Lecture Note 19

Chapter 7 : Risk Associated with Corporate Governance

Chapter Overview

- Evaluation of Risk Associated with Governance
- Description and evaluation of framework for Board level consideration of risk
- OECD Guidelines for Corporate Governance

EVALUATION OF RISK ASSOCIATED WITH GOVERNANCE

Governance risks mean significant deficiencies that can impact the reputation, existence and continuity of the organisation. These arise on account of failure of the Board to direct and control the organisation or inappropriate practices adopted by the Board or collusion of management to override significant internal control mechanism causing financial losses or inability of the Board to identify principal risk factors that can impact business continuity.

Governance Risks

- Absence of effective corporate governance framework and documented governance policies
- The rights of shareholders and key ownership functions are not defined and communicated
- There is no equitable treatment of shareholders
- The role of stakeholders in corporate governance is not defined, communicated and monitored
- Disclosure and transparency norms are not articulated
- The responsibilities of the Board of directors are not defined
- Board has not defined risk capacity, appetite and risk response strategies
- Risk not managed on an enterprise basis and not adjusted to corporate strategy.
- Risk managers separated from management and not regarded as an essential part of implementing the company's strategy.
- Risk management and control functions be independent of profit centres and the "Chief Risk Officer" (CRO) or equivalent should report directly to the board of directors along the lines
- Corporations developing their risk management and oversight practices face challenges
- Boards simply review and approve management's proposed strategies.
- Insignificant Board time spent on business risk management
- Boards have incomplete understanding of the risks faced by the company.
- Boards receive information that is short-term.
- The process of risk management and the results of risk assessments should be appropriately disclosed.
- Whistle blower matters
- Negative media reports
- Shareholder activism
- Unauthorised related party transactions
- Ownership /Shareholder disputes

Sound Risk Governance Practices recommended by the Financial Stability Board in 2013.

The list extracts some of the better practices exemplified by national authorities and firms.

The Board of Directors

- avoids conflicts of interest arising from the concentration of power at the board
- comprises members who collectively bring a balance of expertise
- comprises largely independent directors and there is a clear definition of independence that distinguishes between independent directors and non-executive directors
- sets out clear terms of references for itself and its sub-committees and establishes a regular and transparent communication mechanism to ensure continuous and robust dialogue and information sharing between the board and its sub-committees;
- conducts periodic reviews of performance of the board and its sub-committees
- sets the tone from the top, and seeks to effectively inculcate an appropriate risk culture throughout the firm
- responsible for overseeing management's effective implementation of a firm-wide risk management framework and policies within the firm
- approves the risk appetite framework and ensures it is directly linked to the business strategy, capital plan, financial plan and compensation
- has access to any information requested and receives information from its committees at least quarterly
- meets with national authorities, at least quarterly, either individually or as a group.

The risk committee

- is required to be a stand-alone committee, distinct from the audit committee;
- has a chair who is an independent director and avoids "dual-hatting" with the chair of the board, or any other committee;
- includes members who are independent;
- includes members who have experience with regard to risk management issues and practices;
- discusses all risk strategies on both an aggregated basis and by type of risk;
- is required to review and approve the firm's risk policies at least annually;
- oversees that management has in place processes to ensure the firm's adherence to the approved risk policies.

The audit committee

- is required to be a stand-alone committee, distinct from the risk committee;
- has a chair who is an independent director and avoids "dual-hatting" with the chair of the board, or any other committee;
- includes members who are independent;
- includes members who have experience with regard to audit practices and financial literacy at a financial institution;
- reviews the audits of internal controls over the risk governance framework established by management to confirm that they operate as intended;
- reviews the third party opinion of the design and effectiveness of the overall risk governance framework on an annual basis.

The CRO

- has the organisational stature, skill set, authority, and character needed to oversee and monitor the firm's risk management and related processes and to ensure that key management and board constituents are apprised of the firm's risk profile and relevant risk issues on a timely and regular basis
- meets periodically with the board and risk committee without executive directors or management present
- is appointed and dismissed with input or approval from the risk committee or the board and such

appointments and dismissals are disclosed publicly;

- is independent of business lines and has the appropriate stature in the firm as his/her performance, compensation and budget is reviewed and approved by the risk committee
- is responsible for ensuring that the risk management function is adequately resourced
- is actively involved in key decision-making processes from a risk perspective
- is involved in the setting of risk-related performance indicators for business units
- meets, at a minimum quarterly, with the firm's supervisor to discuss the scope and coverage of the work of the risk management function.

THE RISK MANAGEMENT FUNCTION

- It is independent of business and reports to the CRO
- It has authority to influence decisions that affect the firm's risk exposures
- It is responsible for establishing and periodically reviewing the enterprise risk governance framework which incorporates the Risk Appetite Framework (RAF), Risk Appetite Statement (RAS) and risk limits.
  - The RAF incorporates an RAS that is forward-looking as well as information on the types of risks that the firm is willing or not willing to undertake and under what circumstances.
  - The RAS is linked to the firm's strategic, capital, and financial plans and includes both qualitative and quantitative measures that can be aggregated and disaggregated such as measures of loss or negative events
  - Risk limits are linked to the firm's RAS and allocated by risk types, business units, business lines or product level.
- It has access to relevant affiliates, subsidiaries, and concise and complete risk information on a consolidated basis
- It provides risk information to the board and senior management that is accurate and reliable and periodically reviewed by a third party (internal audit) to ensure completeness and integrity
- It conducts stress tests (including reverse stress tests) periodically and by demand.

INDEPENDENT ASSESSMENT OF THE RISK GOVERNANCE FRAMEWORK

Determining when to review the RMF and the frequency for undertaking the review.	Deciding who is responsible for the review.	Selecting the scope and method for a review.	Manner of circulation of results.

ENTITY'S RISK ASSESSMENT PROCESS WITH RESPECT TO FINANCIAL REPORTING

Risks can arise or change due to the following circumstances:	
Changes in operating environment.	Changes in the regulatory or operating environment can result in changes in competitive pressures and significantly different risks.
New personnel	New personnel may have a different focus on or understanding of internal control.
New or revamped information systems.	Significant and rapid changes in information systems can change the risk relating to internal control.
Rapid growth.	Significant and rapid expansion of operations can strain controls and increase the risk of a breakdown in controls.
New technology	Incorporating new technologies into production processes or information

	systems may change the risk associated with internal control.
New business models, products, or activities.	Entering into business areas or transactions with which an entity has little experience may introduce new risks associated with internal control.
Corporate restructurings.	Restructurings may be accompanied by staff reductions and changes in supervision and segregation of duties that may change the risk associated with internal control.
Expanded foreign operations.	The expansion or acquisition of foreign operations carries new and often unique risks that may affect internal control, for example, additional or changed risks from foreign currency transactions.
New accounting pronouncements.	Adoption of new accounting principles or changing accounting principles may affect risks in preparing financial statements.

Role of Risk Assessment with respect to Financial Reporting

Risk assessment underlines the entire audit process described by the ICAI guidance note, including the determination of significant accounts and disclosures and relevant assertions, the selection of controls to test, and the determination of the evidence necessary for a given control.

Risk Based Internal Auditing (RBIA)

The definition of internal audit, as described in the Preface to the Standards on Internal Audit, issued by the Institute of Chartered Accountants of India, amply reflects the current thinking as to what is an internal audit: Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity's strategic risk management and internal control system.

The 21st century internal auditors have the following vital areas of responsibility in the field of risk management:

- Review operations, policies, and procedures.
- Help ensure that goals and objectives are met.
- Understanding the “big picture” and diverse operations.
- Make recommendations to improve economy and efficiency.

Audit Risk & Sampling

Audit risk includes both uncertainties due to sampling and uncertainties due to factors other than sampling. These aspects of audit risk are sampling risk and non-sampling risk, respectively. Sampling risk arises from the possibility that, when a test of controls or a substantive test is restricted to a sample, the auditor's conclusions may be different from the conclusions he would reach if the test were applied in the same way to all items in the account balance or class of transactions.

Non-sampling risk includes all the aspects of audit risk that are not due to sampling. An auditor may apply a procedure to all transactions or balances and still fail to detect a material misstatement.

RISK MANAGEMENT DISCLOSURES IN INDIA

Indian Scenario

Provisions of the Indian Companies Act, 2013

- The Annual Report of the Board of Directors must include a statement indicating the development and implementation of a risk management policy for the company.
- The audit committee is directed to act in accordance with the terms of reference specified in writing by the Board, which shall, inter alia, include evaluation of risk management systems.
- The code of conduct prescribes that the Independent Directors should satisfy themselves that

systems of risk management are robust and defensible.

Provisions of the SEBI LODR Regulations 2015

- **Under responsibility of Directors** - Ensuring the integrity of the listed entity's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.
- The board of directors shall ensure that, while rightly encouraging positive thinking
- The board of directors shall have ability to "step back" to assist executive management by challenging the assumptions underlying
- The listed entity shall lay down procedures to inform members of board of directors about risk assessment and minimization procedures.
- The board of directors shall be responsible for framing, implementing and monitoring the risk management plan for the listed entity.
- The board of directors shall constitute a Risk Management Committee.
- Under minimum information to be placed before the Board on a quarterly basis- Quarterly details of foreign exchange exposures and the steps taken by management to limit the risks of adverse exchange rate movement, if material.
- Under disclosures in Annual Reports applicable to all listed entities except banks

Management Discussion and Analysis

This section shall include discussion on the following matters

- Industry structure and developments.
- Opportunities and Threats.
- Segment–wise or product-wise performance.
- Outlook
- Risks and concerns.
- Internal control systems and their adequacy.
- Discussion on financial performance with respect to operational performance.
- Material developments in Human Resources / Industrial Relations front, including number of people employed.
- Details of significant changes
  - ✓ Debtors Turnover
  - ✓ Inventory Turnover
  - ✓ Interest Coverage Ratio
  - ✓ Current Ratio
  - ✓ Debt Equity Ratio
  - ✓ Operating Profit Margin (%)
  - ✓ Net Profit Margin (%) or sector-specific equivalent ratios, as applicable.
- Details of any change in Return on Net Worth as compared to the immediately previous financial year along with a detailed explanation thereof.

Risk Management Disclosures – Global Scenario

In US, the Companies listed with the Securities and Exchange Commission (SEC), have to describe the risks faced by the business (in some form or another) since the 1970s. In Europe, the EU Accounts Modernisation Directive of 2003 said that companies should describe the risks they face, in both annual and interim reports. Two countries have gone further than the Europe-wide requirements – Germany has its own risk reporting standard (GAS 5), while the UK's Corporate Governance Code says that companies should report at least annually on the effectiveness of their risk-management procedures. The UK's Corporate Governance Code still goes further where a more integrated approach to risk reporting, linking risk management to internal controls and going concern is included.

Enhancing Organizational Reporting: Integrated Reporting Key

There is emergence of Integrated Reporting Framework (IRF) on the global landscape. It is fast emerging as holistic framework of corporate reporting that goes beyond the traditional financial reporting frameworks. The key objective of the IRF is to align capital allocation and corporate behaviour to wider goals of financial stability and sustainable development through the cycle of integrated reporting and thinking.

Risk & Opportunity Reporting (ROR)

ROR is a key component in the IRF.

- Key risks impacting ability to create value in short term, medium term and long term
  - ✓ Internal sources – business related risks
  - ✓ External sources-from external environment
- Key opportunities like those related to process improvement, employee training and relationships management.
- Organisation assessment of likelihood that the risk or opportunity will fructify and probability or certainty of same.
- Steps taken to mitigate or manage key risks or create value from key opportunities including identification of associated strategic objectives, policies, targets and KPIs.

Risk Management Disclosures – A Global Case Study	•Annual report of Global major operating in the retail sector in 2016 •ICAI Study Mat Page No 7.13
Risk & Opportunity Disclosures – An Indian Example	•Annual report of a leading manufacturing company in India operating in the steel sector; •ICAI Study Mat Page No 7.14

DESCRIPTION AND EVALUATION OF FRAMEWORK FOR BOARD LEVEL CONSIDERATION OF RISK

Directors and boards need to ensure that policies, frameworks and governance arrangements are in place to ensue ethical conduct and decision making and effective risk governance and management. They must also make sure that their own conduct and the vision, mission, values, goals, objectives and priorities they set are conducive of them and do not undermine them.

Some of the issues that directors may have to consider and the questions they should ask

A degree of risk is inevitable in business operations. To obtain higher returns, innovate and secure market leadership one may need to adopt a higher risk strategy.

- Which stakeholder should be involved and how should they be engaged?
- Does the risk culture of the board match to that of the organization and its aspirations?
- If not, what changes are required and how might they be brought about?
- What are the risk oversight functions of the board and how effectively are they being discharged?
- Is annual reporting of risk to shareholders fair and balanced?
- Would confidence accounting present a clearer picture?
- Within the governance structure, what arrangements have been made for risk governance which

involves setting a strategy and policies for the management of risks and monitoring the performance of those to whom risk and security responsibilities are delegated?

- Policies could cover the transfer of risk, such as whether or not to hedge or insure against certain risks, depending upon the costs and practicalities involved.
  - How complex and comprehensive do these needs to be once the most likely and significant risks have been addressed?
- Assumptions and business models should be periodically challenged.
  - Should an interruption in certain supplies occur, might just in time approaches result in shortages?
  - What external and objective advice does the board receive in relation to risk?
  - Overall, from the board perspective, what more needs to be done to build a risk resilient enterprise?

Corporate Risk Management

- Are people within the organization and its supply chain aware of the diversity, incidence and severity of some categories of risk?
- A small account might have growth potential and could become strategically significant in the future.
- Directors need to make sure that a management team and executives are not so focused upon listing and addressing individual risks that they overlook the interrelationship of different risk factors.
- How well positioned is a company in respect of certain risks?
- Is the risk culture of the organization appropriate in relation to its activities, its operations and the opportunities it faces?
- Processes and systems need to be adaptive as well as resilient.
- Are risk registers and management reports relating to risk over generalized?
- How realistic are they in relation to assessments of risk and planned corporate responses?
- Do they provide sufficient evidence and explanation to inform the board's own reporting of risk to shareholders?

Risk Management Frameworks, Approaches and Techniques

Points to be considered by the Board :

- Has the management team established an effective risk prevention, management and control framework?
- Are people equipped with the skills, tools, techniques and other support they need to effectively operate it?
- Are the techniques used adequate in the situation and circumstances?
- How outward looking and inclusive does risk management need to be?
- Are the risks of major and strategic customers and business partners understood?
- Are business opportunities being identified for how the company might use its capabilities to help customers and others to mitigate, prevent or manage the risks they face?
- Does the company's risk management framework, policies and practices extend to its supply chain?
- In particular, are supplier risks and the risks of activities such as outsourcing and joint ventures assessed and managed?
- Does this involve collaborative action where relevant?
- Is the risk registering a living document?
- Are the prioritization of risks, mitigation measures, responsibilities and residual risks regularly reviewed?
- Are risk reports color coded to reflect likelihood of occurrence and impact?

- Is the direction of travel given?
- Are movements in relation to high priority "red rated" risks monitored by the board?
- Are there trigger points at which additional advice is sought and/or further resources deployed or other action taken?
- Are risk factors understood, appropriately categorized and mapped?
- Are the risk assessment criteria used reasonably and fair in the circumstances?
- Do the results of risk analysis inform business and management decisions?
- Are they inhibiting or supporting innovation and entrepreneurship?
- To whom should risk management responsibilities be delegated?
- Is there a Chief Risk Officer (CRO)?
- If so, how is the role of the CRO changing?
- What skills and experience are required by risk management professionals?
- What steps are taken to ensure that other people do not abdicate their responsibilities in relation to risk by leaving too much to the CRO and his or her team?
- Responsibilities for risk prevention, mitigation and management need to be delegated with care.
- What should be done to ensure that adopted approaches to risk management are current and that knowledge of changing risks and how they might best be addressed is up-to-date?
- Within the governance structure, how does the CRO relate to and collaborate with the audit, compliance, finance and legal teams?
- Are regular formal and/or informal meetings held to identify and discuss patterns, trends and common root causes?

For More Details : See ICAI Study Mat 7.18 to 7.20

Striking the Right Balance in Action and Reaction
An organization that is prepared is able to respond quickly and aptly when unwelcome risks materialize. Having a moral compass and reacting in a proportionate, fair and responsible way can help a company and its board to restore confidence, maintain trust and build relationships with stakeholders. This can be achieved by listening to peers and learning, thereby building resilience and a balanced perspective. It is important to both recover and move forward while responding to incidents.

OECD Guidelines (Principles) For Corporate Governance	
Ensuring the basis for an effective corporate governance framework	The corporate governance framework should be developed keeping in mind the macroeconomic changes, market situation and legislation requirements.
The rights and equitable treatment of shareholders and key ownership functions	Under the Companies Act, shareholders are classified under different categories like equity shareholders, preference shareholders etc. Shareholders can influence an organization's core functioning as they have right to participate and vote in general shareholders meeting, elect the board member, make amendments to company's organic documents, approval of extraordinary transactions, etc.
Institutional investors, stock markets, and other intermediaries	The corporate governance framework should provide sound incentives throughout the investment chain and provide for stock markets to function in a way that contributes to good corporate governance.
The role of stakeholders in corporate governance	The corporate governance framework should recognize the rights of stakeholders established by law or through mutual agreements and encourage active co-operation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises.

Disclosures and Transparency	• The financial and operating results of the company. • Company objectives and non-financial information. • Major share ownership, including beneficial owners, and voting rights. • Remuneration of members of the board and key executives, Information about board members, including their qualifications, the selection process, other company directorships and whether they are regarded as independent by the board. • Related party transactions. • Foreseeable risk factors. • Issues regarding employees and other stakeholders. • Governance structures and policies, including the content of any corporate governance code or policy and the process by which it is implemented.
The responsibilities of the board	• The Board members should act in good faith, diligently and in the best interest of the company and the shareholders. • The Board should also adopt high ethical standards. • The Board should also review and guide corporate strategy, action plans, management policies and procedures etc. • The Board should also monitor the company's governing practices and make required changes as and when required. • Monitoring and executing the selection, remuneration and replacement of key executives. • Ensuring a formal and transparent board nomination and election process. • Monitor and manage conflicts of interest of management, misuse of corporate assets and abuse in related party transactions. • Ensure the integrity of the company's accounting and financial reporting systems and make sure that appropriate systems are in place for risk management, financial and operating control. • The Board should oversee the process of disclosure and communications.