Invited Article

Enterprise Risk Management - Corporate India's Strategic Approach to Build a Sustainable and Resilient Organization

*Delzad Dinyar Jivaasha**

I. Broad Concept and Overview of Corporate Enterprise Risk Management

Enterprise Risk Management (ERM) is an integrated approach to look at entity level risks in a holistic way and evaluate the same at an organizational level. **The broad strategic approach is to identify and assess core perceived risks and put in place robust strategies &mitigation plans to counter the core perceived risks faced by an organization.**

The core fundamental of ERM is to add value to all stakeholder functions in the company through identifying existing and potential risks and ensuring that the identified risks are controlled - thereby resulting in successful attainment of defined business objectives and strategic plans.

One critical aspect needs to be appreciated at all points in time - ERM is neither a compliance nor an audit activity - it is a business partner in the growth story of an organization and focuses on ensuring that the business navigates smoothly even during challenging times.

Influencing cross functional stakeholders across layers of hierarchy is critical to ensure that Corporate ERM succeeds in a dynamic environment.

In the world of Volatility, Uncertainty, Complexity and Ambiguity (VUCA), the organization balance sheet can be protected and the entity can maintain its leadership position built through perseverance, innovation and commitment - only through ENTERPRISE RISK MANAGEMENT.

Most organizations at some point in time are likely to face certain crisis scenarios and the objective is to ensure that the organization tides over and manages the crisis effectively through effective Corporate ERM and Business Continuity Planning.

Integrating ERM into the organizational strategy, performance and day-to-day workflow is of utmost importance for the long term viability and sustainability of an organization.

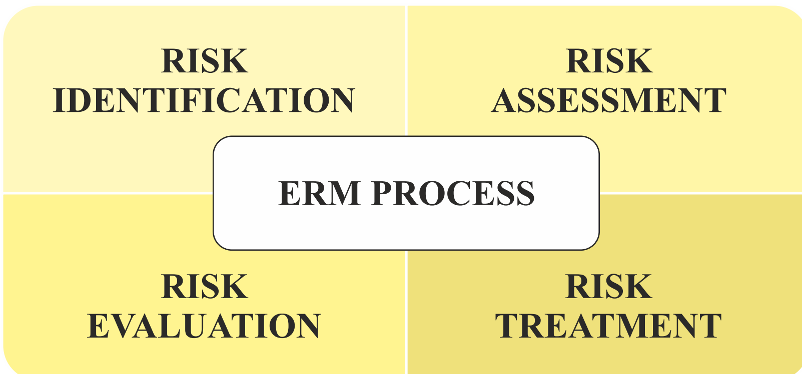
* *B.Com., ACA, ACS, ACMA, LL.B., DISA (ICAI), FIII*
Associate Vice President - Risk Management & Finance, ICICI Lombard General Insurance Company Limited
E-mail: delzad.jivaasha@icicilombard.com

If there is one function which can be regarded as **The Eyes, Ears and Heart of Business - It Is The Corporate ERM Function as It is A Great Asset in Protecting The Balance Sheet and Bottom Line of the Organization.**

Successful Corporate Governance is difficult to achieve in the absence of effective Enterprise Risk Management.

II. The Enterprise Risk Management Process

The Enterprise Risk Management process is built on four pillars:-



The four pillars are as contained below:-

i. Risk Identification

Risk identification is the first and one of the most pivotal legs of the Corporate ERM process.

It is aimed at identifying existing and prospective risks for an organization.

Broad strategies for risk identification would include:-

- Risk identification workshops,
- Brain storming sessions with various functions,
- Studying economy as well as industry related reports,
- Utilizing past risk, audit and incident reports and a slew of other measures.

ii. Risk Assessment

Risk assessment is based on the following parameters:-

a) Frequency

Frequency refers to the likelihood or the probability that the organization would be exposed to the risk event or incident.

This involves asking one basic question:- **How often can the concerned risk event/ incident hit the entity?**

b) Severity

Severity refers to the impact an organization would face or suffer if the risk event was to actually occur.

This again involves asking one basic fundamental question:- **If the risk event materializes, how would it impact the company as a whole?**

Whilst the acceptance of velocity as a concept for risk assessment is increasingly gaining prominence, majority of the organizations continue to assess risks on the basis of the abovementioned two parameters.

iii. Risk Evaluation

All risks which have been assessed, are never going to be at one level.

Based on the assessed levels of frequency and severity, the risk evaluation would have to be undertaken by categorizing the assessed risks into various pre-defined grades/levels of risk as decided by each organization e.g. Severe/Very High Risks, High Risks, Medium Risks, Low Risks, etc.

Risk Gradation is one of the biggest factors affecting prioritization of risks and thereby determining the order of risk treatment.

iv. Risk Treatment

Risk Treatment approaches are focused on devising suitable plans to mitigate the evaluated risk and bring them down to acceptable levels for an organization.

Risk Treatment can broadly be achieved through:-

- Risk Acceptance
- Risk Avoidance
- Risk Treatment/Mitigation and
- Risk Transfer

III. The Organizational ERM Governance Structure

The placement of the ERM function in the overall organizational structure plays a crucial part in determining the success of Enterprise Risk Management:-

i. Risk Management Committee

From a corporate governance perspective, an organization should have a Board Level Risk Management Committee, comprising of atleast a two-third majority of independent non-executive directors, with the Chairman of the Risk Committee also being a non-executive independent director.

The Risk Management Committee would be a Committee reporting to the Board and would be responsible for reviewing and approving the Enterprise Wide Risk Management frameworks, Risk Management policies and other critical risk management decisions impacting the organization.

Every critical decision with respect to the entity level risk management strategy adopted by an organization would have to be reviewed and approved by The Risk Management Committee, prior to being approved by the Board of Directors.

ii. Chief Risk Officer

At a Company level, the ERM function should be headed by a Chief Risk Officer (CRO), who would also be a MANCOM (Management Committee) member.

From a hierarchy perspective, the CRO should either report into the CEO or directly into the Risk Management Committee of the Company.

Broad Responsibilities and Duties of the Chief Risk Officer would include:-

- Identification of top risks affecting an organization
- Ensuring integration of Enterprise Risk Management with organizational performance and strategy
- Cultivating a risk based decision making culture in the entity
- Keeping a close watch on timely implementation of defined risk mitigation plans

- Ensuring that the organization is resilient to risks and most importantly is stable during times of adversity

iii. Corporate Enterprise Risk Management (ERM) Team

The CRO would be assisted in his day-to-day duties by the ERM team. The Corporate ERM team should be made up of individuals having the required educational background, work experience and exposure to the identification and overall management of risks.

The Corporate ERM function is expected to proactively interact and engage with all stakeholder functions, from the perspective of building up a robust risk management culture where in proactive management of existing and potential future risks is undertaken continually as a part of day-to-day work flow management in the organization.

The Corporate ERM Function would be expected to conduct company wide risk management training sessions and create strong awareness on key risk management issues confronting every function and the organization.

The Corporate ERM function would be expected to take the lead in terms of working closely with all functional teams for identification, assessment, evaluation and treatment of risks and thereby build a resilient organization through robust risk management practices.

IV. The Three Lines of Defence Model for Effective Corporate Governance

The Three Lines of Defence Model is a structure to ensure effective corporate governance and protect the organization against internal and external risks which can adversely impact its strategies, growth, achievement of objectives and overall performance.

As the name would logically suggest, there are three identified functions which protect and defend the Company against risks.

a. First Line of Defence:- The Business/Functional Unit

Every unit which does a particular job 24*7 is in the best position to understand its risks including effectively structure their control mechanism towards mitigating risk.

Therefore, every function/unit in an organization, should focus on building up strong risk management practices and integrate their decision making process with the overall enterprise risk management framework in the organization.

The above referred approach is a pivotal step in the direction of building a strong risk management culture in an organization.

b. Second Line of Defence:- The Enterprise Risk Management Function

The second line of defence is the ERM function which would focus on reducing material risks confronting an entity, along with devising and monitoring the formulation and timely implementation of the enterprise wide risk mitigation plans.

The ERM function would be expected to work closely with business units and proactively assist them in mitigation of their risks, including continually educating them on critical risk management aspects.

The ERM function has to be a business partner with a robust and defined plan to protect the entity against risk adversities which could impact the achievement of the laid down objectives.

c. Third Line of Defence:- The Internal Audit Function

The third line of defence is the Internal Audit Function which would independently assess the risks and controls of every function in the Company in accordance with the Risk Based Internal Audit Plan, approved by the Audit Committee of the organization. The Internal Audit Function would have an accountability to the Audit Committee of the organization.

V. Broad Risk Categorization

From an Enterprise Risk Management perspective, the different types of risk can be classified into four broad categories:-

- Operational Risk
- Market Risk
- Strategic Risk
- Credit Risk

a) Operational Risk

Operational Risk, as commonly defined and understood, is basically the risk of loss on account of inadequate or failed people, process, system and/or event.

Operational Risk, can result in several leakages and losses for an organization, and hence must be controlled through robust internal control mechanisms.

It is imperative for Organizations to have an Operational Risk Management Committee (ORMC) comprising of The Heads of Functions to ensure that Operational Risk Management issues are extensively discussed and deliberated, along with decisions being taken for Company wide implementation on pertinent aspects related to Operational Risk.

Key Elements of Operational Risk Management

Operational risk requires the following elements to succeed:-

1. A Board Approved Operational Risk Management Policy
2. Operational Risk Management Standard Operating Procedures
3. A robust Risk and Control Self-Assessment (R & CSA) Framework
4. Lead and lag Key Risk Indicators (KRI's) to proactively track the movement of key factors which drive the movement of operational risk
5. Stress Testing the key operational risks in a Company
6. Culture building and awareness creation in the space of Operational Risk Management

Business Functions should have an Operational Risk Manager (ORM) within their team, for effective accountability and related management of the operational risks.

The ORM's would report into their respective Functional Heads, however would also work closely with the ERM function in mitigating organization wide operational risks.

b) Market Risk

Market Risk is the risk faced by an organization on account of market movements and fluctuations.

An organization is exposed to the liquidity risks, the risk of the drop in the prices of equity shares, foreign exchange fluctuations, risk of interest rate movements including reinvestment risk, Asset Liability Management (ALM) related Risks and similar other risks, arising as a result of the continual interplay of various market forces.

Key Elements of Market Risk Management

Organizations look to manage their Market risks through the following broad methodologies:-

- Board Approved Market Risk Management Policy
- Dedicated teams to continually monitor debt and equity market movements,
- Continual stress testing of the investments portfolio,
- Strong procedures for investments related risk management,
- Controlling concentration/exposure in specific asset classes including building capping limits for investments,
- Hedging Strategies,
- Well-defined Stop Loss Limits,
- Effectively monitoring Value at Risk (VAR) and other similar measures.

c) Strategic Risk

Strategic Risk refer to material risks which can impact the laid down strategic plans of an organization.

Key Elements of Strategic Risk

Broad categories of strategic risks could be:-

- Risks which would affect the market share of the Company,
- Risks pertaining to non-attainment of targeted bottom line,
- Organizational downgrade by rating agencies,
- Regulatory fines, penalties and warnings;

and similar risks which have a core linking to organizational strategy.

Management of strategic risks is very crucial and requires the close involvement of stakeholders including the MANCOM of an organization.

d) Credit Risk

Credit Risk refers to the risk of a counter-party not honouring their obligations and defaulting in making timely payments to the organization.

The same can in turn affect the potential of a company to fulfill their obligations on a timely basis.

Key Elements of Credit Risk Management

Credit Risks would include therein:-

- Risks related to the solvency position of a company,
- Downgrade in the rating of counter-parties a company deals with,
- Concentration risk with specific counter-parties, etc.

Management of credit risks can be achieved majorly through:-

- Deciding upon the maximum quantum of concentration limits with counter-parties,
- Monitoring downgrades in the ratings of counter-parties,
- Appropriate investment diversification strategies to avoid excessive exposure to any one counter party;

and similar mechanisms.

VI. Key Risk Management Terminologies

a) Risk Appetite

Risk Appetite refers to the level of risk an entity is willing to accept in pursuit of their organizational objectives.

CRO's always prioritize one aspect in ERM - having in place a clearly well-articulated Board approved risk appetite statement, to ensure that everybody in the organization understands the nature of decisions to be made.

Risk appetite plays a key role in channelizing the organizational resources in the right direction as the leaders of the organization have a clear road map in terms of understanding what is acceptable and what should be rejected/avoided.

Risk Appetite is Fundamental to the risk management process because whenever a new business opportunity is available, accepting or rejecting the same, is decided keeping in perspective the overall Risk Appetite of the organization.

b) Risk Tolerance

Risk Tolerance refers to maximum downside an organization can withstand, on account of a risk materializing.

Risk Tolerance is a crucial risk management concept and tolerance levels should be crystallized for key risk areas in an organization, for benchmarking and controlling the level of risk for every crucial risk category and sub-category.

Risk Tolerances are often expressed in terms of high, medium and low risk categories, with the traffic light status of red, amber and green being used to denote the high, medium and low risk categories respectively.

c) Risk Universe

Risk Universe is the complete universe of risks an organization is exposed to, broadly covering therein the risks associated with the industry the organization is operating in, the internal organizational risks and controls and the external ecosystem risks.

VII. Common Pitfalls to Avoid

It is essential to avoid the following pitfalls for effective enterprise wide risk management in an organization:-

a) As mentioned earlier - ERM is not be perceived as another Compliance or Audit Function. **A major perception error would be to treat it as a tick-the-box activity.**

   The fundamental aspect to note here is that it is never: - Business Unit/Function v/s Risk Management. Business Functions/Units and the Risk Management function will always be in the same team, focused on protecting the organization against a common foe, which is – Any risk which can affect the growth, profitability and sustainability of the Company.

b) ERM cannot be classified as the exclusive responsibility of the company Risk Management function. **All employees should perceive themselves to be risk managers for the company.** Successful Corporate ERM requires continual engagement and alignment of senior management, middle and lower management.

c) ERM can only be achieved when we make a conscious decision to move out of silos. Therefore, it is crucial to ensure that a **holistic view on risks** is undertaken at all times, with a conscious focus on risk assessment from an organizational perspective.

d) ERM basically stands for **being proactive in managing risks.** Hence it is important to continually keep reviewing existing ERM practices, evolve continually through examining the changes in business conditions, the economic environment, processes, systems and procedures to ensure that all risks are identified and treated before they affect an entity in a major way.

ERM is a 24 x 7 activity.

VIII. Conclusion

An organization which adopts and implements ERM in its true form and spirit, is certain to be in a strong position to withstand adversities and would evolve into a global market leader over a time horizon.

ERM is imperative in today's volatile environment and organizations that have **ERM as their foundation stone will continue to demonstrate healthy growth along with strong protection of their balance sheet and company bottom line.**

Risk Management = Long Term Organizational Sustainability and Viability

References

- Enterprise Risk Management – A Strategy to Build a Resilient Organization & be a Business Partner – By Delzad D. Jivaasha – Legal Era Magazine - October 2017 issue
- Enterprise Risk Management – A New Paradigm to Protect Corporate India & Ensure Sustainable Growth - By Delzad D. Jivaasha – Insurance Institute of India Journal – July to September 2019 issue

♦♦♦