Lesson 11
Risk Management

LESSON OUTLINE

- Introduction
- Risk Management
- Risk Identification
- Risk Analysis
- Risk Assessment
- Risk Mitigation
- Classification of Risk
- Risk Management and Corporate Governance
- Standard on Implementation of Risk Management
- Fraud Risk Management
- Reputation Risk Management
- Responsibility of Risk Management
- Risk Governance
- Glossary
- Lesson Round-UP
- Self Test Questions

LEARNING OBJECTIVES

This study lesson explains the concepts, process, its advantages and steps for implementation of risk management. It also deals with the fraud and reputation risk management and how the negative reputation of an entity may have adverse impact on the operations and profitability.

The objective of this study lesson is to enable the students to understand risk management framework, the definition and types of risks; risk management process; advantages of risk management; steps in risk management; legal provisions on risk management; who is responsible for risk management etc.

This chapter may be useful in performing the advisory role in Risk Management and Risk Governance.

"The biggest risk is not taking any risk... In a world that's changing really quickly, the only strategy that is guaranteed to fail is not taking risks."

Mark Zuckerberg

INTRODUCTION

Risk and reward go hand by hand. We have often heard the statement that without risk there is no gain. Risk is inherent in the business. Different types of risk exist in the business according to the nature of the business and they are to be controlled and managed. Better risk management techniques provide early warning signals so that the same may addressed in time. In traditional concept the natural calamities like fire, earthquake, flood, etc. were only treated as risk and keeping the safe guard equipments etc. were assumed to have mitigated the risk. But due to rapid changes, the various types of risks have emerged viz. compliance risk, legal risk, country risk, operational risk (which we will discuss in this chapter). So in the ear of fast changing global economy, multiplicity of legal compliances, cross border business transactions and to ensure the survival, viability and sustainability of business, the management of the various types of risks have gained utmost importance.

Definition of Risk: 1A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.

RISK MANAGEMENT

What is Risk Management? It is not a particular event management rather it is a continuous process of identifying, evaluating and assessing the inherent and potential risk, adopting the methods for its systematic reduction in order to sustainable business development.

Risk is inherent in every business, whether it be of financial nature or non-financial nature. Thus, management of the risk is very important. Risk management begins with the risk identification, analyzing the risk factors, making assessment of the risk and mitigation of the risk (which may be either the risk avoidance, risk reduction, risk optimization, risk sharing or finally risk retention).

To effectively manage risk, and seize the opportunity within every challenge, institutions must manage a variety of business dimensions. In today's world they must focus on maximizing digital capabilities, building ongoing expertise, driving fluid collaboration, developing top-notch analytics and fostering a risk culture that can withstand disruptive change. Turn unknown risk into opportunities to newly tap possibility by preparing your people, activities and services for the path ahead.

Better risk management techniques provide early warning signals so that the same may addressed in time. In traditional concept the natural calamities like fire, earthquake, flood, etc were only treated as risk and keeping the safe guard equipments etc were assumed to have mitigated the risk. But due to rapid changes in the technologies, business dimensions and complexities, regulatory changes and environmental concerns, new and various types of risks have emerged. So in the era of fast changing global economy, multiplicity of legal compliances, cross border business transactions and to ensure the survival, viability and sustainability of business, the management of various types of risks have gained utmost importance.

Risk management requires commitment from the top management. It is no longer discretion. It is a tool necessary to have for creating opportunities for the businesses as they develop during the risk management process. Thus, Risk Management Process provides a framework to:

1. Ensure that all the foreseeable risks involved are actually understood and accepted before important decisions are taken.

1 http://www.businessdictionary.com/definition/risk.html

2. Monitor new projects and ongoing operations to ensure that they continue to develop satisfactorily and no problems or new risks emerge.

It is desirable to have a holistic approach to risk management that avoids compartmentalization of risks.

Risk Management is part of the corporate strategy. It is a key management tool to safeguard the business assets for its use for the productive purposes. Risk Management is a logical and systematic process of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process, in a way that enables an organisation to minimise losses and maximise opportunities.

We take an example of a Forex Department of a bank. How the Forex Department keep a track on the currency risk since it is very much volatile. It uses the sophisticated techniques like, Dealer exposure limit, over the night exposure limit, hedging, merchant wise exposure limit, Value at Risk (VaR) etc to keep the risk within the manageable limits.

Risk may be controllable or uncontrollable. In other words, the systematic risk which stands at macro level is not controllable, but the unsystematic risk which is at micro level is controllable with the risk mitigation techniques.

The process of risk management may be studied by risk identification, risk analysis, risk assessment and finally risk mitigation.

RISK IDENTIFICATION

Risk identification is the first stage of the risk management strategy. By risk identification the organization is able to study the activities and places where its resources are placed to risk. Correct risk identification ensures effective risk management. If risk managers do not succeed in identifying all possible losses or gains that challenge the organization, then these non-identified risks will become non manageable. The first task of the risk management is to classify the corporate risks according to their different types. The first step in organizing the implementation of the risk management function is to establish the crucial observation areas inside and outside the corporation. Then, the departments and the employees must be assigned with responsibilities to identify specific risks.

The results of risk identification are normally documented in a risk register, which includes a list of identified risks along with their sources, potential risk responses and risk categories. This information is used for risk analysis, which in turn will support creating risk responses. Identified risks can also be represented in a risk breakdown structure - a hierarchical structure used to categorize potential project risks by source.

Though the major work on risk identification is usually done in the beginning of a project, it is important to remember that risk identification is an iterative process; new risks can be identified throughout the project life cycle as the result of internal or external changes to a project.

Purpose

The objective of the risk identification process is to ensure that all potential project risks are identified. The strategies for dealing with these risks will be devised during later risk management steps.

The ultimate purpose of risk identification is to minimize the negative impact of project hiccups and threats, and to maximize the positive impact of project opportunities. Awareness of potential project risks reduces the number of surprises during the project delivery and, thus, improves the chances of project success, allowing the team to meet the time, schedule and quality objectives of the project.

Finally, the purpose of risk identification is to provide information for the next step of the risk management process.

Example:

Let's try to identify potential risks for the website development project. To carry out risk identification, one might want to involve the project team and hold a brainstorming session. Combining the experience of different team members will decrease the probability of omitting an important risk. Additionally, if the company already has carried out similar development projects, then the team will be able to utilize the risk checklists and lessons learned from previous projects.

Process of Risk Identification

The process for risk identification starts by taking inventory of the potential project risks that can affect the project delivery. This step is crucial for efficient risk management throughout the project. The outputs of the risk identification are used as an input for risk analysis, and they reduce a project manager's uncertainty. It is an iterative process that needs to be continuously repeated throughout the duration of a project. The process needs to be rigorous to make sure that all possible risks are identified.

An effective risk identification process should include the following steps:

1. Creating a systematic process - The risk identification process should begin with project objectives and success factors.
2. Gathering information from various sources - Reliable and high quality information is essential for effective risk management.
3. Applying risk identification tools and techniques - The choice of the best suitable techniques will depend on the types of risks and activities, as well as organizational maturity.
4. Documenting the risks - Identified risks should be documented in a risk register and a risk breakdown structure, along with its causes and consequences.
5. Documenting the risk identification process - To improve and ease the risk identification process for future projects, the approach, participants, and scope of the process should be recorded.
6 Assessing the process' effectiveness - To improve it for future use, the effectiveness of the chosen process should be critically assessed after the project is completed.

Seven Identification Essentials

Identification is a process of brainstorming. It isn’t an exact science and should involve continuous implementation as new phases, experiences, and viewpoints are introduced. Being vital to the management process, there are some essentials to risk identification that guarantee maximum results.

1. **Team Participation:**

   Face-to-face interactions between project managers and the team promise better and more comprehensive communication. The team must feel comfortable to share and find hidden or elusive risks.

2. **Repetition**

   Information changes appears as the risk management process proceeds. Keeping identified risks current and updated means the system is focused on mitigating the most prevalent issues.

3. **Approach**

   Certain objectives require distinct approaches to best combat identification failure. One method is to identify all root causes, undesirable events and map their potential impacts. Another is to identify essential performance functions the project must enact, then find possible issues with each function or goal. Both methods work well, but the latter may be easier due to its defined scope.

4. **Documentation**

   Consistent and exhaustive documentation leads to comprehensive and reliable solutions for a specific project or future risk management team's analysis. Most communication is recorded by a project manager and data is copied, stored, and updated for continued risk prevention.

5. **Roots and Symptoms**

   It is essential in the risk identification phase to find the root causes of a risk instead of mistaking them with the symptoms. A symptom can be confused with the root cause, making it critical to discover the origin of risks and denote what are their symptoms. Other essentials of risk identification involve the analysis phase. This is where identified risks are further researched and understood.

6. **Project Definition Rating Index (PDRI)**

   PDRI is a risk assessment tool that helps develop mitigation programs for high-risk areas. It facilitates the team's risk assessment within the defined project scope, budget and deadlines. It also provides further detail of individual risks and their magnitude, represented by a score. The summation of scores is statistically compared to the project performance as a certainty level for the entire project

7. **Event Trees**

   Commonly used in reliability studies and probabilistic risk assessments, event trees represent an event followed by all factors and faults related to it. The top of the tree is the event and it is supported by any condition that may lead to that event, helping with likelihood visibility.

   Risk identification is the first step towards risk minimization and understanding. If a risk isn't discovered in the first phase, it may be found and included later due to the nature of risk identification. It is a non-stop process involving teamwork and communication.

SWOT Analysis

A useful tool for systematic risk identification is SWOT analysis. It consisting of four elements:

- Strengths - Internal organizational characteristics that can help to achieve project objectives.
- Weaknesses - Internal organizational characteristics that can prevent a project from achieving its objectives.
- Opportunities - External conditions that can help to achieve project objectives.
- Threats - External conditions that can prevent a project from achieving its objectives.

A sample SWOT analysis for launching a new all-natural iced drink.

Both opportunities and threats are risks that can have a positive or negative effect on a project, and each require risk responses.

RISK ANALYSIS

After identification of the risk parameters, the second stage is of analyzing the risk which helps to identify and manage potential problems that could undermine key business initiatives or projects.

To carry out a Risk Analysis, first identify the possible threats and then estimate the likelihood that these threats will materialize. The analysis should be objective and should be industry specific. Within the industry, the scenario based analysis may be adopted taking into consideration of possible events that may occur and its alternative ways to achieve the given target.

Risk Analysis can be complex, as it requires to draw on detailed information such as project plans, financial data, security protocols, marketing forecasts and other relevant information. However, it's an essential planning tool, and one that could save time, money, and reputations.

Use of Risk Analysis

- Risk analysis is useful in many situations:
- While planning projects, to help in anticipating and neutralizing possible problems.
- While deciding whether or not to move forward with a project.
- While improving safety and managing potential risks in the workplace.
- While preparing for events such as equipment or technology failure, theft, staff sickness, or natural disasters.
- While planning for changes in environment, such as new competitors coming into the market, or changes to government policy.
- When all the permutations-combinations of possible events/ threats are listed while analyzing the risk

parameters and the steps taken to manage such risks, the risk matrix is designed / popped-up before the decision making and implementing authority.

How to Use Risk Analysis

To carry out a risk analysis, follow these steps:

1. Identify Threats

The first step in Risk Analysis is to identify the existing and possible threats that one might face. These can come from many different sources. For instance, they could be:

- Human – Illness, death, injury, or other loss of a key individual.
- Operational – Disruption to supplies and operations, loss of access to essential assets, or failures in distribution.
- Reputational – Loss of customer or employee confidence, or damage to market reputation.
- Procedural – Failures of accountability, internal systems, or controls, or from fraud.
- Project – Going over budget, taking too long on key tasks, or experiencing issues with product or service quality.
- Financial – Business failure, stock market fluctuations, interest rate changes, or non-availability of funding.
- Technical – Advances in technology, or from technical failure.
- Natural – Weather, natural disasters, or disease.
- Political – Changes in tax, public opinion, government policy, or foreign influence.
- Structural – Dangerous chemicals, poor lighting, falling boxes, or any situation where staff, products, or technology can be harmed.

A number of different approaches can be used to carry out a thorough analysis:

- Run through a list such as the one above to see if any of these threats are relevant.
- Think about the systems, processes, or structures used and analyze risks to any part of these.
- Ask others who might have different perspectives. Ask for input from team members and consult others in the organization, or those who run similar projects.
- Tools such as SWOT Analysis and Failure Mode and Effects Analysis can also help to uncover threats, while Scenario Analysis helps to explore possible future threats.

2. Estimate Risk

Once the threats are identified, it is required to calculate both the likelihood of these threats being realized, and their possible impact.

One way of doing this is to make best estimate of the probability of the event occurring, and then to multiply this by the amount it will cost to set things on the right track. This gives a value for the risk:

$$\text{Risk Value} = \text{Probability of Event} \times \text{Cost of Event}$$

As a simple example, imagine that a risk has been identified that your rent may increase substantially.

You think that there's 80 percent chance of this happening within the next year, because your landlord has recently increased rents for other businesses. If this happens, it will cost your business an extra Rs. 500,000 over the next year.

So the risk value of the rent increase is:

0.80 (Probability of Event) x ₹ 500,000 (Cost of Event) = ₹400,000 (Risk Value)

You can also use a Risk Impact/Probability Chart to assess risk. This will help you to identify which risks you need to focus on.

RISK ASSESSMENT

After identifying the risk, the third step is to have an assessment of each of the risk in terms of quantitatively and qualitatively. In judging the quantitative aspects the tools of the statistical methods may be used. The management has to take the decision on each of the assessment of the risk so derived by the various departments of the organisations, since the raw data do not reveal the clear picture.

RISK MITIGATION

Risk mitigation is defined as taking steps to reduce adverse effects. Risk mitigation is the process by which an organization introduces specific measures to minimize or eliminate unacceptable risks associated with its operations. Risk mitigation measures can be directed towards reducing the severity of risk consequences, reducing the probability of the risk materializing, or reducing the organizations exposure to the risk.

Strategies for Risk Mitigation

There are four types of risk mitigation strategies that hold unique to Business Continuity and Disaster Recovery. It's important to develop a strategy that closely relates to and matches the profile of any company.

The risk mitigation step involves development of mitigation plans designed to manage, eliminate, or reduce risk to an acceptable level. Once a plan is implemented, it is continually monitored to assess its efficacy with the intent of revising the course-of-action if needed.

Once risks have been identified and assessed, the strategies to manage the risk fall into one or more of the following categories:

(i) Transfer Risk: Normally in projects assignments or multifaceted exercises, execution is fought with risks. Different agencies work together and these agencies take care to transfer risk in their areas to another agency which is better equipped to take care of a risk for a consideration. Here the concept of core competence curves in and whenever a particular agency, individual or a firm finds that it is dealing in an area where it does not have the core competence to deal with it seeks the help of another agency which has the specific core competence to transfer its own risk. The risk may be in the form of loss of reputation or sub quality performance and this risk is taken care of through transfer.

(ii) Tolerate Risk or Risk Retention: It is retention of the risk. It is accepting the loss when it occurs. True self insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks

that are not avoided, reduced or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible.

War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amount of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

(iii) Reduce Risk: By far the greater number of risks will belong to this category. The purpose of treatment is not necessarily to obviate the risk, but more likely to contain the risk to an acceptable level. Internal controls are actions instigated from within the organization (although their effects may be felt outside of the organization) which are designed to contain risk to acceptable levels.

Outsourcing could be an example of risk reduction if the outsourcer can demonstrate higher capability at managing or reducing risks. In this case companies outsource only some of their departmental needs. For example, a company may outsource only its software development, the manufacturing of hard goods, or customer support needs to another company, while handling the business management itself. This way, the company can concentrate more on business development without having to worry as much about the manufacturing process.

Modern software development methodologies reduce risk by developing and delivering software incrementally. Early methodologies suffered from the fact that they only delivered software in the final phase of development; any problems encountered in earlier phases meant costly rework and often jeopardized the whole project.

(iv) Avoid Risk: This method results in complete elimination of exposure to loss due to a specific risk. It can be established by either avoiding to undertake the risky project or discontinuance of an activity to avoid risk. This means that no risky projects are undertaken. Alternatively, a project may be abandoned midway to mitigate the risk while handling a project.

It is not performing an activity which could carry risk. An example would be not buying a property or business in order to not take on the liability that comes with it. Another would be not flying in order to not take the risk that the aeroplaneswere to be hijacked. 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 profits.

(v) Combine Risk: When the business faces two or three risks the overall risk is reduced by combination. This strategy is suitable mainly in the areas of financial risk. Different financial instruments say, shares and debentures are taken in a single portfolio to reduce the risk.

(vi) Sharing Risk: Insurance is a method of sharing risk for a consideration. For example by paying insurance premium the company shares the risk with companies and the insurance companies themselves share their risk by doing re-insurance.

(vii) Hedging Risk: Exposure of funds to fluctuations in foreign exchange rates, prices etc., bring about financial risks resulting in losses or gain. The downside risk is often taken care.

MAINTAINING THE RISK STRATEGY

It has already been noted that the risk environment of any organization is constantly changing and developing, and that the priorities of objectives and the consequent importance of risks will shift and change. The risk management process is therefore a dynamic and ongoing one, not an issue for a one off exercise. The process has to allow for periodic review of risks and for consequent adjustment of the control response.

Whatever option is adopted, it is important that those charged with control of the risk management process should regularly review it. One useful technique for doing this is to actively review the risks associated with each of the key organizational objectives.

Suitable tools needs to be identified to assist with the task of keeping the risk strategy up to date. A key tool is the use of ongoing Control and Risk Self Assessment (CRSA) procedures. This procedure embeds review of risk and control into the organization at every level and uses the knowledge and experience of the staff that are closest to each function to assess the movement in risks and the appropriateness of control.

CLASSIFICATION OF RISK

According to controllability: Risk may be classified according to controllability, i.e Controllable risk and Uncontrollable risk. In other words, the controllable risk is categorised as Unsystematic Risk and uncontrollable risk is categorised as Systematic Risk. The concept of controllable and uncontrollable risk may be further explained as under:

1. Systematic Risk:

- It is uncontrollable by an organisation.
- It is not predictable.
- It is of Macro nature.
- It affects a large number of organisations operating under a similar stream.
- It cannot be assessed in advance.
- It depends on the influence of external factors on an organisation which are normally uncontrollable by an organisation.
- The example of such type of risk is Interest Rate Risk, Market Risk, Purchasing Power Risk.

2. Unsystematic Risk:

- It is controllable by an organisation.
- It is predictable.
- It is Micro in nature.
- It affects the individual organisation.
- It can be assessed well in advance and risk mitigation can be made with proper planning and risk assessment techniques.
- The example of such risk is Business Risk, Liquidity Risk, Financial Risk, Credit Risk, and Operational Risk.

Systematic Risk	Unsystematic Risk
This type of risk is associated with the whole market or market segment.	This type of risk is associated with a particular industry or security.
It is uncontrollable	It is controllable.
Systematic risk affects the overall market and is difficult to predict.	Unsystematic risk affects a particular industry hence it is easy to predict.
The systematic risk is a result of external and uncontrollable variables.	The unsystematic risk is the result of internal hence may be controllable.

According to Segment wise: Project Risk Management, Operational Risk Management, Financial Risk Management, Quantitative Risk Management, Credit Risk Management,& Market Risk Management.

Classification of risks: Risk may be classified according to controllability, i.e Controllable risk and Uncontrollable risk. In other words, the controllable risk is categorised as Unsystematic Risk and uncontrollable risk is categorised as Systematic Risk. The concept of controllable and uncontrollable risk may be further explained as under:

(a) Systematic Risk:

- It is uncontrollable by an organisation.
- It is not predictable.
- It is of Macro nature.
- It affects a large number of organisations operating under a similar stream.
- It cannot be assessed in advance.
- It depends on the influence of external factors on an organisation which are normally uncontrollable by an organisation.
- The example of such type of risk is Interest Rate Risk, Market Risk, Purchasing Power Risk.

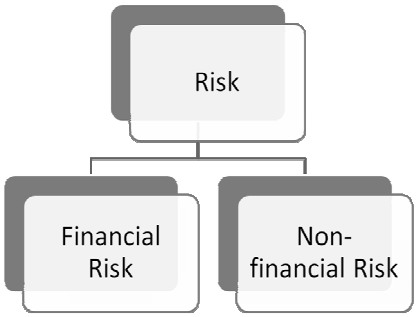
(b) Unsystematic Risk:

- It is controllable by an organisation.
- It is predictable.
- It is Micro in nature.

- It affects the individual organisation.
- It can be assessed well in advance and risk mitigation can be made with proper planning and risk assessment techniques.

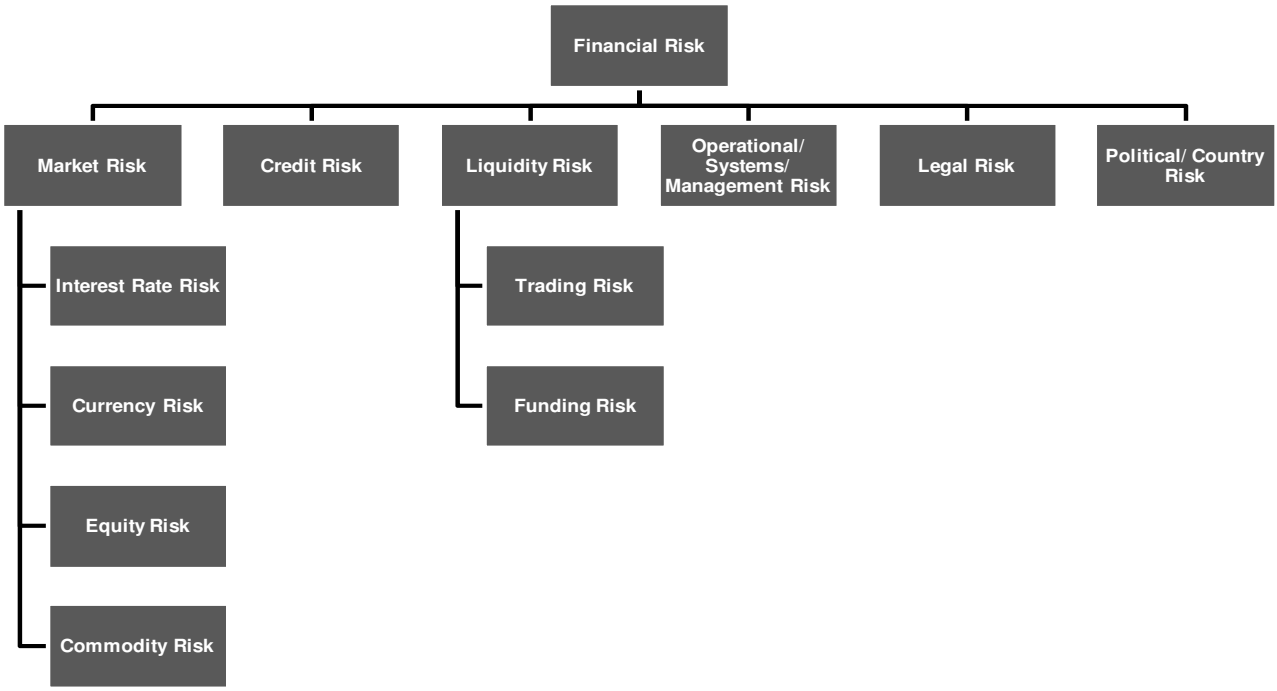
The example of such risk is Business Risk, Liquidity Risk, Financial Risk, Credit Risk, Operational Risk.

Segregation of Risk into Financial Vs. Non-financial: The risk may broadly be segregate as Financial Risk and Non-financial Risk.



Financial Risk: The risk which has some financial impact on the business entity is treated as financial risk. These risks may be market risk, credit risk Liquidity risk, Operational Risk, Legal Risk and Country Risk. The following chart depicts the various types of financial risks.

1. **Market Risk:** This type of risk is associated with market ups and down. It refers to the risk of loss arising from the change/volatility in the market prices or economic values which are the deciding factors for the pricing of the product/financial assets. The market risks may be Absolute Risk (when it can be measured in rupee/currency term) and Relative Risk (relative to bench mark index). Hence the market risk may be defined as the risk to a firm due to the adverse changes in interest rates, currency rates, equity prices and commodity prices.



(a) Interest Rate Risk: The financial assets which are connected with interest factors such as bonds/ debentures, faces the interest rate risk. Interest rate risk adversely affects value of fixed income securities. Any increase in the interest reduces the price of bonds and debts instruments in debt market and vice versa. So it can be said that the changes in the interested rates have an inverse relationship with the price of bonds.

(b) Currency Risk: The volatility in the currency rates is called the currency risk. These risks affect the firms which have international operations of business and the quantum of the risk depends on the nature and extent of transactions with the external market.

(c) Equity Risk: It means the depreciation in one's investment due to the change in market index. Beta (β) of a stock tells us the market risk of that stock and it is associated with the day-to-day fluctuations in the market.

(d) Commodity Risk: This type of risk is associated with the absolute changes in the price of the commodity. Since commodities are physical assets, hence the prices are changed on account of the demand and supply factor.

2. Credit Risk: When a counter party is unable or unwilling to fulfil their contractual obligation, the credit risk arises. This type of risk is related to the probability of default and recovery date. Its effect is measured by cost of replacing cash flow if the other party defaults. For example, in case of loan given by a bank to the borrower and the borrower defaults in making payments of the instalments or due interest on the due date, is termed as credit risk.

[2]Credit risk is most simply defined as the potential that a bank borrower or counterparty will fail to meet its obligations in accordance with agreed terms. The goal of credit risk management is to maximise a bank's risk-adjusted rate of return by maintaining credit risk exposure within acceptable parameters. Banks need to manage the credit risk inherent in the entire portfolio as well as the risk in individual credits or transactions. Banks should also consider the relationships between credit risk and other risks. The effective management of credit risk is a critical component of a comprehensive approach to risk management and essential to the long-term success of any banking organisation.

3. Liquidity Risk: The liquidity risk arises due to mis-matches in the cash flow i.e. absence of adequate funds in the market. Liquidity is altogether different from the word solvency. A firm may be in sound position as per the balance sheet, but if the current assets are not in the form of cash or near cash assets, the firm may not make payment to the creditors which adversely affect the reputation of the firm. The liquidity risk may be of two types, trading risk and funding risk.

(a) Trading Risk: It may mean the absence of the market liquidity i.e. inability to enter into derivative transactions with counter parties or make sales or purchase of securities.

(b) Funding Risk: It refers to the inability to meet the obligations by either borrowing or the sale of securities. It arises where the balance sheet of a firm contains illiquid financial assets which cannot be turned in to cash within a very short time.

4. Operational /System/ Management Risk: It arises due to inadequate systems, system capacities, system failure, obsolescence risk, management failure on account co-ordination, faulty control or human error. Some best practice against the operational risk includes clear separation of responsibilities with strong internal control and regular contingency planning.

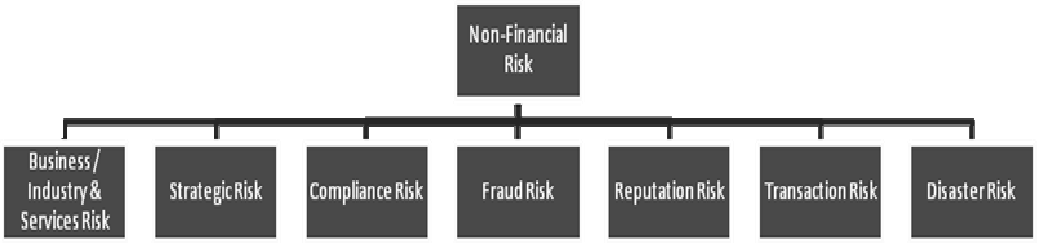
---

[2]https://www.bis.org/publ/bcbs54.htm

5. Legal Risk: This risk arises when a counter party does not have the legal or regulatory authority to engage in the transactions. It also includes the compliance and regulatory risk like insider trading, market manipulations etc.

6. Political/Country Risk: Political risk may be on account of declaration of elections in the territory, area specific risk. The Country risk arises where the firm have its business operations abroad. This risk may arise due to out-break of war between countries, imposition of the ban on the business transaction of particular commodity/product.

Non-Financial Risk: This type of risk do not have immediate financial impact on the business, but its consequence are very serious and later may have the financial impact. This type of risk may include, Business/Industry & Service Risk, Strategic Risk, Compliance Risk, Fraud Risk, Reputation Risk, Transaction risk, Disaster Risk.



1. **Business/ Industry & Services Risk:** Business risks implies uncertainty in profits or danger of loss and the events that could pose a risk due to some unforeseen events in future, which causes business to fail. Business risk refers to the possibility of inadequate profits or even losses due to uncertainties e.g., changes in tastes, preferences of consumers, strikes, increased competition, change in government policy, obsolescence etc .Every business organization contains various risk elements while doing the business. Such type of risk may also arise due to business dynamics, competition risks affecting tariff prices, customer relation risk etc.
2. **Strategic Risk:** Unsuccessful business plan since its inception may lead to strategic risk. For example, strategic risk might arise from making poor business decisions, from the substandard execution of decisions, from inadequate resource allocation, or from a failure to respond well to changes in the business environment.
3. **Compliance Risk:** This risk arises on account of non-compliance of breaches of laws/ regulations which the entity is supposed to adhere. It may result to deterioration to public reputation, penalty and penal provisions.
4. **Fraud Risk:** Fraud is perpetrated through the abuse of systems, controls, procedures and working practices. It may be performed by the outsider or even from the insider. Often the most trusted employee attempt to do this. Fraud may not be detected immediately, but is still usually discovered by chance, but the detection should be proactive rather than reactive.
5. **Reputation Risk:** This type of risk arises from the negative public opinion. Such type of risk may arise from the failure to assess and control compliance risk and can result in harm to existing or potential business relationships.
6. **Transaction Risk:** Transaction risk arises due to the failure or inadequacy of internal system, information channels, employees integrity or operating processes.

7. **Disaster Risk:** On account of natural calamities like floods, fire, earthquake, man-made risks due to extensive exploitation of land for mines activity, land escalation, risk of failure of disaster management plans formulated by the company etc.

Advantages of Risk Management

Risk management plays vital role in strategic planning. It is an integral part of project management. An effective risk management focuses on identifying and assessing possible risks. The advantages of having risk management are as under:

- Risk Management always results in significant cost savings and prevents wastage of time and effort in firefighting. It develops a Robust contingency planning.
- It can help plan and prepare for the opportunities that unravel during the course of a project or business.
- Risk Management improves strategic and business planning. It reduces costs by limiting legal action or preventing breakages.
- It establishes improved reliability among the stake holders leading to an enhanced reputation.
- Sound Risk Management practices reassure key stakeholders throughout the organization.
- Risk Management strongly favours for a focused internal audit programme.

RISK MANAGEMENT AND CORPORATE GOVERNANCE

Corporate governance concerns the relationships among the management, board of directors, controlling shareholders, minority shareholders, and other stakeholders. Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital. Incorporating risk management in corporate governance of an organisation is very important.

Risk management and corporate governance principles are strongly interrelated. An organization implements strategies in order to reach their goals. Each strategy has related risks that must be managed in order to meet these goals. Following strong corporate governance principles that focus on risk management allows organizations to reach their goals.

Risk governance includes the skills, infrastructure (i.e., organization structure, controls and information systems), and culture deployed as directors exercise their oversight. Good risk governance provides clearly defined accountability, authority, and communication/reporting mechanisms.

A process for risk management cannot be initiated unless there is a perception and knowledge of risk surrounding the business. Businesses evolve and are exposed to change dynamics of the external environment. Hence it is important to have the risk oversight function, as one of the areas of responsibility of the board of directors of any enterprise. The Board may form a separate committee to support the board function depending on the complexities of the business enterprise and the complexities associated with its transactions and events. It would also depend on the size and extent of delegation of responsibilities by the board of directors. While everyone understands that risk is all pervasive, risk management must be voiced from the top and the tone should indicate a serious approach by the top management. The board shall have to identify the extent and type of risks it faces and the planning necessary to manage and mitigate the same for ensuring growth for the benefit of all the stakeholders. Therefore, the Board has to define a risk philosophy and the extent to which it is willing to accept any consequence of taking of risks by the organization and its functionaries in its day to day functioning.

Board members need to have a good understanding of risk management, even when they lack expertise in that area. Boards may lean on the expertise of outside consultants to help them review company risk management systems and analyze business specific risks. Boards should perform a formal review of risk management systems, at least once in a year.

As part of the annual review, boards should review risk oversight policies and procedures at the board and committee levels and assess risk on an ongoing basis. It's helpful to familiarize the board with expectations within the industry or regulatory bodies that the organization operates in by arranging for a formal presentation on risk management best practices. The annual risk management review should include communication from management about lessons learned from past mistakes. Risk oversight is the responsibility of the entire Board and the same can be achieved through a review mechanism which inter-alia could include:

1. Developing policies and procedures around risk those are consistent with the organization's strategy and risk appetite.
2. Taking steps to foster risk awareness.
3. Encourage an organizational culture of risk adjusting awareness
4. Maintenance of a Risk Register
5. A compliance certificate on the identification of risks and establishment of mitigation measures.

The updated G20/OECD Principles of Corporate Governance provides on considering the establishment of specialized board committees in areas such as remuneration, audit and risk management. The sixth principle which deals with the responsibilities of the board provides-

- The board should fulfill certain key functions, including - Reviewing and guiding corporate strategy, major plans of action, risk management policies and procedures, annual budgets and business plans; setting performance objectives; monitoring implementation and corporate performance; and overseeing major capital expenditures, acquisitions and divestitures.
- Ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.

The Board should demonstrate a leadership role to ensure that an effective means of risk oversight is in place. Ensuring the integrity of the essential reporting and monitoring systems will require the board to set and enforce clear lines of responsibility and accountability throughout the organisation. The board will also need to ensure that there is appropriate oversight by senior management. Normally, this includes the establishment of an internal audit system directly reporting to the board. It is considered good practice for the internal auditors to report to an independent audit committee of the board or an equivalent body which is also responsible for managing the relationship with the external auditor, thereby allowing a co-ordinated response by the board. It should also be regarded as good practice for this committee, or equivalent body, to review and report to the board the most critical accounting policies which are the basis for financial reports. However, the board should retain final responsibility for oversight of the company's risk management system and for ensuring the integrity of the reporting systems. Some jurisdictions have provided for the chair of the board to report on the internal control process. Companies with large or complex risks (financial and non-financial), not only in the financial sector, should consider introducing similar reporting systems, including direct reporting to the board, with regard to risk management.

The ICGN Global Governance Principles which describe the responsibilities of boards and shareholders respectively and aim to enhance dialogue between the two parties also provides that it is the responsibility of the board to oversee the implementation of effective risk management and proactively review the risk management approach and policies annually or with any significant business change. It provides that one of the major roles of the board is risk oversight.

Principles on Risk oversight provides for-

Proactive oversight: The board should proactively oversee, review and approve the approach to risk management regularly or with any significant business change and satisfy itself that the approach is functioning effectively. Strategy and risk are inseparable and should permeate all board discussions and, as such, the board should consider range of plausible outcomes that could result from its decision-making and actions needed to manage those outcomes.

- Comprehensive approach: The board should adopt a comprehensive approach to the oversight of risk which includes all material aspects of risk including financial, strategic, operational, environmental, and social risks (including political and legal ramifications of such risks), as well as any reputational consequences.
- Risk culture: The board should lead by example and foster an effective risk culture that encourages openness and constructive challenge of judgment's and assumptions. The company's culture with regard to risk and the process by which issues are escalated and de-escalated withinthe company should be evaluated at intervals as appropriate to the situation.
- Dynamic process: The board should ensure that risk is appropriately reflected in the company's strategy and capital allocation. Risk should be managed accordingly in a rational, appropriately independent, dynamic and forward-looking way. This process of managing risks should be continual and include consideration of a range of plausible impacts.
- Risk committee: While ultimate responsibility for a company's risk management approach rests with the full board, having a risk committee(be it a stand-alone risk committee, a combined risk committee with nomination and governance, strategy, audit or other) can be an effective mechanism to bring the transparency, focus and independent judgment needed to oversee the company's risk management approach.

STANDARD ON IMPLEMENTATION OF RISK MANAGEMENT

ISO 31000:2009: International Organization for Standardization (ISO)) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. The main task of technical committees is to prepare International Standards.

Every activity of an organization involves risk. Organizations manage risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. This International Standard describes this systematic and logical process in detail. Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

ISO 31000 published on the 13th of November 2009, provides a standard on the implementation of risk management. ISO 31000 seeks to provide a universally recognised paradigm for practitioners and companies employing risk management processes. Accordingly, the general scope of ISO 31000 - is not developed for a particular industry group, management system or subject matter field in mind, rather it provides best practice structure and guidance to all operations concerned with risk management. The scope of this approach to risk management is to enable all strategic, management and operational tasks of an organization throughout projects, functions, and processes be aligned to a common set of risk management objectives.

ISO 31000 contains 11 key principles that position risk management as a fundamental process in the success of the organization.

ISO 31000 is designed to help organizations:

- Increase the likelihood of achieving objectives
- Encourage proactive management
- Be aware of the need to identify and treat risk throughout the organization
- Improve the identification of opportunities and threats
- Comply with relevant legal and regulatory requirements and international norms
- Improve financial reporting
- Improve governance
- Improve stakeholder confidence and trust
- Establish a reliable basis for decision making and planning
- Improve controls
- Effectively allocate and use resources for risk treatment
- Improve operational effectiveness and efficiency
- Enhance health and safety performance, as well as environmental protection
- Improve loss prevention and incident management
- Minimize losses
- Improve organizational learning
- Improve organizational resilience.

ISO 31000 provides that risk oversight is a key duty of the board, as failure to manage risk can threaten the existence of the entity being governed. Countries are exploring how to improve the overall risk management framework including examining the responsibilities of different board committees.

FRAUDS RISK MANAGEMENT

Fraud is a deliberate action to deceive another person with the intention of gaining some things. Fraud can loosely be defined as “any behavior by which one person intends to gain a dishonest advantage over

another". In other words, fraud is an act or omission which is intended to cause wrongful gain to one person and wrongful loss to the other, either by way of concealment of facts or otherwise.

Section 25 of the Indian Penal Code, 1860 defines the word, “Fraudulently", which means, a person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

Further according to section 17 of the Indian Contract Act, 1872, ‘fraud’ means and includes any of the following acts committed by a party to a contract, or with his connivance (intentional active or passive acquiescence), or by his agent with intent to deceive or to induce a person to enter into a contract.

1. The suggestion that a fact is true when it is not true and the persons making the suggestion does not believe it to be true;
2. The active concealment of a fact by a person having knowledge or belief of the fact;
3. A promise made without any intention of performing it;
4. Any other act fitted to deceive;
5. Any such act or omission as the law specially declares to be fraudulent.

The Companies Act 2013 has also explained fraud. Explantion to Section 447 defines “fraud”, which reads as under:

“fraud” in relation to affairs of a company or anybody corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss.

A definition of fraud has been suggested in the context of electronic banking in the Report of RBI Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, which reads as under: “A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank”.

For prevention of the fraud, there should be in existence a robust internal check and control systems. For example in banking there is a concept of ‘maker’ and ‘checker’. The day today transactions are entered by the maker and another person validates the transactions. So it is a self balancing system. Further the internal/concurrent audit also helps in early detection of the frauds.

The management should be pro-active in fraud related matter. A fraud is usually not detected until and unless it is unearthed. Fraud Risk Management Policy be incorporated, aligned to its internal control and risk management. Such policy/plan protects the company from any kind of uncertain happening which leads the company to a huge loss or damage (brand reputation, financial loss, assets).

The Fraud Risk Management Policy will help to strengthen the existing anti-fraud controls by raising the awareness across the Company and (i) Promote an open and transparent communication culture (ii) Promote zero tolerance to fraud/misconduct (iii) Encourage employees to report suspicious cases of fraud/misconduct. (iv) Spread awareness amongst employees and educate them on risks faced by the company.

Such a policy may include the following:

- **Defining fraud:** This shall cover activities which the company would consider as fraudulent.
- **Defining Role & responsibilities:** The policy may define the responsibilities of the officers who shall be involved in effective prevention, detection, monitoring & investigation of fraud. The company may also consider constituting a committee or operational structure that shall ensure an effective implementation of anti-fraud strategy of the company. This shall ensure effective investigation in fraud cases and prompt as well as accurate reporting of fraud cases to appropriate regulatory and law enforcement authorities.
- **Communication channel:** Encourage employees to report suspicious cases of fraud/misconduct. Any person with knowledge of suspected or confirmed incident of fraud/misconduct must report the case immediately through effective and efficient communication channel or mechanism.
- **Disciplinary action:** After due investigations disciplinary action against the fraudster may be considered as per the company's policy.
- **Reviewing the policy:** The employees should educate their team members on the importance of complying with Company's policies & procedures and identifying/ reporting of suspicious activity, where a situation arises. Based on the developments, the policy should be reviewed on periodical basis.

Reporting of fraud under Companies Act 2013

The Companies Act, 2013 has introduced many new reporting requirements for the statutory auditors of companies. One of these requirements is given under the Section 143(12) of the Companies Act, 2013 which requires the statutory auditors or cost accountant or company secretary in practice to report to the Central Government about the fraud/suspected fraud committed against the company by the officers or employees of the company.

Sub-section 12 of Section 143 of the Companies Act, 2013 reads as under:

"Notwithstanding anything contained in this section, if an auditor of a company in the course of the performance of his duties as auditor, has reason to believe that an offence of fraud involving such amount or amounts as may be prescribed, is being or has been committed in the company by its officers or employees, the auditor shall report the matter to the Central Government within such time and in such manner as may be prescribed:

Provided that in case of a fraud involving lesser than the specified amount, the auditor shall report the matter to the audit committee constituted under section 177 or to the Board in other cases within such time and in such manner as may be prescribed:

Provided further that the companies, whose auditors have reported frauds under this sub-section to the audit committee or the Board but not reported to the Central Government, shall disclose the details about such frauds in the Board's report in such manner as may be prescribed."

Sub-section 14 of Section 143 further provides that the provisions of this section shall mutatis mutandis apply to—

(a) the cost accountant conducting cost audit under section 148; or

(b) the company secretary in practice conducting secretarial audit under section 204.

Consequence of non-compliance: Sub-section 15 of section 143 states that if any auditor, cost accountant or company secretary in practice do not comply with the provisions of sub-section (12), he shall be punishable with fine which shall not be less than one lakh rupees but which may extend to twenty-five lakh rupees.

Section 143(12) includes only fraud by officers or employees of the company and does not include fraud by third parties such as vendors and customers.

Secretarial Audit

Secretarial Audit is a process to check compliance with the provisions of all applicable laws and rules/regulations/procedures; **adherence to good governance practices** with regard to the systems and processes of seeking and obtaining approvals of the Board and/or shareholders, as may be necessary, for the business and activities of the company, carrying out activities in a lawful manner and the maintenance of minutes and records relating to such approvals or decisions and implementation.

Section 204 of Companies Act 2013 provides for Secretarial audit for bigger companies.

(1) Every listed company and a company belonging to other class of companies as may be prescribed shall annex with its Board's report made in terms of sub-section (3) of section 134, a secretarial audit report, given by a company secretary in practice, in such form as may be prescribed. Rule 9 of Companies (Appointment and Remuneration of Managing Personnel) Rules, 2014 provides that for the purposes of sub-section (1) of section 204, the other class of companies shall be as under-

- every public company having a paid-up share capital of fifty crore rupees or more; or
- every public company having a turnover of two hundred fifty crore rupees or more.

(2) It shall be the duty of the company to give all assistance and facilities to the company secretary in practice, for auditing the secretarial and related records of the company.

(3) The Board of Directors, in their report made in terms of sub-section (3) of section 134, shall explain in full any qualification or observation or other remarks made by the company secretary in practice in his report under sub-section (1).

(4) If a company or any officer of the company or the company secretary in practice, contravenes the provisions of this section, the company, every officer of the company or the company secretary in practice, who is in default, shall be punishable with fine which shall not be less than one lakh rupees but which may extend to five lakh rupees.

REPUTATION RISK MANAGEMENT

The Reserve Bank of India in its Master Circular number RBI/2015-16/85 DBR.No.BP.BC.4./21.06.001/2015-16 July 1, 2015 has defined the Reputation Risk as the risk arising from negative perception on the part of customers, counterparties, shareholders, investors, debt-holders, market analysts, other relevant parties or regulators that can adversely affect a bank's ability to maintain existing, or establish new, business relationships and continued access to sources of funding (eg through the interbank or securitization markets). Reputational risk is multidimensional and reflects the perception of other market participants. Furthermore, it exists throughout the organisation and exposure to reputational risk is essentially a function of the adequacy of the bank's internal risk management processes, as well as the manner and efficiency with which management responds to external influences on bank-related transactions.

Loss of Reputation has long lasting damages:

- It destroys the Brand Value
- Steep downtrend in share value.
- Ruined of Strategic Relationship

- Regulatory relationship is damaged which leads to stringent norms.
- Recruitment to fetch qualified staff as well the retention of the old employees becomes difficult.

For managing the reputation risk, the following principles are worth noting:

- Integration of risk while formulating business strategy.
- Effective board oversight.
- Image building through effective communication.
- Promoting compliance culture to have good governance.
- Persistently following up the Corporate Values.
- Due care, interaction and feedback from the stakeholders.
- Strong internal checks and controls
- Peer review and evaluating the company's performance.
- Quality report/ newsletter publications
- Cultural alignments

RESPONSIBILITY OF RISK MANAGEMENT

Section 134(3) (n) of the Companies Act, 2013 provides that 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.

SEBI (LODR) Regulations, 2015 also provides that company shall lay down procedures to inform Board members about the risk assessment and minimization procedures. The Board shall be responsible for framing, implementing and monitoring the risk management plan for the company.

The Risk Management Plan must include all elements of risks. The traditional elements of potential likelihood and potential consequences of an event must be combined with other factors like the timing of the risks, the correlation of the possibility of an event occurring with others, and the confidence in risk estimates.

Risk management policies should reflect the company's risk profile and should clearly describe all elements of the risk management and internal control system and any internal audit function. A company's risk management policies should clearly describe the roles and accountabilities of the board, audit committee, or other appropriate board committee, management and any internal audit function.

A company should have identified Chief Risk Officer manned by an individual with the vision and the diplomatic skills to forge a new approach. He may be supported by "risk groups" to oversee the initial assessment work and to continue the work till it is completed.

An integrated approach to risk management deals with various risks as they affect organizational objectives and limitations. The aim must be to develop a culture of risk awareness and understanding. This helps better decision making in day-to-day work by all employees.

1. Risk Management Committee:

Regulation 21 of SEBI (LODR) Regulations, 2015, requires that every listed company should have a Risk Management Committee. It reads as under:

(1) The board of directors shall constitute a Risk Management Committee.

(2) The majority of members of Risk Management Committee shall consist of members of the board of directors.

(3) The Chairperson of the Risk management committee shall be a member of the board of directors and senior executives of the listed entity may be members of the committee.

[3][(3A) The risk management committee shall meet at least once in a year.]

(4) The board of directors shall define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit [4][such function shall specifically cover cyber security].

(5) The provisions of this regulation shall be applicable to top [5][500] listed entities, determined on the basis of market capitalisation, as at the end of the immediate previous financial year.

The terms of reference of the Risk Management Committee inter-alia may include the following:

- Framing of Risk Management and Policy
- Overseeing implementation of Risk Management and Policy
- Monitoring of Risk Management and Policy
- Validating the process of Risk Management
- Validating the procedure for Risk Mitigation
- Periodically reviewing and evaluating the Risk Management Policy andpractices with respect to risk assessment and risk management processes.
- Continually obtaining reasonable assurance from management that allknown and emerging risks have been identified and mitigated or managed.
- Performing such other functions as may be necessary or appropriate forthe performance of its oversight function.

Role of Company Secretary in Risk Management

The company secretaries are governance professionals whose role is to enforce a compliance framework to safeguard the integrity of the organization and to promote high standards of ethical behavior. He has a significant role in assisting the board of the organization to achieve its vision and strategy. The activities of the governance professional encompass legal and regulatory duties and obligations and additional responsibilities assigned by the employer. However, in essence, the functions of a Governance Professional include:

- Advising on best practice in governance, risk management and compliance.
- Championing the compliance framework to safeguard organizational integrity.

---

[3] Inserted by the SEBI (Listing Obligations and Disclosure Requirements) (Amendment) Regulations, 2018, w.e.f. **1-4-2019**.

[4]Inserted by the SEBI (Listing Obligations and Disclosure Requirements) (Amendment) Regulations, 2018, w.e.f. **1-4-2019**.

[5]Substituted for "100" the SEBI (Listing Obligations and Disclosure Requirements) (Amendment) Regulations, 2018, w.e.f. **1-4-2019**.

- Promoting and acting as a ‘sounding board’ on standards of ethical and corporate behavior.
- Balancing the interests of the Board or governing body, management and other stakeholders.

Section 205 (1) of the Companies Act, 2013 deals with the functions of the company secretary. It provides that the functions of the company secretary shall include,—

(a) to report to the Board about compliance with the provisions of this Act, the rules made thereunder and other laws applicable to the company;

(b) to ensure that the company complies with the applicable secretarial standards;

(c) to discharge such other duties as may be prescribed.

Explanation.—For the purpose of this section, the expression "secretarial standards" means secretarial standards issued by the Institute of Company Secretaries of India constituted under section 3 of the Company Secretaries Act, 1980 (56 of 1980) and approved by the Central Government.

Rule 10 of the Companies (Appointment & Remuneration of Managerial Personnel) Rules 2014 specifies that the duties of Company Secretary shall also discharge, the following duties, namely:-

(1) to provide to the directors of the company, collectively and individually, such guidance as they may require, with regard to their duties, responsibilities and powers;

(2) to facilitate the convening of meetings and attend Board, committee and general meetings and maintain the minutes of these meetings;

(3) to obtain approvals from the Board, general meeting, the government and such other authorities as required under the provisions of the Act;

(4) to represent before various regulators, and other authorities under the Act in connection with discharge of various duties under the Act;

(5) to assist the Board in the conduct of the affairs of the company;

(6) to assist and advise the Board in ensuring good corporate governance and in complying with the corporate governance requirements and best practices; and

(7) to discharge such other duties as have been specified under the Act or rules; and

(8) such other duties as may be assigned by the Board from time to time.

The listing agreement also provides for the establishment of the Risk Management Committee as per Regulations. Since it is the part of the Corporate Governance norms and non-compliance of the same is to be reported by the Company Secretary.

In terms of Section 203(1)(ii), a Company Secretary is a Key Managerial Person. Hence being a top level officer and board confidante, a Company Secretary can pay a role in ensuring that a sound Enterprise wide Risk Management [ERM] which is effective throughout the company is in place. The board of directors may have a risk management sub-committee assisted by a Risk Management Officer. As an advisor to the board in ensuring good governance, a Company Secretary shall ensure that there is an Integrated Framework on which a strong system of internal control is built. Such a Framework will become a model for discussing and evaluating risk management efforts in the organization. Risk and control consciousness should spread throughout the organization. A Company Secretary can ensure that this happens so that the risk factor will come into consideration at the every stage of formulation of a strategy. It will also create awareness about inter-relationships of risks across business units and at every level of the organization. A Company Secretary

can ensure that the following questions [an illustrative list] are effectively addressed at the board level:

- What is the organization's risk management philosophy?
- Is that philosophy clearly understood by all personnel?
- What are the relationships among ERM, performance, and value?
- How is ERM integrated within organizational initiatives?
- What is the desired risk culture of the organization and at what point has its risk appetite been set?
- What strategic objectives have been set for the organization and what strategies have been or will be implemented to achieve those objectives?
- What related operational objectives have been set to add and preserve value?
- What internal and external factors and events might positively or negatively impact the organization's ability to implement its strategies and achieve its objectives?
- What is the organization's level of risk tolerance?
- Is the chosen risk response appropriate for and in line with the risk tolerance level?
- Are appropriate control activities (i.e., approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, segregation of duties) in place at every level throughout the organization?
- Is communication effective — from the top down, across, and from the bottom up the organization?
- How effective is the process currently in place for exchanging information with external parties?
- What is the process for assessing the presence and performance quality of all eight ERM components over time?

RISK GOVERNANCE

There is an enhanced realisation that the risk governance demands a holistic approach and that risk appreciation should start at the top. A strengthened management information system (MIS) supported by robust information technology platform is a necessary pre-requisite for enhancing Board efficiency in oversight and decision making. Similarly, augmented skill sets and experience at the level of independent directors would go a long way in enhancing the Board capacity. Strong MIS facilitates risk reporting to the boards in an effective and comprehensive manner, which in turn enhances transparency and causes informed decision taking. Robust information technology systems are a necessary condition for supporting the MIS framework as the quality of risk information that the Boards and the top management receive depends largely on the quality and robustness of the information technology systems.

In addition to prescribing the risk appetite for the company, the board also needs to lay down appropriate risk strategy and ensure that this is institutionalised throughout the organization. This would entail, aligning risk management processes with the overall business strategy, clearly defining the roles and responsibilities down the hierarchy, establishing accountability and reinforcing change with communication and training. The Board and the senior management oversight must be supplemented with effective leadership by the Chairman and the chief executive officer (CEO), and informed non-executive directors. The Boards must get much more intimately involved in risk matters and have a firmer understanding of the key risks faced by the business.

Effective risk governance also demands that each director is aware of the breadth of risks faced by the

company. Directors add value to the Board when they have financial expertise, are aware of risk fundamentals and techniques, and are able to manage dynamics with executives.

Here, the risk management committees have an important role to play in the overall risk governance framework. Apart from monitoring the company's strategic-risk profile on an on-going basis, such committees would also be responsible for defining the company's overall risk appetite; approving major transactions above a company's risk threshold, and; establishing limit structures and risk policies for use within individual businesses.

Presence of a Chief Risk Officer (CRO) is expected to strengthen the risk management framework. However, independence of the CRO, with necessary stature to influence decisions, would be a critical element in ensuring the effectiveness of the post in risk management process as also the strategic risk management related decisions. The CRO must report directly to the CEO and the Board and be responsible for all risks, risk management and control functions. Another important requirement is integrating risk with business strategy and compensation. Risk – and return on risk – need to be core component of any performance measure, and should be explicitly factored into incentive and compensation schemes. Compensation must be formally aligned with actual performance, such as through adding more rigorous risk-based measures to scorecards. This would also involve moving to longer vesting periods, and increasing deferred compensation.

The fragmented organisation of risk data into separate silos slows down risk management process and hinders the capability to respond to new regulatory requirements. The financial crisis has pushed both supervisors and market players to move towards an integrated approach to risk data that brings down the silos in organisation. Only by integrating data models, processes and methodologies can a bank achieve higher performance in terms of data quality.

The risk management systems must take into account the technical limitations of risk models, such as Value at Risk (VaR). Stress testing and scenario analysis need to be established as truly effective management tools and should be integrated and standardized across business lines, types of risk and asset classes.

The risk profile of a company may be represented through a Risk Register, a suggestive template of which is illustrated below:

Sl.No	**Risk Area**	**Key risks**	**Root cause**	**Mitigation measures**
1.	Business Risk	Decreasing market share	Lack of innovation, market survey etc.,	Keeping a vigil on latest developments and continuous monitoring
2.	Financial risk	Leveraging capital structure and the cash flows	Inability to assess the appropriate funding requirements	Adoptiong a Resource planning policy
3.	Regulatory & Compliance Risk	Non-compliance of applicable laws	Not keeping abreast of the latest changes in the Regulatory environment	Knowledge updation& maintenance of a robust compliance check list

Risk Matrix

Risk Matrix is a matrix that is used during Risk & Control Self Assessment (RCSA)activity to define the various levels of risk at each stage, activity, process and sub process.

Risk Matrix comprises of:

1) Impact analysis
2) Likelihood
3) Operating Effectiveness
4) Design Effectiveness

Ratings are assigned to all above categories, pre and post control environment. Based on the ratings a Gross/Inherent Risk Level and Residual Risk level is determined (HIGH/MEDIUM/LOW), respectively.

In the event where Residual Risk level is HIGH and/ or a particular control environment is weak, these are mitigated with additional controls.

The Inherent and Residual Risks follow the RED-AMBER-GREEN color coding mapped to HIGH-MEDIUM-LOW Risks, respectively.

Model risk management policy

A risk management policy serves two main purposes: to identify, reduce and prevent undesirable incidents or outcomes and to review past incidents and implement changes to prevent or reduce future incidents. A risk management policy should include the following sections:

- Risk management and internal control objectives (governance)
- Statement of the attitude of the organisation to risk (risk strategy)
- Description of the risk aware culture or control environment
- Level and nature of risk that is acceptable (risk appetite)
- Risk management organisation and arrangements (risk architecture)
- Details of procedures for risk recognition and ranking (risk assessment)
- List of documentation for analysing and reporting risk (risk protocols)
- Risk mitigation requirements and control mechanisms (risk response)
- Allocation of risk management roles and responsibilities
- Risk management training topics and priorities
- Criteria for monitoring and benchmarking of risks
- Allocation of appropriate resources to risk management
- Risk activities and risk priorities for the coming year

GLOSSARY OF TECHNICAL WORDS

- **Risk Management:** Risk management is the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities..
- **SWOT:** SWOT analysis is a framework used to evaluate a company's competitive position by identifying its strengths, weaknesses, opportunities and threats. Specifically, SWOT analysis is a foundational assessment model that measures what an organization can and cannot do, and its potential opportunities and threats.
- **Fraud Risk** : A fraud risk assessment is a tool used by management to identify and understand risks to its business and weaknesses in controls that present a fraud risk to the organization
- **Secretarial Audit :** Secretarial Audit is an audit to check compliance of various legislations including the Companies Act and other corporate and economic laws applicable to the company. It provides necessary comfort to the management, regulators and the stakeholders, as to the statutory compliance, good governance and the existence of proper and adequate systems and processes..

LESSON ROUND UP

- Risk is inherent in the business. Different types of risk exist in the business according to the nature of the business and they are to be controlled and managed.
- In traditional concept the natural calamities like fire, earthquake, flood, etc were only treated as risk and keeping the safe guard equipments etc were assumed to have mitigated the risk. But due to rapid changes, the various types of risks have emerged viz. Compliance risk, legal risk, country risk, operational risk.
- Risk may be controllable or uncontrollable. In other words, the systematic risk which stands at macro level is not controllable, but the unsystematic risk which is at micro level is controllable with the risk mitigation techniques.
- The risk may broadly be segregate as Financial Risk and Non-financial Risk.
- Financial Risk includes market risk, credit risk Liquidity risk, Operational Risk, Legal Risk and Country Risk. Non-financial risk does not have immediate financial impact on the business, but its consequence is serious.
- Non-Financial Risk do not have immediate financial impact on the business, but its consequence are very serious and later may have the financial impact. This type of risk may include, Business/Industry & Service Risk, Strategic Risk, Compliance Risk, Fraud Risk, Reputation Risk, Transaction risk, Disaster Risk.
- To mitigate the various types of risks, which a business entity faces, a proper risk management process should be in force. It is a continuous process and is applied across the organisation. It is basically the identification of risk areas, assessment thereof, evaluating the impact of such risk, develop the risk mitigation techniques, establishing the sound internal control process and continuous monitoring thereof, setting of standards for each process and abnormal variances to be vetted.
- Risk management plays vital role in strategic planning. It is an integral part of project management. An effective risk management focuses on identifying and assessing possible risks.
- The process of risk management consists of the following logical and sequential steps, Identification of risk, Assessment of risk, Analysing and evaluating the risk, Handling of risk (Risk may be handled through the Risk Avoidance, Risk Retention/ absorption, Risk Reduction, Risk Transfer) and Implementation of risk management decision.

- ISO 31000 published as a standard on the 13th of November 2009, provides a standard on the implementation of risk management. ISO 31000 contains 11 key principles that position risk management as a fundamental process in the success of the organization.
- Fraud has been defined as, 'A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank".
- Reputation Risk as the risk arising from negative perception on the part of customers, counterparties, shareholders, investors, debt-holders, market analysts, other relevant parties or regulators that can adversely affect a bank's ability to maintain existing, or establish new, business relationships and continued access to sources of funding (e.g. through the interbank or securitisation markets).
- SEBI (LODR) Regulations, requires that every listed company should have a Risk Management Committee.
- Secretarial Audit is a process to check compliance with the provisions of all applicable laws and rules/regulations/procedures; adherence to good governance practices with regard to the systems and processes of seeking and obtaining approvals of the Board and/or shareholders, as may be necessary, for the business and activities of the company, carrying out activities in a lawful manner and the maintenance of minutes and records relating to such approvals or decisions and implementation.
- Secretarial Audit helps the companies to build their corporate image. Secretarial Audit facilitates monitoring compliances with the requirements of law through a formal compliance management programme which can produce positive results to the stakeholders of a company.

SELF TEST QUESTIONS

1. What do you mean by Risk Management?
2. Discuss about the Controllable and Un-controllable Risks.
3. Elaborate on different types of Financial and Non-financial Risk.
4. Describe the Risk Management Process and its advantages?
5. What do you understand by Fraud risk? What strategy can adopt to mitigate such a risk?
6. Write short notes on:

a. ISO 31000:2009 relating to the Risk Management.

b. Fraud Risk Management.

c. Reputation Risk Management.

d. Secretarial Audit and Role of Company Secretary.

e. Reporting of fraud by Statutory Auditor.