CHAPTER 8

ENTERPRISE RISK MANAGEMENT

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

- Definition
- Scope
- Techniques

1. DEFINITION AND SCOPE OF ENTERPRISE RISK MANAGEMENT

Fast-changing business scenario, uncertainty arising from global events, disruptive competition, and protectionist agenda of cultural majorities and volatility of commodity and currency prices creates stress and complexity in managing businesses. Gradually, these events start playing on the minds of stakeholders. The occurrence of risk events coupled with their poor handling impacts organisational performance. Enterprise Risk Management (ERM)/ Business Risk Management (BRM) is a structured form to assists organisations in preparing for the worst-case scenario, while aspiring to be "better, faster and cheaper". ERM is arguably the only effective tool in contemporary times that assists in the evaluation and bridging of the gap between uncertainty and performance in organisations; also a simplified approach to problem solving and making the organisation nimble footed. Iconic entities that feature in the top global rankings consistently practice integrated risk management.

Enterprise risk management (ERM) is a leading best practice approach to effectively manage and optimize business events that have the potential to impact business objectives or risks, enabling a company to determine how much uncertainty and risk are acceptable to an organization. Various definitions of risk management are enumerated as below :

Write in answer

Nov 2020
MTP CS - 2

CIMA Official Terminology, 2005

'A process of understanding and managing the risks that the entity is inevitably subject to in attempting to achieve its corporate objectives. For management purposes, risks are usually divided into categories such as operational, financial, legal compliance, information and personnel. One example of an integrated solution to risk management is enterprise risk management.'

Webster's New World Law Dictionary

The process of assessing risk and acting in such a manner, or prescribing policies and procedures, so as to avoid or minimize loss associated with such risk.

With a company-wide span, ERM serves as a strategic analysis tool, cutting across business units and departments, and considering end-to-end processes. In adopting an ERM approach, companies gain the ability to align their risk criteria to business strategy by identifying events that could have an adverse effect on their organizations and then developing an action plan to mitigate them. Nov 2020 MTP CS - 2 How is ERM"Classified"

By applying ERM in conjunction with other operational elements in the current business environment, companies can also accomplish many of their governance-related tasks.

Specifically, ERM can help organizations: May be called as "Benefits of ERM"

1. Identify strategic risk opportunities that, if undertaken, can facilitate achieving organizational goals.
2. Introduce a common language within the organization where people recognize problems and adopt a problem solving approach by developing risk treatment actions.
3. Provide senior management with the most up-to-date information regarding risk that may be used in the decision-making process.
4. Establish linkage between the ERM initiative and adherence to capital market reporting disclosures and other corporate laws and regulations.
5. Align annual performance goals with risk identification and management.
6. Encourage and reward upstream reporting of business-risk opportunities and challenges.
7. Align other risk monitoring initiatives such as self-appraisals, internal auditing activities, control assessments, continuous control monitoring, to organizational objectives.
8. Imagining key Risk Scenarios that could potentially result in a stress on the financial position of the company.
9. Financial Risk monitoring a part of the ERM initiative can balance the financial stability equation of the company

Among the more widely known frameworks and/or standard, and the related ERM definitions that they promulgate are:

- **ISO 31000 Risk Management Standard:** provides a set of principles, a framework and a process for managing risk.
- **COSO ERM Framework:** This framework defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management.

Enterprise risk management (ERM) is a plan-based business strategy that aims to identify, assess and prepare for any dangers, hazards and other potentials for disaster – both physical and figurative – that may interfere with an organization's operations and objectives. Relatively new (it's less than a decade old), the discipline not only calls for corporations to identify all the risks they face and to decide which risks to manage actively; it also involves making that plan of action available to all stakeholders, shareholders and potential investors, as part of their annual reports. Industries as varied as aviation, construction, public health, international development, energy, finance and insurance all utilize ERM. *(Source : Investopedia)*

Risk management in an organization minimizes the impact of risk on the business with the help of a chief risk officer or a risk committee but it does not give a guarantee that the organization will become risk free.

Nov 18 MCQ

2. IMPLEMENTING ERM

COSO framework states that Enterprise Risk Management (ERM) is defined as a process, affected by an entity's board of directors, management, and other personal, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. ERM includes the following activities:

- Determining the risk appetite.
- Establishing an appropriate internal environment, including a risk management policy and framework.
- Identifying potential threats to the achievement of its objectives and assessing the risk, i.e., the impact and likelihood of the threat occurring.
- Undertaking control and other response activities.
- Communicating information on risks in a consistent manner at all levels in the organization.
- Centrally monitoring and coordinating the risk management processes and the outcomes, and
- Providing assurance on the effectiveness with which risks are managed.

The term 'risk appetite' used in the above definition refers to the extent of risk that the Board is willing to take to pursue the objectives. Risk appetite setting is done at different levels, viz. for the organization at the entity level, process level, and different risk groups and for individual key risks. Risk appetite provides a standard against which a risk can be compared and where the risk is

above the risk appetite, it is considered a threat to the reasonable assurance that the objective will be achieved.

While risk appetite is to be set lower than the risk capacity; however, with an aggressive Board, the risk appetite can be higher than the risk capacity. For example, the Board may decide on utilizing the cash flow for operational purposes in the short term for earmarked funds meant for payment of quarterly installment of taxes. This could result in default of payment on due date and hence becomes a significant risk which needs to be covered by the internal auditor and reported upon even though the risk may be within the risk appetite. However, in the normal course, internal auditors are expected to take the risk appetite as a given and evaluating the risk appetite is out of audit scope. Internal auditors can, however, do a consulting activity of assisting the Board in fixing the risk appetite and its documentation.

ERM is a new approach in the ways organizations are assessing, managing and communicating business risks. By assisting organizations climb up on the risk maturity scale, ERM makes a major contribution towards helping an organization manage risks to achieve its objectives. ERM helps an organization become a risk managed business.

An ERM policy is first put in place which defines the guiding principles showing responsibility of line management for ERM and the broad activities covered by the risk management processes. A risk management framework to implement the ERM policy is then finalized showing the activities which need to be carried out and how they are to be carried out under three processes, viz.

- Risk assessment.
- Risk management.
- Risk communication.

Implementation is facilitated by a risk manager or the internal auditor as a consulting assignment. Subsequently risk based internal audit is carried out.

Risk Register See Nov 19 Exam - Sample risk register - CS - 2

Important

- Risk register is a record of risk, risk assessments; risk mitigation and action plans prepared by the responsible parties that help to support overall ERM and controls disclosures reporting process.
- Risk register is continuously updated and has columns for risk, causes, consequences, ownership, inherent risk score, controls, residual risk score, process, action for further mitigation, action owner, due date, etc.

3. TECHNIQUES OF ENTERPRISE RISK MANAGEMENT (ISO 31000 SUGGESTS KEYS TO ERM IMPLEMENTATION)

It starts with themes to provide management with a strong foundation for an effective ERM program as they develop and tailor their specific approach to implementing ERM. These themes "Keys to Success" for organizations that are starting ERM initiatives and provide a useful

foundation for specific actions detailed. These keys also help company's board to address some of the recognized barriers and resistance points to ERM adoption.

Key 1: Winning support and sponsorship from the Top management is a pre-cursor

The Board of directors should sponsor the ERM function and activities by providing the right focus, resources and attention for ERM. ERM must be truly enterprise wide, and understood and embraced by all personnel, and driven from the top through clear and consistent communication and messaging from the company's board to senior management and to the organization as a whole.

The Board needs to put in place an effective ERM leader who is widely respected across the organization and who has accepted responsibility for overall ERM leadership, resources and support to accomplish the effort.

Key 2: Building ERM using small but solid steps Nov 2018 MCQ + May 20 MTP MCQ

Organisation can start with a simple process and build from there using incremental steps rather than trying to make a quantum leap to fully implement a complete ERM process.

By doing so, they are able to:

- Identify and implement key practices to achieve immediate, tangible results.
- Provide an opportunity to change and further tailor ERM processes.

Key 3: Focus on a simple Risk model with Small Number of Top Risks

The ERM team should identify small number of critical and strategic risks that can be managed, and then evolve from this start.

Focusing initially on a smaller, manageable number of key risks would also be beneficial in developing related processes such as monitoring and reporting for those specific risks. This focused approach also keeps the developing ERM processes simple and lends itself to subsequent incremental steps to expand the risk universe and ERM processes.

Key 4: Leverage Existing Resources

Organizations often discover that they can rely on their existing staffs, with the knowledge and capabilities relating to risks and risk management that can be effectively used to start the ERM process. For example, some organizations have used their Chief Audit Executive or their Chief Financial Officer as the catalyst to begin an ERM initiative. In other instances, organizations have appointed a management committee, sometimes headed by their Chief Finance Officer (CFO), to bring together a wide array of personnel from across the entity that collectively have sufficient knowledge of the organization's core business model and related risks and risk management practices to get ERM moving.

In addition, most organizations start their ERM effort without any specific enabling technology or automated tools other than basic spreadsheets and word-processing capabilities.

Key 5: Build on Existing Risk Management Activities

Existing functions such as internal audit, compliance, ethics and other support function could be leveraged to build on the ERM blocks and activities.

Key 6: Embed ERM into the Business Fabric of the Organization

May 19 MTP

ERM is a management process, ultimately owned by the board of directors and involves people at every level of the organization. The comprehensive nature of the ERM process and its pervasiveness across the organization and its people provides the basis for its effectiveness.

ERM cannot be viewed or implemented as a stand-alone staff function or unit outside of the organization's core business processes. In some companies and industries, such as large banks, it is common to see a dedicated enterprise risk management unit to support the overall ERM effort including establishing ERM policies and practices for their business units.

Key 7: Provide On-going ERM Updates and Continuing Education for Directors and Senior Management

ERM practices, processes and information continue to evolve. Thus, it is important for directors and senior executives to ensure that they are receiving appropriate updates, new releases and continuing education on ERM, including information about regulatory requirements and best practices.

This information provides the opportunity for directors and senior management to update their risk management processes as they become aware of new or developing practices. This ongoing improvement process is particularly important with the increased focus on ERM by regulators, rating agencies, and the capital market authorities.

ICAI Case Study - 2

4. RISK MATURITY OF AN ORGANIZATION

Some organizations especially those in a fast growth mode have an organizational culture which promotes operational managers to remain at the risk naïve/ risk aware level. This means that the line managers are not expected to identify risks and if they do, it is confined to their personal knowledge or within their functional team. The internal control environment may be well defined but again it is to be operated by the staff management (such as the accounts manager), the logic being that line managers need to spend maximum time in operations and not be defocused by unnecessary paper work or issues other than their operations. In this mindset, coordinating activities and problem solving is considered as operations while risk assessment and management is considered a staff function. This model works well in a supply side market wherein the organization sells whatever it produces but flounders in a competitive and dynamic market wherein new risks arise periodically and the staff management who are not market facing are not fast enough to incorporate new controls to address these risks.

A risk naïve/risk aware organization in today's dynamic environment exhibits inefficiencies as a continuous long list of pending issues at all times with the line manager or even mundane issues

as goods received but unreconciled with Purchase Orders, delayed supplier payments resulting in line managers chasing accounts department for release of payment, etc., wherein the root cause is usually a risk which has not been addressed. In a risk aware organization, the silo approach culture wherein the manager tracks and addresses new risks related to his department only rather than in the business process usually throws up big losses arising out of customer dissatisfaction or failure of an enterprise wide activity such as implementing ERP.

The audit strategy depends upon the organization's risk-maturity. Organizations at low risk maturity levels may require internal auditors to consult by promoting and advising on identification of and response to risks. For organisations with high risk maturity, the internal auditor would need to concentrate more on carrying out process audits of the risk management processes and especially reviewing the risk assessment process wherein the inherent risk (untreated) are identified, estimated (scored) and evaluated (compared with risk appetite).

Nov 2018 MCQ

Risk Maturity Levels Nov 18 MCQ + Nov 2019 MTP + May 2018 MCQ

The following aspects in the organisation indicate its risk maturity. Internal auditors should refer to the same for concluding on the organisation's risk maturity:-

- Business objectives are defined and communicated.
- Risk appetite is defined and communicated across the organisation.
- Control environment is strong including the tone from the top.
- Adequate processes exist for the assessment, management and communication of risks.

The table given below shows the levels of risk maturity. Key Characteristics at Different Levels of Risk Maturity:- Nov 2019 Exam Question

Risk Maturity	*Key Characteristics* Important
Risk Naive	No formal approach developed for risk management.
Risk Aware	Scattered silo based approach to risk management. Risks identified within functions and not across processes. Also risks not communicated across enterprise.
Risk Defined	Strategy and policy in place and communicated. Risk appetite defined.
Risk Managed	Enterprise wide approach to risk management developed and communicated. Risk register in place.
Risk Enabled	Risk management and internal control fully embedded into operations. Organization in readiness to convert market uncertainties into opportunities.

ICAI CS 2

MTP MCQ Nov18

May 18 MTP MCQ

5. PROCESS OF ENTERPRISE RISK MANAGEMENT AND INTERNAL AUDIT

Enterprise Risk Management is a structured, consistent and continuous process of measuring or assessing risk and developing strategies to manage risk within the risk appetite. It involves identification, assessment, mitigation, planning and implementation of risk and developing an appropriate risk response policy. Management is responsible for establishing and operating the risk management framework. The Enterprise Risk Management process consists of Risk identification, prioritization and reporting, Risk mitigation, Risk monitoring and assurance. Internal audit is a key part of the lifecycle of risk management. The corporate risk function establishes the policies and procedures, and the assurance phase is accomplished by internal audit.

6. STAKEHOLDER VALUE CREATION BY ENTERPRISE RISK MANAGEMENT

Benefits of ERM - also see page no. 8.2

Effective implementation of Enterprise risk management leads to number of benefits to the business and society. The full value of payoff is realised over a period of time. It is similar to a business entity implementing and Enterprise Resource Planning Package where the return on investment in over a period of time likewise when ERM is implemented the payoff is realised over few years of the business life-cycle. The gains from ERM implementation are realised in two stages intermediate/ short term and long term.

The Risk Management Payoff Model of Epstein and Rejc, 2005, demonstrates how improved risk measurement and management provides benefits throughout the organization. Benefits extend to

(a) enhanced working environment,

(b) improved allocation of resources to the risks that really matter,

(c) Sustained or improved corporate reputation, and

(d) Other gains, all of which lead to prevention of loss, better performance and profitability, and increased shareholder value.

Successful Stakeholder Risk Management

Nov 20
MTP
CS -5

It is necessary to evaluate all types of risks impacting all categories of stakeholders and find solutions to pre-empt the threats before the risk occurs. The more one knows about the stakeholders and their levels of importance, the more effective and purposeful the risk management strategy will be. The risk management program should look at the big picture and identify not only short term risk factors but also long term factors impacting the entire value chain of business activities and connected communities.