UNIT-3 Introduction to Enterprise Risk Management

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Recognize the Benefits of Enterprise Risk Management
- ✓ Discuss the mechanism of Enterprise Risk Management
- ✓ Explore the strategies of Business Growth through Risk Taking

Unit 3

Introduction to Enterprise Risk Management

The process of an Enterprise Risk Management Framework (ERM) enables the administration of a business management to recognise all the risks it faces, quantify them, evaluate the sufficiency of controls, and report about the existing risk profile of the business.

Managing risk within the enterprise traditionally meant making sure that adequate insurance policy, sufficient capital resources and procedures for physical protection, like fire extinguishers were available to deal with the most common forms of risk to the business. The primary considerations for safeguarding the business were physical protection and asset protection. Over time, people realised that businesses are exposed to all kinds of risks, such as those described in unit 2. These risks to the organisation have become more complex and interrelated; therefore, a centralised approach towards managing enterprise-wide risks is now critical.

The American Risk and Insurance Association defines business risk management as:

…a systematic process of managing an organization's exposure to risk to achieve its goals in a manner that is consistent with human safety, public interest, environmental factors, and the law. It consists of the planning, organizing, leading, coordinating, and controlling activities undertaken with the intention to provide an efficient pre-loss plan that minimizes the adverse impact of risk on the organization's resources, earnings, and cash flows.

All organisations, irrespective of their size, customer base or industry, face a certain degree of business risk. Smaller businesses may be extremely vulnerable to even the smallest unplanned incident, such as the closing of a specific supplier or temporary unavailability of a resource or utility. On the other hand, as a direct result of their size and operational complexity, even large and stable multinational companies are at risk. All organisations face risk on a daily basis and accept it to be just a part of doing business.

An old proverb describes this phenomenon very appropriately: 'No guts, no glory.' There can be no rewards without taking risks. The only way to maximise the probabilities of success is to understand the possible risks, evaluate their probability, assess the potential impact if a risk incident occurs, and plan for minimising that impact.

However, understanding and assessing the risks is even more complex than it appears on the surface. As if the types of risks described above are not enough to worry today's business managers, the reality is that companies are not subjected to only one type of risk because enterprise risk is truly a multi-faceted problem. The four main categories of risk are all interconnected and may have a severe combinatorial consequence for the enterprise if they are not considered as an integrated whole.

Evaluating, planning for, and managing business risks is increasingly becoming a significant process, yet many organisations still have not addressed it. Being prepared puts organisations in a better position to respond if and when an incident occurs, rather than merely reacting. Ignoring the need to manage business risk could indeed be the biggest risk of all for many organisations.

Because of the centralised nature of true ERM, it is important that the person or group responsible for this role should be a fundamental part of the organisation. Originally, risk management was handled by an administrative department within the company, not directly related to the business, such as Finance or Security. Many companies are now creating a special executive or senior management function, that of the chief risk officer (CRO), as they realise that the responsibilities of managing business risk are a crucial part of the well-being of the organisation. Although this may be one person or a set of responsibilities and processes given to several members of the organisation, ultimately, the responsibility to provide a safe and resilient organisation is within the jurisdiction of the company's senior management and its board.

The Chief Risk Officer

The CRO, which is also known by the nickname *Chief Worry Officer*, is ultimately responsible for dealing with ERM within the company. Not all organisations will need or want a full-time person dedicated to risk management, but the responsibilities of the ERM person should be as visible and as important as other significant business functions. As described in the previous section, the activities involved in ERM are likely to overlap with many other functions within the organisation, consequently it is important that the person responsible for evaluating and managing risks should have the necessary authority to get the job done. ERM is all about discovering problems and either fixing them before they occur, or creating procedures to deal with them, if and when they occur.

The CRO function can co-exist as the title and responsibility of a current executive or senior-level manager. Generally, areas in which the CRO title may lie are in the operational (the Chief Operating Officer), legal (the Chief Legal Officer), financial (the Chief Financial Officer), or IT (the Chief Information Officer) domains. In smaller companies, the chief executive officer could function as the CRO, but for larger organisations this is usually not practical or appropriate. The individual or group taking on the ERM responsibilities should be very familiar with how the organisation conducts business.

Since the CRO must protect the organisation against any real or perceived threats or risks, someone who does not know the actual business functions of the company may miss things that could be particularly important to the line of business, operational processes or market conditions in which the company operates.

Board of Directors

Senior executives need to be made aware of their role in risk management and understand the types of risks that are present within the company. Ultimately, the board of directors must approve the overall

approach towards risk-taking. The organisation's risk management policies and procedures should provide guidance and operating parameters that allow for the risks involved with its business lines and other significant activities to be identified, monitored, measured and controlled. Also, the lines of risk-taking authority and accountability should be clearly defined.

The board is responsible for the following:

- An annual review of risk policies and critical procedures must be created: This is the most critical practice through which the board of directors can express its tolerance for and attitude toward risk management.
- Be involved in approving the risk limits: Limits are an explicit statement of the company's appreciation for risk. Defining limits is an important technique for controlling risks.
- Build a new product development procedure: This is a significant means of controlling future risks. The board should make sure that all new products are comprehensively reviewed by risk management, legal, compliance and operations.
- Monitor policy exceptions: It is just as important for the board to make sure that the proactive elements of risk management defined above are in place, as it has to determine a reactive approach. How to handle exceptions to risk policies should be well defined, strictly audited, and closely monitored by the board.

Benefits of Enterprise Risk Management

Risk management processes can never create a risk-free environment. However, enterprise risk management should enable managers to operate effectively in a business environment filled with ever-changing risks.

Enterprise risk management should provide the capability to:

- Align risk appetite and strategy: Risk appetite is the extent of risk on a broad-based level, which a company is prepared to accept in pursuing its objectives. The management takes the business's risk appetite into consideration first when assessing strategic options, and then in setting limits for downside risk.
- Reduce operational surprises and losses: Businesses should identify potential risk incidents, evaluate risks and determine responses. In doing so, they reduce the occurrence of unpleasant surprises and related losses or costs.
- Improve risk response decisions: ERM provides the ability to identify and select an appropriate risk response, such as risk acceptance, transfer, removal or reduction.
- Resources: A clear understanding of the risks that the business is facing can improve the effectiveness and use of the management's time and the company's resources to manage the risk.

- Recognise and manage cross-enterprise risks: Every organisation faces numerous risks, which affect various parts of the company. The benefits of ERM are only realised when an enterprise-wide approach is used by integrating the different approaches to risk management within a company. There are three ways in which integration has to be effective: centralised risk reporting, integrating risk transfer strategies and integrating risk management into the business processes of a corporation. It can be a useful tool for increasing opportunities rather than being a purely defensive mechanism.
- Link growth, risk and return: Organisations accept that risk is part of wealth creation and preservation and they expect returns proportionate to the risks. ERM provides an enhanced capability to identify and evaluate risks, and establish acceptable levels of risk relative to the likely growth and attainment of objectives.
- Seize opportunities: The process of detecting risks can stimulate thinking and create opportunities along with threats. Responses should be developed to address identified threats to a business and also to seize opportunities.
- Rationalise capital: More accurate information on risk exposure enables management to assess overall capital needs more effectively and improve capital allocation.

Benefits of implementing ERM

Type of Risk	Expected Benefit
Business interruption	Avoid production loss, legal liability, and business failure. Achieve operational reliability.
Environmental	Reduce insurance premiums. Avoid litigation from government regulatory authorities and other groups.
Health and safety	Prevent worker injuries or fatalities, evade worker litigation and decrease insurance premiums.
Marketing	Avoid damage to brand or reputation, gain competitive advantage and maintain or increase market share.
IT	Gain access to information, prevent or avoid operational failures due to technology e.g. inability to pay or invoice.
Product liability	Prevent litigation. Protect customers from damage or harm.
Technical	Prevent production stoppages. Avoid using out-dated equipment, manufacturing techniques or technologies.
Theft and fraud	Avoid losing money, assets, or intellectual property. Avoid damage to reputation. Prevent loss of market share.

Putting a formal ERM plan in place provides many direct benefits to the organisation. However, there are also some indirect benefits, like improved communication because of interdepartmental interaction that takes place during the ERM assessment and planning phases. This improved communication can lead to

higher awareness of how operations in different areas of the organisation affect each other, giving rise to better enterprise-wide support and interoperability.

Both businesses and governments are being scrutinised over how they are managing their business risks and protecting their organisational assets. Corporate executives are discovering that they have an increasing responsibility to assure their shareholders that their investments are stable and secure.

Although organisations can be proactive in developing their own risk management plans, many of them are now demanding that their first- and, often, second-tier suppliers have documented continuity of operations and disaster recovery plans in place before doing business with them. This measure is progressively becoming a requirement in all industries. Customers' expectations are higher as they have become more sophisticated. The increasing use of internet-based technology and commercial capabilities has given customers constant access to more products and services than ever before. As a result, downtime is met with zero tolerance.

Components of Enterprise Risk Management

The ultimate goal of ERM is to avoid damage to the organisation or disruption in its processes caused by unexpected or uncontrolled risk incidents. To achieve this, ERM must ask two fundamental questions:

1. Can a risk be removed before it affects the organisation?
2. What must be done to reduce the impact of risks on the organisation and to minimise its effects if it cannot be avoided?

Business executives are responsible for ensuring that the organisation's mission critical operations and assets are adequately protected. To do this, a cost-effective strategy must be established with emphasis on broad thinking and problem solving.

Developing a comprehensive ERM strategy involves three major aspects: risk awareness, risk assessment and measurement, and risk control. These aspects focus on risks related to the unplanned interruptions of the mission-critical operations of a business so that it may continue to function at a predetermined acceptable level and that normal functioning may be restored as soon as possible when a problem occurs.

Risk awareness, risk measurement, and risk control processes must be on-going in order to remain active, current, and valid. In addition, as risks in one area are exposed and worked through, another previously hidden layer may surface, requiring further investigation, assessment, and management.

Risk Awareness

Risk awareness is the initial step in the development an effective ERM strategy. This aspect involves two elements: the need for internal corporate education about enterprise risk, as well as for effective communication to all corporate stakeholders to take place. The first element is the responsibility of the

enterprise's control sections, such as the one headed by the CRO. The second could be a shared effort involving business executives and directors including the CRO, company communications groups, such as, public relations, investor relations, and line-of-business managers.

The first key component of risk awareness is for executive management to recognise that significant business risks exist and may threaten the welfare of the organisation. Although this sounds obvious, it is surprising how many executives ignore or misjudge the potential threats to their business, until it is too late.

Once the reality of business risks has been accepted, the next step is to identify the types of risks and where they may lie. A great deal of creative thinking is required because the organisation's vulnerabilities may not always be obvious. The CRO must be closely familiar with the company's primary business model and operational processes. The type of business it conducts and the way the company operates has a direct effect on the types of potential risks that face the company. Unit 2 provided a partial list of several types of risks faced by today's companies.

At this point, the aim of the risk awareness process would be to draw up a comprehensive list of all the known or perceived, physical and logical, risks and hazards to the organisation. At this stage of the ERM process, even imagined threats can be listed. It is wise to start with a large and comprehensive list and then remove those risks that are shown not to exist, instead of recovering from a risk that was missed during this phase and therefore, not addressed in the ERM plan.

Finally, communication will be the most important element which will ensure that all stakeholders are aware of the possible risks to the organisation. Many stakeholders, both internal and external, have an interest in business risks. This includes company employees and executives, vendors and suppliers, subcontractors, individual and institutional investors, government and regulatory agencies, customers, and even, the general public. Any or all of them will require comprehensive, careful, and distinctly targeted messages about the risks or threats to the organisation, subject to the nature and scope of the company's business activities.

Risk Assessment and Measurement

Compiling a list of possible threats to the organisation forms a good starting point for an ERM programme, but is not sufficient by itself for developing an accurate and beneficial communication as described in the risk awareness phase. Once all potential risks have been identified, assessing their odds and their potential influence on the business is the next step. This step comprises the allocation of a quantifiable and objective value and a probability to the risks that have been identified in the previous phase.

To do this, many organisations use reporting tools and analytical techniques specifically designed for risk management. These kinds of tools were developed originally by the financial, credit and insurance sectors to define the level of risk exposure and the probable financial and operational impacts if a

business disruption occurs. These tools have become more sophisticated over time and can provide exceptional scenario-based simulations of actual risk events and how organisations are likely to be affected.

Because of the inter-relationships of many corporate risks, these tools and techniques are particularly crucial for developing realistic scenarios and estimations of their impact. However, these analytical tools are not automatic. Data must be fed into the tools which must come from the company's own information systems. If the information in these systems is neither sufficient nor available in a way that the analytical tools require, then the company's overall technology infrastructure may need to be updated so that the risk management tools can be used.

This is a major challenge for the CRO. Although most organisations work towards integrating and connecting their entire information infrastructure, the systems and data stores used to provide a complete and comprehensive view of the company's portfolio, material and logical assets, as well as business processes, are often in separate unrelated systems.

A very important constituent of this stage of ERM is to get an objective and impartial understanding of the true potential impact of the identified risks can to the organisation. Once this phase has been completed, the next step is to concentrate on controlling or eliminating these risks in order to reduce the impact on the company.

Risk Control

Merely identifying and quantifying the risks that enterprises face is not sufficient to effectively protect the enterprise against them. For this, the risk control portion of the ERM plan is needed. Risk control involves the steps needed to minutely examine and limit the vulnerabilities to which the company is exposed. This is where active 'management' of risk management is required.

Organisations may control risks in a number of ways; by adopting only one technique or a combination of several practices. The first strategy is to control the risk at its point of origin, such as by improving a configuration or change a management process to reduce the possibility of errors being introduced into systems, or re-engineering a manufacturing process that could result in flawed products, or by discontinuing a risky investment. In this case, line management will have to be involved to make the essential changes outlined in the ERM document.

Another way to control risks is to examine the interrelated company risks and reduce the overall level of risk for the company. This type of control method usually requires delving into the most risk-prone areas of the business, for example, business and product development, research, trading partner or customer support and relationship management. The goal is to discover where the interconnected risks put the company in the most danger and see whether a comprehensive change to the business activities can eliminate them completely or limit the risks substantially. For example, these limiting measures could indicate that the organisation should stop working with a subcontractor that continually engages in risky

practices or otherwise that a method of customer relationship development be stopped or changed to limit the chance of reputation liability and damage to the company.

Such changes have to be dictated by executive management and implemented by the affected line managers and business units. They cannot be implemented by the company's line management alone as they often involve multiple areas within the business that are frequently interrelated.

Finally, if the risks cannot be controlled sufficiently within the company, it might become necessary and appropriate to transfer them outside of the company. Allocating risk capital to cover the expected costs of a specific risk event or acquiring additional insurance policies for security against the event are typical ways of doing this.

However, not all risks are insurable and for those that are, it may not be practical or cost effective to insure against all of them. Ultimately, the goal of ERM is to balance risk and return for the whole company.

Business Growth through Risk Taking

Risk is unavoidable in business activity. Virtually all operational tasks and processes are now seen through the prism of risk (Hunt 2001). Undeniably, the term *risk* has become shorthand for any corporate activity and it is considered impossible to "create a business that doesn't take risks" (Boulton*et al.* 2000). The final outcome of successful strategic direction settings must be the capacity to accept a greater risk, as this is the only way to improve business performance. However, businesses must understand the risks that they take to extend this capacity. While in many situations risk cannot be eliminated but only reduced, it is essential that only the right risks are taken.

Taking and managing risk is the essence of business survival and growth.

Risk and Opportunity

Risk Management of both upside risks or opportunities and downside risks or threats is at the heart of business growth. Organisations should not be preoccupied only with downside risk. When a board has developed its vision, mission and values, it must also set its corporate strategy, which is its method of achieving the company's vision. Strategy setting is about strategic thinking. Setting the strategy is about being thoughtful and reflective, and then directing, showing the way ahead and providing leadership. Whatever strategy is selected, the board must decide what present and future opportunities it wants to pursue and what risks it is willing to take in developing the selected opportunities. Risk and opportunity management must be given equal attention. It is very important that boards select the right balance.

All businesses face risk from inception, and while risks are important, they are not grounds for action but restraints on action. Therefore, risk management is about enabling a business to maximise its opportunities while controlling risk as far as possible. Development of a risk policy should be a creative

initiative, revealing exciting opportunities for value growth and innovative handling of risk, not a depressing task, full of reticence, warning and pessimism (Knight and Petty 2001). Thus, ERM is about managing both risks and opportunities.

Enterprise risk management is about protecting and improving share value to satisfy the primary business objective of *shareholder wealth maximisation.* It must be a multifaceted approach, addressing all facets of the business plan from the strategic plan through to the business controls:

- Strategic plan;
- Marketing plan;
- Operations plan;
- Research and development;
- Management and organisation;
- Forecasts and financial data;
- Financing;
- Risk management processes; and
- Business controls

Businesses operating in today's environment are characterised by constant change and the need for a totally integrated approach towards risk management.

There are many key areas in which the success of a complete ERM discipline could make a significant difference.

These are:

- Planning for extreme events;
- Responding to wide-scale disasters;
- Controlling risk exposure;
- Managing company assets and capital; and
- Communicating to the company's stakeholders

The following discussion investigates each of these additional benefits in greater detail and explains why ERM can be so helpful in dealing with crises.

Planning for Extreme Events

The benefit of ERM to a company under *normal* risk conditions is obvious. However, ERM planning can offer additional value by preparing the organisation for extraordinary circumstances, such as those experienced during the attacks on WTC and Pentagon.

The ERM discipline can be used to investigate even the most extreme events and develop scenarios to give businesses an idea of how such an event would look, the types of actions and resources that might be needed to deal with it, and the kind of outlook the business will have post-event.

To some degree, governments and municipalities have planned for severe risk situations, such as catastrophic earthquakes and nuclear attacks. These are the sorts of events that are highly unlikely and rare, yet would have devastating effects on businesses, geographic areas, and industry segments. In cooperation with government sections, businesses could work together to decide what a reasonable and practical response would be towards such extreme events and also decide in advance where government or regulatory assistance might be needed to restore order.

Responding to Wide-Scale Disasters

Following the topic of extreme events, the next natural topic is that of handling responses to wide-scale disasters, such as the catastrophic earthquake mentioned previously. ERM's modelling and scenario-building ability is tailor-made for creating effective plans for responding to major crises. Many modelling tools are designed to deal with the total complexity that interrelated risks create and businesses can use these to develop effective anticipatory response plans.

Enterprises that devote resources and time towards planning for such situations before they occur will be in a far better position to respond and recover if and when they actually occur.

Managing Risk Exposure

The ability of an ERM to consider the interdependencies of risks to the business and create scenario-based models of envisaged catastrophic events is valuable in helping companies understand where they may suffer heavily from related risks.

If a scenario shows that a particular event can cause an especially strong impact, as a result of the interaction of multiple vulnerabilities, then, the company has the knowledge with which they need to develop more efficient ways of managing that impact.

Perhaps the management could decide that the organisation stops doing business in a particular way that exposes it to more risk in a certain area. Alternatively, risk can be transferred out to a third party or resource in order to avoid the combinatorial effects of multiple, cascading risks. In either situation, the information that ERM provides these companies about their interrelated risk scenarios can help in preventing or reducing catastrophic effects when extreme events occur.

Managing Company Assets and Capital

One problem many organisations may be thinking about after the recent disasters may be 'Do we have sufficient resources to deal with a true emergency?'Organisations are very committed towards managing capital and assets to support day-to-day operations, but a major crisis, such as 11 September, 2001 can

have a huge impact on their overall resource requirements. In the event of a catastrophe, an organisation may need substantially more cash to handle recovery or response efforts, than it would normally have available. Yet, this cash may usually have lower liquidity than would be required during such times. The company needs access to funds and a catastrophic event should not be made more problematic by needing to extract these funds out of less liquid holdings. On the other hand, it is equally problematic to have too much of the company's reserves held in low-return but more liquid investments 'just in case' of a highly unlikely disaster.

Using the ERM, the company can develop an appropriate model that provides a suitable balance between deep assets and capital fluidity. This provides an informed basis from which to make the very important decisions about capital and asset allocation, both before a catastrophic event takes place, and during the recovery and rebuilding efforts after the incident.

Communicating to the Company's Stakeholders

ERM can have a positive effect on effective communication with the organisation's stakeholders in the event of a catastrophic occurrence. This communication is definitely important for all the categories of affected parties, including the company's employees, trading partners, etc. However, there are groups of stakeholders for whom this communication is particularly important, including the insurance sector, banks and lending institutions, as well as securities and investment groups. For these groups, having an effective ERM strategy in place can be a huge benefit to the organisation prior to, during and after crisis times.

Although much of the ERM communication is concerned with proactive communication about the organisation's preparation and contingency plans, there is another kind of communication that is an equally important part of any business continuity planning, namely crisis communication. If crisis communication is not planned for and executed properly when a difficult situation actually arises, it can make or break even the best of organisations.

Crisis Communication

While Risk Management is focused on strategies for anticipating and managing both mundane and urgent problems, Crisis Management is basically concerned with only the most dramatic circumstances and events that could disrupt operations entirely or make it impossible to continue working.

Conclusion

ERM is mainly concerned with creating risk awareness within the organisation, evaluating and measuring that risk, and then, taking the steps which are needed to manage it. ERM helps the company in making sensible, educated decisions about the various kinds and scope of business risks being faced, how to reduce them and whether to transfer them to an outside party when all efforts at internal control still result in unacceptable levels of possible return weighed against risk.

Although it may appear to be a waste of time and resources to focus on the unthinkable or unlikely, but when the unthinkable actually happens, ERM will prove to be an invaluable tool, providing companies the peace of mind that effective plans are in place.

Further Reading:

- ✓ ***John Fraser, Betty Simkins, (2010), Enterprise Risk Management***
- ✓ ***James Lam, (2003), Enterprise Risk Management***
- ✓ ***Gregory Monahan, (2008), Enterprise Risk Management: a Methodology for Achieving Strategic Objectives***