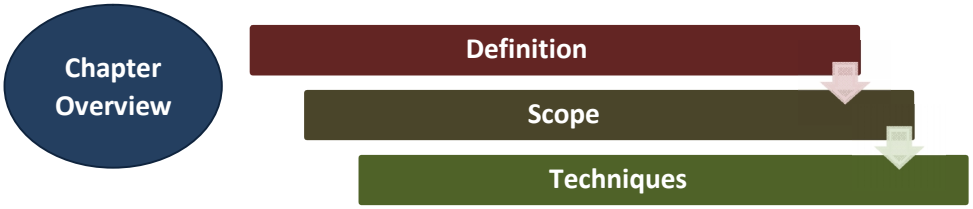
Lecture Note 22

Chapter 8 : Enterprise Risk Management



Definition and Scope of Enterprise Risk Management
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.
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.
Important Point:
✓ ERM serves as a strategic analysis tool, cutting across business units and departments ✓ 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.

ERM can help organizations
• Identify strategic risk opportunities • Introduce a common language within the organization where people recognize problems and adopt a problem solving approach by developing risk treatment actions. • Provide senior management with the most up-to-date information regarding risk that may be used in the decision-making process. • Establish linkage between the ERM initiative and adherence to capital market reporting disclosures and other corporate laws and regulations. • Align annual performance goals with risk identification and management. • Encourage and reward upstream reporting of business-risk opportunities and challenges. • Align other risk monitoring initiatives such as self-appraisals, internal auditing activities, control

assessments, continuous control monitoring, to organizational objectives.

- Imagining key Risk Scenarios that could potentially result in a stress on the financial position of the company.
- Financial Risk monitoring a part of the ERM initiative can balance the financial stability equation of the company

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

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.

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.

Risk Appetite

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.

Risk Register

- 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.

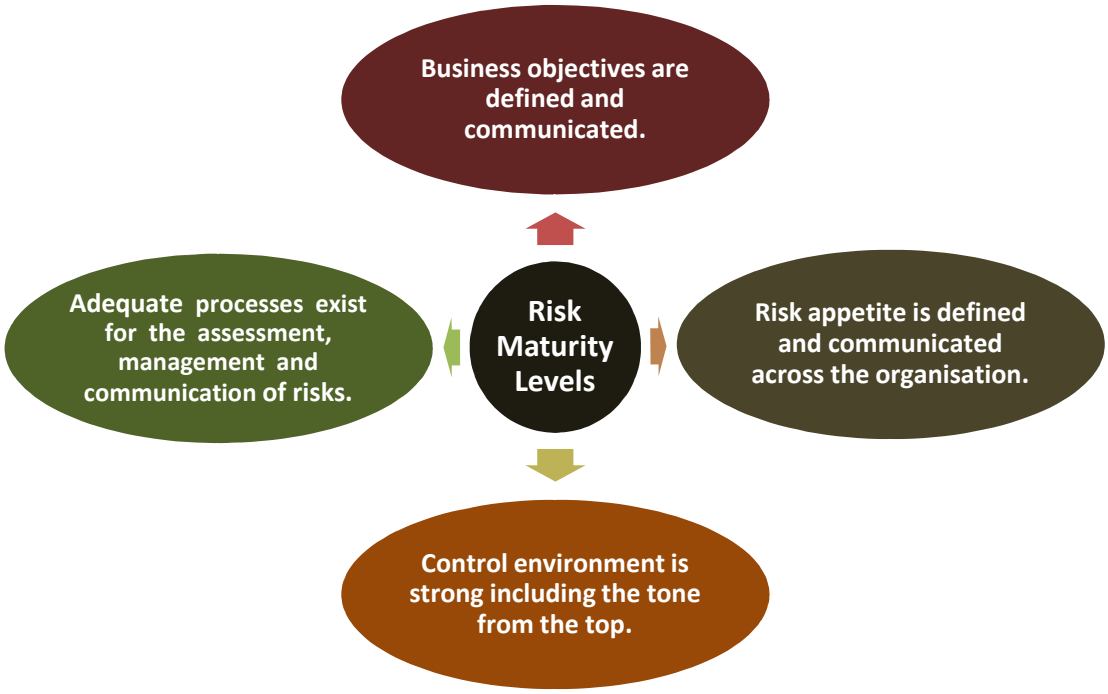
TECHNIQUES OF ENTERPRISE RISK MANAGEMENT (ISO 31000 SUGGESTS KEYS TO ERM IMPLEMENTATION)

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.
Key 2: Building ERM using small but solid steps	•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.
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.
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
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	•ERM is a management process, ultimately owned by the board of directors and involves people at every level of the organization.
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.

RISK MATURITY OF AN ORGANIZATION

An organizational culture which promotes operational managers to remain at the risk naïve/ risk aware level.

Risk Maturity



Key Characteristics at Different Levels of Risk Maturity	
Risk Maturity	**Key Characteristics**
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.

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.

STAKEHOLDER VALUE CREATION BY ENTERPRISE RISK MANAGEMENT
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.
Benefits (As per The Risk Management Payoff Model of Epstein and Rejc, 2005)
• enhanced working environment

- improved allocation of resources to the risks that really matter
- Sustained or improved corporate reputation, and
- Other gains, all of which lead to prevention of loss, better performance and profitability, and increased shareholder value.

Successful Stakeholder Risk Management
• It is necessary to evaluate all types of risks impacting all categories of stakeholders • Knows about the stakeholders and their levels of importance • More effective and purposeful the risk management strategy • 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.