CHAPTER I
INTRODUCTION TO THE STUDY

1.1 Introduction

The word ‘risk’ is derived from the Italian word ‘risicare’, which means ‘to run into danger’ (Douglas, Wildavsky, 1982). Generally, risk is considered to be synonymous with uncertainty. In the early 1920s, Frank Knight introduced an important distinction between the two concepts. He defines ‘risk’ as variability that can be quantified in terms of probabilities, while immeasurable variability is best thought of as ‘uncertainty’. In this context, Miller (1992) states that uncertainty reduces the predictability and therefore increases risk. Organisations are always aiming to balance these risks and reward ratio, but the implications of not managing these risks seems to be increasing exponentially. Crouhy et. al. (2006) define risk as “The volatility of returns leading to unexpected losses, with higher volatility indicating higher risk”. The essence of risk is the uncertainty of outcome (whether positive or negative). The term exposure refers to the combination of the probability of these potential events and magnitude of their impact. Risk is the possibility of negative deviation of actual results from expected results or company objectives.

1.2 Definition of Risk

Harold Skipper “No universally accepted definition of risk exists. Risk is commonly used to refer to insured items, to causes of loss and to the chance of loss. Statisticians and economists associate risk with variability”. A situation is risky if a range of outcomes exist and actual outcome is not known in advance.
Risk is defined in the Oxford dictionary (1989) as ‘possibility of meeting danger, or suffering harm, loss etc.; or a person or thing insured or representing a source of risk’. To take an action involving a risk implies the inability to fully control for possible adverse outcomes consequent to that action (Moore, 1983). The word ‘risk’ entered the English Language from France in the 1830s, for use in connection with insurance transactions. Prior to this, the word ‘hazard’ had the closest meaning.

Risk is defined as the “variation in outcomes around an expectation”. In other words, we expect certain things to occur or not occur and ‘risk’ refers to how life differs from what we expect.

Collier and Agyei-Ampomah (2006) note the following. Risk as a hazard or threat (downside risk): this is what managers often mean when talking about risk. It is referred to as a negative event or threat to the organization. Managing risk in this context means using management techniques to reduce the probability or impact of the negative event without undue cost.

1.3 Risk Management

The term Risk management emerged in the mid-1950s. It is not clear whether this term arose first from the academic or the practitioner worlds. Traditional risk management can be defined as an interdisciplinary function that is concerned with the management of (largely) insurable risks. Today Risk management is: A process of understanding and managing the risks that the entity is inevitably subject to in attempting to achieve its corporate objectives. Risk Management can be adapted to meet the needs of each business. It can be used to educate staff, and to give them a deeper understanding of the corporate risks. This
turns managers into business people, and makes the business more effective.

Risk Management is defined as “Coordinated activities to direct and control an organisation with regard to risk” (ISO Guide 73 BS 31100).

According to Institute of Risk Management, “Risk Management is a process which aims to help organisations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure”.

1.4 History of Risk Management

The word hazard, another term integral to discussions of risk management, comes from a game of chance invented at a castle named Hasart, in Palestine, while it was under siege (Oxford English Dictionary, 1989).

Risk management is not something new. One of the earliest examples of risk management appears in the Old Testament of the Bible. An Egyptian Pharaoh had a dream which Joseph interpreted as seven years of plenty to be followed by seven years of famine. To deal with this risk, the Pharaoh purchased and stored large quantities of corn during the good times. As a result, Egypt prospered during the famine. Even though the term “risk management” in the sense of cost-effectively preventing and paying for accidental losses, did not appear until the mid-1950s, people have been managing risk in this sense throughout the history, for example working to
• Assure their communities supplies ample of healthful food despite pests, droughts, floods, and other natural disasters;
• Erect walls and other barriers, physical and diplomatic, to keep enemies at bay;
• Foster co-operative governmental and other community efforts to restore neighbor’s properties that had been damaged and to cloth, feed and shelter those whose homes and lives might otherwise have been lost.

Between the 1970s and 1990s, derivatives, complicated financial contracts so named because they derive their value from one or more assets, became popular among individuals and organizations. Derivatives are used to hedge or protect against a financial loss and are particularly useful in conditions where there is significant volatility (i.e., financial risk); futures and options are two very simple forms of derivatives. Financial deregulation, inflation, volatility in interest and exchange rates and commodity prices all combined to create an environment where the conventional forms of risk management were ill equipped. The term “Risk Management” became more commonly used in the 1970s. The corporate treasury function also began to develop in the 1970s.

Use of derivatives by corporates, banks and speculators increased, resulting in some classic cases of misuse and fraud. In the early 1990s, many companies burnt their fingers in derivative deals. These included Procter & Gamble, Gibson Greetings and Metallgesellschaft. In 1995, Barings, Britain’s oldest merchant bank went bankrupt because of the risky deals of a reckless trader, Nick Leeson. On January 4, 2000, Electrolux, lost $11.25 million because of unauthorised currency trading by an unnamed employee. Most of these disasters resulted because corporate executives considered low probability events as impossible and
given a choice between a certain loss and a gamble, chose the gamble. As understanding of derivatives improves, the current paranoia will disappear. Derivatives will find their rightful place in the corporate treasurer’s tool kit.

From the mid-1990s, a new approach to risk management began to take shape. No longer were companies obsessed with external hazards affecting the company. Managers became increasingly concerned about the unexpected consequences of decisions. They also realised they needed more information about the risks involved while taking crucial decisions. Risk management became more proactive and attempted to ensure better cross-functional coordination. The range of risk faced by the companies increased significantly.

1.5 Importance of Risk Management

At one time, Risk Management meant buying insurance and having enough fire extinguishers. But in the last ten years, the scope and mission of corporate risk management have well expanded beyond and opportunistic hedging to include all kinds of corporate operating and strategic risks. Corporate Risk Management is no longer “just series of isolated transactions; it’s a strategic activity that encompasses everything from operating changes to financial hedging to buying and selling of plants or new businesses anything that affect the level and variability of cash flowing forward”. When viewed from this light, Risk Management is clearly senior management responsibility, one that requires input from and coordination of the company at all operating levels. Together, they make risk an important board room issue. The factors driving the transformation of Corporate Risk Management are increasing in the scale and varieties of uncertainties facing today’s companies, everything from
fluctuating commodity prices to threats of re-regulation and terrorist attacks. In late 1970s, Finance Scholars began to research for how Risk Management can increase corporate values.

1.6 Types of Risk

Understanding the different types of risk is important because tackling each risk requires different set of management skills. Classification is important because the risk management strategies are devised according to the type of risk faced by the companies. To obtain a general understanding of risk is not an easy task, as there are numerous definitions of risks of different types and on top of that, many different views on how risks ought to be classified (Esther et. al.) .There are various types of risks faced by the organisation. The Economist Intelligence Unit divides risks into four categories namely Hazard risk, Financial risk, Operational risk and Strategic risk. Kit Sadgrove in the book entitled “The Complete guide to Business Risk Management” has classified the risk into two levels namely strategic and operational.

Coughry et. al. in their book classified risk into eight types. They are Market Risk, Credit Risk, Liquidity Risk, Operational Risk, Legal &Regulatory Risk, Business Risk, Strategic risk and Reputational risk. Mark and Oscar in their book entitled “Risk Management: Text and Cases” have examined the risk under the following major headings: Property risk and personnel risk, Marketing risk, Finance risk, Personnel, Production and Environment. Terry Caroll et. al. in their book on “Risk Factor” have given a typical list of business or Organisational risks, based on their practical experience working with a variety of organisations in both the private and public sector. A sample of risks quoted includes Business risk, Currency risk, Environmental risk, Financial risk,
Reputation & Brand risk, Treasury products risk, Operational risk, and Interest rate risk.

Vedupuriswar in his book “Enterprise Risk Management (Vol III) has discussed about a few types of risk faced by the organisation. The discussed risks are Strategic risk, Financial Risk, Technology Risk, Political Risk, Environmental Risk and Legal Risk.


The important types of risks faced by the companies are discussed below.

1.6.1 Credit Risk

Credit Risk is the risk that any obligator may fail to perform as promised. Common sources of Credit Risk for a company are trade receivables, vendor financing, long term contacts, short and long-term investments, outright loans, joint ventures and partnerships. There are number of components of Credit Risk, the most important Credit Risk are the counterparty risk, concentration risk and settlement risk.

1.6.2 Counterparty Risk

The Risk of loss when replacing the cash flow of a transaction if the counterparty to the transaction fails to perform in terms of the contract.
1.6.3 Concentration Risk

The Risk that a debtor book incurs losses owing to concentrated exposure to certain geographic, industry or demographic.

1.6.4 Settlement Risk

The risk that the competition or settlement of a financial transaction will not take place as expected.

1.6.5 Market Risk

Market Risk is the risk of financial loss as a result of unfavourable movements in market rates or prices such as interest rates, foreign exchange rates, equity prices and/or commodity prices. The four classes of Market Risk, which mirror underlying financial markets, are:

1.6.6 Interest Rate Risk

It is the risk that future cash flows or earnings that are sensitive to movements in interest rates or the value of interest rates or the value of interest-rate sensitive assets and liabilities will be adversely affected by changes in interest rates;

1.6.7 Equity Price Risk

This is the popular change in the value of a company’s equity-related holdings.

1.6.8 Commodity Price Risk

It is the risk that a change in the price of commodity that is a key input or output of a business will adversely impact its financial performance.
1.6.9 Environmental Risk

Environmental Risk is the actual or potential threat of adverse effects on living organisms and environment by effluents, emissions, wastes, resource depletion, etc., arising out of an organization's activities. Environmental Risk management seeks to determine what environmental risks exist and then determines how to sustainably manage, reduce, or eliminate those risks to protect human health and the environment. Risks related to the natural environment that could result in damage to buildings, restricted access to raw materials, or loss of human capital. Companies which do not take steps to protect the natural environment, face the risk of resistance and hostility from society.

1.6.10 Regulatory Risk

Risks related to meeting legal and regulatory requirements with respect to corporate governance, labour relations, industry standards, the environment, etc., Regulatory or compliance risk is the risk to earnings or capital arising from violations of, or non-conformance with, laws, rules, regulations, prescribed practices, or ethical standards. This risk also arises in situations where the laws or rules governing certain products or activities may be ambiguous or untested. Compliance risk exposes the institution to fines, civil money penalties, payment of damages, and the voiding of contracts. Regulatory and compliance risk can lead to a diminished reputation, reduced franchise value, limited business opportunities, lessened expansion potential, and the lack of contract enforceability. It also includes:

- Inability to meet regulatory requirements;
- Breaching existing capital requirements;
- Failure to anticipate forthcoming regulatory requirements.
1.6.11 Reputational Risk

Risks related to the perception of the organisation by its stakeholders, the media and the general public that could impact liquidity, capital or credit rating. Reputation Risk is the risk to earnings or capital arising from negative public opinion. This affects the institution's ability to establish new relationships or services, or to continue servicing existing relationships. This risk can expose the institution to litigation, financial loss, or damage its reputation. Reputation Risk exposure is present throughout the organization and is why banks always exercise caution in dealing with their customers and the community.

1.6.12 Industry Risk

Risks related to competitive positioning, industry profit margins, market structure and competition laws. Examples of Industry Risks are changes in supply and demand, industry concentration, or competitive structure, introduction of new products and service.

1.6.13 Political Risk

Risks related to changes in government, public policy, and federal oversight, and global risks related to political instability. Political Risk refers to the complications businesses and governments may face as a result of what are commonly referred to as political decisions or “any political change that alters the expected outcome and value of a given economic action by changing the probability of achieving business objectives”. Political Risk faced by firms can be defined as “the risk of a strategic, financial, or personnel loss for a firm because of such nonmarket factors as macroeconomic and social policies (fiscal, monetary, trade, investment, industrial, income, labour, and
developmental), or events related to political instability (terrorism, riots, coups, civil war, and insurrection).” Risks related to changes in government, public policy, and federal oversight, and global risks related to political instability.

1.6.14 Operational Risk

Operational Risk is the risk of loss from inadequate, inappropriate or failed internal processes, people and systems, or from external events. It is the risk that failures in computer systems, internal supervision and control or events. Other aspects of operational risk relate to personnel quality and internal controls.

1.6.15 Strategic Risk

Relates to doing wrong things. It is related to insufficient forward planning or horizon scanning, Incorrect strategic priorities, community planning oversight or errors, policy decisions based on incomplete or faulty information, failure to exploit opportunities, inappropriate capital investment decisions. Risks related to activities undertaken to initiate significant change in strategic direction.

1.6.16 Information Technology Risk

Risk that relate to the loss of inaccuracy of data and the use of reliance on technology. Information technology risk includes systems and management data not up to date, ineffective prediction of trends and poor forecasting, breaches of security of network and data, Obsolescence of technology, lack of network resilience. Technological risks: Risks related to technological progress and technological-driven disruptive forces. Technology risk has become important in this age of rapid innovation. Companies which do not have a strategy to cope with changing
technology will find themselves at a severe disadvantage. The key decision in technology risk management is whether to move early or to wait and see the impact of a new technology as it emerges.

1.6.17 Human Capital Risk

Risk related to the adequacy and execution of human resource standards, policies and practices. Risks associated with employees and the management structure. Human Capital risk includes over-reliance on key officers, inefficient/ineffective management processes, failure to recruit/retain qualified staff, lack of investment in training, poor absence management, ethical/unethical conduct by management and employees. Succession planning is probably the most strategic of these risks.

1.6.18 Financing Risk

This risk refers to the difficulty in raising finance (e.g. high price of funding, shorter than requested loan period).

1.6.19 Natural Hazard Risk

It is a threat of a naturally occurring event that will have a negative impact on people or environment.

1.6.20 Currency Risk or Treasury Risk

The risk that volatility in foreign exchange rates exposes that organisation to economic and accounting losses. Currency Risk occurs due to exposure in a foreign currency. This risk includes:

- **Convertibility Risk** - This is the inability to convert one currency into another as a result of political/economic policy (i.e. exchange rate controls, devaluation etc.).
• **Translation Risk** - This is the profit/loss due to translation of financial statements of an overseas subsidiary into the home currency for consolidation.

• **Transaction Risk** - This is risk of movements in the foreign exchange rates when credit transactions are denominated in a foreign currency.

1.6.21 Economic Risk

Risk related to macroeconomic policies and economic cycles (e.g. hike in the price for raw materials).

1.6.22 Social Risk

Risks related to changing demographics and social norms. For example failing to adequately manage cultural heritage impacts can lead to community dissents, leading to protests.

1.6.23 Country Risk

Country Risk is the risk faced by institutions undertaking business in various countries around the globe. It includes components such as political, financial and economic risks as well as risks related to the general business concerns of stability and social turmoil. Many institutions have suffered substantial losses due to financial, political and social instabilities in many Far Eastern former 'tiger economies'.

1.6.24 Organisational Risk

Risks related to control systems, business policies and business culture.
1.7 PRINCIPLES OF RISK MANAGEMENT

Aswath Damodaran (2008) has given eleven principles of Risk Management.

1.7.1 Risk is everywhere: Our biggest risks will come from places where we least expects them to come from and in unanticipated forms.

1.7.2 Risk is threat and opportunity: Good risk management is about striking the right balance between seeking out and avoiding risk.

1.7.3 We are ambivalent about risks and not always rational: A risk management system is only as good as the people manning it.

1.7.4 Not all risk is created equal: Different risks have different implications for different stakeholders.

1.7.5 Risk can be measured: The debate should be about what tools to use to assess risk than whether they can be assessed.

1.7.6 Good risk measurement should lead to better decisions: The risk assessment tools should be tailored to the decision making process.

1.7.7 The key to good risk management is deciding which risks avoiding, which ones to pass through and which to exploit: Hedging risk is only a small part of risk management.

1.7.8 The payoff to better risk management is higher value: To manage risk right, we must understand the value drivers of the business.

1.7.9 Risk management is part of everyone’s job: Ultimately, managing risks well is the essence of good business practice and is everyone’s responsibility.
1.7.10 Successful risk taking organizations do not get there by accident: The risk management philosophy must be embedded in the company’s structure and culture.

1.7.11 Aligning the interests of managers and owners, good and timely information, solid analysis, flexibility and good people is key: Indeed, these are the key building blocks of a successful risk taking organization.

1.8 Risk Management process

In the project management literature, a rather more prescriptive interpretation of risk management is expounded. To develop the concept as a management tool, authors tend to describe the process by which risk management is undertaken.

According to Smith (1995), the risk management process involves: Identification of risks/uncertainties, analysis of implications, response to minimize risks, allocation of appropriate contingencies. Risk management is a continuous loop rather than a linear process so that, as an investment or project progresses, a cycle of identification, analysis or control and reporting of risks is continuously undertaken. Risk analysis and risk management have been carried out in many fields for a number of decades and are being increasingly used as an integral part of the overall business management approach and on major projects; in some cases they have become a mandatory requirement for financial planning and regulatory approval.

Despite risk analysis being growing major elements in organisations, there is no standard to which references may be made for techniques, factors and approaches. To overcome this, a number of
organisations and research authorities have identified ways to describe risk management process. Typically there are number of phases associated with this process. Many reflect a variation of the model as proposed in texts authored by C. Arthur Williams, Jr. For example, the model in the sixth edition of Williams and Heins (1989) contains six steps: defining the objectives of the organization wishes to achieve; identifying loss exposures; measuring the potential losses; selecting the best ways to solve the problem; implementing the decisions made; and monitoring and evaluating those decisions. However, in the eighth edition (Williams et.al. 1998) the risk management model contains five steps: mission identification; risk assessment; risk control; risk financing; and program administration.

In contrast, Dickson (1995) takes a three-step approach to the risk management process, which he describes as the identification, analysis, and economic control of possible risks. He states that his definition (model) is highly subjective, and welcomes a difference of opinion. Dickson's model reflects standards also used in the risk control auditing community. For example, Mc Namee (1998) reports that the Committee of Sponsoring Organizations (COSO) adopts a three-step financial model to monitor risk control. These steps are: to establish objectives; to assess risks (identifying, measuring, and prioritizing them); and to determine the controls needed.

Pritchett et. al. (1996) suggest a seven-step process, where the actions are: setting objectives; identifying problems; evaluating problems; identifying and evaluating alternatives; choosing alternatives; implementing alternatives; and monitoring the system. Vaughan (1997) presents six steps: determining objectives; identifying risks; evaluating the risks; considering alternatives and selecting the risk treatment device;
implementing the decision; and evaluating and reviewing. Vaughan and Vaughan (1999) retain these six steps. Merna (2002) took three processes namely risk identification, analysis and response, and implemented a 15-step sequence to account for risk management. However, four responses had been identified Boswick’s 1987 paper (PMBOK 1996). Harrington and Niehaus (1999) present a five-step process: identifying; evaluating; developing and selecting methods; implementing; and monitoring. Trieschmann et.al. (2001) suggest a four-step risk management process: identifying risk management techniques; evaluating them; selecting them; and implementing and reviewing decision.

FIGURE 1.1 RISK MANAGEMENT PROCESS

1.8.1 Establishing the Context

Establishing the context means all the possible risks that are identified and the possible ramifications are analyzed thoroughly. Various
strategies are discussed and decisions are made for dealing with the risk. The break-up of various activities in this stage are as follows:

- Identification of a risk in one particular domain.
- Planning out the entire management process.
- Mapping the manifestations of the risk, identification of objectives of risk etc.
- Outlining a framework.
- Designing an analysis of risks involved at each stage.
- Deciding upon the risk solutions.

1.8.2 Risk Assessment

Risk assessment is a systematic process for identifying and evaluating events that could affect the objectives positively or negatively. Risk assessment is the essential part of the Risk Management process. Risk assessment is intended to provide management with a view of events that could impact the achievement of objectives. Therefore Risk assessment is the overall process of Risk identification and Risk evaluation. The risk assessment process seeks to identify the risks to be managed. When areas of risks have been identified it is important that these are described in a manner that accurately and comprehensively ensures that the exact nature and magnitude of the risk is captured. The two components of Risk assessment namely Risk Identification and Risk evaluation is detailed below.
1.8.2.1 Risk Identification

The identification of potential risks is the first stage of the risk assessment process. This requires a systematic approach, involving techniques that may be largely quantitative or qualitative, or that contains elements of both. The importance of the risk identification stage cannot be underestimated. Frank (1986) noted that if the early warning signs of potential threats are ignored or misinterpreted a crisis may result. Early detection of such signals are pivotal if action is to taken in time to reduce the likelihood or the magnitude of the threat, and preferably both (Hensgen et.al.).

A range of techniques can be brought to the systematic identification of both possible opportunities and the potential risk factors associated with them. These techniques include individual and group activities, desk-based exercises, physical inspections and computer modeling. A number of these techniques are described below:

1.8.2.1.1 Brainstorming

Many organisations utilize brainstorming workshops as a means of encouraging creative thinking. Brainstorming can be used in an attempt to identify threats at strategic level of the organisation, such as changes in legislation or client expectations, major fraud or inadequate pension funds. A brainstorming exercise will generate random lists of potential threats, which can be grouped into categories of risk and used as the basis for further exploration and evaluation.

1.8.2.1.2 Questionnaire or Surveys

Questionnaire or surveys can be used to gather information from various individuals and parts of the organisation. This method can assist
in the identification of factors that have, or may, lead to loss-producing situations, and record how these are presently being treated. The results may allow for comparisons to be made between departments or locations and indicate area requiring further investigations. Questionnaires are also used to explore the attitude of employees to the risks that there are present in their working environment.

1.8.2.1.3 Historical data analysis

Historical data analysis in the form of accident records, loss histories and insurance claims can be useful in highlighting current areas of weakness and trends over time. The value of such information is, of course, dependent on its completeness and accuracy and it is worth recommending that past trends are not necessarily good indicators of experience in future.

1.8.2.1.4 Physical inspection

Physical inspections are an essential part of the assessment of fire, health and safety risks. Simply walking through an organisation’s premises will identify the situations and materials that could cause a hazard. Typical office risks include trailing computer and phone cables, high-levels storage, poor or harsh lighting.

1.8.2.1.5 Flow charts

More quantitative techniques are found in the risk engineering and safety functions of organisations, where flow charts are used to explore the ‘flow’ of liquids, solids and production process. The technique can be used for the routine flow of money, people and information that a public service organisation will experience on a daily basis. A quantitative element can be added to such charts by estimating how likely a failure is
to occur in each of the key points of the flow, and the impact that this might have. Specialist software allows such data to be modeled and makes it possible to test the impact of proposed changes before they are implemented.

1.8.2.1.6 Risk registers

Once identified, risks may be classified into categories or types of threat. Entering on a risk register allows a number of related issues to be addressed. Issues include the ‘ownership’ of the risk, current preventive measures in place to treat it, and recommended action for the future. The register can also be used to note when actions have to be undertaken and by whom. There must be sufficient data to make collating the information worthwhile, but each organisation will need to decide its own content requirements for each entry (Great Britain, Office of Government Commerce, 2002).

1.8.2.2 Risk Evaluation

List of potential threats are of little value in isolation and need to be implemented by an estimation of the likelihood (probability) of occurrence. This estimation can be expressed in a number of different ways, for example as an occurrence over time or as a statistical probability. In turn, these estimates can be grouped and expressed on a grading scale as ‘high’, ‘medium’ or ‘low risk’ or ranked from one to five, where one represents ‘very low’ while five may be ‘very high’. Assessing risks in terms of likelihood is important because it is only part of the overall evaluation process. Risk categorized as low likelihood, for example, may differ considerably in terms of the impact or magnitude of damage associated with each type of risk needs also to be made. A rating scale is developed that reflects the organisations view of the magnitude of
the risk, from the catastrophic to the insignificant. The scores for both likelihood and magnitude can be combined (multiplied) and displayed on a risk matrix.

**TABLE 1.1 MEASUREMENT MATRIX**

<table>
<thead>
<tr>
<th>Probability of Occurrence</th>
<th>Impact of Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very Low</td>
</tr>
<tr>
<td>Very Low</td>
<td>1</td>
</tr>
<tr>
<td>Low</td>
<td>2</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
</tr>
<tr>
<td>Very High</td>
<td>5</td>
</tr>
</tbody>
</table>

Composite Risk Index = Probability of Occurrence X Impact of Risk event

When the risk analysis process has been completed, it is necessary to compare the estimated risks against risk criteria which the organisation has established. The risk criteria may include associated costs and benefits, legal requirements, socioeconomic and environmental factors, concerns of stakeholders, etc. Risk evaluation therefore, is used to make decisions about the significance of risks to the organisation and whether each specific risk should be accepted or treated.

The purpose of risk evaluation is to make decisions, based on the outcomes of risk analysis, about which risks need treatment and treatment priorities. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. The objectives of the organization and the extent of opportunity that could result should be considered. Where a choice is to
be made between options, higher potential losses may be associated with higher potential gains and the appropriate choice will depend on an organization’s context.

Decisions should take into account of the wider context of the risk and include consideration of the tolerability of the risks borne by parties other than the organization that benefit from it. In some circumstances, the risk evaluation may lead to a decision to undertake further analysis.

1.8.3 Risk Treatment

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Risk treatment involves a cyclical process of assessing a risk treatment; deciding whether residual risk levels are tolerable or not; if not tolerable generating a new risk treatment; and assessing the effect of that treatment until the residual risk reached complies with the organization’s risk criteria. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. It is important to note that there is no right response to risk. The choice of response will depend on issues such as the organisation’s risk appetite, the impact and probability of the risk and the costs and benefits of the mitigation plans. Responses to risk generally fall into the following categories:

1.8.3.1 Risk Avoidance

Action is taken to halt the activities giving rise to risk, such as a product line, a geographical market or a whole business unit.
1.8.3.2 Risk Reduction

Action is taken to mitigate the risk of likelihood or impact or both, generally via internal controls.

1.8.3.3 Risk Sharing or Transfer

Action is taken to transfer a portion of the risk through insurance, outsourcing or hedging.

1.8.3.4 Risk Acceptance

No action is taken to affect likelihood or impact. Implementation of the chosen risk responses involves developing a risk plan outlining the management processes that will be used to manage the risk of opportunity to a level defined by the organisation’s risk appetite and culture. An important part of the risk response in the ongoing monitoring to determine the effectiveness (or performance) of the risk response.

1.8.3.1 Selection of risk treatment options

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived having regard to legal, regulatory, and other requirements, social responsibility and the protection of the natural environment. Decisions should also take into account risks that can warrant risk treatment actions that are not justifiable on economic grounds e.g. severe (high negative consequence) but rare (low likelihood) risks. A number of treatment options can be considered and applied either individually or in combination. The organization can benefit from the adoption of a combination of treatment options.
When selecting risk treatment options, the organization should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Where risk treatment options can impact on risk elsewhere in the organization, these areas should be involved in the decision. Though equally effective, some risk treatments can be more acceptable to stakeholders than others. If the resources for risk treatment are limited, the treatment plan should clearly identify the priority order in which individual risk treatments should be implemented. Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part of the risk treatment plan to give assurance that the measures remain effective. Risk treatment can also introduce secondary risks that need to be assessed, treated, monitored and reviewed. These secondary risks should be incorporated into the same treatment plan as the original risk and not treated as a new risk, and the link between the two risks should be identified. Decision makers and other stakeholders should be aware of the nature and extent of the residual risk after risk treatment. The residual risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

1.8.3.2 Preparing and implementing risk treatment plans

The purpose of risk treatment plans is to document how the chosen treatment options will be implemented. The information provided in treatment plans should include:

- expected benefit to be gained;
- performance measures and constraints;
• persons who are accountable for approving the plan and those responsible for implementing the plan;
• proposed actions;
• reporting and monitoring requirements;
• resource requirements; and
• timing and schedule.
• treatment plans should be integrated with the management processes of the organization and discussed with
• appropriate stakeholders.

1.8.4 Monitoring and review

Monitoring and review should be a planned part of the risk management process. Responsibilities for monitoring and review should be clearly defined.

The organization’s monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

• Analyzing and learning lessons from events, changes and trends;
• Detecting changes in the external and internal context including changes to the risk itself which can require revision of risk treatments and priorities;
• Ensuring that the risk control and treatment measures are effective in both design and operation; and
• Identifying emerging risks.

Actual progress in implementing risk treatment plans provides a performance measure and can be incorporated into the organization’s performance management, measurement and internal and external
reporting activities. Monitoring and review can involve regular checking or surveillance of what is already present or can be periodic or ad hoc. Both aspects should be planned. The results of monitoring and review should be recorded and internally or externally reported as appropriate and should also be used as an input to the review of the risk management framework.

1.8.5 Recording the risk management process

Risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods and tools as well as the overall process. Decisions concerning the creation of records should take into account:

- Benefits of re-using information for management purposes;
- Costs and efforts involved in creating and maintaining records;
- Legal, regulatory, and operational needs for records;
- Method of access, ease of irretrievability and storage media;
- Retention period and Sensitivity of information.

1.9 Integrated Risk Management

Integrated risk management also popularly called Enterprise wide Risk Management (ERM), looks at various kinds of risk - market risk, credit risk, liquidity risk, operational risk and business risk in a holistic fashion. An integrated view generates a better picture of the risk climate of the organization and also helps in making the risk management process more efficient and effective. Considerable cost savings can be achieved by aggregating and netting out positions. A firm wide approach can reveal natural hedges and guide the firm’s strategy towards activities that are less risky when considered as a whole. ERM also acts as a check on
risk migration, i.e., movement towards other types of risk that are less visible but may be more dangerous. Last but not the least, by providing an aggregate measure of risk, ERM helps companies to decide what the optimal level of capital they must hold.

1.9.1 The need for an integrated approach

Integrated risk management is all about the identification and assessment of the risks of the company as a whole and formulation and implementation of a companywide strategy to manage them. In the past, a systematic and integrated approach to risk management was more an exception than the rule. Fortunately, the scenario is changing. The cumulative experience of the past few decades in managing risks, development of management and probability theories, powerful computer software and the availability of a wide range of financial instruments has made ERM a reality.

1.9.2 The role of System and process in ERM

The systems and processes of the organization should enable managers to know what risks are being taken, quantify them and assess whether they are within prescribed limits. They should also facilitate corrective action, where necessary. Good management control systems can protect a company from avoidable risks by defining performance standards, measuring actual performance and taking corrective action on a regular basis.

A key objective of Enterprise Risk Management is to ingrain risk management into the organization culture by making it a core value of the organization culture and building it into day-day practices. A system of checks and balances is necessary to keep risks within the specified limits.
System and process must be designed in such a way that they align individual goals with corporate objectives and discourage excessive risk taking. The standards against which performance is compared can be decided by the top management. By evaluating, monitoring and controlling sub units, an organization can ensure there is effective and efficient allocation and utilization of resources. Auditing and testing should be undertaken periodically to check the robustness of processes, procedures and controls. Along with the systems and processes, it is also important to shape the culture of organization and check dysfunctional tendencies. The ‘right culture’ encourages entrepreneurial risk taking but discourages gambling.

The board and the senior managers need to send strong signals that they consider risk management a priority. The board should pay an active role in identifying the risks that may have a significant impact on the fulfillment of corporate objectives. It should review information on these significant risks from time to time. The board should come to a consensus regarding what risks are acceptable, the probability of their occurrence and the type of mechanisms and processes needed to reduce their impact. The board should realize that whatever is the sophistication of the control systems and processes, risk due to poor judgment, human error and unforeseen circumstances can never be completely eliminated. It should be emphasized that the role of the board is not to advocated complete elimination of risk. The board and the senior management team should play an active role in the following areas:

- Understanding the Profile
- Setting policy
- Establishing Controls
- Setting up systems
• Checking compliance
• Periodic review

a) Understanding the Risk Profile: The board members should clearly understand the risks to which the company is exposed. The board should further decide which risks are acceptable and which must be eliminated through the use of hedging techniques.

b) Setting Policy: The board should prepare policy guidelines, including the corrective action to be taken when things go wrong. For example, there should be guidelines on when and how to unwind an unprofitable trading position, if rates move unfavourably. The exit strategy should be based on the amount of money the company is willing to put to risk. A risk policy explains the objectives of risk management and indicates how the responsibilities in this regard will be distributed. A risk policy can provide guidelines on what type of exposures to cover, what to leave uncovered and the type of derivative instruments, which may be used. The policy is not about compliance and disclosure, important as these may be, but it is about developing a strategic approach to enterprise risks that release value to shareholders.

c) Establishing Controls: Steps should be taken to ensure effective implementation of policies. An independent risk management unit is desirable. It is a good practice to make risk managers report to people one level higher than those who execute and approve various market transactions, especially those involving derivatives.

d) Setting up systems: An integral part of ERM is consolidation and integration of data from a number of different systems across the company’s operations.
e) **Checking compliance:** The risk manager should send reports regularly to the senior management and the board. These reports should check compliance with policies and procedures and make independent evaluations of various trading positions.

f) **Periodic Review:** The board must make it clear to managers in general and traders and treasury managers in particular that any violation of policies, guidelines or controls will be punished. When limits are violated, the board should not hesitate to take action.

### 1.10 Statement of the Problem

Risk Management is the top of the agenda in the wake of subprime crisis. The American automotive giants, General Motors (GM), Ford and Chrysler were in big trouble (A.V Vedupuriswar, 2008). These crises have woken the Indian companies to the importance of Risk Management to tide over future crisis.

Tightening capital markets, adoption of global initiative to promote business integrity is forcing many Indian companies to pay attention to recent developments in Risk Management across the globe. Risk has been recognized as core competence in banking, and has gained recognition in risk intensive industries like Insurance, Stock Brokerage etc. The report published by Conference Board of Canada stresses that Risk Management is gaining recognition outside of the finance industries. The Indian Information Technology giant Satyam’s bankruptcy and failure have forced the regulators around the world to become more active. So it is understood that 2008 economic meltdown and the Satyam scandal made many Indian companies sit up right. The growing complexity of business transactions, advancement in technology, globalization continues to increase the volume and nature of risks faced
by Indian organisations and they demand a more focused approach towards foreseeing and managing risks. Balancing risk is the only effective way to manage a corporation in a complex world (Berinato, 2006). The organisations success depends upon the risk management (Jorion, 2001). Risk Management is a central part of any organisations strategic management (Anadi Kishore sethi).

Intense global competition and rapid growth are forcing Indian firms to Corporate Risk Management practices (Conference Board study, 2008). Managers fail to understand the firm’s sensitiveness to different types of risks (Kaplan and Norton, 1992). It is understood that risk management among Corporate is gaining more and more importance (Gabriel Khan, 2008). According to KPMG survey 2008, Indian companies do not have proper Risk Management strategies. Indian companies lag far behind their global peers in managing risk (Deloitte research report). Broadly speaking the problems to be examined in this study can be posed in the form of the following questions:

- What kind of risks do these organisations face?
- Do these organizations have general risk management objectives?
- Do the organisations use some tools to measure risks and tackle the risks?
- Do the organisations adopt some Risk Management Practices?
1.11 Objectives of the Study

This research is essentially centered on gaining insights into Corporate Risk Management practices. To highlight the above, the following objectives were formulated:

1. To identify and measure the intensity of different types of risks faced by the organizations.
2. To ascertain the corporate objectives in managing risks.
3. To identify the tools used by the organisations to measure and manage the risks.
5. To frame and suggest a model for Risk Management practices.

1.12 Scope of the study

The present study seeks to ascertain the corporate objectives of managing risk, corporate risk practices for managing risk of Tamil Nadu based companies listed in Bombay Stock Exchange. Fourteen types of risk namely Credit Risk, Financing Risk, Market Risk, Treasury Risk, Regulatory Risk, IT Risk, Strategic Risk, Environmental Risk, Operational Risk, Reputational Risk, Political Risk, Natural Hazard Risk, Human Capital Risk and Industry Risk were considered. The tools used to measure Credit Risk and Market Risk was identified. These two risks were considered because they are quantifiable risk. Similarly, for tools used for managing risk, Credit Risk, Operating risk and Foreign exchange risks were considered. Various sectors covered in the study are Automotive, Manufacturing, Chemicals, FMCG (Fast Moving Consumer Goods), Resources, IT & Technology and Construction. Service sector companies were eliminated because the risks faced by them, strategies
and practices are different. The geographical coverage of this study is restricted to companies with registered office in Tamil Nadu. This covers all the districts of Tamil Nadu.

1.13 Limitations of the study

A few respondents were reluctant to respond, as they had the fear of disclosing information, in spite of the assurance given to them of maintaining the confidentiality. Data of such non-responding companies were one of the limitations.

The survey was conducted only in Tamil Nadu. Hence, the results arrived from the study may or may not be applicable to other states.

The study is based on primary data and hence some of the information is confidential to the management and its non availability also limited the scope of the study.

Since the respondents were senior Managers (Finance Directors) who were professionally busy and faced constraints in filling and submitting the questionnaires on time.

The tools and techniques used also suffer from certain limitations by themselves and hence naturally the same limitations also affect this study.

1.14 Chapter Scheme

Broadly the present study has been divided into Six Chapters.

The first chapter gives an Introduction to the study. It consists of introduction, Statement of the problem, Research questions, objectives of
the study, scope of the study, limitations of the study and chapter schemes.

The second chapter presents the **Review of Literature**. It deals with the important earlier studies relating to the present topic and research gap.

The third chapter is concerned with **Research Methodology**. It includes research design, Sources of data, Data collection methodology, Hypotheses of the study and tools for analysis.

The fourth chapter attempts to find out the **Intensity of Risks** faced by the organizations. It also outlines the corporate objectives in managing the risks. The risks measurement and management tools used by the organizations were also identified.

The fifth chapter is devoted for testing the **Model** identified in the present study. The linkage between the Effective Risk Management practices, Outcomes of Successful Risk Management and Risk score is statistically analysed.

The sixth chapter presents a summary of the findings of the study and conclusion. The chapter also contains suggestions and areas for further research.