Unit : I Introduction to Risk Management

1.1 Introduction, Meaning, Definition of Risk Management.
1.2 Risk Management Process.
1.3 Risk Management Approaches and Methods.
1.4 Risk Reporting Process.
1.5 Risk Organization.

Introduction :

Risk can be defined as the **chance of loss** or **an unfavorable outcome** associated with an action. Uncertainty does not know what will happen in the future, the **greater the uncertainty, the greater the risk**. For an individual, risk management involves optimizing expected returns subject to the risks involved and risk tolerance. Risk is what makes it possible to make a profit. If there was no risk, there would be no return to the ability to successfully manage it. For each decision there is a **risk return trade-off.** Anytime there is a possibility of loss (risk), there should be an opportunity for profit.

Risk management is the process of **identifying, assessing and controlling** threats to an organization's capital and earnings. These threats, or risk, could stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents and natural disasters. IT security threats and data-related risks, and the risk management strategies to alleviate them have become a top priority for digitized companies. As a result, a risk management plan increasingly includes companies' processes for identifying and controlling threats to its digital assets, including proprietary corporate data, a customer's personally identifiable information and intellectual property.

Definition of Risk Management :

1) *Risk management is an integrated process of delineating (define) specific areas of risk, developing a comprehensive plan, integrating the plan, and conducting the ongoing evaluation'* – Dr. P.K. Gupta.

2) ***Risk Management is the process of measuring, or assessing risk and then developing strategies to manage the risk'*** – Wikipedia.

3) *Managing the risk can involve taking out insurance against a loss, hedging a loan against interest rate rises, and protecting an investment against a fall in interest rates'* – Oxford Business Dictionary.

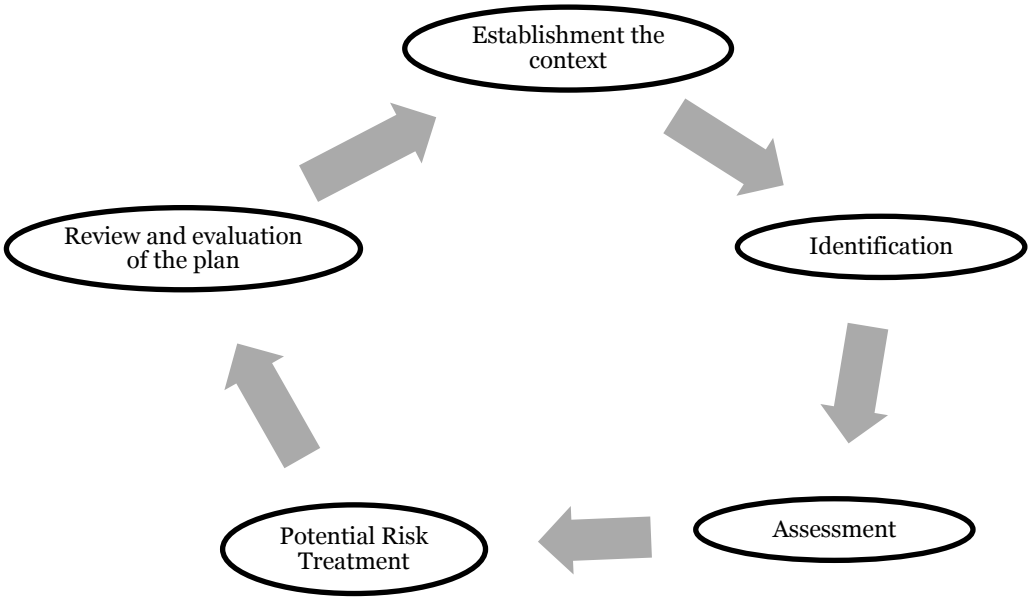
When an entity makes an investment decision, it exposes itself to a number of financial risks. The quantum of such risks depends on the type of financial instrument. These financial risks might be in the form of **high inflation, volatility in capital markets, recession, bankruptcy**, etc. So, in order to minimize and control the exposure of investment to such risks, fund managers and investors practice risk

management. Not giving due importance to risk management while making investment decisions, but risk arises due to change in an economy. Different levels of risk come attached with different categories of asset classes.

For example, a fixed deposit is considered a less risky investment. On the other hand, investment in equity is considered a risky venture. While practicing risk management, equity investors and fund managers tend to diversify their portfolio so as to minimize the exposure to risk.

The traditional view of risk management has been one of protecting the organization from loss through conformance procedures and hedging techniques. This is about avoiding the downside. The new approach to risk management is about 'seeking the upside while managing the downside'.

Risk Management Process :



1. Establish the Context :

The purpose of this stage of planning enables to **understand the environment** in which the respective organization operates, that means the thoroughly understand the external environment and the internal culture of the organization. You cannot resolve a risk if you do not know that it is. At the initial stage it is necessary to establish the context of risk. To establish the context there is a need to collect relevant data. There is a need to map the **scope of the risks and objectives of the organization**.

2. Identification :

After establishing the context, the next step in the process of managing risk is to identify potential risks. Risks are about events that, when triggered, will cause problems. Hence, risk identification can start with the source of problems, or with the problem itself.

Risk identification requires knowledge of the organization, the market in which it operates, the legal, social, economic, political, and climatic environment in which it does its business, its financial strengths and weaknesses, its helplessness to unplanned losses, the manufacturing processes, and the management systems and business mechanism by which it operates.

Any failure at this stage to identify risk may cause a major loss for the organization. Risk identification provides the foundation of risk management. The identification methods are formed by templates or the development of templates for identifying source, problem or event. **The various methods of risk identification are – Brainstorming, interview, checklists, structured 'What-if' technique (SWIFT), scenario analysis, Fault Tree Analysis (FTA), Bow Tie Analysis, Direct observations, incident analysis, surveys, etc.**

3. Assessment :

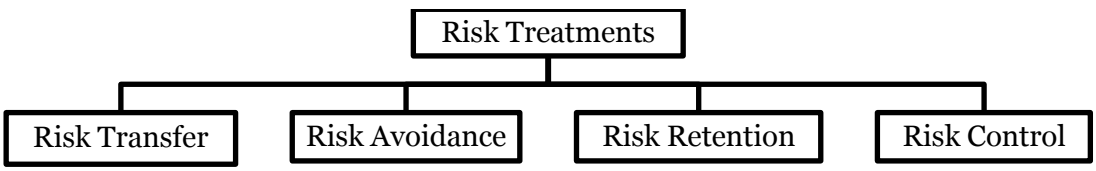
Once risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated guesses possible in order to properly prioritize the implementation of the risk management plan. The fundamental difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kind of past incidents.

Nevertheless, risk assessment should produce such information for the management of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized. Thus, there have been several theories and attempts to quantify risks.

Numerous different risk formula exist but perhaps the most widely accepted formula for risk quantification is **rate of occurrence multiplied by impact of the event [Rate of occurrence x Impact of the event]**.

4. Potential Risk Treatments :

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories.



a) Risk Transfer : Risk transfer means that the expected party transfers whole or part of the losses consequential to risk exposure to another party for a cost. The insurance

contracts fundamentally involve risk transfers. Apart from the insurance device, there are certain other techniques by which the risk may be transferred.

b) Risk Avoidance : Avoid the risk or the circumstances which may lead to losses in another way, includes not performing an activity that could carry risk. Avoidance may seem the answer to all risks but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning the profits.

c) Risk Retention : Risk retention implies that the losses arising due to a risk exposure shall be retained or assumed by the party or the organization. Risk retention is generally a deliberate decision for business organizations inherited with the following characteristics. **Self-insurance and Captive insurance are the two methods of retention**.

A '*captive insurer*' is generally *defined* as an *insurance* company that is wholly owned and controlled by its insured's; its primary purpose is to *insure* the risks of its owners, and its insured's benefit from the *captive insurer's* underwriting profits

d) Risk Control : Risk can be controlled wither by avoidance or by controlling losses. Avoidance implies that either a certain loss exposure is not acquired or an existing one is neglected. Loss control can be exercised in two ways – (i) Create the plan and (ii) Risk Control.

i. Create the Plan :

Decide on the combination of methods to be used for each risk. Each risk management decision should be recorded and approved by the appropriate level of management.

For example, a risk concerning the image of the organization should have top management decision behind it. Whereas, IT management would have the authority to decide on computer virus risks.

The risk management plan should propose applicable and effective security controls for managing the risks. A good risk management plan should contain a schedule for control implementation and responsible persons for those actions. The risk management concept is old but is still not very effectively measured. Example – An observed high risk of computer viruses could be mitigated by acquiring and implementing antivirus software.

ii. Risk Control :

Once the risk is evaluated, it has to be controlled. In the case of the worker working under the machine that will fall any moment on top of him, risk control implies primarily moving the worker from under there and then fixing the machine so as it does

not fall on anyone. Thus the steps involved are immediate directions preventing the risk and isolating or better removing the hazard to eliminate the risk.

Avoiding the risk is the decision of either proceeding in the planned direction or opts for an alternate route which has less risk and is in line with the final objective. Reducing the risk occurrence probability or impact of its consequences or both can be considered while facing a risk. Transferring the risk is another option, mostly done through buying insurance. Other ways include lease agreements waivers, disclaimers, tickets, and warning signs. Retaining the risk can be another strategy where one knows that it is an inherent part of the event.

After the control measures are implemented it has to be documented. This has multiple benefits such as understanding what was done to tackle a risk thereby allowing similar risks to be tackled in that fashion, to prove that sufficient measures were taken to minimize and eliminate risks and due diligence were exercised etc.

5. Review and evaluation of the plan :

Initial risk management plans will never be perfect. Practice, experience and actual loss results, will necessitate changes in the plan and contribute information to allow possible different decisions to be made in dealing with the risk being faced. Risk analysis results and management plans should be updated periodically. There are two primary reasons for this –

a) To evaluate whether the previously selected security controls are still applicable and effective and

b) To evaluate the possible risk level changes in the business movement.

There are risks that do no change and are static in nature. However, other dynamic risks of not continually monitored and reviewed may grow like a bubble and their financial, legal and ethical impacts soon get out of control.

An integrated approach to Corporate Risk Management :

Corporate risk management refers to all of the methods that a company uses to minimize financial losses. Risk managers, executives, line mangers and middle managers, as well as all employees, perform practices to prevent loss exposure through internal controls of people and technologies. Risk management also relates to external threats to a corporation, such as the fluctuations in the financial market that affect its financial assets.

a) Protecting shareholders :

A corporation has at least one shareholder. A large corporation, such as a publicly traded or employee owned firm, has thousands, or even millions, of shareholders. Corporate risk management protects the investment of shareholders through specific measures to control risk. For example, a company needs to ensure that its funds for

capital projects, such as construction or technology development, are protected until they are ready to use.

b) Types of risk :

Consider the types of risk that corporation must address every day. A corporation may become insolvent if it has not bought insurance, implemented loss control measures and used other practices to prevent financial loss. Insurance is no substitute for successfully identifying measures to prevent losses, such as safety training to prevent worker injuries and deaths. Risks can include hazard risks, financial risks, personal injury and death, business interruption / loss of services, damage to a corporation's reputation, errors and omissions and lawsuits.

c) Probability and consequences :

To prevent financial losses, a corporation engages in a certain amount of speculation. A risk manager calculates the probability of each type of event that would damage the firm's financial position and the consequences. Calculating the likelihood that something will happen and its associated costs enables a risk manager to recommend ways to address the most probable risks to senior management, the board of directors and owners of the corporation.

d) Solutions :

A corporate risk manger is a multi disciplinary professional with an understanding of internal business processes and many financial instruments. This professional might have a background in business management, finance, insurance or actuarial science. He might suggest solutions to a corporation to protect its assets. For instance, he might recommend buying millions of dollars in commercial liability insurance coverage. Some risks that he calculates, as potentially damaging to the corporation, are ignored while others are covered by this liability policy. He might recommend buying other types of insurance, such as fire or fraud, after first weighting the costs versus the benefits of each type of coverage.

Risk Management Approaches and Methods :

If you are a business leader, then you already know the importance of risk control. It is imperative that your business has a formal policy to limit the loss of assets and income. Here are the6 techniques associated with risk management.

a) Avoidance :

Avoidance is the best means of loss control. This is because, as the name implies, you are avoiding the risk completely. If your efforts at avoiding the loss have been successful, then there is a 0% probability that you will suffer a loss. This is why avoidance is generally the first of the risk management techniques that is considered. It is a means of completely eliminating a threat.

b) Loss Prevention :

Loss prevention is a technique that limits, rather than eliminates, loss instead of avoiding a risk completely, this technique accepts a risk but attempts to minimize the loss as a result of it. For example, storing inventory in a warehouse means that it is susceptible to theft. However, since there really is no way to avoid it, a loss prevention program is put in place to minimize the loss. This program can include patrolling security guards, video cameras, and secured storage facilities.

c) Loss Reduction :

Loss reduction is a technique that not only accepts risks, but accepts the fact that loss might occur as a result of the risk. This technique will seek to minimize the loss in the event of some type of threat. For example, a company might need to store flammable material in a warehouse. Company management realizes that this is a necessary risk and decides to install state-of-the-art water sprinklers in the warehouse. If a fire occurs, the amount of loss will be minimized.

d) Separation :

Separation is a risk management technique that involves dispersing key assets. This ensures that if something catastrophic occurs at one location, the impact to the business is limited to the assets only at that location. On the other hand, if all assets were at that location, then the business would face a much more serious challenge. An example of this is when a company utilizes a geographically diversified workforce.

e) Duplication :

Duplication is a risk management technique that essentially involves the creation of a backup plan. This is often necessary with technology. A failure with an information systems server should not bring the whole business to a halt. Instead, a backup or fail-over server should be really available for access in the event that the primary serve fails. Another example of duplication as a risk management technique is when a company makes use of disaster recovery service.

f) Diversification :

Diversification is a risk management technique that allocates business resources to create multiple lines of business that offer a variety of products and / or services in different industries. With diversification, a significant revenue loss from one line of business will not cause irreparable harm to the company's bottom line.

Risk management is a key component in any sound company strategy. It is necessary to ensure long term organization sustainability and profitability.

Risk Reporting Process :

Risk reporting is communication of risk and risk management outcomes for the purpose of comparing the results with the policy.

An organization should ensure that information about risks derived from the risk management process is adequately reported, and used as a basis for decision making at all relevant levels. For this, clear reporting line mechanisms and strong inter-department knowledge sharing should be established in order to encourage accountability of risk, and to ensure reports are delivered in an accurate, consistent and timely manner. Moreover, the risk management policy should clearly state the way risk management performance will be reported.

Inadequate risk reporting can lead to a failure to fully integrate identified risks into strategic and operational decisions. The organization should report on progress against the risk management plan by proving how well the risk management policy is being followed, to ensure that risk management is effective and continues to support organizational performance.

More specifically :

1. The results from risk monitoring and review should be recorded and reported internally and externally, if appropriate.
2. Development in implementation of risk treatment plans should be incorporated into the organization's overall performance management.
3. Enhanced risk management includes continual communications with external and internal stakeholders.

The quality and success of risk reporting depends on the following factors –

a) Target audience.
b) Input and processes.
c) Frequency
d) Content
e) Format
f) Dissemination channels.

There are two areas of risk reporting –

a) Reporting to internal audiences
b) Reporting to external audiences.

The reporting of risks is essential for internal decision makers to integrate risk evaluation into their operational and investment strategy, to review performance and to review compensation / reward decisions.

External risk reporting has rapidly developed in recent years, corporate governance reports also focus attention on internal control, and a review of risks is generally included in the annual reports.

Both internal and external audiences can be further divided in subgroups, on the one hand some audiences (i.e. boards of directors and regulators, among external

audiences) must be informed about the organizational risks and risk management processes because of regulation or recommendations. Voluntary disclosure to other internal audiences (i.e. employees) and external stakeholders (i.e. media, citizens, associations) is recommended because of anticipated benefits to an improved decision making.

'Inputs' and 'processes' are also critical. **The most important inputs are represented by** –

a) The various risks an organization is facing.
b) The stakeholder risk reporting requirements and expectations.
c) The organization's existing risk management governance that provides the context for establishing risk reporting processes.
d) The organizational resources (such as individuals with the necessary skills and experience financial resources, and access to required information).

Decision must be taken on which risks to report in what detail, and with what reporting frequency.

a) Internal Reporting :

The organization should establish internal reporting mechanisms in order to support and encourage accountability and ownership of risk. These mechanisms should ensure that, key components of the risk management framework, its effectiveness and the outcomes and any subsequent modifications, are properly disseminated, relevant information derived from the application of risk management is available at appropriate levels and times, and there are processes for consultation with internal stakeholders. These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information. Internal risk reports can either be real-time or periodic.

The main purpose of periodic internal risk reports is to provide aggregate information about various relevant organizational risks, with trend indicators and periodic comparisons highlighting changes in risks. Periodic internal risk reporting contributes to strategic oversight and decision making, as well as improved operational business decisions. Risk information may be organized around specific key risk categories rather than around phases of the risk management process. Residual risk reporting involves comparing gross risk (the assessment of risk before controls or risk responses are applied) and net risk (the assessment or risk, taking into account any controls or risk responses applied) to enables a review of risk response effectiveness and alternative management options. Risk reporting to the board and committees should be made at least quarterly.

Internal audiences will not only interest in disclosure of specific risks, but also in the risk management process. A well established and properly managed process will assure internal audiences about the reliability of risk reports; organizations must therefore include information on the quality of their risk management process, particularly in their period risk reports.

b) External reporting :

Organizations are under increasing pressure for greater transparency, mandated or voluntary, and a better alignment of externally reported information with that which is reported internally. Stakeholders expect intensified corporate dissemination regarding risk, and awareness of the critical role of proper risk management.

In view of this, an organization should provide accurate, timely and high quality reports to meet the external stakeholder's needs. Specifically, it should periodically conduct a review of the effectiveness of the risk management system and report to stakeholders on that, and a robust assessment of the principal risks, describing them and explaining how they are being managed or mitigated.

Organizations may consider preparing different, customized risk reports for different external stakeholders. Whilst internal risk reports aim exclusively at internal audiences, external risk reporting, including corporate annual reports, may more broadly include both external users and interested internal groups.

Risk Management Organization Structure :

Organizational structure is the framework that holds an organization together and defines the lines of authority within a company, nonprofit organization or governmental agency. A well defined organizational structure provides a clear path for risk assessment procedures. Before risk assessment teams can begin to work, each member of the team must have a good working understanding of how the company is organized. The organizational structure will show team members who is responsible for each area or operation being evaluated.

a) Traditional Structures :

Traditional organizational structures typically show clear lines of authority that emanate from a central manager at the top of the organization. The authority vested in each department is clearly defined by its place within the organizational structure. Risk assessment operations can become bogged down when assessment operations are required to strictly follow established lines of authority in the company. The management of risks that cross these established lines can become a complicated process requiring intervention from the senior leadership.

b) Modern Structures :

Modern organizational structures are arranged around teams, organizational processes, organizational functions and virtual operations. These types of organizational structures allow companies greater flexibility to react and adjust to changing market conditions and advancing technology. Risk assessment teams may find modern organizational structures difficult to understand because there may not be clear lines of authority for reporting identified risks. In response to these changing business realities, many organizations are turning to enterprise risk management systems to evaluate and control risks. Effective Risk Management (ERM) helps management define how risk factors are interrelated in an organization

*****