COSO Enterprise Risk Management (ERM) Framework and a Study of ERM in Indian Context

Over past two decades we have seen companies implementing Enterprise Risk Management (ERM). The implementation was more of a compliance requirement due to various legislations across countries. As the organizations and the risk management practices mature, a need was felt to integrate the business strategy and business objective with the ERM practice. Taking this lead, ERM frameworks are being updated to suit the business requirement. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM Framework, one of the most widely recognized and applied risk management frameworks in the world, has also taken an initiative and updated its framework in June 2017. This article will sequentially flow with review of history of COSO ERM framework, need for the change of framework, key changes in the new framework, a brief discussion on five inter-related components and principles of the new COSO framework. Further, in this article we will understand the Statutory need for Risk Management in Indian Companies and understand how ERM will have a competitive advantage over Risk Management. In the last section we will look into the initiation taken by the ICAI, to equip its members in the area of Risk Management.

CA. Chethan Jayantha

(The author is a member of the Institute. He can be reached at chethan2525@gmail.com)

History

Committee of Sponsoring Organizations of the Treadway Commission (COSO) was organized in 1985 and is funded by five main professional accounting associations and institutes headquartered in the United States namely the American Institute of Certified Public Accountants (AICPA), American Accounting Association

(AAA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) and the Institute of Management Accountants (IMA). COSO's goal is to provide thought leadership dealing with three interrelated subjects: ERM, Internal Control, and Fraud Deterrence.

During the year 2004, COSO recognized that many organizations during that period were engaging in some aspects of ERM, there has been no common base of knowledge and principles to enable boards and senior management to evaluate an organization's approach to risk management and assist them in building effective programs to identify, measure, priorities and respond to risks. This was the time when COSO came up with the first framework named "Enterprise Risk Management – Integrated Framework".

The framework of ERM model was illustrated in the form of a cube. (Image 1 : ©2017 Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission) The intention of this cube model is to illustration the link between the objectives and the components and to portray that model has the ability to focus on entire organization.

Although this framework attracted much criticism, because of its simplicity and ease of implementation, it has become one of the most widely recognized and applied risk management frameworks in the world.

Need for Change

Over past dozen years since the introduction of the original framework, significant changes have undergone the way businesses operate. Operating environment for business has grow-n more complex, technologically driven, and global. Hence there was a need to relook at the framework and tweak it to the current business environment and with an eye on the future needs. Following are the key drivers for the update of ERM Framework.

1. Ever-changing complexity of doing business.
2. Need for integrating Strategy and Risk management practice.
3. Greater need for transparency in business.
4. New risks continue to emerge at a faster pace than has been seen in the past.
5. Unpredictable global economic landscape.
6. Technology evolution and associated risks.

What's new?

The new ERM framework named as "Enterprise Risk Management Framework: Integrating with Strategy and Performance" has introduced various changes in the existing Framework. Here are some of the key changes to the Framework.

1. Definition of ERM

New framework defines ERM as

"The culture, capabilities, and practices, integrated with strategy-setting and its execution, that organizations rely on to manage risk in creating, preserving, and realizing value."

The new definition of ERM emphasizes its focus on managing risk through:

- Recognizing culture and capabilities.
- Applying practices.
- Integrating with strategy-setting and its execution.
- Managing risk to strategy and business objectives.
- Linking to creating, preserving, and realizing value.

2. **Introduces a new structure**

   The frameworks has introduced new structure with an objective to cover the process from governance to day-to-day activities which has five components and twenty three principles aligned to the business cycle. This will be discussed in-depth in following paragraphs.

3. **Explores the different benefits of ERM**

   Unlike other framework, this framework presents clear case for integrating ERM practices with strategy-setting and performance management practices with practical examples and case studies.

4. **Focus on integrating strategy and risk management**

   The framework focus on integrating the strategy, internal control and risk management which facilitates all level of management from the top level involved in the strategy setting to the lower level management involved in the actual execution of the strategy through day today business operations.

5. **Detailed discussion on the challenging topic**

   Risk Appetite, Risk Profile, Acceptable Variation in Performance are the few areas which are untouched and the challenging topic which are not explored by other framework. This Framework examines such topics and addresses some misconceptions that exist today and provides a deeper insight.

6. **Establishing the need for Attracting, Developing and Retaining Talented Individuals**

   The Framework recognizes the importance of building the human capital and talent of individuals in alignment with business objectives. It stipulates that Management must define the knowledge, skills and experience needed to execute the strategy; set appropriate performance expectations; attract, develop and retain the appropriate personnel and strategic partners; and arrange for succession.

Components of New Framework

The new framework of ERM model with five components is illustrated in the below image. (Image 2 : ©2017 Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission)

Component 1: Risk Governance and Culture:

Risk governance and culture together form a strong foundation for the ERM and basis for all other components. *Risk governance* sets the entity's tone at the top which percolate down to all the level of the management, reinforcing the importance of ERM. *Culture* pertains to ethical values, desired behaviors, and understanding of risk in the entity.

Principles:

1. Exercises Board Risk Oversight

Risk oversight is possible only when the Board understands the entity's strategy and industry, and stays informed on issues affecting the entity. An entity's board of directors plays an important role in risk governance and significantly influences ERM. The board member should have the required Skills, Experience, and Business Knowledge. They need to be Independent, Accountable and Responsible towards the stake holders. Further, it is the board who can understand the complexity of the entity and determine how ERM will help the entity, including what benefits it will derive.

2. Establishes Governance and Operating Model

In an entity, the board delegates to management the authority to design and implement practices

that support the achievement of strategy and business objectives. In turn, management defines roles and responsibilities for the overall entity and its operating units. Management also defines roles, responsibilities, and accountabilities of individuals, teams, divisions, operating units, and functions aligned to strategy and business objectives. The organization establishes an operating model and designs reporting lines to execute the strategy and business objectives. Similarly ERM should be tailored to the capabilities of the entity, considering both what the organization is seeking to attain and the way it manages risk.

3. Defines Desired Organizational Behaviors

The culture drives the desired behaviors in day-to-day decision-making in order to meet the expectations of internal and external stakeholders. An entity's culture is reflected in its core values and approach to ERM.

Culture is evident in decisions made throughout the entity—decisions ranging from those made about developing and implementing strategy to those affecting day-to-day tasks.

4. Demonstrates Commitment to Integrity and Ethics

The tone of an organization is fundamental to ERM. Without a strong and supportive tone that is communicated from the top of the organization in support of an ethical culture risk awareness can be undermined, responses to risks may be inappropriate, information and communication channels may falter, and feedback from monitoring entity performance may not be heard or acted on. When management and the board of directors behave ethically and responsibly, and demonstrate a commitment to addressing misconduct, they communicate to everyone that the organization strongly supports integrity.

Standards of conduct guide the organization in its pursuit of strategy and business objectives by establishing acceptable and unacceptable conduct and providing guidance for navigating what lies between acceptable and unacceptable. Further, Deviations from standards of conduct must be addressed in a timely and consistent manner.

5. Enforces Accountability

The primary responsibility for ERM lies with the Board of Directors of the Company and this can be delegated to the Risk Management Committee. Board or the Internal Committee intern expects that the management defines roles and responsibilities, standards and guidance for the overall entity and its operating units thereby ensuring that each and every member is in the organization is responsible and accountable to the ERM.

6. Attracts, Develops, and Retains Talented Individuals

The human resources function helps promote competence by developing job descriptions and roles and responsibilities, facilitating training, and evaluating individual performance for managing risk. Management at different levels establishes the structure and process to Attract, Train, mentor, evaluate and retain talent.

Component 2: Risk, Strategy, and Objective-Setting:

Setting strategy and business objectives are the key activity of an Organization and the ERM has to be integrated at this level. This gives organization an insight into internal and external factors and their impact to risk. An organization sets its risk appetite in conjunction with strategy-setting. The business objectives allow strategy to be put into practice and shape the entity's day-to-day operations and priorities.

Principles:

7. Considers Risk and Business Context

An organization considers business context when developing strategy to support its Mission, Vision, and Core Values.

"Business context" refers to the trends, relationships, and other factors that influence, clarify, or drive change to an organization's current and future strategy and business objectives. Business context is not just internal environment (Capital, People, Process, Technology) but also include the external environment (political, economic, social, technological, legal, and environmental and external stake holders ((customers, suppliers, competitors, government, regulators etc.).

8. Defines Risk Appetite

Risk Appetite refers to the types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value. Risk appetite is communicated by management, endorsed by the board, and disseminated throughout the entity.

Risk appetite guides an organization in determining the types and amount of risk it is willing to accept. Management and the board of directors choose a risk appetite with full understanding of the trade-offs involved.

9. Evaluates Alternative Strategies

An organization must evaluate alternative strategies as part of its strategy-setting process and assess the risk and opportunities of each option. When evaluating alternative strategies, the organization seeks to identify and understand the potential risks of each strategy being considered. Further the same should be aligned with the Risk Appetite.

10. Considers Risk while Establishing Business Objectives

The organization develops business objectives that are measurable or observable, attainable, and relevant. Business objectives provide the link to practices within the entity to support the achievement of the strategy. Business objectives should also align with the entity's risk appetite. Further, the organization sets targets to monitor the performance of the entity and support the achievement of the business objectives.

11. Defines Acceptable Variation in Performance

Acceptable variation in performance, closely linked to risk appetite, is sometimes referred to as "Risk Tolerance." It describes the range of acceptable outcomes related to achieving a business objective within the risk appetite. It also provides an approach for measuring whether risks to the achievement of strategy and business objectives are acceptable or unacceptable. Operating within acceptable variation in performance provides management with greater confidence that the entity remains within its risk appetite and provides a higher degree of comfort that the entity will achieve its business objectives. Performance measures related to a business objective help confirm that actual performance is within an established acceptable variation in performance.

Component 3: Risk in Execution:

This component of the Framework focuses on ERM practices that support the organization in making decisions and achieving strategy and business objectives. This is similar to the traditional approach of the Risk management with only difference is that in ERM there is Risk Portfolio view. An organization identifies and assesses risks that may affect an entity's ability to achieve its strategy and business objectives. It prioritizes risks according to their severity and considering the entity's risk appetite. The organization then selects risk responses and monitors performance for change. In this way, it develops a portfolio view of the amount of risk the entity has assumed in the pursuit of its strategy and business objectives.

Principles:

12. Develops Portfolio View

The key differentiator of ERM as compared to the traditional risk management is the development of Portfolio view of the risk. A portfolio view allows management and the board to consider the type, severity, and interdependencies of risks, and how they may affect performance. This also facilitate the management in determining if the entity's residual risk profile aligns with the overall risk appetite.

13. Assesses Risk in Execution

Performance of the organization need to be reviewed to determine the impact of risk on the strategy and business objective as compared to the risk appetite of the entity. Further, necessary corrective action has to be initiated if the performance fall short of the acceptable variation.

14. Identifies Risk in Execution

The organization identifies new, emerging, and changing risks to the achievement of its strategy and business objectives. Risk identification should occur at all levels: entity, division, operating unit, function, and process. Depending on the size, geographic footprint, and complexity of an entity,

management may use more than one technique. These range from simple questionnaires to sophisticated facilitated workshops and meetings with approaches enabled by technology, such as on-line surveys, data tracking, and complex analytics.

15. Assesses Severity of Risk

The risks identified and included in an entity's risk universe are assessed in order to understand the severity of each risk to the achievement of an entity's strategy and business objectives. The risk universe forms the basis from which an organization is able to construct a risk profile. The severity of risk (i.e. *Impact*: Result or effect of a risk and *Likelihood*: The possibility of a risk occurring) is assessed at multiple levels of the entity as it will not be the same across divisions, functions, and operating units. Risk assessment approaches may be qualitative, quantitative, or both.

16. Prioritizes Risks

For informed decision-making and optimize the allocation of resources the Organizations has to prioritize risks. The risks can be prioritized based on the *Adaptability, Complexity, Velocity, Persistence, Recovery or other criteria.* Further, Risk prioritization occurs at all levels of an entity, and different risks may be assigned different priorities at different levels.

17. Identifies and Selects Risk Responses

Risk Response should be deployed for all identified risks. Risk responses are Accept, Avoid, Pursue, Reduce and Share.

While selection of risk response the Management have to consider the factors namely: *Business context, Costs and benefits, Obligations and expectations, Risk priority, Risk severity, Risk Appetite,* Regulatory Obligations, Expectations of Stakeholders.

Component 4 : Risk Information, Communication, and Reporting:

Management uses relevant and quality information from both internal and external sources to support ERM. The organization leverages information systems to capture, process, and manage data and information. By using information that applies to all components, the organization reports on risk, culture, and performance.

Principles:

18. Uses Relevant Information

To ascertain the achievement of strategy and business objective, the management has to obtain relevant information. The management evaluate source, availability and the cost associated with the required information. Further, the quality of the information has be ensured as the sound judgment, estimates or decision is depended on the said information.

19. Leverages Information Systems

Organizations can leverage information systems to help sustain ERM. Information systems range from a simple spreadsheets to a more complex and fully integrated systems. When selecting or developing supporting technologies organizations need to consider the following factors namely:

- *Scope,*
- *Aggregation,*
- *Information Quality,*
- *Consistency and Standards,*
- *Risk Assessment,*
- *Reporting,*
- *Integration,*
- *Cost benefits.*

20. Communicates Risk Information

Communicating the risk data and information to the internal and external stakeholders can done through various channels namely:

- *Electronic messages (e.g., emails, social media, text messages, instant messaging);*
- *External/third-party materials,*
- *Informal/verbal,*
- *Public events,*
- *Training and seminars,*
- *Written internal documents.*

In addition to the above mentioned formal channels of communication, there can be other

communication channels namely whistle-blower hotline, ombudsmen for communicating matters requiring heightened attention.

21. Reports on Risk, Culture, and Performance

The need of reports /information is different for different level of management. Each report user will require different levels of detail of risk and performance information in order to fulfill their responsibilities in the entity. Reporting supports personnel at all levels to understand the relationships between risk, culture, and performance and to improve decision-making in strategy- and objective-setting, governance, and day-to-day operations. Few key risk reports are:

- Portfolio view of risk,
- *Sensitivity analysis, Trend analysis,*
- *Disclosure of incidents, breaches, and losses,*
- *Tracking ERM plans and initiatives.*

The frequency of reporting should be commensurate with the severity and priority of the risk.

Component 5: Monitoring Enterprise Risk Management Performance:

Monitoring provides insight into how well the organization has implemented ERM within the entity and how well the components are functioning over time and in light of substantial changes.

Principles:

22. Monitoring Substantial Change

Change can be both in internal and external environment. The organization has to identify the changes in both the internal and external environment related to business context as well as the culture. Further organization has to access how the change can affect the ERM and the achievement of strategy and business objectives. This is a continuous activity. Additionally organization can conduct a "Post-Mortem" analysis after a risk event has occurred to review how well the organization responded and to consider what lessons learned could be applied to future events.

23. Monitors ERM

There is always a scope of improvement even for an entity which has most effective ERM. With continuous evaluation of the ERM system the organization can identify the potential improvement areas. Further the change in the external and internal environment will mandate the organization to revisit and improve the efficiency and usefulness of ERM. Further, Separate evaluation from an external/third person will give an in-depth insight for the potential improvement areas.

Need in India – Statutory and Operational

Globalization has paved way for more and more Indian companies to expanding their operations to the different geographical locations. The availability of skilled and low cost of labor has made foreign entities to setup their organization in India or outsource its operations to India. This has expos the Indian companies to potentially newer and greater risks arising from different economic, political, cultural, and other global uncertainties. Further, the investors and foreign buyers of outsourcing services are also exposed to various risks, which they need to be informed about. These developments have made adoption of ERM very critical for the success and growth of the companies in India. However, ERM practice and its implementation in Indian organization is still in infancy stage. Unlike other developed countries, in India there was no legislation promoting Risk management practice, until the introduction of Companies Act, 2013.

Companies Act, 2013 has introduced various provisions relating to easy of doing business while ensuring the governance and transparency are maintained in the way the business is conducted. One of the key compliance requirement introduced towards the governance and transparency is the introduction of Risk Management as a policy and process in the Companies.

Companies Act, 2013 has introduced various provisions relating to ease of doing business while ensuring the governance and transparency are maintained in the way the business is conducted. One of the key compliance requirement introduced towards the governance and transparency is the introduction of Risk Management as a policy and process in the Companies. Following are the two sections in the Companies Act, by which the board and audit committee have been vested with specific responsibilities in assessing the robustness of risk management policy, process and systems.

- Sec 134 (3) There shall be attached to *(Financial)* statements laid before a company in general meeting, a report by its Board of Directors, which shall include—

  (*n*) 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;

- Sec 177 (4) Every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which *shall, inter alia,* include,—

  (*vii*) evaluation of internal financial controls and risk management systems;

Hence as per Companies Act, 2013 it is mandatory for the Companies to development and implementation of a risk management policy and Audit Committee shall evaluate the risk management systems.

Now the question still remains is whether the Companies have to mandatorily implement ERM. Answer lies in understanding the difference between the between the Risk management and ERM. Following are the key differences between the Risk Management and ERM as highlighted in the book Managing Business Risk – An Integrated Approach, by A Anderson and the Economist Intelligence Unit.

Risk Management	Enterprise Risk Management
Retrospective	Analysis strategy
Ad hoc activity	Ongoing activity
Accounting, treasury and internal audit	All management activities
Fragmentation	Centralization and coordination
Financial risk	Business risk
Inspection, detection, reaction	Anticipation, prevention, monitoring, controlling
Focus on people	Focus on processes and people

This is self-explanatory, there is a lot of difference between the ERM and the risk management. Further, Companies Act, 2013 has reference only to the Risk Management and not the ERM.

Companies before investing this time and resources on the traditional Risk management process for statutory compliance needs to understand the benefits of the ERM which has a competitive advantages. Few of the key benefits of ERM are enumerated below.

- ERM is an extension of traditional risk management. Therefore implementation of ERM will be in compliance with the statutory requirement of Risk management.
- Traditional risk management approaches tend to be fragmented, treating risks as unique and disparate, whereas the ERM has a portfolio view which gives insight of the new risks.
- Risk management approaches limit the focus to managing loss prevention around physical and financial assets, rather than adding value.

Our prestigious institute had introduced "Post Qualification Course in Insurance and Risk Management" way back in 2003 which give the members an opportunity to get equipped with the necessary skill sets required in the area of Risk Management by offering a rich curriculum that sets the learning standards in Insurance and Risk Management.

Whereas ERM focus on the integrated risk management with the holistic approach on existing management processes, identifying future events that can have both positive and negative effects.

- ERM transforms risk management to a proactive, continuous, value-based, focused and process-driven activity Risk.
- An ERM approach is integrated into an organizations business decisions by involving people at all level of organization across functions.

In the new CA Final syllabus issued in 2017, the institute has incorporated an Elective Paper on "Risk Management", ensuring that the upcoming CAs are equipped with the expert knowledge on the said subject.

Hence it is advisable to implement ERM which has a holistic and integrated approach and have an operational advantage rather than just to satisfy the statutory requirement.

Initiatives taken by the ICAI

With regard to the implementation and practice of Risk Management, currently there are two big challenges. As on date there are approximately 5000 companies listed in BSE and 2000 companies listed in NSE and this list is increasing day by day. Hence on one side there are thousands of companies who have been made mandatory to implement Risk Management. On the other side Risk management is a highly specialized field that requires extensive knowledge, specific skills, proper training and solid experience. Further, there are no specific courses offered in the area of Risk Management in India. Hence the companies are relaying on the expertise of Chartered Accountants in the said area.

Taking this lead our prestigious institute had introduced "Post Qualification Course in Insurance and Risk Management" way back in 2003 which give the members an opportunity to get equipped with the necessary skill sets required in the area of Risk Management by offering a rich

curriculum that sets the learning standards in Insurance and Risk Management. Additionally, in the new CA Final syllabus issued in 2017, the institute has incorporated an Elective Paper on "Risk Management", ensuring that the upcoming CAs are equipped with the expert knowledge on the said subject.

Conclusion:

Considering that many Companies in India are implementing the Risk Management for the compliance of Companies Act, 2013, we are still a long way to go for being matured to integrating the business strategy with the ERM process. However, companies have to realize the competitive advantages in investing in the ERM rather than investing in the Traditional Risk Management just for the sake of statutory compliance.

There is tremendous scope for CAs, as there are vast varieties of Companies ranging from small size to mid-size and multinational companies who are looking forward for the help in implementing more sustainable, effective and efficient Risk Management practice, which the CAs can deliver with the continued support and training by the our prestigious ICAI institute.

Further, there is tremendous scope for CAs, as there are vast varieties of Companies ranging from small size to mid-size and multinational companies who are looking forward for the help in implementing more sustainable, effective and efficient Risk Management practice, which the CAs can deliver with the continued support and training by the our prestigious ICAI institute. ■