Guide to Implementing Enterprise Risk Management

Celebrating the 60th Year of Excellence

The Institute of Chartered Accountants of India

(Set up by an Act of Parliament)

New Delhi

Guide to Implementing Enterprise Risk Management

The basic draft of this Guide was prepared by a study group under the convenorship of CA. Deepak Wadhawan, its members being CA. Neville Dumasia, CA. Anthony Crasto, and CA. Chandrashekar Mantha.

Overall insightful reviews have been carried out by CA. R.N. Joshi, CA. Shrikant Sarpotdar, CA. Pankaj Sahai, CA. Nikhil Kochhar and a select number of independent directors.

The Institute of Chartered Accountants of India

(Set up by an Act of Parliament)

New Delhi

Edition : December, 2008

Price : Rs. 150/- *(Including CD)*

ISBN : 978-81-8441-157-7

Email : cia@icai.in

Website : www.icai.org

Published by : The Publication Department on behalf of CA. Puja Wadhera, Sr. Asst. Director, Internal Audit Standards Board, The Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi – 110 002.

Printed by : Sahitya Bhawan Publications, Hospital Road, Agra 282 003. December/2008/ 3000 Copies

Foreword

The concepts of risk and risk management are core of enterprises. An Enterprise Risk Management (ERM) system anticipates how an enterprise could be affected by a particular risk. ERM, in a contemporary entrepreneurial venture, is all pervasive, cutting across management levels and functional/departmental lines. Besides, ERM is equally important, not withstanding the nature, type, sector or commercial/philanthropic objectives of the entity. Members of the Institute have a valuable role to play, in both in helping entities to design and implement ERM framework and as internal auditors, in assessing the efficiency in functioning of that framework.

The Institute of Chartered Accountants of India, in its role as the regulator of the profession of chartered accountancy in India, has also been working proactively to keep its members well informed and abreast of the various technical intricacies involved in performing the attest function. I am happy to note that as another step in this direction, the Internal Audit Standards Board of the Institute has brought out the Guide to Implementing Enterprise Risk Management.

I wish to place my appreciation to CA. Abhijit Bandyopadhyay, Chairman, Internal Audit Standards Board for bringing out this Guide to Implementing Enterprise Risk Management. I am pleased to note that the range of topics is broad and carefully chosen for its applicability to practice.

I am sure the Guide would provide the readers the essential analytical foundations of risk management and would be another benchmark as the technical literature brought out by the Institute.

New Delhi ***Ved Jain***

17th December, 2008 ***President, ICAI***

Preface

The primary objective of the Internal Audit Standards Board when it was established in 2004 was to enable the members to provide more effective and efficient value added services related to this field to the Industry and others and help them systematise and strengthen their governance process by systematising and strengthening their control and risk management process.

Developing internationally benchmarked technical literature is integral to the achievement of the above objective. In that line, the Board has, on the one hand, brought out a number of Standards on Internal Audit, codifying the best practices in the area of internal audit, on the other, it has also been bringing out generic as well as industry specific guides on various contemporary issues in the area of internal audit.

Enterprise risk management (ERM) is a concept which has come up in a significant way for the modern business enterprises. Managements have realized that even with huge human, physical and capital resources at their disposal, survival and growth of an organisation cannot be ensured if the latter does not have an adequate and formal system to identify and manage its risks. With the growing volatility and uncertainty in the operating environment for organisations, enterprise risk management is emerging as an area critical to effective decision making and resource planning. Organisations today are therefore, deploying considerable amounts of resources in understanding, establishing and ensuring effective working of an ERM system. The current economic scenario has only reiterated the need for an ERM system that can withstand the test of time.

This Guide to Implementing ERM has been written with the primary objective of helping the readers understand the essentials of implementing an ERM system in an organisation. It provides, in a simple manner, a step by step guidance to implementing ERM framework as also the issues that would be faced during implementation. At this juncture, I am grateful to CA. Deepak Wadhawan, New Delhi, CA. Neville Dumasia, CA. Anothony Crasto and CA. Chandrashekhar Mantha for squeezing time out of their professional and

personal preoccupations to share their years of experience, knowledge and expertise in the area of enterprise risk management in the form of this Guide. I am also grateful to CA RN Joshi, CA. Shrikant Sarpotdar, CA Pankaj Sahai, CA Nikhil Kochhar and other professionals who have provided their invaluable suggestions to give this Guide a final shape.

I also wish to thank CA. Ved Jain, President and CA. Uttam P Aggarwal, Vice President, ICAI for their continuous support and encouragement to the initiatives of the Board. I must also thank my colleagues from the Council at the Internal Audit Standards Board, viz., CA. Bhavna G Doshi, Vice Chairperson, CA. Sunil H Talati, CA. Mahesh P Sarda, CA. Shanti Lal Daga, CA. K P Khandelwal, CA. Manoj Fadnis, CA. Anuj Goyal, CA. Amarjit Chopra, Shri Manoj K Sarkar, Shri A K Awasthi, Dr. Pritam Singh and Shri O P Vaish for their vision and support. I also wish to place on records my gratitude for the co-opted members on the Board, viz., CA. Paratha Sarathi De, CA. N K Aneja, CA. Charanjit S Attra, CA. Nagesh D Pinge as also special invitees on the Board, viz., CA. Harinderjit Singh (my Council colleague), CA. Deepak Wadhawan, CA. Manu Chadha, CA. Santosh Nair and CA. Amit Roy for their devotion in terms of time as well as views and opinions to the cause of the professional and the national development. I also wish to place on record the efforts put in by CA. Puja Wadhera, Secretary, Internal Audit Standards Board and CA. Arti Agarwal, Executive Officer, in finalising the Guide.

I am sure that the readers would find this Guide immensely useful. I eagerly look forward to the feedback of the readers on the Guide.

Kolkata **Abhijit Bandyopadhyay**

15th December, 2008 ***Chairman, Internal Audit Standards Board***

Glossary

Risk	Risks are those uncertainties which impede the achievement of the objective.
Risk Capacity	Risk capacity is the quantum of risk that an organization can absorb without affecting its business objectives.
Risk Appetite	Risk appetite is the level of risk which an organization is willing to accept.
Risk Response	Risk response is the measures that an organization takes to ensure that the overall risk levels within the organization are within its risk appetite.
Inherent Risk	Inherent risk is the quantum of risk without considering the existing controls within the organization to mitigate that risk.
Residual Risk	Residual risk is the quantum of risk after considering the existing controls within the organization to mitigate that risk.
Internal Risk	Internal risks arise from the events taking place within the business enterprise. Such risks arise during the ordinary course of a business.
External Risk	External risks arise due to the events triggered in the environment outside the business organization.
Controllable Risk	Controllable risks are those risks where the management is able to implement measures either to prevent those risks or minimize their impact.
Non-Controllable Risk	Non-Controllable risks are those risks which the management may not be able to anticipate effectively and will need to resort to detective measures or procedures post the risks has occurred to minimize their impact.

Enterprise Risk Management	A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives – COSO Enterprise Risk Management – Integrated Framework, 2004.
Residual Risk	Residual risk is the quantum of risk after considering the existing controls within the organization to mitigate that risk.
Risk Quantification	Risk quantification involves assigning an economic value to the risk based on its likelihood and impact.
Risk Events	Events which negatively impact the organization's objectives.
Opportunities	Events which could positively impact the organization in achieving its objectives.
Risk Assessment	Risk assessment is a process of classifying and prioritization of risks based on their impact and likelihood.
Controls	Controls are activities which ensure that the risk response is implemented for the identified risks.
Residual Risk Portfolio	Residual risk portfolio is an inventory of risks after considering the existing mitigating controls.

Contents

Chapter 1

Introduction

1.1 Rapid and continuous change in the business environment is encouraging management to increasingly become more risk focused. Global extraordinary events as the financial meltdown has further enhanced the need for companies either to strengthen their risk management procedures or implement a robust framework to consolidate their fragmented risk management activities.

1.2 Business planning and annual budgeting process is a key tool for management to operationalise its vision and goals. The business planning process has matured significantly over the last two decades. Earlier, planning meant taking out a yearly business plan based on usually a percentage change from the previous year. Increasing competition since the 1990s has resulted in business plans being based more on the outcome of a strategy and less on working on the previous year's spreadsheets. Late 1990's saw a strong correlation between current market price (CMP) of shares and management's performance in meeting their quarterly forecasts. This necessitated managing risks more effectively in shorter time spans of a quarter instead of six months or a year as earlier. The importance of bringing qualitative improvements in quarterly plans and carrying out tactical measures to meet them has also become an important agenda in the short run. Leading companies are now considering risk management as an integral element of the annual budgeting process wherein costs (e.g., capital expenditure, increase in operational costs, insurance costs, etc.) to manage risks effectively are adequately estimated and planned for.

Table 1: Basis of Making the Yearly Business Plan

Period	*Driver of plan*	*Basis of the plan*
1980's	Business- as usual	New targets were prepared by making a percentage change to last year's figures.
1990's onwards	Competition	Outcome of strategy meetings drove targets in the new business plan.
2010's (projected)	Events arising out of the business environment	Anticipated risks that threaten objectives have started playing a crucial role in framing strategies.

1.3 One of the ways entities managed risks in shorter duration of time has been to create a risk management culture at different levels of the entity. The higher the level of risk maturity of an entity, the better prepared it is to either convert market uncertainties into opportunities or implement the measures to reduce their exposures. The aim of a robust Enterprise Risk Management (ERM) framework is to help the organisations manage their risks effectively, reduce the possibilities of any surprises with large exposures and continuously enhance the maturity levels. ERM is evolving more as an important strategic tool for management in turbulent market environment.

1.4 The objective of this Guide is to provide guidance on implementing an Enterprise Risk Management (ERM) Framework.

Chapter 2

Risk Management

Understanding Risk and Its Assessment

Meaning of Risk

2.1 Entities exist for a purpose. For private sector, the purpose is to enhance shareholder value. Government or not-for-profit organizations may have the main purpose of delivering service or other benefits in public interest.

2.2 Achievement of organisational objectives is surrounded by the uncertainties which pose threats to and offer the opportunity for increasing success. Changing circumstances, such as rising interest rates, can be an opportunity for an entity with surplus cash but a risk for a borrower. Hence, these circumstances need to be seen with reference to the organisation's objectives:

- When used in the broad sense, risks are those uncertainties of outcome, whether an opportunity or threat, arising out of actions and events.
- When defined narrowly, risks are those uncertainties which impede the achievement of the objective.

2.3 In this Guide, 'risk' is used in the narrow sense.

Classification of Business Risks

2.4 Business risks impede the achievement of the organisation's goals and objectives. In order to make an inventory of risks, *viz.* the risk register, it is important to understand the broad classification of risks. For example, risks can be classified into various categories such as internal and external risks; controllable and uncontrollable risks, etc.

2.5 Classifications helps in a better understanding of the interplay between the risks themselves and between objectives, strategies, processes, risks and controls during risk assessment.

Internal and External Risks

2.6 Internal risks arise from events taking place within the business enterprise. Such risks arise during the ordinary course of a business. Risks of this nature can be effectively controlled/managed through implementing processes/controls within the organisation. Management is able to exert a significant influence in managing these risks. Examples of internal factors giving rise to such risks include:

- *Human factors* such as strikes and lock-outs by trade unions; negligence and dishonesty of an employee; accidents or deaths in the factory, etc.
- *Technological factors* such as unforeseen changes in the techniques of production or distribution resulting into technological obsolescence, etc.
- *Physical factors* such as fire in the factory, damages to goods in transit, etc.

2.7 External risks arise due to the events triggered in the environment outside the business organisation. Such events are generally beyond the control of the management. Hence, determining the likelihood of the resulting risks cannot be done with accuracy. Examples of external factors giving rise to such risks include:

- *Economic factors* such as price fluctuations, changes in consumer preferences, inflation, etc.
- *Natural factors* such as natural calamities such as an earthquake, flood, cyclone, etc.
- *Political factors* such as the fall or change in the Government resulting into changes in government policies and regulations, communal violence or riots, hostilities with the neighboring countries, etc.

Controllable and Non-Controllable Risks

2.8 Controllable risks arise from the events taking place within the business enterprise. Such risks arise during the ordinary course of business. These risks can be forecasted and the probability of their occurrence can be determined. Hence, they can be controlled by the management to an appreciable extent (e.g., risks of fire, storms, etc.,). Controllable risks need not necessarily be prevented, but the financial loss can be minimised (e.g., insurance cover can be purchased to recover the financial loss due to fire).

2.9 Uncontrollable risks, however, are those that would have a detrimental financial impact but cannot be controlled. Some uncontrollable risks that are common to many businesses include:

- Recessionary economy
- New competitor locating nearby
- New technology

Each organisation faces risks that are unique to its line of business. Organisation should consider these carefully and briefly describe what steps would be taken if an uncontrollable risk actually happens to the business (contingency plan). For example, if the risk of a recession would severely affect the company, the management may consider what products or services could be offered that would not be as sensitive to a recessionary economy.

Table 2: Typical Pattern of Risks in an Entity

	Controllable	***Uncontrollable***
Internal risks	**Maximum number of risks**	
External risks		**Maximum number of risks**

Risk Quantification Method - Attributes, Measurement and Risk Score

2.10 All risks are measured on two attributes i.e.,

- Likelihood of risk occurrence
- Risk consequence

All risks need to be evaluated at two levels, i.e., Inherent Risk Level and Residual Risk Level.

2.11 To facilitate an understanding and usability in decision making of the risk, comparison helps. To enable comparison a risk score is used. By measuring the two risk attributes, a risk score can be derived for that risk. However, care should be taken to avoid misplaced focus on numbers. Risk score is meant for comparison between a cut off point, normally, the 'risk appetite'' or comparing to other risks, thereby, filtering for 'significant risks'.

2.12 The measurement of the likelihood of the risk is normally on a scale of five, *viz.*

- Remote (score 1)
- Unlikely (score 2)
- Possible (score 3)
- Likely (score 4)
- Almost certain (score 5)

Exhibit 1: Measurement Yardstick for the Likelihood of Risk

Likelihood of Risk Occurrence		
Level	***Description***	***Ranking Criteria***
1	Remote	Event may only occur in exceptional circumstances
2	Unlikely	Event could occur in rare circumstances
3	Possible	Event could occur at some time
4	Likely	Event could occur in most circumstances
5	Almost certain	Event is expected to occur in most circumstances

2.13 Risk consequences can also similarly be measured on a scale of five, *viz.*

- Insignificant (score 1)
- Minor (score 2)
- Moderate (score 3)
- Major (score 4)
- Catastrophic (score 5)

Exhibit 2: Measurement Yardstick for Risk Consequences

Risk Consequence		
Level	**Description**	**Ranking Criteria**
1	Insignificant	• Rs. 50 lakhs impact on profitability • No impact on market share • No impact on reputation

2	Minor	• Rs. 50 lakhs Rs. 2 crores impact on profitability • Consequences can be absorbed under normal operating conditions • Potential impact on market share • Potential impact on reputation
3	Moderate	• Rs. 2 crores to Rs 5 crores impact on profitability • There is some impact on market share • There is some impact on reputation
4	Major	• Rs. 5 crores to Rs 10 crores impact on profitability • Market share will be affected in the short term • Reputation is affected in the short term
5	Catastrophic	• Rs. 10 crores impact on profitability • Serious diminution in reputation • Sustained loss of market share

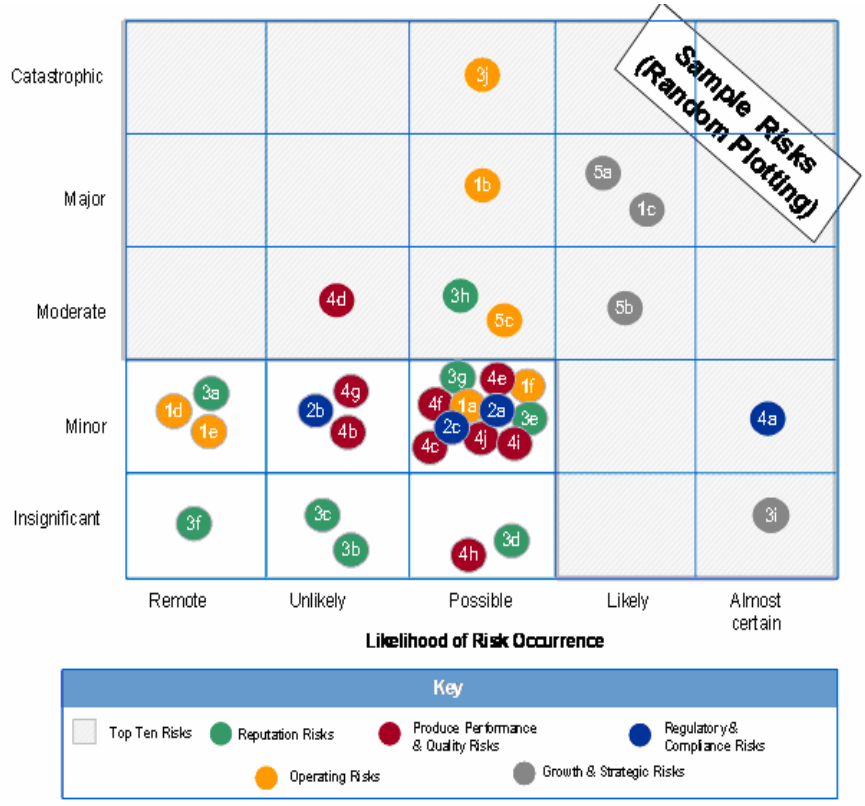
Level	Description	Impact	Resulting in	Illustrations
1	Insignificant	Low	Causes minor inconvenience without impacting the achievement of objectives	• No potential impact on market share • No impact on brand value • Issues would be delegated to junior management and staff to resolve
2	Minor	Low to Moderate	Causes inconvenience without impacting the achievement of objectives	• Consequences can be absorbed under normal operating conditions • There is a potential impact on market share and brand values • Issues will be delegated to middle management for resolution

3	Moderate	Moderate	Preventing the organisation from achieving some of it's objective for limited period	• Market share and/or brand value will be affected in the short term • The event will require senior and middle management intervention
4	Major	Moderate to High	Preventing the organisation from achieving majority of it's objective for a long time	• Serious diminution in brand value and market share with adverse publicity • Key alliances are threatened • Events and problems will require Board and senior management attention
5	Catastrophic	High	Closing down of the organisation/ operation or significant part for a long time	• Loss of key alliances • Sustained, serious loss in market share

A risk with the lowest level of likelihood – i.e., remote (score 1) can nevertheless have the highest level of consequences – i.e., catastrophic (score 5). This can be explained by way of an example. The likelihood of floods causing a damage to the distribution network of an electricity distribution company can be 'remote' but the consequences of the damage can be catastrophic. In such a scenario, the existence of a contingency plan becomes important.

Risk score for that risk is a numeric multiple of the likelihood of the risk and the risk consequences. As an example, the Board may have a risk appetite of 12 and any risk with a score above 12 becomes a significant risk for which a risk response is required. For a better understanding, risk score can be plotted on a chart as below which is known as a *"risk heat map".*

Figure 1: Risk Prioritisation Map



Basic Concepts of Risk Management

Risk Capacity

2.14 Risk capacity shows how much risk the organization can absorb.

Risk Appetite

2.15 Risk appetite shows how much risk the management is willing to accept.

Risk Response

2.16 The purpose of assessing and addressing risks is:

- To constrain them to a tolerable level within the risk appetite of the organization (i.e., how much risk the management is ready to accept).
- To give a response to risks (i.e., aspects of addressing risks).

2.17 Risk response can be of the following types:

Avoid	Exiting the activities giving rise to risk. Risk avoidance may involve exiting a product line, declining expansion to a new geographical market, or selling a division.
Reduce	Action is taken to reduce the risk likelihood or impact, or both. This, typically, involves any of a myriad of everyday business decisions.
Share/Transfer	Reducing the risk likelihood or impact by transferring or, otherwise, sharing a portion of the risk. Common techniques include purchasing insurance cover, outsourcing activities, engaging in hedging transactions.
Accept	No action is taken to affect the risk likelihood or impact. This is mainly in cases where the risk implications are lower than the Company's risk appetite levels.

Inherent Risk and Residual Risk

2.18 Inherent risk is the level of risk, assuming no internal controls, while residual risk is the level of risk after considering the impact of internal controls. E.g., the risk of 'over/understatement of revenue' without considering any internal controls indicates an inherent risk. The above risk when considered with internal controls in place (say, monthly reconciliation of revenue and follow up, correction of discrepancies, etc.) indicates a residual risk.

Control Score

2.19 The objective of internal controls is to reduce the inherent risk and keep the residual risk within the organization's risk appetite. The gap between the inherent risk and residual risk shows the strength of the control and is known as the control score.

Risk Register

2.20 Risk register is a detailed record of each risk.

2.21 Typically, a risk register contains information in columns which shows against each risk - the process and sub process that individual risk belongs to,

the risk score before and after controls are applied, which controls to apply, name of the process owner, etc.

Risk Maturity of an Organization

Importance of Risk Maturity and the Four Questions

2.22 A matured outlook to risk facilitates quality business decisions. To take a matured view, there is a need to know against objectives:

- What events can trigger what risks?
- What is the risk score (likelihood and magnitude) of the risk?
- How does the risk score measure against the risk appetite?
- What should the risk response be?

Most of us at an individual level do not follow the above four questions in a formal and structured way. However, after setbacks we form a pattern of action which works for us and we do this by subconsciously figuring out the answers to the above four questions.

2.23 Certain entrepreneurial driven entities, especially, those which are highly successful in a relatively short span appear to have an extraordinary risk appetite and risk capacity. They seem to work on a very high residual risk and are seen as risk takers. Case histories point out that sustainable success has mainly come to those entities where the risk maturity is at the *risk enabled level, i.e., the entity in a readiness position to convert market uncertainties into opportunities.*

2.24 The way entities have an outlook to managing risks defines their level of risk maturity.

2.25 Some organizations, especially, those in the fast growth mode have an organizational culture which promotes operational mangers to remain at the risk naïve/risk aware maturity level. Following are the typical characteristics:

- Line managers are not expected to identify risks and if they do it is confined to their personal knowledge or within their functional team.
- Control environment may be well defined but again it is to be operated by the staff management (as the Accounts Manager). The logic being that line management as Marketing or Production managers need to spend the maximum time in operations and not defocused on unnecessary paper work or issues other than their operations.

In this mindset, coordinating activities and problem solving is considered as operations while risk assessment and management is considered a staff function. This model works well in a supply side market but not in a dynamically changing competitive market wherein new risks arise periodically and the staff management who are not market facing are not fast enough to incorporate new controls to address these risks.

Risk Maturity Levels

2.26 Following aspects in the organisation indicate its risk maturity:

- Business objectives are defined and communicated;
- Risk appetite is defined and communicated across the organisation;
- Control environment is strong, including the tone at the top; and
- Adequate processes exist for the assessment, management and communication of risks.

A model score card to assess risk maturity is given in **Appendix 1.**

2.27 The table given below shows the levels of risk maturity.

Table 3: Key Characteristics at Different Levels of Risk Maturity

Risk Maturity	Key Characteristics
Risk Naïve	No formal approach is developed for risk management.
Risk Aware	Risks are identified within functions and not across processes. Also risks are not communicated across enterprise. Also known as '*silos based approach to managing risks.'*
Risk Defined	Risk strategy, policy and framework in place and communicated. Risk appetite is defined. Risks start getting viewed across processes. Enterprise wide approach to risk management being developed.
Risk Managed	Enterprise wide approach to risk management is implemented and communicated. Risk register is in place. Also known as *'satisfactory implementation of ERM* stage'.
Risk Enabled	Risk management and internal control are fully embedded into operations. Entity is in readiness position to convert market uncertainties into opportunities.

***A. Risk Enabled and Risk Managed*:**

This entity represents a high level of understanding on the management of risk.

***B. Risk Defined*:**

Approach to risk identification is within functions and not across end-to-end processes. Risk register is incomplete.

C. Risk Aware and Risk Naïve:

Risks are either not identified or each person maintains his/her risk within personal knowledge.

Risk Management as Part of Clause 49 Compliance and Later as a Strategic Management Tool

2.28 As per Clause 49 of the Listing Agreement, disclosures to the Board are to be made on whether the following is being carried out on risk management.

"The company shall lay down procedures to inform Board members about the risk assessment and minimization procedures. These procedures shall be, periodically, reviewed to ensure that the executive management controls risk through a proper defined framework".

2.29 To comply with the requirements of the above clause, organizations tend to introduce certain risk management processes and identify strategic risks mainly to fulfill compliance requirements. Over a period of time, as the management realises the advantages of improving the level of risk maturity within the organization, it reassesses risks through an enterprise wide structured, consistent and continuous process and implements risk management in a full fledged way as a strategic management initiative.

2.30 This methodology is known as Enterprise Risk Management or ERM. First, an ERM policy is put in place which defines the guiding principles showing the responsibility of line management for ERM and the broad activities covered by the risk management processes. A risk management framework to implement the ERM policy is, then, finalized showing the activities which need to be carried out and how they are to be carried out under three processes, *viz.*

- Risk assessment
- Risk management

- Risk communication

A model risk assessment process is given in **Appendix 2**.

Implementation is facilitated by a risk manager or the internal auditor as a consulting assignment. Subsequently, risk-based internal audit is carried out.

2.31 ERM includes the following activities:

- Establishing an appropriate internal environment, including a risk management policy and framework;
- Defining risk appetite;
- Identifying potential threats to the achievement of its objectives and assessing the risk i.e., the impact and likelihood of the threat occurring;
- Undertaking control and other response activities;
- Communicating information on risks in a consistent manner at all levels in the organization;
- Centrally monitoring and coordinating the risk management processes and the outcomes, and
- Providing an assurance on the effectiveness with which risks are managed.

Need for Clarity on the Risk Appetite of the Board

2.33 Determining the risk appetite for the organisation is central to the ERM methodology. *Risk appetite* refers to the extent of the risk that the organsations are willing to take to pursue the objectives. Risk appetite setting is done at different levels, *viz.,* for the organization at the entity level, process level, different risk groups and for individual key risks. Risk appetite provides a standard against which a risk can be compared and where the risk is above the risk appetite. It is considered a threat to the reasonable assurance that the objective will be achieved. The risk appetite is a key fundamental of the ERM methodology and needs to be approved by the Board of Directors.

Chapter 3

Implementing COSO* ERM

Introduction to COSO's ERM

Definition of Enterprise Risk Management

3.1 *"Enterprise Risk Management is a process, effected by an entity's Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide a reasonable assurance regarding the achievement of entity objectives"*. – COSO Enterprise Risk Management – Integrated Framework, 2004.

3.2 As per the COSO definition, enterprise risk management encompasses:

- **Aligning risk appetite and strategy**. The management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- **Enhancing risk response decisions**. Enterprise risk management provides the rigor to identify and select among alternative risk responses—risk avoidance, reduction, sharing, and acceptance.
- **Reducing operational surprises and losses.** Entities gain an enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.

---

* Comprising the professional associations listed below, the Committee of Sponsoring Organizations (COSO) is a voluntary private-sector organization:

- American Accounting Association
- American Institute of Certified Public Accountants
- Financial Executives International
- Institute of Management Accountants
- The Institute of Internal Auditors

COSO is dedicated to guiding the executive management and governance entities toward the establishment of more effective, efficient, and ethical business operations on a global basis. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis, and best practices.

- **Identifying and managing multiple and return cross-enterprise risks.** Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates an effective response to the interrelated impacts and integrated responses to multiple risks.
- **Seizing opportunities.** By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
- **Improving deployment of capital.** Obtaining a robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

3.3 The COSO definition is an advanced framework for ERM; however, each organization may adopt a framework suitable to its need and gradually move from a risk naive to the risk enabled level.

The Approach is at an Enterprise-wide Level and not at a Departmental/Function Level

3.4 Enterprise wide means an elimination of functional, departmental or cultural barriers so that a truly holistic, integrated, proactive, and process oriented approach is taken to manage all key business risks and opportunities – not just financial risks. Further, an entity-wide approach also assists the management in consolidating all the fragmented risk initiatives various departments and channelise resources effectively to manage the most important risks. This new risk management is a shift from the old process of managing risk. The transformation is depicted as below:

3.5 COSO ERM is always implemented across an entity and covers the entire spectrum of business organizations, i.e., subsidiary, business unit, division, etc.

Benefits of Enterprise Risk Management

3.6 ERM when implemented in a right manner can yield substantial benefits to an organization. Companies which are considered to be well governed get a premium both by rating agencies and shareholders. Some primary benefits include:

- Better-informed decisions
- Greater management consensus
- Increased management accountability
- Smoother governance practices
- Ability to meet strategic goals
- Better communication to Board
- Reduced earnings volatility
- Increased profitability
- Use risk as a competitive tool
- Accurate risk-adjusted pricing

Source: 'Beyond Compliance – The Future of Risk Management', The Conference Board (Jan 2005).

In addition, ERM helps to reduce the level of surprises which impact organizational goals. Organizations who implement ERM define a risk appetite which they are able to operate effectively and take more informed and appropriate decisions.

Why COSO ERM

3.7 Organizations are becoming more and more aware of the need and importance of implementing an enterprise risk management framework. The challenge in implementing ERM is applying the theory in practice since, COSO framework is the most widely accepted framework for ERM, in this guide we try to break down and analyze the COSO components of ERM to facilitate practical implementation.

Before Getting Started

3.8 In any ERM, before starting the implementation there are certain

important infrastructural requirements to be put in place, without which the implementation may not be successful. These are as follows:

- Creating an awareness amongst the Board and senior management about the need and requirement of ERM. This is important to set the tone at the top.
- It is also important to understand the extent of ERM implementation required. There are various levels at which ERM could be implemented e.g., Low (naïve) to High (enabled). Hence, it is necessary to set the expectations right at the beginning by defining expectations.
- An organization may have an existing risk management framework, so it is necessary to highlight the changes from the existing approach. Further, the organization should be open enough to admit the shortcomings of the existing process and appreciate the need for a more integrated and detailed approach towards risk management.
- Creating an adequate project sponsorship, requisite fund allocation for various activities to ensure that the objectives are met. The project funding would determine the extent of implementation.
- Define the project organization and ensuring the involvement of various executive levels across the organization starting from the Board of Directors to the lower levels of management. The number and extent of the involvement at each level would vary with every organization.

Above all, each organization must understand that it is unique and has its own inherent complexities, industry culture, organizational cultures which it needs to respond. Thus, the ERM approach to be followed needs to be customized to suit each company. In this guide, we try to generalize the implementation steps.

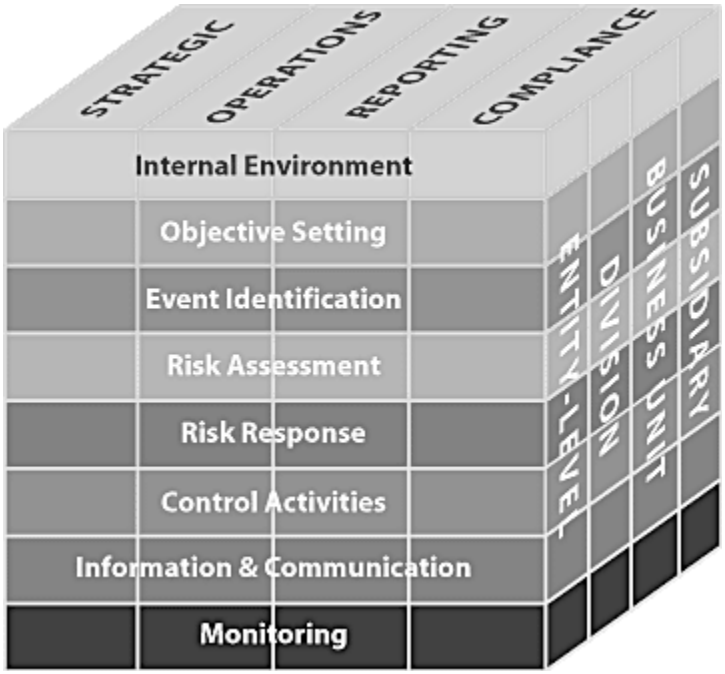
COSO ERM Implementation

Components of ERM Implementation

3.9 Having established that the implementation has to be across an entity, the components to be implemented are:

- Preparing the internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response

- Control activities
- Information and communication
- Monitoring.



Source: COSO Integrated Framework

Step 1: Preparing the Internal Environment

3.10 The first step is to prepare the internal environment of an organization for the ERM implementation. This would involve the preparedness of the organization from the Board to the junior management level for the ERM. The organization would also define its risk management philosophy and risk appetite during this stage. Any organization aiming at an ERM needs to set the right ethical culture within the organization, this includes establishing a code of conduct, and whistle blower policy to ensure an appropriate ethical culture within the organization which is a premise for risk management. Once the internal environment is set up, the organization would then define the ERM project structure, assign the project responsibility and authority.

3.11 Key output of this stage are:

- Risk Management Philosophy
- Risk Management Survey and its outcomes
- Code of Conduct
- Project Structure

3.12 Guidance to preparing the internal environment is given in **Appendix 3**.

Step 2: Objective Setting

3.13 Once the internal environment of an organization is ready for the ERM initiative, the next step is to set the objectives. The ERM requires that the organisation's mission, its strategic objectives, derived objectives be aligned. Further, the derived objectives should also reflect that they are in line with the overall organizational objective. The strategic objectives thus translate into operational, reporting and compliance objectives. Such an alignment facilitates further steps of event identification, risk assessment and mitigation in an ERM implementation process. Another important aspect is defining an organisation's risk appetite at an overall level and even at the sub unit levels. The risk appetite defines the extent of risks that an organization is prepared to accept. Based on the risk appetite, the organization then defines the risk tolerance levels.

3.14 Key output of this stage are:

- Linkage of mission-strategic objectives-derived objectives
- Defining strategies by using risk management techniques
- Defining overall risk appetite for various business activities
- Defining risk tolerances for sub activities in line with the overall risk appetite for the business activities.

3.15 Guidance on Objective setting is given in **Appendix 4**.

Step 3: Event Identification

3.16 The next step in an ERM implementation is the identification of the events which may affect the entity positively or negatively in achieving its objectives. Such events can be classified as risks and opportunities, depending on their impact. An organization should also consider the interdependencies of events on the organization as whole. An event, individually, may not affect an organization, however together with other events, it might increase the impact. These events are also termed as risks.

3.17 There are various techniques for the identification of events, e.g., interviews, questionnaires, workshops, etc. Some of these techniques are discussed in detail in this Guide.

3.18 Key outputs of this stage are:

- Interviews, workshop for event identification
- Linkage of events to objectives
- Event inventory for further actions

3.19 Guidance on Event Identification is given in **Appendix 5**.

Step 4: Risk Assessment

3.20 Once events/risks are identified, the next step is assessing the risks in terms of their impact on the objectives and the likelihood of such an impact. This is done by assigning qualitative and quantitative values to each risk event and its likelihood. All risk events need to be first evaluated on an inherent basis (considering their impact assuming that there is no remediation or response mechanism). These risks should then also be assessed after consideration of the available response mechanism to assess their residual risk. Such assessment would facilitate in risk ranking and subsequent prioritization for remediation.

3.21 Guidance on Risk Assessment is given in **Appendices 2** and **6**.

Step 5: Risk Response

3.22 The next step to risk assessment is developing a response to the risks identified in earlier stages. Management needs to evaluate each risk based on its gross risk (identified earlier) and develop or identify existing response mechanism to ensure that the net/residual risk (after considering the response) is within the risk tolerance levels of the organization. Management should also perform a cost benefit evaluation of the risk response, since all responses may not be suitable in a particular scenario and response needs to be customized to each organization. Response to the risk can be as follows:

1) Avoid
2) Reduce
3) Share
4) Accept

3.23 Key output at this stage are:

- Risk Response for risks identified
- Risk portfolio after considering the residual risk

3.24 Guidance on risk assessment is given in **Appendix 7**.

Step 6: Control Activities

3.25 Risk response is the starting point of risk mitigation; however risks can be mitigated only when the response is implemented. Similarly, responses across the organization at various levels should also be implemented. Controls are activities which ensure that the risk response is implemented for the identified risks. Thus, each of the risk response would have a control activity to support the risk response. Control activities include activities like reviews, approvals, authorizations, schedule of authority, policies, procedures, segregation of duty, safeguarding of assets and key performance indicators.

3.26 Guidance on Control Activities is given in **Appendix 8**.

Actioning the Balance Components of COSO ERM

Information and Communication

3.27 The first seven stages of the COSO framework are sequential. However, information and communication flow has to be smooth and efficient throughout all other phases. A successful ERM implementation requires that right information is captured in the right amount of detail across all levels of the organization. Management needs to develop efficient information flows within and outside the organization. Further, obtaining the right information is just one aspect, the most important part is to effectively communicate the information throughout the organization from top to bottom and otherwise. Each individual within an organization needs to understand his roles and responsibilities in the implementation. Further, there should be adequate escalation mechanisms. Communication also involves communication with various stakeholders within and outside the organization (e.g., suppliers, customers, regulators, etc).

3.28 The following should be ensured while establishing information and communication flows within an organization:

- Information should be captured at various points within an organization.

- Information should also be obtained from external sources (internet, subscribed databases, research agencies, external consultants, newsletters, industry forums, etc).
- Information obtained should have adequate detail, must be relevant, structured, accessible, usable and accurate.
- Information repositories should be created at various levels for retrieving the data as per need.
- Systems need to be developed which provide the required data for all risk management purposes.
- Management information systems should ensure that performance indicators for all activities within the organization are captured accurately for a review and monitoring of activities.
- Degree of sophistication and usage of technology should commensurate the organization's need, maturity and capability.

Communication

3.29 The organization needs to ensure that communication systems are established throughout the organization. There are various means by which communication systems can be established, some of them are:

- Intranet and intranet databases
- Emails
- Communiqués
- Discussion Forums
- Corporate newsletters
- Meetings among risk management teams, executive and line functions
- Resource database for enterprise risk management
- Anonymous emails for reporting incidents

At any point, effective communication is imperative since each and every individual within the organization should be aware of his roles and responsibilities in managing business and managing risks.

Monitoring Activities

3.30 Once the ERM implementation is underway, the next step is to ensure that there is adequate monitoring of the activities, to ensure that the risk response mechanisms and control activities are ensuring that the objectives are achieved. Monitoring mechanisms need to be instituted

internally and at periodic intervals by way of external assessments. External assessments would provide an assurance that the internal monitoring is working effectively. In addition to monitoring mechanisms, there should also be adequate escalation of significant issues to middle, senior management and Board of Directors.

3.31 Most common monitoring mechanisms include:

- Periodic operational performance monitoring against targets.
- Monitoring of key performance indicators.
- Monitoring of critical success factors for projects and new businesses.
- Embedded controls which escalate deviations as a trigger for adequate corrective actions.

3.32 Most common evaluation mechanisms include:

Internal Evaluations

- Management Information Systems.
- Self Assessment Questionnaires.
- Internal Control Assessment.

External Evaluations

- Internal audit reviews.
- Cross functional team reviews.
- External consultant reviews.
- Project audit reviews.

3.33 Essentials for effective monitoring include:

- Pre-determine the methodology for evaluations
- Ensure adequate documentation with respect to ERM (e.g. The model implemented, the ERM organization structure, roles and responsibilities, risk framework, risk registers, control framework, self assessment questionnaires, etc).

Chapter 4

Implementation Issues

Implementing ERM

4.1 Based on the understanding mentioned herein, the ERM implementation activities could be summarized as follows:

Board Level Activities

4.2 The Board level activities include:

- Provide ERM education at the Board level.
- Establish buy out at the Board level for risk appetite and risk strategy.
- Develop the ‘‘ownership’’ of risk management oversight by the Board.
- Review the risk report of the enterprise.

Management Level Activities

4.3 The Management activities include:

- Create a high level risk strategy (policy) aligned with business objectives.
- Create a risk management organizational structure and ensure clear reporting lines.
- Develop and assign the responsibilities for risk management.
- Communicate Board vision, strategy, policy, responsibilities and reporting lines to all employees.

Establish a Common Risk Culture

4.4 These include:

- Using a common risk language and concepts.
- Communicating about the risk using appropriate channels and technology.

- Developing training programs for risk management.
- Identifying and training "risk officers".
- Providing success stories and identifying quick wins.
- Aligning risk management techniques with the company culture.
- Developing a knowledge sharing system.

Embed Risk Activities Into Ongoing Business Processes

4.5 These include:

- Aligning and integrating risk management process within business processes.
- Embedding real time controls related to the risk into digital systems as appropriate.
- Developing continuous improvement processes related to the risk.

Measure and Monitor Risk

4.6 These include:

- Identifying key performance indicators and critical success factors related to the risk.
- Establishing success measures for risk strategy and activities.
- Providing a periodic process for measuring the risk/return.
- Identifying and implementing monitoring processes and methods of feed back.

Guide Identifying and Assessing a Risk from an ERM Perspective

4.7 At various places in this Guide, identifying and assessing risks have been mentioned. However, these activities although sounding straight forward and simple, are the most difficult aspects of an ERM implementation. Identification and assessment of risks needs to be comprehensive and all aspects need to be considered while performing these activities. For a better understanding of these activities, certain aspects that need to be considered while performing risk identification and assessment have been discussed below.

4.8 Risks can be categorized into the following broad categories:

(i) Strategic Risk
(ii) Operational Risk
(iii) Reputation Risk
(iv) Financial Reporting
(v) Regulatory or Contractual Risk
(vi) Financial Risk
(vii) Information Risk
(viii) New Risks not identified or categorized erstwhile

4.9 One needs to identify a certain set of questions while identifying and assessing the above risks. Some indicative questions are as follows:

Strategic Risk

- Are critical strategies appropriate to enable the organization to meet its objectives?
- What are the risks inherent in those strategies and how might the organization identify, quantify, and manage these risks?
- How much risk is the organization willing to take?
- What risks result from e-business developments?

Operational Risk

- What are the risks inherent in the processes that have been chosen to implement the strategies?
- How does the organization identify, quantify and manage these risks given its appetite for risk? How does it adapt its activities as strategies and processes change?

Reputation Risk

- What are the risks inherent to brand and reputation inherent in how the organization executes its strategies?

Financial Reporting

- What are the key risks which if not managed effectively will lead to an incorrect reporting of financial results/performance and disclosures to stakeholders?

Regulatory or Contractual Risk

- What risks are related to the compliance with regulations or contractual arrangements- not just those which are financially based?

Financial Risk

- Have operating processes put financial resources at undue risk?
- Has the organization incurred an unreasonable liability to support operating processes?
- Has the organization succeeded in meeting measurable business objectives?

Information Risk

- Is our data/ information/knowledge reliable, relevant and timely?
- Are our information systems reliable?
- Do our security systems reflect our e-business strategy?

New Risks

- These might include the risks from new competitors, emerging business models, recession risks, relationship risks, outsourcing risks, political risks, financial risk disasters (rogue traders), and other crisis and disasters risks.

Approach to Risk Management by Organizations (Centralized vs. Decentralized)

4.10 ERM could be implemented in an organization using both centralized or a decentralized approach. This would depend on the nature and preferences of each organization. There is no prescribed method for ERM and organizations may select any of the approach or even a hybrid version of both the approaches. Some important aspects in respect of centralized and decentralized risk management have been discussed below.

Centralized Risk Management

- Focus on the risks that affect the achievement of key corporate objectives and strategies and significantly affect most if not all functions and processes (e.g., reputation). These risks are referred to as enterprise wide risks.
- Accountability for these enterprise wide risks is with the CEO, risk committee and the Board of Directors.

- Responsibility for these risks may be dispersed throughout the organization.
- Risks which require specialized skill sets which are not available at division levels or those which require partnering or contracting at the corporate level are also handled centrally.

Decentralized Risk Management

- Decentralized management pushes the risk management activities to those who live with it on a day to day basis.
- Such an approach is more suited for the risks at the division or process level, such risks are significant for the division/process but may not significantly affect the organisation's ability to achieve its overall objectives.

4.11 Certain organizations are now embedding a hybrid version of the above approaches and using centralized approach for entity wide risks and decentralized for the division or process level risks. In this manner they incorporate the best features of both the approaches.

Sustaining ERM and Continuous Improvement Processes

4.12 Once a certain degree of assurance of the adequate functioning of the ERM program is achieved, organizations should focus on sustaining ERM and continuous improvement opportunities. The following mechanisms could be used for this purpose:

Benchmarking

4.13 Organizations should continuously focus on Benchmarking ERM programs with the best in the class companies and align the best practices across related entities.

Knowledge Management

4.14 Organizations should develop effective communication channels within and outside the organization to ensure a smooth flow of information at all levels within the organization. This facilitates knowledge sharing of the risks and opportunities within the organization.

Risk Management Triggers

4.15 Focus on developing a robust ERM management information system which will highlight key risk exposures to the senior management in case and

key risk indicators e.g., increased levels of credit exposures, increased cost of capital, etc., are breached or on the occurrence of certain triggers e.g., high volatility in foreign exchange rates, sharp increase or decrease in commodity prices, etc.

Organization Learning

4.16 Creating an awareness and educating the employees throughout the organization about risk management inculcates a risk culture within an organization. This would then be beneficial for the smooth implementation and absorption of the entities risk strategy, policy and processes throughout the organization. This would also help the alignment of processes and technology in line with the ERM plan. Learning and awareness should be ensured in the following areas:

- Linking risk management with business operations.
- The existing risk management organization and infrastructure.
- Risk strategies and policies.
- Risk language and risk assessment process.
- Objectivity in self assessment.
- Risk quantification methods used by the company.
- Escalation protocols across the organization.

4.17 Such an emphasis on the continuous improvement of risk strategies, policies and processes would result in:

- Continuous improvement and knowledge transfer.
- Enhancing capabilities even in cases where the people, processes and technology change.
- Development of a risk management process independent of the people and philosophies.
- Avoidance of subjectivity due to personal perception and the organization would speak the organization's language and not the individual's language with respect to ERM.

This would result in a continuously evolving ERM program which would be in line with the dynamics of the changing business environment within and outside the organization.

Chapter 5

Case Studies

After understanding the process of ERM implementation within organizations, in this section, how some of the leading Indian companies have approached ERM is discussed. This would help in understanding the practices followed by select companies who have already recognized the value of ERM and have embedded ERM in their operations. In this Guide, three detailed case studies of large companies in the IT sector which have matured in their ERM practices are discussed. In addition, four brief case studies are also discussed wherein the risk management framework/practices implemented by companies in other industries are highlighted.

CASE STUDY-1

An IT Company Having Operations in Various Countries

Risk Management Objectives

- The Enterprise Risk Management (ERM) program is aimed at meeting stakeholder expectations and avoiding surprises which affect the business adversely.
- Risk management practices are used for achieving competitive advantage.

Risk Management Approach

- To ensure that the overall risk exposure is within the risk appetite of the organization.
- Perform a cost benefit analysis of risk responses to ensure that the best alternative is implemented.

Risk Management Methodology

- Escalation mechanisms have been developed within the organization to identify the significant risk for taking necessary actions.

- The company conducts a risk survey and obtains the inputs from key stakeholders.
- Responsibility is attached to individuals within the organization for risks and their mitigation.
- Risks, risk mitigation and controls are tracked to ensure that the overall exposure is within the requirements.
- Risks are periodically reported to the risk council and risk management committee for their review and insights.

Risk Organization

Level	*Role*
Board of Directors	Oversees risk management performed by the Executive Management
Risk Management Committee	Comprises completely of Independent Directors Oversees risk management on behalf of the Board Makes recommendations on the risk management program
Risk Council	Comprises the CEO, COO and CFO Formulates risk management guidelines and policies Reviews enterprise risks periodically, initiates action and reviews progress
Office of Risk Management	Comprises a network of risk managers from all businesses and support groups across the group, and is led by the Chief Risk Officer (CRO) Facilitates the execution of risk management in the enterprise as mandated by the Risk Council
Unit Heads	Manage their functions as per risk management philosophy Manage risks at the unit level, in consultation with the Risk Council
Operational Management	Implement ascribed risk actions Provide a feedback on the efficacy of risk management and warnings for early detection of risk events

Classification of Risks

The company classifies the risk under the following broad categories:

- Strategy risks
- Sector risks
- Human Resources risks
- Business Risks
- Regulatory risks

Key Risk Management Activities

- Company conducted a risk perception survey to prioritize risks to integrate risks with a strategic planning.
- Risks were refined by key stakeholders and the Risk Council members.
- The company has implemented advanced risk quantification techniques to identify risk mitigation and reporting alternatives.
- The company interacted with global companies to identify the best in the class risk management practices.

CASE STUDY -2

An IT Group Operating in Various Countries and also Involved in Non-IT Business

Risk Management Objectives

- Customer oriented
- Employee oriented
- Risk Optimization
- Enhanced Governance

Risk Management Approach

- The company uses a participative approach wherein various stakeholders are trained to implement control activities for their processes.
- The company has implemented certain system based tools to monitor control activities.

- The company aims at creating an awareness on risk management within the organization.
- Risk optimization and monitoring mechanisms are highly valued.
- Risk management is a tool to provide an assurance on compliance levels within the organization and good governing practices.

Risk Management Methodology

- Follow an integrated approach to optimize risks and identifying opportunities.
- The following phases are involved:
    1) Risk Identification,
    2) Risk assessment,
    3) Risk quantification,
    4) Risk mitigation, and
    5) Ongoing monitoring of business risks.
- The company focuses on risk management as an ongoing activity to identify:
    1) Worst case scenarios,
    2) Likelihood of the worst case scenario, and
    3) Steps to mitigate such a scenario.
- The company identifies top 10 events which affect the organization.

Steps Followed	***Activities at each step***
Risk Summary	• Discussions with risk owners • Analysis of external factors
Risk Rating	• Rate risks on Probability and Impact
Risk mitigation	• Evaluate mitigation plans • Identifying responsibility
Major risks at Business unit level	• Business Unit heads prioritise the risks at the business unit level
Major risks at Corporate level	• Consolidate Business Unit level risks to arrive at an aggregate

	corporate exposure • Consider risk interdependencies to arrive at top key risks
Monitoring Mechanism	• Report mitigation plan status and net risk exposure on a periodic basis at appropriate levels

Risk Organization

- The company has adapted a decentralized approach for risk management and hence risks are managed across levels at each business unit, function level.
- The Chief Risk office is the project leader and the risk management assists the business unit heads to identify key risks.
- Risk officers are appointed at local unit levels to manage risks pertaining to the unit.
- Respective functions are responsible for identifying, devising mitigation plans and to monitor them on an ongoing basis.

Risk Management Activities

- Projects are subjected to risk management.
- Reporting mechanisms are installed which identify the events which affect business objectives.
- The company invited experts for conducting a seminar from the industry to discuss risk management practices and pitfalls in implementation.
- Awareness on risks management is created through workshops and training programs and has developed a web based tool in this regards.
- An employee survey was conducted to identify the risks across various business units, subsidiaries. Risks identified were assessed for the impact and likelihood.

CASE STUDY -3

An IT Company with Global Operations

The framework is broadly aligned to the COSO framework.

Risk Management Objective

- Investor Satisfaction

- Customer Satisfaction
- Employee Satisfaction

Risk Management Methodology

- The Enterprise Risk Management is carried out at four levels, namely, (i) Project Level, (ii) Business unit Level, (iii) Unit Level and (iv) Company Level.
- The net risks at each of these levels are aggregated to the next level.
- A detailed ERM Policy Manual which details the risks is accessible to all stakeholders.
- The risk identification is based on a survey conducted across the entity.
- Key elements in the ERM Process are risk assessment, risk management and risk monitoring.
  - **Risk Assessment:** The heads at each level identify the events at project, business and unit level. Risk exposure is assessed on a scale of 1-5, 1 being the low risk and 5 being high risk determining their inherent and likelihood of occurrence.
  - **Risk Management:** The risk management strategy considers the risk appetite of the company. Response strategies are developed for identified risks.
  - **Risk Monitoring:** Risk response strategy is tracked at the Project, Unit, and Company level for resolution. An automated tool is put in place for an effective monitoring of the ERM process at all levels. Each business unit is given a risk rating to monitor its performance.

Risk Organization

- The ERM team consists of the heads of Finance, Corporate governance function, legal function, Information technology and quality.
- The Board of Directors periodically reviews the ERM framework and its effectiveness.

ERM step	*Performed by*
Risk Assessment	• Project level • Business unit • Corporate team
Risk Management	• Project heads • Business Unit heads

	• Corporate heads
Risk Monitoring	• Project heads and business unit heads • Board of Directors

Risk Categories

All the risks are classified under four categories as follows:

- Hazard Risks - Fire, Earthquake, other natural perils, etc.
- Financial Risks - Liquidity, inflation, currency fluctuations, etc.
- Operational Risk - HR management, compliances, project management, etc.
- Strategic Risk - Competition, market conditions, political environment, etc.

This classification forms the basis for the identification, monitoring and reporting of the risks.

CASE STUDY - 4

An Indian Pharmaceutical Multinational Company

This company consulted external advisors for developing a basic ERM framework. Key highlights of its ERM initiative are as follows.

Risk Management Methodology

It comprises of three phases:

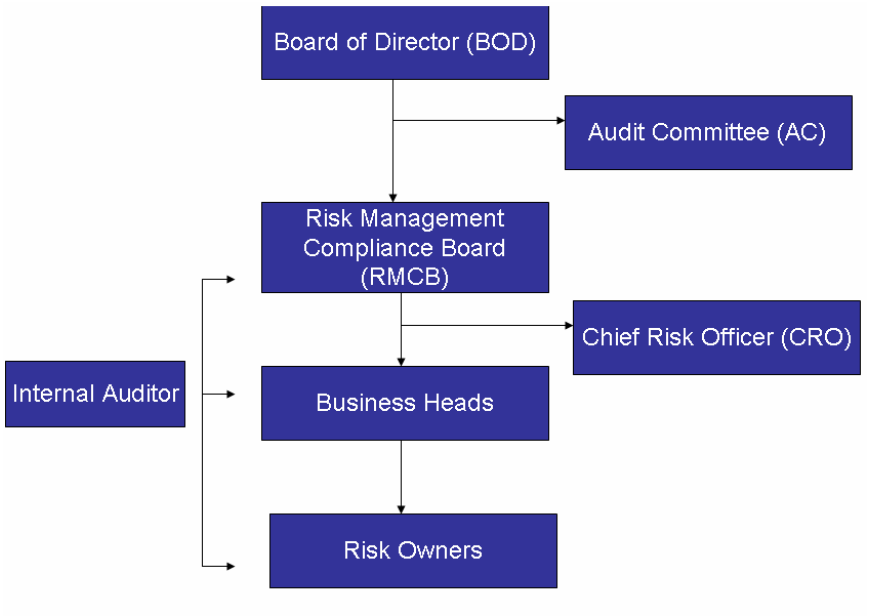
- ***Assess***: Identify, classify risks, rate risks and develop a risk inventory.
- ***Enhance***: Prioritize the risks based on workshops, perform root cause analysis and develop mitigation plans.
- ***Monitor***: Devise an organization framework; maintain the framework on a continuous basis.

Risk Organization

Level	*Roles and Responsibilities*
Board of Directors through Audit Committee	• Performs oversight role • Monitors risk management activities.
Business Unit Heads	• Monitor risks on an ongoing basis within the risk management framework. • Provide regular updates to the

	audit committee through the risk officer.
Functional Heads	• Perform risk management activities while managing business activities.

Risk Organization Structure – Sample



CASE STUDY -5

A Metals and Mining Group

Risk Management Approach

- Risk Management policies are documented and used effectively and embed risk management in business operations.

Risk Management Methodology

- A system is in place wherein risk owners at all levels and within all subsidiaries are actively involved in risk identification.
- Responsibility of risks is assigned at a senior level within the group.

- Periodic updates are made to risk quantification in terms of its likelihood and impact.
- Business unit heads maintain and update the risk inventory on a regular basis.

Risk Organization

- The internal audit function coordinates the risk management initiative and this function provides periodic updates to the Audit Committee. The Board of Directors has delegated its duties to the internal audit function.
- Operating performance is reviewed on a monthly basis by the senior management wherein risk management related issues are also highlighted.
- Key business decisions are taken only after an appropriate risk analysis.

CASE STUDY - 6

A Chemicals Manufacturing Company of a Large Group

Risk Management Methodology

- ERM process includes the risk identification, risk assessment, creating risk response and an ongoing monitoring.
- Risk management is embedded in the organisation's planning process. It is used as a tool in taking strategic and business decisions. Risks and opportunities are managed to achieve business goals.
- The residual risk and mitigation plan of the organization is periodically assessed by the senior management.
- Board of Directors and Audit Committee perform an oversight role and monitor activities on a periodic basis.
- Benchmarking process is carried out by the company to ensure that its internal audit and risk management processes are in line with global practices.
- The company has implemented a detailed control and self assessment model which operates on an ongoing basis.

CASE STUDY - 7

A Large Banking Company Operating in Various Countries

Risk Management Approach

- Risks and opportunities are managed in such a manner that the company provides the maximum value to the shareholder. Risk management is an integral part of managing the business.
- The company aims at streamlining and structuring the risk management activities and monitors them on an ongoing basis.
- Organizational activities are well documented and assessed against global practices on an ongoing basis.

Risk Organization

- The company has dedicated groups for various categories of risk. These risk management groups assess, manage and mitigate specific risks allocated to them and thus ensure an enterprise wide risk management
- These risk management groups also monitor the adherence to regulatory compliances and internal authorization requirements.
- Independence is ensured since these groups are only involved in risk monitoring and are devoid of business responsibilities.
- General risk groups are further classified into specific risks groups to ensure that risk management is linked to competencies.
- Various risk functions report to the Audit committee.
- Each risk management group/sub-group develops risk management policies, identifies risks, quantifies them and develops action plans to manage these risks.

Appendix 1

Score Card for Assessing Risk Maturity

I. Check list for assessing risk maturity[1]		
Risk maturity is the degree to which the organisation understands its risk and has implemented ERM.		
S.No.	**Checklist**	**Score**
A. Understanding on objectives and their associated risks		
1	The organisation's objectives are documented and understood.	
2	Management has been trained to understand as to what risks are and their responsibilities for them.	
B. Installation and usage of risk management within the organization		
3	Process have been defined to determine risks and these have been followed.	
4	A scoring system for assessing risks has been defined.	
5	All risks have been assessed in accordance with the defined scoring system.	
6	Response to the risks have been selected and implemented.	
7	The risk appetite has been defined using the scoring system.	
8	Risks have been allocated to specific job titles in the risk register.	
9	Management has set up monitoring controls on processes, responses and action plans.	
10	Risks are regularly reviewed by the organization and the risk register updated.	
11	Management reports risks to Directors where responses have not managed the risks to a level acceptable to the Board.	
12	All significantly new projects/products are routinely assessed for risks.	

[1] Based on An approach to Implementing Risk Based Internal Auditing, IIA, UK and Ireland.

C. Assessment on managers understanding and usage of risk management		
13	Responsibility for determination, assessment and management of risks is included in job description.	
14	Managers provide an assurance on the effectiveness of their risk management.	
15	Managers are assessed on their risk management performance.	
II. Suggested scoring and its interpretation		
	Score	
	0- No	
	1- Yes, Incomplete/ Possibly	
	2- Yes	
	Conclusion on Risk maturity	
	0-7 : Risk Naïve	
	8-14: Risk aware	
	15 -20: Risk defined	
	21- 25: Risk managed	
	26 and above: Risk enabled	

Appendix 2

Model Process for Assessing and Evaluating Risks

Steps in Risk Assessment

1. Activities in risk assessment can be put in three processes, *viz.*

- Risk identification
- Risk estimation
- Risk evaluation

Risk Assessment Tools

2. Following are some of the popular analytical methods used during risk assessment:

- Market survey
- Dependency Modeling
- SWOT (Strength, Weakness, Opportunity and Threat) analysis
- Event tree analysis
- BPEST (Business, Political, Economical, Social and Technological) analysis
- Fault tree analysis (Root cause analysis)
- FMEA (Failure Mode and Effect Analysis)

Risk Identification

3. This is the starting point for all risk assessment initiatives. As mentioned earlier, all organizations are exposed to varieties of threats and uncertainties which impact the objectives for which they have been established. It is essential that the risk identification process be planned and activities within streamlined. This process should ideally cover all risks and scenarios to which an organization is exposed to during the normal course of its business and also the various business activities which are a source of these risks.

4. Some of the business activities, which are a source of risk, are:

- **Strategic -** These concern the long-term strategic objectives of the organization. They can be affected by the capital availability, sovereign and political risks, legal and regulatory changes, reputation and changes in the physical environment.

- **Operational** - These concern the day-to-day issues that the organization is confronted with as it strives to deliver its strategic objectives.
- **Financial** - These concern the effective management and control of the finances of the organization and are affected by external factors such as the availability of credit, foreign exchange rates, interest rate movement and other market exposures.
- **Human resources and knowledge management** - These concern the effective management and control of the knowledge resources, the production, protection and communication thereof. External risks include the unauthorized use or abuse of intellectual property. Internal risk could be the loss of key staff.
- **Compliance** - These concern issues as health and safety, environmental, trade regulations, consumer protection, data protection, employment practices and regulatory issues.
- **Fraud** - All large organizations are exposed to fraud risks. Also, various regulatory requirement as Clause 49 require organizations to have sound fraud control mechanisms in place.

5. What is the best way to identify these risks? Whether it should be identified by the people within the organization? Or external resources who specialize in these areas? Or a blend of both internal and external specialists? Who are the best resources internally to perform the risk identification?

Once again, there is no standard practice or guideline which is followed. This decision would depend upon the management, expertise of internal resources, etc. Generally, Internal Auditors are considered to be the appropriate personnel to facilitate this activity. The ownership of identifying the risks correctly remains with line management.

During the risk identification, care should be taken to identify 'inherent/gross' risk rather than concentrating on 'residual/net' risk. If this is not done, the organization will not know what its exposure will be should controls fail. Knowledge on the inherent risk also allows a better consideration of whether there is over-control in place – if the inherent risk is within the risk appetite, resources may not need to be expended on controlling that risk. Knowledge about both 'inherent' and 'net' risk is important because the extent to which the risk needs to be addressed is informed by the inherent risk whereas the adequacy of the means chosen to address the risk can only be considered when the residual risk has been assessed.

Risk Identification Methods

1. To identify risks one of the following methods are used:

- Surveys
- Interviews
- Workshops

2. Following is the illustrative list of questions which could be used for surveys/interviews/ workshops:

- From your perspective, what are your key business and/or your area objectives?
- What are some of the significant internal and external risks faced by the organization in the achievement of the business and area objectives?
- From your perspective what is the likelihood of the risk occurring?
- From your perspective what is the consequence of the risk?
- What are some of the measurable performance targets and key performance indicators (KPIs) that can be linked to monitoring/mitigating the risks identified? (For example, Budget to actual, ratings performance ranking).
- What is the frequency of measuring these KPIs?
- What other actions are taken to mitigate/manage the risks identified?
- What is the frequency of these actions?
- Who is responsible for monitoring these risks?

Industry risk models

3. In addition to these generally used methodologies, an Industry-sector wise risk model can also be used. Generally, these models are developed by professional organizations. The Industry-sector model is helpful in identifying dynamic risks to which an organization is exposed to.

Which method to use

4. What is the most effective method or whether a combination of these methods should be used? This depends on various factors including the organizational culture, time available to complete risk identification, etc. Normally, this comes with an experience to the risk practitioner.

Typical risk areas

5. Identification of the risks associated with business activities and decision making may be strategic/tactical and/or project/operational. It is important to incorporate risk management at the conceptual stage of projects as well as throughout the life of a specific project.

6. During identification of internal risks, it would be important to consider aspects as organizational structure, locations, objectives of the organization, key business processes and functions, strategic partners, outsourced service providers, etc.

7. During the identification of external risks, the political, economic, social and regulatory aspects in which the organization is functioning needs to be considered. Since identifying external risks is a complex activity, generally organizations utilize forecasts and current events/scenarios. Because of its complexity, the organization can utilize specialized external sources in this area.

8. An illustrative listing of the areas in an organization where the risk arises is given below:

GOVERNANCE	FINANCE	OPERATIONAL	PREPAREDNESS	INTEGRITY
Authority	Funding	Quality	Morale	Management fraud
Leadership	Financial instruments	Customer service	Workplace environment	Employee fraud
Performance	Financial reporting	Pricing	Confidentiality	Illegal acts
Corporate directionand strategy	Foreign exchange/ currency	Obsolescence	Communication flow	Unauthorized use
Incentives	Cash flow	Sourcing	Communication infrastructure	
	Investment evaluation	Product development	Change acceptance	
	Treasury	Product failure	Change readiness	
	Payroll	Business interruption	Challenge	
	Debtor/creditor management	Contingency Planning	Ethics	

COMPLIANCE	ENVIRON-MENT	HUMAN RESOURCES	REPUTA-TION	TECHNO-LOGY
Health and safety	Seasonality	Competencies	Brand	Reliability
Environment	Globalization	Recruitment	Reputation	Management information systems
Copyright and trademarks	Competition	Retention	Intellectual property	Access /availability
Contractual liability	E-commerce	Performance measurement	Stakeholder perception	IT security
Taxation	Share price	Leadership development		
Data protection	Strategic uncertainty	Succession planning		

Risk estimation (or risk measurement/ risk scoring)

9. Risk estimation can be defined as 'assessing the impact of the risk on the organization.' During the risk estimation, the following should be kept in mind:

- Difference between, inherent and residual risk needs to be established.
- Ensure that there is a clear process methodology on the risk estimation so that both the likelihood and impact are considered for each risk.
- Record the estimation of the risk in a way which facilitates the monitoring and identification of risk priorities.

10. As discussed earlier, all organizations are exposed to various categories and nature of risks, and quantitative methodology may not be sufficient and relevant to complete risk estimation. Hence, qualitative characteristics and judgment, knowledge of the management on the organization needs to be utilized (e.g. in the case of reputation risk - a subjective view is all that is possible). Hence, risk evaluation is more of an art, than science.

11. Risk estimation can be quantitative, semi-quantitative or qualitative in terms of the probability of occurrence and the possible consequence. The use of a well designed structure is necessary to ensure a comprehensive risk identification, estimation and evaluation process. Different organizations will find their own measures of consequence and probability that will suit their needs best. For example, many organizations find that assessing the consequence and probability as high, medium or low is adequate for their needs and can be

presented as a 3 x 3 matrix. Other organizations find that assessing the consequence and probability using a 5 x 5 matrix gives them a better evaluation. If clear quantitative evaluation can be applied to the particular risk - "5x5" matrices are often used, with the impact on a scale of "insignificant / minor / moderate/ major/ catastrophic" and the likelihood on a scale of "rare / unlikely / possible / likely / almost certain".

Illustrations for measuring the probability of occurrence and magnitude of impact of the risk (5x5 criteria) are in *Exhibit 1 and 2*. Also refer *Chapter 2* of the Guide.

Risk evaluation

12. When the risk estimation process for each risk has been completed, it is necessary to compare the estimated risks against risk criteria (i.e. risk appetite) which the organization 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 organization and whether each specific risk should be accepted or treated.

13. A common method of evaluation is to use a *'risk heat map'*. The *'risk score'* of a risk is the multiple of *'likelihood score'* and *'significance score'* which is adjusted by the qualitative assessment of the management. (Refer to Exhibit 3 for risk score). The risk heat map has the likelihood of risks and impact of risks as the two axis and individual risks are plotted on it based on their risk score. Further, a *"traffic light"* approach is used to show the risk, where green signifies *do not require action*, those which are amber *should be monitored and managed down to green if possible*, and those which are red *require immediate action* (refer to Exhibit 4 for risk heat map).

Usage of risk scores

14. From the management's perspective when it is reviewing the risk register for CEO/CFO reporting purposes and giving a disclosure in the Annual accounts on the internal controls, it is not the *inherent risk score* but the *residual risk score* which is important; as the management wants to assess whether the residual risk is regarded as tolerable, or how far the exposure is away from tolerability.

15. From the internal auditor's perspective, it is the *inherent risk score* which is important as the internal auditor is to give an assurance on the design and adequacy of the risk identification process as a part of his overall assurance on the risk management process.

Appendix 3

Preparing the Internal Environment

A. Key activities to prepare the internal environment are:

- Assessing and developing a risk management philosophy.
- Assessing the compliance to the risk management philosophy.
- Developing a code of conduct within the organization.
- Developing an infrastructure for the training on ethical behavior and ethical communication within the organization, e.g., hotlines, whistle blower mechanisms, escalation policies, etc.
- Assigning project roles and responsibilities to frame the project organization.

B. Carrying out the key activities for preparing the internal environment to implement ERM

A) Develop a risk management philosophy

While philosophy may vary with each company, a typically risk management philosophy would cover the following aspects:

- The organization's belief in risk management.
- How risk management is embedded in the organizations strategic decisions?
- How risk management is percolated in operational decisions?

Risk management philosophy is best adopted when it is also a part of various policies and procedures. The organization can also adopt risk management as an operational indicator to assess performance. As an illustrative we mention below a sample risk management philosophy.

Your organization believes in a risk based approach towards business activities. The organization ensures that all facets of risks are considered while framing its strategy and it expects that risks are considered while making operational decisions within the organization. We believe that such an approach would allow us to make more rational decisions, make more informed decisions which would benefit all the stakeholders. Such a philosophy would also help us assign the responsibility for our decisions and strengthen the monitoring process within our organization. In line with the

above philosophy, the management and staff is expected to confirm to the following:

- Consider strategic, operational, compliance and reporting risks in decision-making.
- Ensure that risk management begins at business unit level and is integrated to the overall organization wide risk definition.
- Be open to the adoption of risk management as a way of functioning as against compliance.
- Work towards developing a competent risk management framework which is best in the class.
- Be committed to developing a comprehensive risk portfolio and develop an adequate mitigation plan.
- Absorb the ownership and responsibility for risk pertaining to one's activities.

B) Assessing compliance to risk philosophy

Assessing the compliance to risk philosophy is important to confirm that the internal environment is ready for the ERM implementation. The most accepted methodology for such an assessment is risk survey within an organization on a periodic basis. This should also evaluate the current level of compliance and as against the desired level. This would facilitate the gap analysis and subsequent mitigation. Such a survey may cover the following aspects:

Strategy

1) Strategic alignment – Is risk management aligned with the strategy?
2) Are the objectives of the company clearly communicated within the organization?
3) Is the organization culture aligned to risk management?

Policy

1) Are various policies in place and is risk management an integral part of various policies?
2) Is the organization aware of such policy aspects?
3) What is the general level of compliance within the organization?

Structure

1) What is the organization's commitment to competency?
2) Are the people aware of the risk management philosophy of the organization?

3) Is risk management given importance at various levels within the organization?

Process

1) Is there an adequate information flow within the organization across departments to ensure that risk management is comprehensive or are processes aligned to risk management?
2) Is there an adequate knowledge management within the organization to ensure a successful risk management?
3) Are people accountable for risks and responsible for considering risks in making decisions?

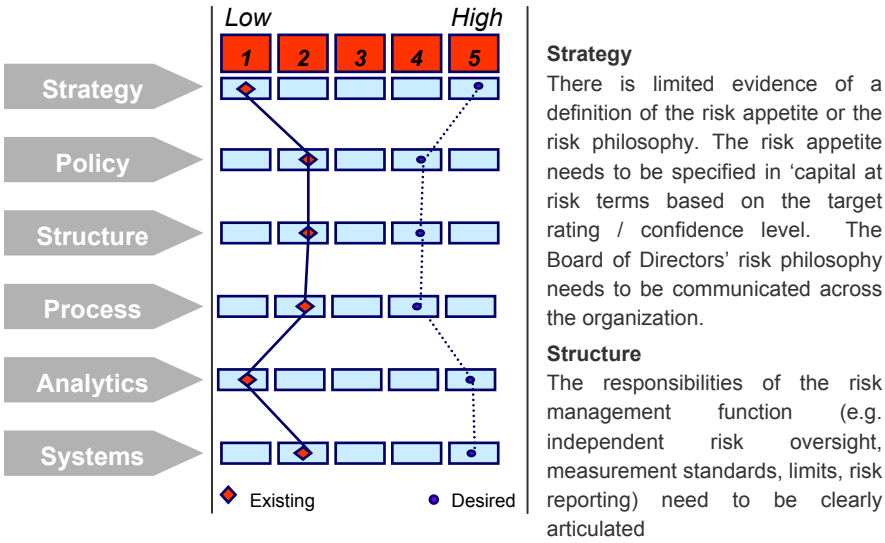
Analytics

1) Is risk management linked to performance?
2) Are risks adequately identified and quantified?
3) Is the risk appetite defined?

Systems

1) Do the systems support risk based decision making?
2) Is the organization structure conducive to risk management and is the risk management structure in place?
3) Is there adequate infrastructure available for risk management activities?

Illustrative



C) Developing a code of conduct

Ethical values and culture within the organization are important for a successful ERM implementation, since they:

- Determine the organization's openness to accepting the existence of a risk and the need for its mitigation.
- Establish the open channels of communication within an organization.
- Affix the responsibility on the pattern of behavior within an organization.
- Determine organization's responsibility towards various compliances and its commitment towards performing ethical activities.

A code of conduct may cover the entity's approach towards to following aspects:

- Purpose of the code of conduct and importance of ethics
- Applicability of the code of conduct
- Result of non compliance
- Relationship with stakeholders
- Disclosure, Reporting and resolution of conflicts
- Policy of gifts and entertainment
- Protection of assets
- Maintenance of confidentiality
- Public responsibility of the organization
- Legal compliance
- Corporate social responsibility
- Whistle blower policy – which covers escalation, treatment of violations and resolution, etc.

D) ERM project Structure

Enterprise wide risk management would be successful when organizations are geared up for the implementation. This would include the support and involvement of the Board, Senior Management and Executive management. As ERM evolves, specialized roles are considered appropriate. In addition, the following specific responsibilities also devolve:

Board of Directors

- Develop a risk culture across the organization.
- Sponsor the ERM program.
- Oversight functions for evaluating the ERM implementation success.

- Facilitate the implementation by monitoring the project at each stage.

Risk Committee

- Act as an oversight for overall risk management initiatives.
- Ensure each stage in the ERM implementation is carried out effectively in line with the objectives.

Chief Risk Officer

- Manages the ERM project along with the risk management team.
- Provides periodic updates to the risk committee and The Board.

Business Unit heads

- Assume the overall responsibility for the risk identification, assessment and mitigation.

Functional heads

- Identify, assess and manage risks for individual processes.

It should be remembered that the above responsibilities should not conflict with other Board functions and responsibilities. The underlying principle being to ensure that the structure is conducive to the degree of implementation within the organization.

Appendix 4

Objective Setting

A. Key Activities to Objective Setting

- Define risk management process linkages with strategic objectives of the organization and the mission of the company.
- Define the risk appetite for the organization related to the strategic objectives.
- Define the risk tolerance levels in business decisions within the overall risk appetite of the organization.

B. Carrying out the Key Activities to Objective Setting

a) Linking risk management to objectives

An illustration is provided below:

Mission	To be the leaders in providing telecommunication services in the country, thereby facilitating the society in which we exist.
Strategic Objectives	• To maintain an annual return on capital employed of 15%. • To grow the customer base by 40% within three years through increasing the network management capacity by 60% during this period.
Strategies	• Develop the network infrastructure in new areas that match our target customer demographics. • Acquire smaller service providers to obtain their existing subscriber base.
Networking services unit Objectives	• Acquire a minimum of 25 new terminals in second tier cities and new formed telecom circles. • Identify 5 potential target service providers in second tier cities. • Enhance existing network capabilities by 30% to support additional customer base.
Human Resources Objectives	• Recruit a senior manager in the networking department. • Annual turnover of customer services staff below 18%. • Recruit and train 175 customer service staff in the coming year.

Once the above linkage is determined, risks/events are identified which may affect in achieving the objectives. For e.g., in the above illustration the risks that could probably impact are as follows:

- Strategic
  - Increase in competition

- Increase in Taxes affecting outlays and hence returns

- Operational
  - Requisite approvals for new terminals may not be obtained.
  - New targets acquisition may not be possible.
  - Attrition rate beyond the norms.
  - Lack of the availability of man power.

Thus, the risk assessment and risk response would then be linked to the strategic and operational goals of the organization.

b) Define risk appetite and risk tolerance

Risk Appetite

Once the objectives are defined as above, the organization needs to define its overall risk appetite. The risk appetite is, normally, defined in terms of a measurable parameter e.g., total cash loss, exposure as a percentage of the capital invested, percentage of net profit, minimum rate of returns, etc. Defining risk appetite would include defining the following:

1) Extent of risk acceptable in a new business selection.
2) Minimum rate of return in new ventures.
3) Degree of importance towards various type of risks namely, Strategic, Operational, Compliance, Reporting.
4) Acceptable exposure in uncertain ventures.
5) Categories of the risk which would be unacceptable to the organization.

Risk Tolerance

After defining the risk appetite of the organization, it also needs to define the risk tolerance which is the degree to which non conformance to risk levels is acceptable to ensure that the overall exposure is within the risk appetite of the organization. For e.g., the overall risk appetite for the organization is 20% of the capital investment of Rs.300 Crores. There are three business units A, B and C with the investment of Rs.100 Crore each. Suppose, the risk exposure for each of them is Rs.8 Crores, Rs.25 Crores and Rs.25 Crores. Thus, the risk tolerance for the business units B and C is 5% (excess over the acceptable level of 20%). At 5% tolerance although the business units individually may exceed the risk appetite levels, at an organization level, the total risk exposure is within its risk appetite (Rs. 58 Crores which is less than Rs. 60 Crores (@20% of capital investment)). However, the entity would continue to monitor the non compliance to tolerance levels in units B and C to identify and mitigate the risks due to which the risks have exceed the unit tolerance levels.

Appendix 5

Event Identification

A. Key Activities to Event Identification

- Identify events which may affect the objectives.
- Use various techniques for event identification.
- Prepare an inventory of events.
- Categorize similar events in one category for a holistic assessment.
- Evaluate interdependencies in events.

B. Carrying Out the Key Activities to Objective Setting

a) Identify the events affecting objectives

There are various techniques used to identify events, some of these are discussed in this Guide. However, it is important to link the events to the objectives for an effective event identification, some examples are given below:

Objective- Production capacity utilization should be at 95% of the planned capacity.

Events/Risk - Machine down time resulting in a lesser utilization of plant capacity.

- Delivery schedules of raw material not adhered to ensure a continuous production.

It is important to associate an event to an objective and then to a business/sub unit or a department.

b) Ensure the effective use of techniques for event identification

Some sample techniques which could be used:

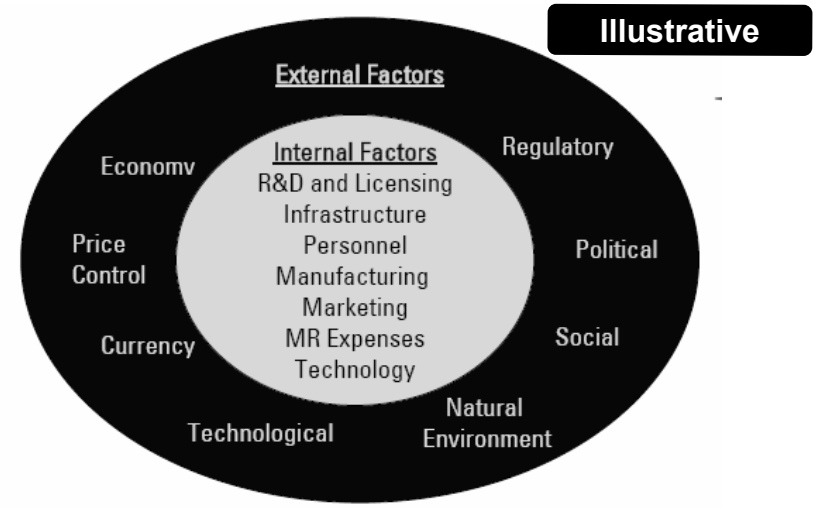
- Interviews
- Surveys
- Questionnaires
- Facilitated workshops

In all the above techniques the answers to following questions need to be obtained:

- Which objectives would be affected by the event?
- What is the degree to which the event would have an impact?

- What is the company's tolerance to that impact?
- Is the event resulting in a risk or opportunity?
- Is the event related to other events or are there other events affecting the given objective?

Event/Risk identification depends on many factors and all need to be taken into account. An illustrative list of the factors affecting the event identification in a pharmaceutical company is mentioned below:



An organization can also develop certain trigger systems which would help in an event identification on an ongoing basis.

- Deviations from acceptable norms
- Deviations from acceptable key performance indicators
- Trend analysis of the event likelihood and impact

c) Prepare event inventory

- Identify the events across various processes, business units.
- Categorize the events based on the business unit, process, sub process, division, department, risk category (Strategic, Operational, Compliance/Regulatory, Reporting/Monitoring).
- Ensure similar events are grouped under one category.
- Evaluate the interdependencies of events to assess the impact of each event.

A sample risk/event inventory is given below:

Process	**Sub Process**	**Division**	**Department**	**Risk Category**	**Risk Owner**	**Risk Description**
Revenue	Billing	Health Care	Finance	Operational	XXX	Incorrect Billing
Treasury	Hedging	Health Care	Treasury	Strategic	XXX	Decrease in Dollar rate
Human Resources	Recruitment	Health Care	Human Resources	Strategic	XXX	Attrition
Legal	Legal	Health Care	Legal and compliance	Regulatory	XXX	Delays in obtaining statutory clearances

Appendix 6

Risk Assessment

A. Key Activities to Risk Assessment

- Evaluate each risk in terms of its likelihood of occurrence and impact.
- Use various qualitative and quantitative techniques for assessing risks.
- Prepare a risk map by plotting various risks in terms of their likelihood and impact.
- Prioritize risks to develop response mechanism.

B. Carrying out the Key Activities in Risk Assessment

a) Evaluate risk in terms of likelihood and impact

One of the most accepted risk assessment practices is conducting risk assessment workshops. The risks identified in the earlier stages are discussed in this workshop and risks are rated based on their likelihood and impact. Each risk needs to be evaluated on two criteria

1) Likelihood - could be classified as –

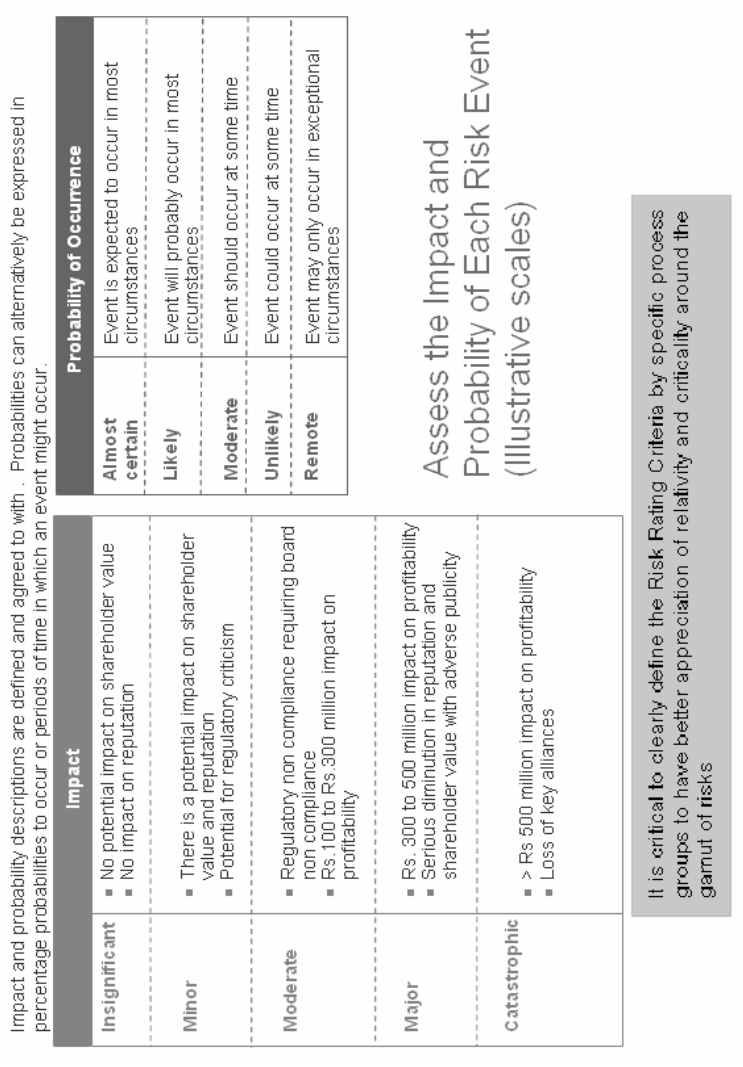
- Remote
- Unlikely
- Moderate
- Likely
- Almost Certain

2) Impact – could be classified as

- Insignificant
- Minor
- Moderate
- Major
- Catastrophic

At this stage, risks would be assessed on an inherent basis, i.e., without considering the existing controls within the organization. There could be various

criteria based on which the above classification could be made. An illustration is given below for further understanding:



b) Prepare a risk assessment inventory

Once the risks are assessed for likelihood and impact in the workshop, gross risk is calculated for each risk. The risks could then be plotted on a graph. Such a graph (risk map) would depict the risk profile of the organization. The following illustration would make it easier.

Risk Assessment

Particulars	Average Gross Impact (A)	Average Gross Likelihood (B)	Average Gross Risk (A*B)
Talent Retention.	4	4	16
Increasing Competition	4	3	12
Lack of robust insider trading control framework	3	3	9
Weak IT security controls	3	2	6
Opportunity Loss of sale in stock out situations	2	2	4
Non compliance with regulatory and legal statues.	2	1	2

There are various, methods available for performing risk quantification. The method mentioned above is the most commonly used method. Companies depending on their need and maturity adopt methods like sensitivity analysis, stress testing, cash exposure criteria, etc for arriving at the gross risk. Further, risks are to be identified and assessed for all business units, locations, and the organization as a whole. This would ensure that the risk identification and assessment is comprehensive.

Risk quantification is dependent on the likelihood and impact. Further, some risks can be quantified while others cannot be quantified. In such a scenario, in some cases, qualitative techniques are used for risk quantification while quantitative techniques are used in others. For example,

Qualitative Techniques would be used when:

- Data analysis for quantification is not cost beneficial.
- Reliable data for analysis is not readily available.
- Risks are of a nature which cannot be quantified.

Quantitative Techniques are used when:

- Adequate and relevant data is available.
- Increase degree of accuracy is required for decision making.
- Qualitative aspects need to be substantiated.

In companies with an advanced level of ERM in place, the methods used for risk quantification for strategic risks is generally as follows: (In the order of most valued method)

- Key Risk Indicators
- Individual self assessments
- Scenario Analysis
- Risk Mapping using impact and frequency
- Facilitated group self assessments
- Economic Value Added
- Value at Risk
- Industry Benchmarks/Loss experience
- Statistical Analysis/Probabilistic modeling

c) Perform risk categorization and prioritizing

Prioritizing and categorizing risks into manageable groups is the most critical aspect of the risk identification. The relevance, probability, impact of risks have to be agreed upon with the risk owners. Risk could be categorized as follows:

Based on Timing

- Short Term – Non achievement of yearly budgets.
- Medium Term – Attrition levels not maintained below desired level in the next three years.
- Long Term – Non achievement of targeted market share in the next five years.

Based on Nature

- Environment Risk (Regulations, Laws, Technology, Shareholder expectations, Availability of capital, Market trends, etc).
- Process Risk (Lack of alignment of business activities in line with business objectives, operational inefficiency, Frauds, misappropriation, employee retention, etc).
- Information for decision making risk (Inaccurate, out dated, irrelevant data used for business decisions).

Appendix 7

Risk Response

A. Key Activities to Risk Response

- Identify the response to risks identified.
- Evaluate each response in terms of cost and benefit by identifying cost and benefit of each option (i.e., Avoid, Reduce, Share/Transfer and Accept).
- Select the most efficient option and identify the net/residual risk portfolio after considering the responses to various risks.
- Ensure that the residual risk is within the risk tolerance limits of the organization/business unit.

B. Carrying Out Key Activities to Risk Response

a) Identify risk responses

Various risk response mechanisms could be classified as mentioned in the below diagram

Avoid	Exiting the activities giving rise to risk. Risk avoidance may involve exiting a product line, declining expansion to a new geographical market, or selling a division.
Reduce	Action is taken to reduce risk likelihood or impact, or both. This typically involves any of a myriad of everyday business decisions.
Share/Transfer	Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common techniques include purchasing insurance cover, outsourcing activities, engaging in hedging transactions.
Accept	No action is taken to affect risk likelihood or impact. This is mainly in cases where the risk implications are lower than the Company's risk appetite levels.

b) Evaluate risk response

Each risk response should be evaluated in terms of costs and benefits. An illustration is given below:

Case:

A large retail chain is dependent on a single supplier for the supply of toys. However, due to production bottlenecks with the supplier, many times there is a non adherence to supply requirements by the toy manufacturer. The non adherence is to the extent of 15% of the required supply quantities. This results in an inadequate supply for meeting the demand for the toys. The retail chain wants to ensure that it meets 90% of the demand for the toys. The related risk to this objective is – Dependency on a single vendor for supply of toys. As a response to this risk the following options are available:

Avoid - Avoid dependency on a single vendor, terminate his contract and develop new vendors.

Accept – Accept the non adherence to supply quantities by the existing vendor and procure the balance quantities from other vendors for meeting the demand.

Transfer – Negotiate with the supplier and obtain the commitment of minimum quantities and include penalty clauses for non adherence.

Reduce – Monitor the performance of the supplier on a periodic basis to ensure that production is at desired levels to ensure timely changes to the procurement plan. Use more sophisticated demand forecasting methods to ensure that the gap between supply and demand is forecasted on a more accurate basis.

Each of the above options has costs and benefits attached to them. One needs to tabulate the cost and benefits to identify the most efficient response.

Response		***Cost***	***Description***	***Benefits***
A	Accept	Rs.50,000	Commercial department efforts required to identify additional suppliers, and additional logistics costs, Rs.50,000	Management predicts it can sell an additional 3% to customers, bringing demand adherence up to 88% Effect on EBIT: increase of Rs.250,000
B	Avoid	Rs.150,000	Unit price increased by 1.5% due to new suppliers charging premium price	Efforts allow meeting of 93% of the demand Effect on EBIT:

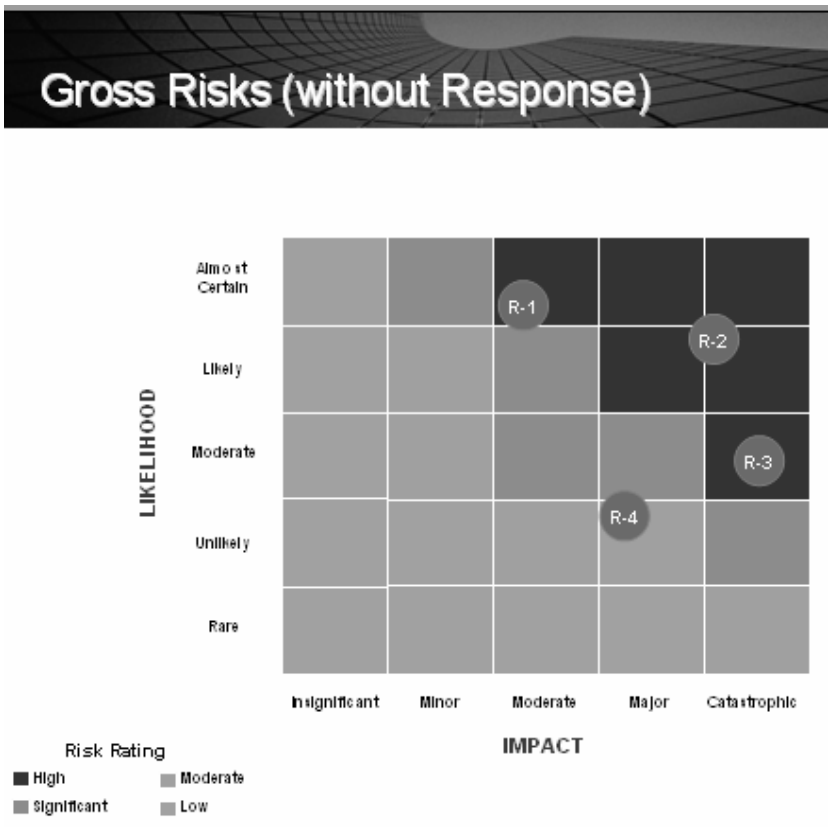
Response		*Cost*	*Description*	*Benefits*
			Rs.20,000 in increased salary costs for personnel required to identify, and sustain new vendors	increase of Rs.600,000
			Rs.80,000 in increased outbound logistics costs due to a larger number of suppliers	
			Rs.50,000 in legal fees to negotiate and finalize new agreements	
C	Transfer	Rs.25,000	Unit price increases 3% due to an increased pressure on supplier for meeting demand and penalty clause inclusion	New contract allows to meet 95% of the market demand Effect on EBIT: increase of Rs.275,000
			Rs.25,000 in legal fees to negotiate and revise contract agreement	
D	Reduce	Rs.150,000	Average unit price drops 1% due to suppliers asking for premium price for small quantities	Demand utilization possible up to 97% Effect on EBIT: increase of Rs.370,000
			Rs.150,000 for increased forecasting , analysis and monitoring of vendor performance on regular basis	

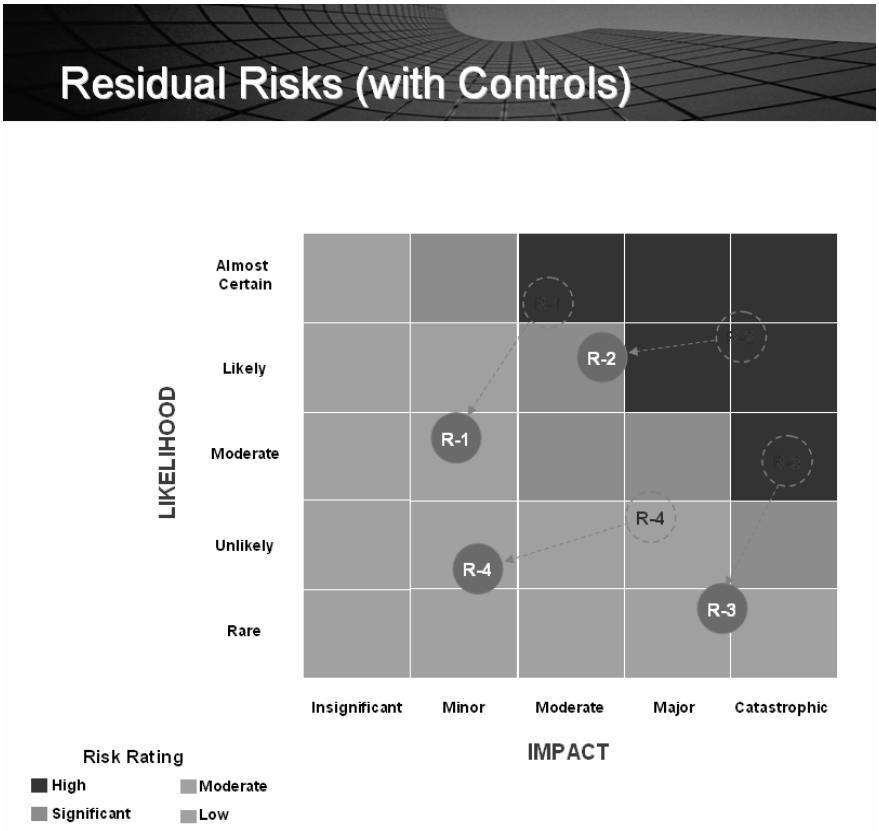
Thus, based on the above evaluation, it could be observed that the response to this risk is the most efficient if the risk is avoided.

c) Prepare residual risk portfolio

Once risk responses are identified, for each risk identified, the company then needs to identify the residual risk profile. This would facilitate in ensuring that the risks are within the tolerance limits defined in the initial stages. Once the risk response for each risk is identified, the likelihood and the impact needs to be

reassessed taking in to consideration the response identified for each risk (Accept, Avoid, Share, Transfer). The scenario would appear as mentioned below:





The risk portfolio would look as mentioned below:

Particulars	Gross Risk	Residual Impact	Type of Response	Residual Likelihood	Residual Risk	Strength of response
Talent Retention.	16	3	Reduce	4	12	4
Increasing Competition	12	3	Accept	3	9	3

Lack of a robust insider trading control framework	9	2	Reduce	3	6	3
Weak IT security controls	6	2	Reduce	2	4	2
Opportunity Loss of sale in stock out situations	4	2	Avoid	1	2	2
Non compliance with regulatory and legal statues.	2	1	Accept	1	1	1

Appendix 8

Control Activities

A. Key activities to Control Activities

- Perform a root cause analysis for the failure of risk response.
- Identify control activities for various risks responses.
- Evaluate the control activities in terms of cost and benefits.
- Implement the control activities for risk responses.

B. How to carry out key activities to Control Activities

a) Perform a root cause analysis for the failure of risk responses and identify control activities.

The following example would help understand the process of a root cause analysis for the failure of risk response and identification of control activities.

Root Causes	Key Controls	Action Plan	Key Performance Indicators
• Not hiring enough resources • High Attrition • Absence of robust performance evaluation system • Non – application of KPIs • Absence of a structured feedback mechanism • Absences of successors/ succession planning • Integration of persons from various organizations • Non - availability of skilled resources	• Identifying and hiring competent personnel • Identifying employee needs and satisfying them to retail talent • Installing a structured performance evaluation and career progression plans • Ensuring that KPIs are enforced and monitored on a periodic basis • Installing a 360 degree feedback mechanism Identifying and training /grooming successors	• Evaluation of employee morale to be carried out by external agencies • Identification of top performers/ successors and identification and satisfaction of their needs • Benchmarking current pay scales with industry	• Number of vacancies • Attrition Rate