of corporate strategy. For this to happen, the board must understand and guide the company's appetite and ability to take risk, and communicate the same to the company's risk management team. Operationally, what does 'tying risk with strategy' mean for management? It means that risk managers must be integrated in implementing the company's strategy and must not be separated from the board and management, so that the actual risk taken is tied to the company's risk appetite and ability. Moreover, the ERM programs must be developed with input from various functions in the organization, such as finance, sales, legal etc.

- *Implementing cost-effective risk management for small and medium-sized enterprises:* While the costs of risk management failures can be high, designing and implementing efficient ERM can also be quite costly, especially for small and medium-sized firms. For example, hiring consultants or the necessary staff to develop stress-testing and early warning systems to alert the board regarding significant risks can be difficult to do in smaller companies. In addition, while large firms can establish a 'chief risk officer' function with direct report to the board, doing so is much harder for smaller companies.

- *Addressing all major areas of risk:* ERM requires a firm to take a portfolio view of risk; boards must consider how various risks inter-relate, rather than treating each business and risk individually. This is a significant challenge for many boards.

- *Mitigating new risks.* In India, many complex areas of risks have emerged in the last decade or so, which has made risk management particularly challenging. For example, some traditional areas of risk, such as political instability and strikes and unrest, appear to have subsided while others, such as information and cyber security as well as terrorism and insurgency, have increased in prominence. Companies in a wide variety of industries have experienced the theft of data and sensitive information. For companies in major

[7]OECD, Risk Management and Corporate Governance (2014), http://www.oecd.org/daf/ca/risk-management-corporate-governance.pdf

cities, the threat of terror attacks has become a growing cause for concern, which can be hard to manage by the company itself. According to a 2015 survey, the top five risks for Indian firms include:

- corruption, bribery and corporate fraud;
- information and cyber security;
- terrorism and insurgency;
- business espionage; and
- Crime;

## 7. Enhancing the Board's risk management role

There are important steps that boards need to take to enhance the risk management system of a firm and the board's own role in risk oversight. A COSO 2009 enterprise risk management release recommends that board members must:

- Understand the company's risk philosophy and concur with its risk appetite
- Review the company's risk portfolio against that appetite
- Know the extent to which management has established effective enterprise risk management
- Be apprised of the most significant risks and whether management is responding appropriately.

To accomplish all these, certain review mechanisms are necessary on the part of the board, which have been detailed in COSO's 2010 progress report; the board must, *inter alia*, review:

- The company's procedures for (a) identifying when risks arise and (b) the actions to be taken if material risks arise;
- The quality and types of risk-related information provided to the board;
- Management's implementation of the company's risk policies and procedures and their communication across the firm;
- The company's risk management functions;
- Reports from internal and external experts, such as auditors, legal counsel and analysts, to ensure that appropriate risks are being considered;
- Whether the board members primarily tasked with risk oversight have the necessary experience, knowledge and expertise to oversee the company's risk management matters, and provide directors risk education as necessary;
- The qualifications and backgrounds of risk management personnel and policies applicable to the risk management personnel, to access wether they are appropriate given the companies size and scope of operations;

The above recommendations must of course be tailored for each company, and must balance the cost and value of each step.

## References

Philip Bromiley et. Al, Enterprise Risk Management: Review, Critique, and Research Directions, Long Range Planning, Volume 48, Issue 4, 2014.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004), Enterprise Risk Management-Integrated Framework, www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2009), Effective Enterprise Risk Oversight - The role of the Board of Directors, http://www.coso.org/documents/cosoboardserm4pager-finalreleaseversion82409_001.pdf

Department of Public Enterprises (DPE) (2010), Guidelines on Corporate Governance for Central Public Sector Enterprises, New Delhi, India, http://dpe.nic.in/sites/upload_files/dpe/files/gcgcpse10.pdf.

N.R. Narayana Murthy et al., Report of the SEBI Committee on Corporate Governance, Securities and Exchange Board of India, 2003, http://www.sebi.gov.in/commreport/corpgov.pdf.

OECD, Risk Management and Corporate Governance (2014), http://www.oecd.org/daf/ca/risk-management-corporate-governance.pdf

Pinkerton & FICCI, India Risk Survey (2015), http://www.pinkerton.com/pinkerton-and-ficci-publish-india-risk-survey-2015

Wachtell, Lipton, Rosen & Katz, Risk Management and the Board of Directors (July 2015), https://corpgov.law.harvard.edu/2015/07/28/risk-management-and-the-board-of-directors-3

## About NSE CECG

Recognizing the important role that stock exchanges play in enhancing corporate governance (CG) standards, NSE has continually endeavoured to organize new initiatives relating to CG. To encourage best standards of CG among the Indian corporates and to keep them abreast of the emerging and existing issues, NSE has set up a Centre for Excellence in Corporate Governance (NSE CECG), which is an independent expert advisory body comprising eminent domain experts, academics and practitioners. The 'Quarterly Briefing' which offers an analysis of emerging CG issues, is brought out by the NSE CECG as a tool for dissemination, particularly among the Directors of the listed companies.