Final Course

(Revised Scheme of Education and Training)

Study Material

Elective Paper 6A

Risk Management

BOARD OF STUDIES

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

This study material has been prepared by the faculty of the Board of Studies. The objective of the study material is to provide teaching material to the students to enable them to obtain knowledge in the subject. In case students need any clarifications or have any suggestions for further improvement of the material contained herein, they may write to the Director of Studies.

All care has been taken to provide interpretations and discussions in a manner useful for the students. However, the study material has not been specifically discussed by the Council of the Institute or any of its Committees and the views expressed herein may not be taken to necessarily represent the views of the Council or any of its Committees.

Permission of the Institute is essential for reproduction of any portion of this material.

Updated Edition	:	August, 2019
Website	:	www.icai.org
E-mail	:	bosnoida@icai.in
Committee/ Department	:	Board of Studies
ISBN No.	:	
Price	:	₹
Published by	:	The Publication Department on behalf of The Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi 110 002, India.
Printed by	:	

SYLLABUS

PAPER 6 A: RISK MANAGEMENT

(One paper – Three hours – 100 marks)

Objective:

1. To gain knowledge and an insight into the spectrum of risks faced by businesses and to learn techniques of managing risks.
2. To build capability for applying such learning to address risk related issues in real business scenarios.

Contents:

1. INTRODUCTION TO RISK

- The Concept of Risk
- Risk and Uncertainty : Distinction
- Classification of Risks
- Dynamic Nature of Risks
- Types of Risk (illustrative list)
  - ❖ Strategic and Operational Risks
  - ❖ Business Risk
  - ❖ Financial Risk
  - ❖ Information Risk
  - ❖ Liquidity Risk

2. SOURCE AND EVALUATION OF RISKS

- Identification and Sources of Risk
- Quantification of Risk and various methodologies
- Impact of Business Risk
- Identify and assess the impact upon the stakeholder involved in Business Risk
- Role of Risk Manager and Risk Committee in identifying Risk

3. RISK MANAGEMENT

- Concept of Risk Management
- Objective and Process of Risk Management
- Importance of Risk Management
- Risk Management techniques

4. EVALUATION OF RISK MANAGEMENT STRATEGIES

- Risk Management Strategy alignment with Business Strategy
- Internal Control environment and linkages with Risk Management
- Risk Culture and attitudes to risk management
- Integrated Risk Reporting and Stakeholder responsibilities
- IT Risk Management – Disaster Recovery

5. RISK MODEL

- VAR
- Stress Testing
- Scenario Analysis
- Country and Sovereign Risk Models and Management

6. CREDIT RISK MEASUREMENT AND MANAGEMENT

- Understanding the component of credit risk
- Evaluating credit risk
- Mitigating Credit risk
- Qualitative and Quantitative techniques to manage risk
- Credit scoring models

7. RISK ASSOCIATED WITH CORPORATE GOVERNANCE

- Evaluation of Risk Associated with Governance
- Description and evaluation of framework for Board level consideration of risk
- OECD Guidelines for Corporate Governance

8. ENTERPRISE RISK MANAGEMENT

- Definition, Scope and Techniques

9. OPERATIONAL RISK MANAGEMENT

- Definition, Scope and Techniques

Following topic are covered in the paper of Financial Management (Paper 7 Part I, Intermediate Level) and Strategic Financial Management (Paper – 2, Final Level) also forms the part of the syllabus

- Risk Management in Investment Decisions
- Foreign Exchange Risk
- Interest Rate Risk

BEFORE WE BEGIN ...

Revised Scheme of Education and Training: Bridging the competence gap

The role of a chartered accountant is evolving continually to assume newer responsibilities in a dynamic environment. There has been a notable shift towards strategic decision making and entrepreneurial roles that add value beyond traditional accounting and auditing. The causative factors for the change include globalisation leading to increase in cross border transactions and consequent business complexities, significant developments in information and technology and financial scams underlining the need for a stringent regulatory set up. These factors necessitate an increase in the competence level of chartered accountants to bridge the gap in competence acquired and competence expected from stakeholders. Towards this end, the scheme of education and training is being continuously reviewed so that it is in sync with the requisites of the dynamic global business environment; the competence requirements are being stepped up to enable aspiring chartered accountants to acquire the requisite professional competence to take on new roles.

Introducing "Electives": Significant feature of the Revised Scheme of Education and Training

In the Revised Scheme of Education and Training, the concept of electives is being introduced at the Final level in line with the school of thought that specialisation is the key to developing professionally competent chartered accountants. As per this school of thought, an emerging chartered accountant has to be geared up to assume new roles as consultants and advisors, necessitated on account of growing business complexity, dynamic changes in legislations and regulatory requirements and client expectations.

The seven core papers, namely, Financial Reporting, Strategic Financial Management, Advanced Auditing and Professional Ethics, Corporate and Economic Laws, Strategic Cost Management and Performance Evaluation, Direct Tax Laws and Indirect Tax Laws, represent the competence areas in respect of which an aspiring chartered accountant has to be technically well equipped, regardless of his intended future specialization or role. These subjects, in fact, provide the base to enable an aspiring chartered accountant to specialize in any professional accounting role. For instance, the core paper on direct tax laws and international taxation lays the foundation for further specialisation in the area of international taxation. Further, consequent to borderless economies, it has become imperative that subjects which transcend the borders be added in the curriculum, for instance, Global Financial Reporting Standards and International Taxation.

The six elective papers introduced in the Revised Scheme are Risk Management, Financial Services and Capital Markets, International Taxation, Economic Laws, Global Financial Reporting

Standards and Multi-disciplinary case study. Students have to opt for one out of these six papers keeping in mind their desired area of specialization.

Framework and brief introduction of chapters

The study material of Elective Paper – Risk Management is prepared by mentioning the current scenarios in the Risk Management wherever required. The chapters are prepared in such a manner so as to give the readers an insight into the Risk Management presently operating in India and abroad. Similarly, students will also get familiarized with the various concepts of Risk Management. In the chapter, Risk Model, some of the new concepts currently in vogue have been introduced such as VAR, Stress Testing, Scenario Analysis and Country and Sovereign Risk Management. Similarly, in the Chapter, Credit Risk Measurement and Management, certain interesting topics such as evaluating and mitigating credit risk, Qualitative and Quantitative techniques to manage risk, Credit Scoring Models has been lucidly explained.

Corporate Governance plays an important role in the arena of Risk Management in India. Therefore, the chapter 'Risk Associated with Corporate Governance' has been added. This chapter throws light on Evaluation of Risk Associated with Governance, Description and evaluation of framework for Board level consideration of risk and OECD Guidelines for Corporate Governance.

Further, chapters namely, Enterprise Risk Management, Operational Risk Management and Evaluation of Risk Management Strategies have been added to give wide coverage to the subject Risk Management. In these chapters, some interesting topics have been added to give a new flavour to this dynamic and ever evolving subject.

Features of this study material

There are several significant characteristics of this study material which are outlined as below:

(i) It comprehensively covers the course requirements of students preparing for Risk Management paper.

(ii) The chapters have been organized in such a manner that the concepts of the students are cleared in a step by step process.

(ii) It is written in a very simple and lucid manner to make the subject understandable to the students.

(iii) At the beginning of each chapter, learning outcomes have been given so that the students have some sort of idea about what he will learn after going through the chapter.

(iv) Efforts have also been made to cover contemporary topics in various chapters of Risk Management Paper e.g. VAR, Stress Testing, Scenario Analysis, Artificial Intelligence and Business Analytics etc.

(v) While preparing the study material, it has been kept in mind that students understand the study material. Therefore, it has been endeavored to keep the chapters concise, giving appropriate headings, sub-headings and mentioning examples at suitable places.

Strategy to approach this study material

It is desired from the students that they cover the entire syllabus and are also required to visit ICAI Website for additional study material in the form of Supplementary, Case lets, etc. Students are also advised to update themselves with the latest changes in the Risk Management field. The students are, therefore, required to refer academic updates in 'Students Journal' published by the Board of Studies, the monthly journal 'The Chartered Accountant', and various newspapers such as Economic Times, Mint, Business Line, Financial Chronicle and Business Standards.

Although, sincere efforts have been made to keep the study material error free, it is possible that some errors might have inadvertently crept in. In this respect, students are encouraged to highlight any mistake they may notice while going through the study material by sending an e-mail at rm-final@icai.in or write to the Director of Studies, The Institute of Chartered Accountants of India, A-29, Sector-62, Noida-201309.

Happy Reading and Best Wishes!

DETAILED CONTENTS

CHAPTER 1 – INTRODUCTION TO RISK

1. Introduction and Definitions 1.1
2. Risk and Uncertainty 1.14
3. Classification of Risks 1.16
4. Types of Risk 1.18

CHAPTER 2 – SOURCE AND EVALUATION OF RISKS

1. Identification and Sources of Risk 2.1
2. Quantification of Risk and various methodologies 2.4
3. Risk Identification and Assessment Approaches 2.10
4. Impact of Business Risk 2.22
5. Identify and assess the impact upon the stakeholder involved in Business Risk 2.26
6. Role of Risk Manager and Risk Committee in identifying Risk 2.29

CHAPTER 3 – RISK MANAGEMENT

1. Concept of Risk Management 3.1
2. Objective and Process of Risk Management 3.5
3. Importance of Risk Management 3.9
4. Risk Management Techniques 3.11
5. Risk Management Case Studies 3.12

CHAPTER 4 – EVALUATION OF RISK MANAGEMENT STRATEGIES

1. Risk Management Strategy alignment with Business Strategy 4.1
2. Internal Control environment and linkages with Risk Management 4.5
3. Risk Culture and attitudes to risk management 4.7
4. Integrated Risk Reporting and Stakeholder responsibilities 4.9
5. Risk and Opportunity Reporting 4.15

6. IT Risk Management – Disaster Recovery 4.18

CHAPTER 5 – RISK MODEL

1. VAR 5.1
2. Stress Testing 5.7
3. Scenario Analysis 5.11
4. Country Risk 5.14

CHAPTER 6 – CREDIT RISK MEASUREMENT AND MANAGEMENT

1. Understanding Credit Risk 6.1
2. Components of Credit Risk 6.2
3. Measurement of Credit Risk in Banking Transactions and Factors Affecting Credit Risk 6.3
4. Types of Credit Facilities 6.4
5. Classification of Assets 6.7
6. Evaluating Credit Risk 6.8
7. Mitigating Credit Risk 6.9
8. Qualitative techniques of Credit Risk Management 6.12
9. Quantitative techniques of Credit Risk Management 6.26
10. Credit Scoring Models 6.33

CHAPTER 7 – RISK ASSOCIATED WITH CORPORATE GOVERNANCE

1. Evaluation of Risk Associated with Governance 7.1
2. The Risk Management Function 7.5
3. Independent Assessment of the Risk Governance Framework 7.6
4. Risk Management Disclosures in India 7.9
5. Description and evaluation of framework for Board level consideration of risk 7.16
6. OECD Guidelines for Corporate Governance 7.20

CHAPTER 8 - ENTERPRISE RISK MANAGEMENT

1. Definition and Scope of Enterprise Risk Management 8.1

2. Implementing ERM 8.3
3. Techniques of Enterprise Risk Management 8.4
4. Risk Maturity of an Organization 8.6
5. Process of Enterprise Risk Management and Internal Audit 8.8
6. Stakeholder Value Creation by Enterprise Risk Management 8.8

CHAPTER 9 – OPERATIONAL RISK MANAGEMENT

1. Introduction 9.1
2. Relevance of Operational Risk 9.2
3. Operational Risk Management Governance 9.5
4. Risk Identification and Risk Types 9.10
5. Understanding of Controls 9.15
6. Risk Control Self-Assessment 9.17
7. Technology Risk 9.17
8. Key Risk Indicators and Scenario Analysis 9.21
9. Business Continuity Plan 9.21
10. Outsourcing Risk 9.25
11. Cyber Risk and Information Security Control 9.25
12. Operational Loss Data Management 9.28
13. Business Analytics and Artificial Intelligence 9.32
14. Insurance 9.36

CHAPTER 1

INTRODUCTION TO RISK

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

- The Concept of Risk
- Risk and Uncertainty : Distinction
- Classification of Risks
- Dynamic Nature of Risks
- Types of Risk (illustrative list)
  - Strategic and Operational Risks
  - Business Risk
  - Financial Risk
  - Information Risk
  - Liquidity Risk

1. INTRODUCTION & DEFINITIONS

Risk derives from the early Italian word "risco" which means danger or "risicare," which means "to dare" or French word "risqué". Risk is a choice rather than a fate. The actions companies dare to take are central to our definition of risk. Risk and reward are two sides of the same coin. Risk leaders choose their risks well. They look at external and internal risks in broad context. They integrate decisions with corporate strategy, and strike a healthy balance between risk management as an opportunity and a protection shield.

A business event if it occurs; can have a positive or negative impact on business's objectives. Generally when we discuss risks we fall into the trap of thinking that risks have inherently negative dimension. However, one should be open to those risks that create positive opportunities; you can make your business faster, better and more profitable. Let us look at a example here say on account of non-compliance with environmental laws few old suppliers of a Corporate entity were restricted from supplying materials to the Corporate entity at preferred rates. This posed a challenge to the corporate entity as they have to find new suppliers who would be compliant with environment laws and also perhaps the new rates would be significantly higher than the preferred rates of the old suppliers. The Corporate entity undertakes a detailed supplier discovery exercise and realises that the new suppliers are willing to supply materials at rates that are lower than the preferred rates (agreed with their old suppliers), thus a potential challenge or threat has been converted into an opportunity to reduce the Corporate entity's procurement spend. Think of the adage – "Accept the inevitable and turn it to your advantage." That is what you do when you take business risks to create opportunities.

Risk arises on account of uncertainty of occurrence and unknown consequences if the risk event were to occur. Uncertainty is unpredictable, and has an uncontrollable outcome; taking risks means taking steps or business actions inspite of uncertainty. The degree of uncertainty or likelihood of occurrence and impact of the risk outcome combined together forms the magnitude of the risk. Therefore, measurement of uncertainty and unknown consequences lie at the heart of risk management. Refer Table 1 for various important definitions of risk.

1.1 ICAI Guide on Risk Based Internal Auditing

Meaning of Risk

Organisations exist for a purpose. Whereas the private sector strives to enhance shareholder value, the Government and Not for Profit organizations have a main purpose of delivering service or other benefits in public interest. Achievement of organisational objectives is clouded by uncertainties that both poses threats to and offers opportunity for increasing success. Businesses operate in dynamic environment where change is a constant. Risks arise on account of internal or external factors and circumstances. These circumstances need to be assessed with reference to the organisation's objective.

In a larger sense, risks are those uncertainties of outcome, whether an opportunity or threat, arising out of actions and events. While looking at them narrowly, risks are those uncertainties which impede the achievement of the objective.

Business Risk

Business risks impede the achievement of the organisation's goals and objectives.

All entities exist to provide recognizable benefits for their stakeholders or, in other words to create value for them. Value is created if a stakeholder gets more of something he finds important. Value is created or destroyed by (management) decisions. Decisions entail the recognition of risk and

opportunity and require that management considers information about the internal and external environment, deploys scarce resources and recalibrates activities to changing circumstances.

Today's business is constantly changing. It is unpredictable, volatile and seems to become more complex every day. By its very nature, it is fraught with risk. Organizations thus face uncertainty, and they are not able to precisely determine likelihood and impact of potential events.

Risk Management enables management to deal with risks by reducing their likelihood or downside impact. It aims to protect the value already created by the organization, but also its future opportunities.

Historically, businesses have viewed risk as an evil that should be minimized or mitigated. In recent years, increased regulatory requirements have forced businesses to contribute significant resources to address risk, and other stakeholders in turn have begun to scrutinize whether businesses have the right risk mitigation controls in place. To achieve sustainable success business entity has to continuously identify, assess, measure and manage risks so as to achieve its business objectives and fulfil promises made to stakeholders. Absence of risk management means inviting "Frog in the Well Syndrome". Frog in the well is a Chinese idiom which means a person who is a narrow or close minded person. A frog living in the well believes that is the only world and nothing beyond it exists.

A fast evolving business scenario, climate change, uncertainty arising from global events especially protectionist regimes, innovation, start-up disruption, robotics and automation, competition and volatility of prices, aggressive organisational cultures, heavy regulatory interventions, creates stress and complexity in managing life and businesses. Black swan events, climate crisis and high profile corporate failures in the world have brought risk into the agenda of governments, regulators, boards and societies. Terrorist acts, extreme weather events and the global financial crisis represent the extreme risks that are facing society, commerce and businesses. These extreme risks exist in addition to the daily, somewhat mundane risks.

The Oxford English Dictionary definition of risk is: 'a chance or possibility of danger, loss, injury or other adverse consequences' and the definition of at risk is 'exposed to danger'. In this context, risk is used to signify negative consequences. However, taking a risk can also result in a positive outcome. There is a possibility that risk is related to uncertainty of outcome.

Take the example of traveling by an aeroplane. For most people, traveling by an aeroplane is an opportunity to save time and gain the related benefits. However, there are uncertainties in traveling by an aeroplane that are related to accidents, delays and higher costs. So there are obvious negative outcomes that can occur.

The outcome of Risk is the potential of gaining or losing something of tangible value. The consequence of risk outcomes shall be on health, social status, emotional well-being, financial wealth or reputation/ goodwill can be gained or lost when taking risk resulting from a given action or inaction, foreseen or unforeseen. In business and monetary terms, the value of risk outcomes shall be on employees, suppliers, customers, strategy, objectives, profits, assets, etc.

Examples

1. A fisherman starting a sea voyage on a fishing expedition may result in loss of life.
2. An infant climbing on a window pane may result in damage or injury.
3. A corporate launching a new product or service in the market place may result in failure thereby leading to financial and reputational losses.

Business Dictionary defines Risk Perception as Belief (whether rational or irrational) held by an individual, group, or society about the chance of occurrence of a risk or about the extent, magnitude, and timing of its effect(s). Risk perception is studied by Corporates, Universities, Societies, Governments and other bodies to assess the opinions and views of a target audience or focussed groups to sharpen decision making and judgments where there is lack of clear data on a subject. The concept of Risk perception is closer to the concept of Cognitive Psychology.

Examples (of more riskier propositions in comparison to above)

1. A family of fishermen starting a sea voyage on a fishing expedition may result in loss of life OR a fishermen starting a sea voyage on a fishing expedition in rainy season.
2. A home alone infant climbing on a window pane.
3. A corporate launching a new product or service in the market place without market research.

Examples of Probability and relationship with Value of the Risk Outcome -

1. The probability that an actual return on an investment will be lower than the expected return.
2. The probability of a satellite launch succeeding or failing.
3. The probability of a company successfully listing on a stock exchange.
4. The probability of a loss or drop in value, in case of Securities Trading.
5. The risk of developing cancer is estimated as the incremental probability of developing cancer over a lifetime as a result of exposure to potential carcinogens (cancer-causing substances).

SA 315 of ICAI defines the term **Significant risk** in the context of auditing as – An identified and assessed risk of material misstatement that, in the auditor's judgment, requires special audit consideration.

ICAI's Standard of Internal Audit

Enterprise Risk Management defines Risk is an event which can prevent, hinder, and fail to further or otherwise obstruct the enterprise in achieving its objectives. A business risk is the threat that an event or action will adversely affect an enterprise's ability to maximize stakeholder value and to achieve its business objectives.

Risk can cause financial disadvantage, for example, additional costs or loss of funds or assets. It

can result in damage, loss of value and /or loss of an opportunity to enhance the enterprise operations or activities.

Risk is the product of probability of occurrence of an event and the financial impact of such occurrence to an enterprise.

SA 315 of ICAI defines Business Risk as

A risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies.

TABLE 1. Important Definitions of Risk, IT Risk, Audit Risk

Source	*Definition of risk*
ISO Guide 73 ISO 31000	Effect of uncertainty on objectives. Note that an effect may be positive, negative, or a deviation from the expected. Also, risk is often described by an event, a change in circumstances or a consequence.
Institute of Risk Management (IRM)	Risk is the combination of the probability of an event and its consequence. Consequences can range from positive to negative.
Institute of Internal Auditors	The uncertainty of an event occurring that could have an impact on the achievement of the objectives. Risk is measured in terms of consequences and likelihood. Risk is defined as the possibility that an event will occur, which will impact an organization's achievement of objectives (The Professional Practices Framework 2004)
Paul Hopkins	Event with the ability to impact (inhibit, enhance or cause doubt about) the mission, strategy, projects, routine operations, objectives, core processes, key dependencies and / or the delivery of stakeholder expectations.
Institute of Chartered Accountants of India, SA 315	Business risk – A risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies.
Oxford English Dictionary	(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility.
International Federation of Accountants,1999 :	Uncertain future events which could influence the achievement of the organization's strategic, operational and financial objectives.
CIMA Official Terminology, 2005	Risk is a condition in which there exists a quantifiable dispersion in the possible outcomes from any activity. It can be classified in a number of ways.

Basel II	Operational risk is defined as the risk of loss resulting from inadequate or failed processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.
ICAI – SA 315	A risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies.
COBIT,ISACA	Risk is generally defined as the combination of the probability of an event and its consequence. COBIT 5 - defines IT risk as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.
ICAI Risk Based Internal Audit Guide	Audit risk relates mainly to the internal and external audit efforts to achieve its objectives, i.e., provide effective, timely and efficient assurance to the Board. Audit risk has traditionally been seen strictly as the risk of incorrect audit conclusions. Contemporary views however include big-picture audit risks; specifically, that the internal audit-function is not doing the right things or working in the best ways. Even from internal auditing perspective, an organization with well-established risk management processes decreases audit risk. Where the organization has a formal enterprise-wide risk management program (ERM) in place, the internal auditor would assess it for design adequacy and compliance to decide whether to rely on the risk register and where found reliable then focus on auditing the risk responses to significant risks. By relying on significant risks as determined by management, internal auditing becomes more efficient.

SA 315 of ICAI requires auditors to design and develop risk assessment procedures. Such risk assessment procedures comprise of – the audit procedures performed to obtain an understanding of the entity and its environment, including the entity's internal control, to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels.

The **International Organization for Standardization** defines **Risk as the 'effect of uncertainty on objectives'**. In this definition, uncertainties include events (which may or may not happen) and uncertainties caused by ambiguity or a lack of information. It also includes both negative and positive impacts on objectives. This definition was developed by an international committee representing over 30 countries and is based on the input of several thousand subject matter experts. Very different approaches to risk management are taken in different fields, e.g. "Risk is the unwanted subset of a set of uncertain outcomes" (Cornelius Keating).

Financial Risks

NASDAQ defines Financial Risks as the risk that the cash flow of an issuer will not be adequate to meet its financial obligations. Also referred to as the additional risk that a firm's stockholder bears when the firm uses debt and equity.

In generic terms finance risk is the possibility that the investment return on an investment will be different from the historical or expected return, and also takes into account the magnitude of the difference. This includes the possibility of losing some or all of the original investment.

A free market reflects this principle in the pricing of an instrument: strong demand for a safer instrument drives its price higher (and its return correspondingly lower) while weak demand for a riskier instrument drives its price lower (and its potential return thereby higher). For example, a US Treasury bond is considered to be one of the safest investments. In comparison to an investment or speculative grade corporate bond, US Treasury notes and bonds yield lower rates of return. The reason for this is that a corporation is more likely to default on debt than the U.S. government. Because the risk of investing in a corporate bond is higher, investors are offered a correspondingly higher rate of return.

In financial markets, one may need to measure market risk, credit risk, information timing and source risk, probability, model risk, operational risk, liquidity risk and legal risk if there are regulatory or civil actions taken.

With the advent of automation in financial markets, the concept of "real-time risk" has gained a lot of attention. Real-time risk is defined as the probability of instantaneous or near-instantaneous loss, and can be due to flash crashes, other market crises, malicious activity by selected market participants and other events. A well-cited example of real-time risk was a US $440 million loss incurred within 30 minutes by Knight Capital Group (KCG) on August 1, 2012; the culprit was a poorly-tested runaway algorithm deployed by the firm. Regulators have taken notice of real-time risk as well. Basel III requires real-time risk management framework for bank stability.

1.2 Occupational Health & Safety Advisory Services (OHSAS)

Occupational Health & Safety Advisory Services (OHSAS) defines risk as the combination of the probability of a hazard resulting in an adverse event, and the severity of the event.

In information security, risk is defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization".

Economic risks can be manifested in lower incomes or higher expenditures than expected. The causes can be many, for instance, the hike in the price for raw materials, the lapsing of deadlines for construction of a new operating facility, disruptions in a production process, emergence of a serious competitor on the market, the loss of key personnel, the change of a political regime, or natural disasters.

In terms of occupational health & safety management, the term 'risk' may be defined as the most

likely consequence of a hazard, combined with the likelihood or probability of its occurring. According to encyclopaedia, a Chemical accident is the unintentional release of one or more hazardous substances which could harm human health or the environment. Chemical hazards are systems where chemical accidents could occur under certain circumstances. Such events include fires, explosions, leakages or releases of toxic or hazardous materials that can cause people illness, injury, disability or death.

While chemical accidents may occur whenever toxic materials are stored, transported or used, the most severe accidents are industrial accidents, involving major chemical manufacturing and storage facilities. The most significant chemical accident in recorded history was the 1984 Bhopal disaster in India, in which more than 3,000 people had died after a highly toxic vapour, (methyl isocyanate), was released at a Union Carbide Pesticides factory.

Under Environmental risk analysis an emerging field practitioners identify the potential events that could cause damage to the environment and assess the likelihood of an adverse outcome. An environmental risk assessment (ERA) is a process of predicting whether there may be a risk of adverse effects on the environment caused by a chemical substance.

Information technology risk, or IT risk, IT-related risk, or Cyber risk is a risk related to information technology. This relatively new term was developed as a result of an increasing awareness that information security is simply one facet of a multitude of risks that are relevant to IT and the real world processes it supports. Security risk management involves protection of assets from harm caused by deliberate acts. A more detailed definition is: "A security risk is any event that could result in the compromise of organizational assets i.e. the unauthorized use, loss, damage, disclosure or modification of organizational assets for the profit, personal interest or political interests of individuals, groups or other entities constitutes a compromise of the asset, and includes the risk of harm to people. Compromise of organizational assets may adversely affect the enterprise, its business units and their clients. As such, consideration of security risk is a vital component of risk management.

One of the growing areas of focus in risk management is the field of human factors where behavioural and organizational psychology underpins our understanding of risk based decision making. This field considers questions such as "how do we make risk based decisions?", "why are we irrationally more scared of sharks and terrorists than we are of motor vehicles and medications?"

Positive and negative feedback about past risk taking can affect future risk taking. In an experiment, people who were led to believe they are very competent at decision making saw more opportunities in a risky choice and took more risks, while those led to believe they were not very competent saw more threats and took fewer risks.

Studies and research papers on the subject of Emotional Intelligence have revealed that when people are anxious or in a state of emotion, they pay close attention to potential threats in the environment and are highly vigilant so as to preserve themselves and their resources (Eysenck,

1997; Pacheco Unguetti, Acosta, Callejas, & Lupiañez, 2010). This attention to threat and vigilance leads people to avoid risk (Loewenstein et al., 2001).

It is common for people to dread some risks but not others. They tend to be very afraid of epidemic diseases, nuclear power plant failures, and plane accidents but are relatively unconcerned about some highly frequent and deadly events, such as traffic crashes, household accidents, and medical errors. One key distinction of dreadful risks seems to be their potential for catastrophic consequences, threatening to kill a large number of people within a short period of time. For example, immediately after the September 11 attacks, many Americans were afraid to fly and took their car instead, a decision that led to a significant increase in the number of fatal crashes in the time period following the 9/11 event compared with the same time period before the attacks.

The concept of risk-based maintenance is an advanced form of Reliability Centered Maintenance. In case of chemical industries, apart from probability of failure, consequences of failure are also very important. Therefore, the selection of maintenance policies should be based on risk, instead of reliability.

Risk in an organizational context is usually defined as any event or action that can impact the fulfilment of corporate objectives. Corporate objectives are usually not fully stated or well defined by most corporates. Where the objectives have been established, they tend to be stated as internal, annual and change objectives. This is particularly true of the personal objectives set for members of staff in the organization, where objectives usually refer to change or developments, rather than the continuing or routine operations of the organization. Refer Table 2 for illustrative risks that Corporates are exposed to while navigating the business environment.

TABLE 2. Illustrative Corporate Risks

Corporate Functions	*Risk Areas*
Human Resources	Poor morale & talent retention
Sales & Marketing	Poor Customer loyalty & retention
Operations	Inability to Digitize/ automate processes
Treasury	Low return on investments
Information Technology	Hacking and unauthorized access
New Product development	Product failure
Treasury	Mismatch in cash flows
Finance & Accounts	Unreliable financial statements

Business risks often vary by industry.

ICAI Risk Based Internal Audit Guide provides guidance on the risk classification, sources of risks and risk categories. Following are illustrated from the said guide:-

1.3 Classification of Business Risk

Business risks are of a diverse nature. For example, risks can be classified as internal and external risks; controllable and uncontrollable risks, etc. These classifications help in risk identification and a better understanding of the interplay between the risks themselves and between objectives, strategies, processes, risks and controls during risk assessment.

Business Risks: Internal and External

Internal risks arise from events taking place within the business enterprise. Such risks arise during the ordinary course of a business. These risks can be forecasted and the probability of their occurrence can be determined. Hence, they can be controlled by management significantly. Internal factors giving rise to such risks include:

- Human factors as strikes and lock-outs by trade unions; negligence and dishonesty of an employee; accidents or deaths in the factory, etc.
- Technological factors 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.

External risks arise due to events occurring 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.

External factors giving rise to such risks include:

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

Business Risks: Controllable and Non-controllable

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 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).

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 business faces risks that are unique to that business. Businesses 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,

1.4 Risk Categories by COSO

The COSO framework categories risks as Operations, Financial Reporting, and Compliance. This categorization is illustrated below:

- Inefficiency and non-effectiveness of operations-e.g., the company does not meet strategic objectives, the process does not operate efficiently, customers are not satisfied with services received, etc.
- Financial Reporting-e.g., the absence of a key financial control causes a material error in the financial statements.
- Non-Compliance with laws and regulations-e.g., the company is in violation of applicable regulatory requirements.

1.5 Inherent Risk and Residual Risk

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. For example, the risk of 'over/ understatement of revenue' without considering any internal controls indicates inherent risk. The above risk when considered with internal controls in place (say, monthly reconciliation of revenue and follow up, correction of discrepancies, etc.) indicate residual risk.

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.

1.6 ICAI's Standard of Internal Audit

Enterprise Risk Management states that Risk may be broadly classified into Strategic, Operational, Financial and Knowledge.

- **Strategic Risks** are associated with the primary long-term purpose, objectives and direction of the business.
- **Operational Risks** are associated with the on-going, day-to-day operations of the enterprise.
- **Financial Risks** are related specifically to the processes, techniques and instruments utilised to manage the finances of the enterprise, as well as those processes involved in sustaining effective financial relationships with customers and third parties.

- **Knowledge Risks** are associated with the management and protection of knowledge and information within the enterprise.

From a risk management perspective, it is useful to classify the risks so that the mitigation of the risks can be executed as expeditiously as possible. One common way for risks to be classified is with respect to impact on the organization, whereby risks with certain impacts have to be addressed by certain levels of governance.

Risks are normally classified as time (schedule), cost (budget), and scope but they could also include client relationship risks, contractual risks, technological risks, scope and complexity risks, environmental (corporate) risks, personnel risks, and client acceptance risks, etc.

Another way is to further classify risks by functional domains. Classifying risks as business, information, applications, talent and technology is useful but there may be organisation specific ways of expressing risk that the corporate enterprise architecture should adopt or extend rather than modify.

1.7 Open Group Standard

The Open Group suggests classifying risks with respect to *effect and frequency* in accordance with scales used within the organization. There are no hard and fast rules with respect to measuring effect and frequency.

Effect could be assessed using the following criteria as an example:

- **Catastrophic** infers critical financial loss that could result in bankruptcy of the organization.
- **Critical** infers serious financial loss in more than one line of business leading to a loss in productivity and no return on investment on the investment.
- **Marginal** infers a minor financial loss in a line of business and a reduced return on investment.
- **Negligible** infers a minimal impact on a line of business' ability to deliver services and/or products.

Frequency could be indicated as follows:

- **Frequent**: Likely to occur very often and/or continuously.
- **Likely**: Occurs several times over the course of a transformation cycle.
- **Occasional**: Occurs sporadically.
- **Seldom**: Remotely possible and would probably occur not more than once in the course of a transformation cycle.
- **Unlikely**: Will probably not occur during the course of a transformation cycle.

Combining the two factors to infer impact would be conducted using a heuristically-based but consistent classification scheme for the risks. A potential scheme to assess corporate impact could be as follows:

- **Extremely High Risk (E)**: The transformation effort will most likely fail with severe consequences.
- **High Risk (H)**: Significant failure of parts of the transformation effort resulting in certain goals not being achieved.
- **Moderate Risk (M)**: Noticeable failure of parts of the transformation effort threatening the success of certain goals.
- **Low Risk (L)**: Certain goals will not be wholly successful.

1.8 The ICAI Guide on Risk Based Internal Audit

It provides relevant information on the subject of Risk Attributes, Measurement and Risk Score. It states the following:

All risks have two attributes, viz.

- Likelihood of risk occurrence.
- Risk consequence.

To facilitate understanding and usability in decision making of 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. This 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'.

The **measurement of the likelihood of risk** is normally against five levels on a scale of 5, viz.

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

Risk consequences can also be against five levels on a scale of 5, viz.

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

- Catastrophic (score 5).

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 damage to the distribution network of an electricity distribution company can be 'remote' but the consequences of damage can be 'catastrophic'. In such a scenario 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 significant risk and to be included in the audit plan.

2. RISK & UNCERTAINTY

In his seminal work *Risk, Uncertainty, and Profit*, Frank Knight (1921) established the distinction between risk and uncertainty.

Uncertainty must be taken in a sense radically distinct from the familiar notion of Risk, from which it has never been properly separated. The term "risk," as loosely used in everyday speech and in economic discussion, really covers two things which, functionally at least, in their causal relations to the phenomena of economic organization, are categorically different. The essential fact is that "risk" means in some cases a quantity susceptible of measurement, while at other times it is something distinctly not of this character; and there are far-reaching and crucial differences in the bearings of the phenomenon depending on which of the two is really present and operating. It will appear that a measurable uncertainty, or "risk" proper, as we shall use the term, is so far different from an immeasurable one that it is not in effect an uncertainty at all. We accordingly restrict the term "uncertainty" to cases of the non-quantitative type.

Thus, Knightian uncertainty is immeasurable, not possible to calculate, while in the Knightian sense risk is measurable.

Another distinction between risk and uncertainty is proposed by Douglas Hubbard:

(i) Uncertainty: The lack of complete certainty, that is, the existence of more than one possibility. The "true" outcome/state/result/value is not known.

Measurement of uncertainty: A set of probabilities assigned to a set of possibilities.

Example: "There is a 60% chance this market will double in five years"

(ii) Risk: A state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome.

Measurement of risk: A set of possibilities each with quantified probabilities and quantified losses. Example: "There is a 40% chance the proposed oil well will be dry with a loss of $12 million in exploratory drilling costs".

In this sense, **one may have uncertainty without risk but not risk without uncertainty**. We can

be uncertain about the winner of a contest, but unless we have some personal stake in it, we have no risk. If we bet money on the outcome of the contest, then we have a risk. In both cases there is more than one outcome. The measure of uncertainty refers only to the probabilities assigned to outcomes, while the measure of risk requires both probabilities for outcomes and losses quantified for outcomes.

Complexity, Volatility, Ambiguity and Uncertainty

If terms are interchanged the acronym becomes VUCA which is used to describe or reflect on the volatility, uncertainty, complexity and ambiguity of general conditions and situations: -

Complexity

Characteristics: the situation has many interconnected parts and variables. Some information is available or can be predicted, but the volume or nature of it can be overwhelming to process.

Example: you are doing business in many countries, all with unique regulatory environments, tariffs, and cultural values.

Approach: Restructure, bring on or develop specialists, and build up resources adequate to address the complexity.

Volatility

Characteristics: The challenge is unexpected or unstable and may be of unknown duration, but it's not necessarily hard to understand; knowledge about it is often available.

Example: Prices fluctuate after a natural disaster takes a supplier off-line.

Approach: Build in slack and devote resources to preparedness-for instances, stockpile inventory or overbuy talent. These steps are typically expensive; your investment should match the risk.

Ambiguity

Characteristics: Casual relationships are completely unclear. No precedents exist; you face "unknown unknowns."

Example: You decide to move into immature or emerging markets or to launch products outside your core competencies.

Approach: Experiment, understanding cause and effect requires generating hypotheses and testing them. Design your experiments so that lessons learned can be broadly applied.

Uncertainty

Characteristics: Despite a lack of other information, the event's basic cause and effect are known. Change is possible but not a given.

Example: A competitor's pending product launch muddies the future of the business and the market.

Approach: Invest in information-collect, interpret, and share it. This works best in conjunction with structural changes, such as adding information analysis networks that can reduce on-going uncertainty.

(Source: - Harvard Business Review/hbr.org/what-vuca-really-means-for-you)

3. CLASSIFICATION OF RISKS

3.1 Nature of Risks

Risk may bear positive or negative results or may simply result in uncertainty. For example where the Municipal authorities of a metropolis decide to implement a Metro Rail project; it is with the objective of reducing traffic and travel time for city residents, however, if there are frequent fatal accidents at the Metro Rail resulting in loss of human life and public property, the decision of Municipal authorities to implement Metro Rail project would be seen in a different light. Therefore, risks may be considered to be related to an opportunity or a loss or the presence of uncertainty for an organization. Every risk has its own unique nature and characteristics that require study, management or analysis.

3.2 Categorisation of Risks

According to Paul Hopkins (in Fundamentals of Risk Management) risks are generally divided into three categories:-

- Hazard (or pure) risks;
- Control (or uncertainty) risks;
- Opportunity (or speculative) risks.

Pure Risks are associated with uncertainties which may cause loss. In a pure risk situation, a loss occurs or no loss occurs – there is no possibility for gain. These uncertainties may be due to perils such as fire, floods, etc. or may arise from human action such as theft, accident etc. There are certain risk events that can only result in negative outcomes such as fire accidents or leakage of harmful chemicals from a manufacturing plant. These risks are hazard risks or pure risks, and these may be thought of as operational or insurable risks. A good example of a hazard risk faced by many organizations is that of theft. There are different types of pure risks:

- Personal risks - It includes early death, sudden accident and disability, unemployment, etc.
- Property risks - reduction in value of assets due to physical damage, fire, theft, etc.
- Liability Risks - the risk of legal liability for damages accruing to customer, suppliers, vendors, etc. Such risks are also connected with compensation payable to employees for injuries and other harm afflicted in the workplace.

Above situations all come under the category of pure risks and are insurable.

Fundamental Risks are impersonal in nature. They are present in nature and the economy, and are beyond the control of man. Their effect is pervasive and usually impacts a large group of people. Earthquakes, war, inflation, mass unemployment, etc., are examples of such fundamental risks. Generally, these risks are not insurable and it is left to the Government to deal with the effects of these events. However, in situations where the occurrences are irregular and the impact in minimal, the insurers can venture to insure these risks.

Particular Risks have their origin in individual events which can be partially controlled. They occur due to the action of the individuals, for example, meeting with an accident while crossing the road. These risks are insurable with conditions.

Dynamic Risks may arise due to changes in the economy like fluctuations in price levels, consumer references, distribution of income, product development, shifts in technology, etc. These are called Dynamic Risks. As they are less predictable, generally, they are not insurable.

Control risks are associated with unknown and unexpected events. They are sometimes referred to as uncertainty risks and they can be extremely difficult to quantify. Control risks are often associated with project management. In these circumstances, it is known that the events will occur, but the precise consequences of those events are difficult to predict and control. Therefore, the approach is based on minimizing the potential consequences of these events.

There are two main aspects associated with opportunity risks. These risks/dangers are associated with taking an opportunity and not taking the opportunity. Opportunity risks may not be visible or physically apparent, and they are often financial in nature. Although opportunity risks are taken with the intention of having a positive outcome, this is not guaranteed. Opportunity risks for small businesses include moving a business to a new location, acquiring new property, expanding a business and diversifying into new products.

Speculative Risks have three possible outcomes: loss, no loss or gain. Examples of such risks include the decision to invest in some shares etc. The statistical techniques used in insurance cannot be applied to speculative risks. Further, these risks are deliberately taken with the hope of gain. Generally, speculative risks are not considered insurable.

It may be noted that there is no 'right' or 'wrong' classification of risks. Risks can be grouped according to their **nature**, **estimated cost or likely impact, likelihood of occurrence, countermeasures required**, etc.

For example, Credit risk, is classified according to the likelihood of the collection of accounts receivable.

The most important issue is that an organization adopts the risk classification system that is most suitable for its own circumstances.

Risks which occur even with no changes in the economy are classified as Static Risks. These include losses due to perils like fire, theft and dishonesty of individuals. Over a period of time, certain regularity may be observed in these occurrences and they may become predictable. Such static risks are more insurable than Dynamic Risks.

Example

In order to understand the distinction between hazard, control and opportunity risks, the example of the use of machines is useful. Technical snag while operating a machine is an operational or hazard risk and there will be no benefit to an organization suffering a technical breakdown in its manufacturing operations. When an organization installs or upgrades a machine, control risks will be associated with the upgraded project.

The selection of new machine is an opportunity risk, where the intention is to achieve better results by installing the machine, but it is possible that the new machine will fail to deliver all of the functionality that was intended and the opportunity benefits will not be delivered. In fact, the failure of the functionality of the new machine may substantially undermine the manufacturing operations of the organization.

4. TYPE OF RISKS

Events can have negative impact, positive impact, or both. Events with a negative impact represent negative risks, which can prevent value creation or erode existing value. Events with positive impact may offset negative impacts or represent opportunities. Risk and opportunity management are closely related, organisations with superior competencies and knowledge database attempt to convert negative risk events into positives by creating a focussed group of experts who brainstorm on breakthrough ideas that could help the organisation move in a positive direction. This is a contemporary phenomenon and is commonly referred to as “catching the ball” or “idea funnel”. Risk management is all about value protection, maximizing gains from risk outcomes and seizing the opportunities by formulating management action plans. Disruptive start up culture is all about identifying real life problems and converting them into business opportunities.

According to webopedia - Risk as part of GRC (Governance, Risk and Compliance) Management is the ability to effectively and cost-efficiently mitigate risks that can hinder an organization's operations or ability to remain competitive in its market.

Businesses face different type and extent of risks, few may cause serious loss of profits or even bankruptcy. Large companies have extensive "risk management" departments; smaller businesses tend not to look at the issue in such a systematic way but may have a more hands on approach to risk management. A successful business needs a comprehensive, well-thought-out business plan. However, business is dynamic; things change, and the best-laid plans can sometimes appear out-dated in quick time. When the company’s strategy becomes less effective in the market place and it struggles to reach its goals as a result; the company is facing strategic risks or model risks. It could be due to technological changes, a powerful new competitor entering the market, shifts in customer demand, spikes in the costs of raw materials, or any number of other large-scale changes.

Business risks can arise due to the influence by two major risks: - internal risks (risks arising from the events taking place within the organization) and external risks (risks arising from the events

taking place outside the organization).

Risks are caused on account of two factors internal and external. Further, these internal factors are controllable and uncontrollable. Let us look at the table below that highlights some examples of internal and external factors:

Internal Factors	*External Factors*
Controllable • Stability and financial position of the entity • Labour strikes • Machine failure • Staff morale ***Uncontrollable*** • Accidents • Attrition of people • Technological change • Frauds	***Controllable*** • Compliance with regulatory changes ***Uncontrollable*** • Economic conditions • Floods • Earthquake • Market/environment

In addition to the business risks, organisation can have following major risks (illustrative) which will be applicable to any organisation:-

- **Financial risk** - These risks are associated with the financial assets, structure and transactions of the particular industry.
- **Credit risk** - The risk of loss arising from outright default due to the inability or unwillingness of the customer or counterparty to meet their commitments. Credit risk is the probability of loss from a credit transaction. It is also called as default risk.
- **Liquidity risk** - The potential inability to meet commitments as they fall due. It arises whenever the bank is unable to generate cash to meet out its liability payment obligations or increase in assets or its failure to manage the unplanned decreases or changes in the funding sources. Liquidity risk also arises on account of its failure to address the changes in the market conditions that affect its ability to liquidate its assets quickly and with minimal losses.

  Liquidity risk may arise due to changes or variations in the market conditions such as, volatility of rate of interest or the Foreign exchange rate /Investment mismatch or risk or poor economic conditions like depression / inflation / loss of confidence in the business by its customers/ rumors about the business and its effects of run on the liquidity/ failure of some of the banks where its deposits got struck or blocked or war like situations with the enemies of state are some of the examples where the businesses will be facing liquidity crisis as it may cause heavy out flow of funds.

- **Market risk** - The risk of losses caused by adverse changes in the market variables such as interest rate, Foreign Exchange rate, equity price and commodity price. RBI has defined the Market Risk as the possibility of loss to a bank caused by the changes in market rates / prices. Market risk is the possibility for an investor to experience losses due to factors that affect the overall performance of the financial markets in which he has invested money. Market risk, also called "systematic risk," cannot be eliminated through diversification, though it can be hedged against. Sources of market risk include recessions, political turmoil, and changes in interest rates, natural disasters and terrorist attacks.
- **Operational Risk**- The risk associated with the operations of an organization. It is the risk of loss resulting from failure of people employed in the organization, internal process, systems or external factors acting upon it to the detriment of the organization. It includes Legal Risk and excludes strategic and Reputational Risks as they are not quantifiable.
- **Strategic Risk** - The current and prospective impact on earnings, capital, reputation or good standing of an organization arising from its poor business decisions, improper implementation of decisions or lack of response to industry, economic or technological changes. Failure of strategies will adversely impact the business objectives and attainment of the goals.
- **Compliance Risk** – It includes material financial loss or loss of reputation which may occur as result of its failure to comply with the laws includes, regulations, rules, related self-regulatory organization, standards and code of conduct applicable to its business activities.
- **Regulatory Risk** - Regulatory Risk arises due to changes made in policies and procedures by the regulators viz, RBI, Central and State Governments, SEBI, IRDA, etc. Withdrawal of licenses, change in capital adequacy requirements, change in NPA norms etc. may be grouped under this category. Any changes in the rules and regulations which may have a negative impact on the business activities can be classified under this risk.
- **Reputation risk** – Adverse publicity regarding an entity's practices will lead to a loss of revenue or litigation. Any event which affects the name or brand image of the entity is Reputational Risk. Any adverse publicity, news coverage, comments etc. has the ability to dent the trust created by the entity and becomes detrimental to the business of the entity.
- **Legal risk** - Arises from the uncertainty due to legal actions or uncertainty in the application, interpretation of contracts, laws or regulations. Legal risk is the risk arising from failure to comply with statutory or legal requirements.
- **Interest rate risk** - Risk where changes in the market interest rates might adversely affect the Net interest Income earnings. It is the threat that interest paid may be more than the interest collected resulting in financial loss.
- **Foreign exchange risk**- Risk of loss that the entity may suffer on account of adverse fluctuations in the exchange rate movements in currencies.
- **Management risk** – Risk of management interference in day to day operations and putting

undue demands and restrictions on staff. Quality of senior management affects the decision making and contributes to management risk. It means the risks associated with ineffective, destructive or underperforming management, which hurts shareholders and the company or fund being managed. This term refers to the risk of the situation in which the company and shareholders would have been better off without the choices made by management.

- **Staffing risk** – Risk of not employing the right person for the right job. Poorly drafted job descriptions, inadequate background verifications and inexperienced personnel contribute to staffing risk.
- **Technology risk** – Risk of not keeping pace with the fast changing technologies for business operations. Usage of outdated technologies could impact the business operations adversely thereby resulting in loss of reputation, market share, customers, etc.
- **Business continuity risk** – Risk arising from inability to restore operations immediately in the event of an incident / disaster.
- **Information (data security) risk** – Risk of unauthorized access to data. Poor access controls both at the network level and application level give rise to this risk. While information has long been appreciated as a valuable and important asset, the rise of the knowledge economy and the Digital Revolution has led to organizations becoming increasingly dependent on information, information processing and especially IT.
- **Country risk** – Helps to address the issues of identifying, measuring, monitoring and controlling country exposure risks. Procedures are in place for ensuring that necessary steps are taken as per RBI guidelines.
- **Fraud risk –** Risk of control failures, management override and deliberate acts of omission and commission that lead to financial losses.
- **Price risk** - Probability of loss occurring from adverse movement in the market price of an asset.
- **Process risk** – Inability of the management to meet its process related objectives on account of failed activities in a business process. It is a risk of loss resulting from failure of internal processes, people and systems or from external events.
- **Security Risk** - A person or situation which poses a possible threat to the security of something. Security arrangements risk - risk which arises from vulnerability of security systems is termed as security arrangements risk.
- **Governance risk** - Refers to in-effective, un-ethical management of a company by its executives and managerial levels.
- **Safety risks** - These are the most common and will be present in most workplaces at one time or another. They include unsafe conditions that can cause injury, illness and death. Safety Hazards include: -

- Spills on floors or tripping hazards, such as blocked aisles or cords running across the floor.
- Working from heights, including ladders, scaffolds, roofs, or any raised work area.
- Unguarded machinery and moving machinery parts; guards removed or moving parts that a worker can accidentally touch.
- Electrical hazards like frayed cords, missing ground pins, improper wiring.
- Confined spaces.
- Machinery-related hazards (lockout/tag out, boiler safety, forklifts, etc.).

CHAPTER 2

SOURCE AND EVALUATION OF RISKS

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

- Identification and Sources of Risk
- Quantification of Risk and various methodologies
- Impact of Business Risk
- Identity and assess the impact upon the stakeholder involved in Business Risk
- Role of Risk Manager and Risk Committee in identifying Risk

1. IDENTIFICATION AND SOURCES OF RISKS

1.1 Risk identification is the initial step in the process of risk management

Risk identification is the action or process of identifying some potential internal or external event, or threat or vulnerability or a fact that could cause damage to the entity or prevent it from achieving its objectives. It includes documenting the potential risks in the form of a risk questionnaire or risk register and communicating the risks to the executive management.

Risk identification is effective when the risk management team understands the business, industry or sector in which the business operates and the key management objectives or key performance indicators. Imaginative thinking and use of what can go wrong pointers forms the essence of a robust risk identification exercise. Risk identification can be approached by a Top down exercise from the senior level to the junior level or vice versa, however, experience suggests that Top down

exercises work more effectively and provide better outcomes to the businesses.

Identification of risks is the process of determining which risks may affect the business/project and documenting their characteristics. Participants in the Identification process will usually include:-

- Business managers
- Project team
- Risk management team
- Subject matter experts
- Customers
- End users
- Other project managers, stakeholders, and
- Outside experts

1.2 Risk identification sets out to identify an organisation's exposure to uncertainty

This exercise can be successfully executed if the risk management team has reasonable degree of business knowledge and related variables in which the business operates. The various risk variables include legal, social, community, political and other factors that impact the business model of the entity. The risk management project team should intimately understand the business strategy and the market place in which the entity operates. Further, the risk management team should undertake a Strength, Weakness, Opportunity and Threat assessment exercise so as to document the factors that could give rise to potential risks in future. The SWOT analysis exercise will facilitate development of sound business knowledge and communication of key business weaknesses, threats and opportunities to seize in the risk management exercise.

The entity becomes aware of various risks through the Risk Identification and thereafter deals with the risks it faces. It must set objectives, integrated with the sales, production, marketing, financial and other activities so that the organization is operating in concert. It also must establish mechanisms to identify analyze and manage the related risks.

The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed. It:

- Involves appropriate levels of management;
- Includes entity, subsidiary division, operating unit, and functional levels;
- Analyzes internal and external factors;
- Estimates significance of risks identified;
- Determines how to respond to risks.

All above activities should be approached in a methodical manner so that any significant business activity or risk item is not missed out by the risk management project team. One of the best ways to identify risks is by flow-charting the key business processes and thereafter undertaking a "what can go wrong exercise".

SA 315 of ICAI states that financial reporting is also subject to risks arising from a number of internal and external transactions, events or circumstances. These factors may adversely affect the company's ability to initiate record, process and report financial data consistent with the assertions of management in the financial statements. Examples of some of these risks are:

- Change in operating environment
- New personnel
- Rapid growth
- New technology
- New business models, products, or activities
- Corporate re-structuring
- Expanded foreign operations
- New accounting pronouncements.

Generally, business functions that can be assessed from a risk perspective are:

- **Strategic –** These include business model risk factors in terms of product demand factors, availability of supply chain inputs at competitive rates, innovation, competition, financial stability and capital access, etc. These relates to the achievement of long-term strategic objectives of the entity. They can be affected by availability of capital, country and political risks, legal and regulatory changes, reputation and changes in the economic environment.
- **Operational –** These include process execution and day-today issues that the entity is exposed to.
- **Financial –** These concern the effective management and control of the finances of the organisation and the effects of external factors such as availability of credit, working capital, foreign exchange rates, interest rate movement and other market exposures.
- **Knowledge management –** Where the entity does not manage effectively it only manages information in its activity stream. The effective management and control of the knowledge resources includes production, protection and communication of knowledge. Factors contributing to knowledge risks include the unauthorised use or abuse of intellectual property/competitive technology. Internal factors may include loss of key staff.
- **Compliance management –** Business entity has to comply with a lot of laws and regulations that are directly or indirectly applicable to its business. The laws vary from environmental

protection to specific state laws in the region which the entity may operate. To manage compliances effectively entities undertake a detailed compliance risk assessment exercise wherein each applicable law is mapped for specific compliance obligation and the mitigating compliance action plan against it is documented. Such activities can be undertaken in-house or externally facilitated, however, the primary ownership and responsibility of compliance management cannot be transferred to a third party such as consultant or auditor.

The Risk Identification process is a constantly evolving process as new risks emerge during the business life cycle. The frequency of iteration and who participates in each cycle will be different with different projects. The project team needs to be involved in the process so that it can develop and maintain a sense of ownership and responsibility for the risks and associated risk-response actions.

1.3 Additional objective information can be provided by persons outside the team

The Risk Identification process usually leads to the Perform Qualitative Risk Analysis process, or it can lead directly to the Perform Quantitative Risk Analysis process when conducted by an experienced risk manager.

The objective of risk identification is the early and continuous identification of events that, if they occur, will have negative impacts on the project's ability to achieve performance or capability outcome goals. They may come from within the project or from external sources.

Organisations undertake Risk Identification by using several techniques and tools. Whilst a **SWOT Analysis** is a quick way to identify new opportunities and identify threats, many organisations have gone beyond this relatively simple approach and embraced more advanced forms of identifying and assessing risks and opportunities. Many organisations have adopted an **Enterprise-wide Risk Management (ERM)** approach that is more structured approach to identifying and managing risk.

2. QUANTIFICATION OF RISK AND VARIOUS METHODOLOGIES

Risk Assessment is an important step in the risk management process. Risk assessment is the determination of qualitative and quantitative values of the risk related to a situation or a recognised threat. Risk assessment is necessary for developing a comprehensive risk mitigation plan.

Risk Measurement - Once risks have been identified, they are assessed and measured in order to determine their probability of occurrence, costs, opportunity, social and eventual impact on the entity's profitability and capital. This can be done using various techniques ranging from simple to sophisticated models. Accurate and timely measurement of risk is essential to effective risk management systems. Good risk measurement systems assess the risks of both individual transactions and portfolios.

Risk assessment is the determination of quantitative or qualitative estimate of risk consequence related to a scenario or situation and an identified threat or hazard.

Risk quantification is the process of evaluating and defining the cost and benefits associated with the risk consequences. For example historical share price data of public listed entities can be mined to make assessments of possible future price movements, in light of past fluctuations of the share price for the purpose of making an investment decision.

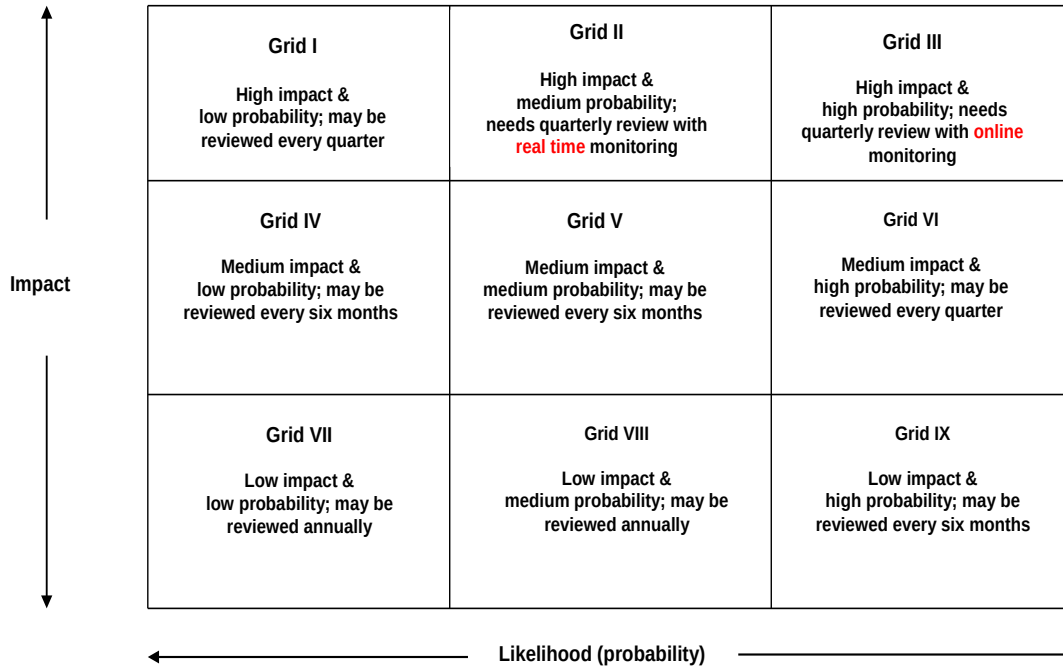
2.1 Qualitative Risk Assessment

Risk Probability and Impact assessment generally finds answers to the following questions -

- What is the probability that a risk will occur?
- What will it cost the business if it does happen?
- The Probability and Impact Matrix indicates which risks need to be managed

Simple way of assessing a risk is by attaching a probability and impact to the happening of an event. If it is certain that an event cannot occur, it is given a probability of 0; if it is certain that it will occur, it is given a probability of 1. Similarly if the impact is significant it can be assigned a weight of 1 and where there is no impact the event can be assigned a weight of 0. Uncertain risks are assigned between 0 and 1 viz., 0.5. Maximum risk impact the event could generate is 1 and in case of uncertainty 0.5. The severity of the risk is a practical measure for quantifying risks that indicates the extent of harm a risk can cause. Generally during a risk assessment exercise a risk probability and impact matrix is prepared where the levels of risk severity are depicted through a colour scheme of red, green and yellow where red being the most severe or critical risk condition. This is also called as the traffic signal risk card.

Risk assessment is a method of analysing the significance and priority of a risk. Under the Qualitative Analysis, all the identified risks are plotted on a matrix. Each risk item is given a position on the matrix chart. An example of the matrix can be seen below. The probability of the risk occurring can be plotted on the horizontal bar, while the impact of the risk can be noted along the vertical bar of the axis. The probability-impact value of a risk is a product of both the values assigned for the risk. Hence, it can be seen that a risk with a value of 9, where the probability and impact rate the highest, requires immediate attention – Grid III. Those with a low rating of 1 or 2 require the least attention and may even be ignored, if insignificant - Grid VII.



2.2 Quantitative Risk Assessment

Quantitative risk management is the process of converting the impact of risk on the business/project into numerical terms. This numerical information is frequently used to determine the cost and time contingencies of the project. Several methods of contingency determination, which are based on the results of a quantitative risk assessment, are explored.

The objective of quantification is to establish a way of arranging the risks in the order of importance.

A clearer understanding of the quantitative risk assessment can be reached by following the example given below on the Decision Making Tree method.

Example

A public event is planned in another city which is entirely dependent on the weather conditions in the city. There are many variables which determine its outcome, but the deciding criteria is that the result to be a value of 65%. As per information generated via weather conditions, the following data is assembled.

Chance of good weather: 40%

Chance of bad weather: 60%

Chance of public event in good weather: 70% = (i.e. 30% chance of no public event)

Chance of public event in bad weather: 30% = (i.e. 70% chance of no public event)

Using the Decision Making Tree for this risk assessment, the data for the entire tree has to be processed and calculated. The procedure for calculating this is;

[probability of public event in good weather] + [probability of public event in bad weather]

i.e. [good conditions] + [bad conditions]

= [0.40 x 0.70] + [0.60 x 0.30]

= 0.28 + 0.18

=0.46

This can also be translated as a 46% probability for a public event. While the cut-off criteria for the public event are 65%, the idea for having a public event can be cancelled. According to the calculations, the risk for holding a public event is very high. It may never succeed.

Risk management is done from very early in the project until the very end.

Risk quantification involves evaluating risks and risk interactions to assess the range of possible outcomes. It is primarily concerned with determining which risk events warrant response. It is complicated by a number of factors including, but not limited to:-

- Opportunities and threats can interact in unanticipated ways (e.g., schedule delays may force consideration of a new strategy that reduces overall project duration).
- One risk event can cause multiple impacts; say late delivery of a key manufacturing component causes cost overruns for the manufacturing facility and delays schedule to customers and results in penalties from the customer.

2.3 Tools and Techniques for Risk Quantification

Following are some of the tools and techniques that are available to assess and evaluate risks:

(a) Judgment and intuition: In many situations, the management and auditors have to use their judgment and intuition for risk assessment. This mainly depends on the personal and professional experience of the management and auditors and their understanding of the business, system and its environment. Together with it is required a systematic education and on-going professional updating.

(b) The Delphi approach: The Delphi technique is defined as: 'a method for structuring a group communication process so that the process is effective in allowing a group of individuals as a whole to deal with a complex problem'. It was originally developed as a technique for the US Department of Defence. The Delphi Technique was first used by the Rand Corporation for obtaining a consensus opinion. Here, a panel of experts is appointed. Each expert gives his/her opinion in a written and independent manner. They enlist the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposures of the system. These estimates are then compiled together. The estimates within a pre-decided acceptable range

are taken. The process may be repeated four times for revising the estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.

(c) Scoring: In the Scoring approach, the risks in the business, system and their respective exposures are listed. Weights are then assigned to the risk and to the exposures depending on the severity, impact on occurrence, and costs involved. The product of the risk weight with the exposure weight of every characteristic gives us the weighted score. The sum of these weighted score gives us the risk and exposure score of the system. System risk and exposure is then ranked according to the scores obtained.

(d) Quantitative techniques: These techniques involve the calculation of an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs. This helps the organization to select cost effective solutions. It is the assessment of potential damage in the event of occurrence of unfavorable events, keeping in mind how often such an event may occur.

(e) Qualitative techniques: These techniques are most widely used approaches to risk analysis. Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies use a number of interrelated elements:

- **Threats:** These are things that can go wrong or that can 'attack' the system. Examples might include fire or fraud. Threats are ever present for every system.
- **Vulnerabilities:** These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire, vulnerability would be the presence of inflammable materials (e.g. Paper).
- **Controls:** These are the countermeasures for vulnerabilities. They are of four types:
  - (i) Deterrent controls reduce the likelihood of a deliberate attack.
  - (ii) Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact.
  - (iii) Corrective controls reduce the effect of an attack.
  - (iv) Detective controls discover attacks and trigger preventative or corrective controls.

(f) Expected monetary value, as a tool for risk quantification, is the product of two numbers.

- Risk event probability--an estimate of the probability that a given risk event will occur.
- Risk event value--an estimate of the gain or loss that will be incurred if the risk event does occur.

The risk event value must reflect both tangibles and intangibles. If Project A predicts little or no intangible effect, while Project B predicts that such a loss will put its performing organization out of business, the two risks are not equivalent.

In similar fashion, failure to include intangibles in this calculation can severely distort the result by equating a small loss with a high probability to a large loss with a small probability. The expected monetary value is generally used as input to further analysis (e.g., in a decision tree) since risk events can occur individually or in groups, in parallel or in sequence.

(g) Simulation uses a representation or model of a system to analyze the behaviour or performance of the system. The most common form of simulation on a project is schedule simulation using the project network as the model of the project. Most schedule simulations are based on some form of Monte Carlo analysis. This technique, adapted from general management, "performs" the project many times to provide a statistical distribution of the calculated results.

(h) Decision Tree is a diagram that depicts key interactions among decisions and associated chance events as they are understood by the decision maker. The branches of the tree represent either decisions (shown as boxes) or chance events (shown as circles).

(i) Expert Judgement can often be applied in lieu of or in addition to the mathematical techniques described above. For example, risk events could be described as having a high, medium, or low probability of occurrence and a severe, moderate, or limited impact.

(j) Frequency of Loss measures the number of times losses occur during a particular period of time. If you have measured this loss in the past, you can use the historical data to make a prediction. An accounts receivable reserve account is an example of frequency of loss. If your company had 2.5% in losses an uncollectable accounts receivable in the previous two years, you would use this estimate for the current year.

(k) Scenario Analysis - Use scenario analysis to assess the risk of a downturn in real estate or other asset prices, an up or down shift in interest rates or other market factors. With scenario analysis, you determine what impact various scenarios could have on the business. For example, a company has a line of credit with a variable interest rate. Using scenario analysis, one could determine the company's default risk if the interest rate jumped three percentage points during the year.

2.4 Other Business Risk Measurements

There are a variety of business risk measurement tools and techniques, few are highly technical, statistical and quantitative, whereas others more subjective, judgement driven and qualitative.

Methods include expected loss, value at risk and unexpected loss measures, tolerance testing, sensitivity analysis, financial ratios, statistical sampling and profit variation to evaluate and quantify risks. It is important to identify the risks, and then measure them using a method that is sufficiently simple for consistent application.

2.5 Outputs from Risk Quantification

The results of risk quantification shall facilitate decision making for the purpose of chalking out risk mitigation strategies. The ultimate purpose of risk identification, quantification and analysis is to

prepare for risk mitigation. A systematic reduction in the extent of exposure to a risk and/or the likelihood of its occurrence is termed as 'Risk Mitigation'. Typically, in cases of risk mitigation, there is a particular threshold that is acceptable below which the risk is attempted to be mitigated. Factor or casual analysis can help to relate characteristics of an event to the probability and severity of the operational losses. This will enable the organization to decide whether or not to invest in technology or people (hazards) so events (frequency) or the effect of events (severity) can be minimized.

A causal understanding is essential to take appropriate action to control and manage risks because causality is a basis for both action and prediction. Knowing 'what causes what' gives an ability to intervene in the environment and implement the necessary controls. Causation is different from correlation, or constant conjunction, in which two things are associated because they change in unison or are found together.

Predictive models (such as loss models) often use correlation as a basis for prediction, but actions based on associations are tentative at best. Simple cause and effect relationships are known from experience, but more complex situations such as those buried in the processes of business operations may not be intuitively obvious from the information at hand. An Information System audit and control professional may be required to establish the cause. Cause models help in the implementation of risk mitigation measures. Cause analysis identifies events and their impact on losses.

Common outputs from risk quantification include Risk Scorecard, Value at Risk Measure, Sampling plan, Simulated Model, Projections, etc.

One of the major outputs from Risk Quantification is a list of possible opportunities that should be pursued and threats that require attention.

3. RISK IDENTIFICATION AND ASSESSMENT APPROACHES

The various **risk identification and assessment approaches** an organisation can choose from are lucidly illustrated by Tony Harb B. The most useful techniques of risk identification are detailed hereunder:-

1. **Analysis of processes** – Under this technique, material or significant business processes are flow chartered. This will facilitate identification of process level operational risks. An approach that helps improves the performance of business activities by analysing current processes and making decisions on new improvements.

2. **Brainstorming** – Under brainstorming a group of employees put forward their ideas or sensation of risk. The employees estimate the risk based on their past experience or intuition involves a focused group of managers working together to identify potential risks, concerns, root causes, failure modes, hazards, opportunities and criteria for decisions and/or options for treatment. Brainstorming should stimulate and encourage free-flowing conversation amongst a group of knowledgeable and focussed people with a fair/objective outlook. The group

should not be biased or critical. It is one of the best and most popular ways to identify both risks and key controls and is the basis for most successful risk workshops.

3. **Questionnaires & Interviews** - Focused on detecting the concerns of staff with respect to the risks or threats that they perceive in their operating environment. During a **Structured interview**, interviewees are asked through a set of prepared questions to encourage the interviewee to present their own perspective and thus identify risks. Structured interviews are frequently used during consultation with key stakeholders when designing the risk management framework. Structured interviews are good to assess risk appetite and tolerance when developing risk appetite statements. A specialist in risk prepares interviews with various management level members of the company in order to elicit the concerns.

4. **Checklists** are information aids to reduce the likelihood of failures from potential hazards, risks or controls that have been developed usually from past experience, either as a result of a previous risk assessment or as a result of past failures or incidents or history or industry learning. Auditors often prepare checklists of key controls to aid in their assessment of control effectiveness and the internal control environment. Checklists are good guiding tools; however, can lead to herd mentality and risk managers can miss out on fresh risk thinking and the big picture.

5. **"What-if" Technique (WIFT)** This is a structured, team exercise, where the expert facilitator utilises a set of "indicators" or "hints" to stimulate participants to identify risks. It is commonly used for decision making purposes.

6. **Scenario Analysis** is a process to analyze future events by considering alternative outcomes or alternative worlds. Scenario making involves preparing a brief narrative or description of a hypothetical situation of how a future event or events might turn out or look like. For each scenario, the management reflects and analyses the potential consequences and potential causes when analysing risk. Scenario analysis can be used effectively to identify opportunities for fraud, forecasting, managing financial risks, etc. Reserve Bank of India prescribes scenario analysis based testing for Liquidity position of banks in India.

7. **Fault Tree Analysis (FTA)** This method is similar to a form of creative thinking called reverse brainstorming. This technique is used for identifying and analysing factors that can contribute to a specified undesired event (called the "top event"). Causal factors are then identified and organized in a logical manner and represented pictorially in a tree diagram.For example, if you want to improve customer service, state the objective in reverse e.g. "How can we really annoy our customers?" and from this statement, use brainstorming to identify causes that could annoy customers.

8. **Bow Tie Analysis** There is a saying that "a picture is worth a thousand words" and this method is a perfect example of this. Bow tie analysis is a diagrammatic way of describing, linking and analysing the pathways of a risk from causes to effects/consequences. Unlike the risk register, there are no numbers in this analysis i.e. there is no risk or control evaluation

involved. This keeps the focus on understanding the relationships between the causes, event and consequences. After a brainstorming session, bow tie analysis is a great way to clean up the ideas generated and consolidate the results into more appropriate risk statements.

9. **Direct Observations** This relatively simple technique is used daily in the workplace by staff who may observe risky situations and hazards regularly. It is also used by emergency services when attending to an emergency and is a form of dynamic risk assessment. It is also heavily used by Workplace Health & Safety professionals during inspections and audits. A risk aware culture and well trained staff will improve people's ability to observe potential risks and implement controls before the risk eventuates into an incident.

10. **Incident Analysis** - Incidents Analysis related to risks that have recently occurred. Recording incidents in a register, conducting root cause analysis and periodically running some trend analysis reports to analyse incidents, can potentially enable new risks to be identified. In addition, a high frequency of like incidents can be a lead risk indicator to a potentially larger problem.

11. **Surveys** - It is similar to structured interviews but involves a larger number of people. It can be used to collect a broad set of ideas, thoughts and opinions across a range of areas covering risks and control effectiveness. One of the best ways for risk managers to use surveys is to assess the organisation's risk culture. Internal auditors use surveys to assess the internal control environment. Some organisations use annual staff surveys to gauge staff understanding of key risk and governance policies and procedures.

12. **Workshops** - Meeting of group of employees in a comfortable atmosphere, in order to identify the risks and assess their possible impact on the company.

13. **Comparison with other organizations** - Benchmarking is the technique used for comparing one's own organization with competitors. Benchmarking means to set a particular level of performance or to set a particular standard of performance that the company should achieve and this standard performance is determined by adopting the highest level of performance as achieved by the rivals or the competitors.

14. **Stakeholder analysis -** Process of identifying individuals or groups who have a vested interest in the objectives and ascertaining how to engage with them to better understand the objective and its associated uncertainties.

15. **Working groups -** Compact working groups can be formed that could be cross functional. Useful to surface detailed information about the risks i.e. source, causes, consequences, stakeholder impacted, existing controls.

16. **Corporate knowledge** - History of risks provide insight into future threats or opportunities through:-

    - **Experiential knowledge** – collection of information that a person has obtained through their experience.

- **Documented knowledge** – collection of information or data that has been documented about a particular subject.
- **Lessons learned** – knowledge that has been organized into information that may be relevant to the different areas within the organization.

Issues experienced and risks identified by other jurisdictions should be identified and evaluated. If it can happen to them, it can happen here. Risk identification techniques vary in complexity and each method has its advantages and disadvantages.

There are multiple types of risk assessments, including program risk assessments, risk assessments to support an investment decision, analysis of alternatives, and assessments of operational or cost uncertainty. This gives context and bounds the scope by which risks are identified and assessed.

How can we identify the causes and effects of the risks in a company?

- In this first stage of the methodology, the possible specific causes of business risks are identified in a systematic manner using one of techniques highlighted above, together with the range and possible effects thereof.
- The proper identification of risks calls for a **detailed knowledge of the company and its business**, of the market in which it operates, of the legal, social, political and cultural environment in which it is set.
- Risk identification must be systematic and begin by identifying the key objectives of success and the threats that could upset the achievement of these objectives.

The ICAI guide on Risk Assessment Methodologies and Applications states the following on the process of Risk Identification:-

The purpose of the risk evaluation is to identify the inherent risk of performing various business functions especially with regard to usage of information technology enabled services. Management and audit resources will be allocated to functions with highest risks. The risk evaluation will directly affect the nature, timing and extent of audit resources allocated.

A risk is anything that could jeopardize the achievement of an objective. For each of the department's objectives, risks should be identified. Asking the following questions helps to identify risks:

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we vulnerable?
- What assets do we need to protect?

- Do we have liquid assets or assets with alternative uses?
- How could someone steal from the department?
- How could someone disrupt our operations?
- How do we know whether we are achieving our objectives?
- On what information do we must rely?
- On what do we spend the most money?
- How do we bill and collect our revenue?
- What decisions require the most judgment?
- What activities are most complex?
- What activities are regulated?
- What is our greatest legal exposure?

It is important that risk identification be comprehensive, Individuals, primarily from the business unit, are the main source of data on all aspects of business operations and assets. For this reason, identifying knowledge individuals to be interviewed and developing interview questions are critical parts of the planning process that require careful attention and close coordination between the business unit manager and senior management. In addition, the risk evaluation of the information technology interface would itself be a part of the audit report on information technology system. The two primary questions to consider when evaluating the risk inherent in a business function are:

- What is the probability that things can go wrong? (Probability) This view will have to be taken strictly on the technical point of view and should not be mixed up with past experience. While deciding on the class to be accorded, one has to focus on the available measures that can prevent such happening.
- What is the cost if what can go wrong does go wrong? (Exposure)

Risk is evaluated by answering the above questions for various risk factors and assessing the probability of failure and the impact of exposure for each risk factor. Risk is the probability of impact of the exposure.

The purpose of a risk evaluation is to:

- Identify the probabilities of failures and threats,
- Calculate the exposure, i.e., the damage or loss to assets, and
- Make control recommendations keeping the cost-benefit analysis in mind.

3.1 Sources for Identification of Risks

Risk identification starts with event identification. Business risks arise on account of two major

factors viz., internal events within the organization and external events outside the organisation.

Internal risks arise from factors (that can be controlled) such as people or human factors (talent management, strikes), technological factors (emerging technologies), physical factors (failure of machines, fire or theft), operational factors (access to credit, cost cutting, advertisement). External risks arise from factors (that cannot be controlled) such as economic factors (market risks, pricing pressure), natural factors (floods, earthquakes), and political factors (compliance and regulations of government).

Sources of risk are all of those company environments, whether internal or external, that can generate threats of losses or obstacles for achieving the company's objectives.

A procedure that facilitates the identification of risks is to ask oneself, with respect to each of the sources, whether weaknesses or threats exist in each case.

A brief list is set out below:-

1. Pressure by competitors
2. The employees
3. The customers
4. The new technologies
5. Changes in the environment
6. Laws and regulations
7. Globalization and global events
8. The operations
9. The suppliers
10. Natural disasters
11. Man-made disasters

For the purpose of risk identification it is advisable to make a SWOT analysis (Strengths, Weaknesses, Opportunities and Threats); particularly the weak points and the threats will offer a view of the risks facing the entrepreneur.

Example - SWOT

Strengths-

- Location of establishments
- Highly flexible cost structure
- Proximity to customers

Weakness-

- Commercial fragmentation
- Limited access to financing
- Lack of specialized and trained personnel

Opportunities-

- Sector in expansion
- Specialization in market niches
- Increasingly better informed customers

Threats-

- Regulatory changes
- Entry of new competitor
- Customer tastes changes quickly

Exhibit

A GENERIC RISK SOURCES MATRIX

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 direction and 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	Environment	Human Resources	Reputation	Technology
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		

Example – Threat Assessment for Mumbai metropolitan city

Vulnerability Profile of Mumbai City:-

1. The fourth largest city in the world with 20 million people, and 6.7 million slum dwellers, according to the World Health Organization (WHO), is also one of the top 10 most vulnerable cities in terms of floods, storms and earthquakes.

2. According to the UN International Strategy for Disaster Reduction (ISDR), Mumbai is the most vulnerable in the world in terms of total population exposed to coastal flood hazard; it is among the world's top six cities most vulnerable to storm surges; and it lies on an earthquake fault-line.

3. Like many of Asia's coastal mega-cities, most of the city is less than a metre above sea-level. With Mumbai accounting for almost 40% of the India's tax revenue, any serious catastrophe here could have drastic economic consequences for the country.

3.2 High Value Threats & Risks Analysed

1. **Fire** and industrial accidents have been part of the landscape of the city. This can be exacerbated with the presence of at least 1,000 hazardous old industrial units in the city. The worst event recorded is the Victoria doc explosion in 1944 which killed up to 6,000 and devastated 1.2 sq. Km. The most recent one was the Mantralaya fire event that occurred at the State Secretariat Building in 2012.

2. **Floods**. Mumbai civic authorities identify 10 sections along the Central Railway and 12 along the Western Railway prone to serious flooding, along 235 other flooding points within the city. The event of July 26, 2005 is maybe the worst that the city has faced in long time, an exceptional series of rainstorm seriously disrupted the lives of many millions: basic amenities, telecommunications, banking services, civic and political organizations were paralyzed in a situation that has not been seen before.
3. **Chemical (transport, handling), biological, and nuclear hazards**. Mumbai is one of the few big urban centers or megacities to count on a nuclear facility within the city limits.
4. **Earthquakes.** Mumbai lies in the Bureau of Indian Standards (BIS) in Seismic Zone III.
5. **Cyclones**, Landslides, Bomb blasts, terrorism, riots and tidal surge are additional hazards that need to be analysed too.

The following factors have been identified that can create vulnerabilities and associated risks in the city:

- Being an "Island city", the transport networks are in poor shape
- Inadequate road width vs. parking space
- Buildings – poor design and construction practices
- High-rise and old buildings
- Change of use of buildings from ordinary to critical functions without retrofitting or strengthening the building
- Utilities: water supply – lack of back-up system; inadequate sewerage system
- Infrastructure: flyovers, hospitals in weak condition
- Power failures
- Poor security infrastructure
- Continuous migration of people to Mumbai
- Illegal construction
- Poor roads and civic amenities

3.3 Global Risk Outlook

One of most important source of information for the purpose of risk identification is the **World Economic Forum (WEF)** that undertakes risk identification surveys and tracks the progress of risk developments across the globe. Study of the global risk surveys undertaken by the WEF enables risk professionals to identify and track developments in the risk management profession.

The WEF report has highlighted the potential of persistent, long-term trends such as inequality and

deepening social and political polarization to exacerbate risks associated with, for example, the weakness of the economic recovery and the speed of technological change.

These trends came into sharp focus during 2016, with rising political discontent and disaffection evident in countries across the world. The highest-profile signs of disruption may have come in Western countries – with the United Kingdom's vote to leave the European Union and President-elect Donald Trump's victory in the US presidential election-but across the globe there is evidence of a growing backlash against elements of the domestic and international status quo.

The global risk indicators that are currently in trend include:-

- Increasing disparity between the rich and poor
- Fast technology evolution leading growing dependency for decision making
- Intelligent devices replacing human intervention impacting employment, manufacturing and services sector
- Terrorism leading to intensified nationalism and regional conflicts
- Global warming and climate changes

Organisational Risks

Epstein and Rejc, 2005 depict organizational risks as:-

Strategic	***Operational***	***Reporting***	***Compliance***
Economic	Environmental, Reputation	Information	Legal and regulatory
Industry	Financial, Commercial, Property	Reporting	Control
Strategic Transaction	Business Continuity		Professional
Social	Innovation		
Technological	Commercial, Project,		
Political	Human Resources, Health and Safety		
Organizational Systems			

3.4 Risk Identification and Root Cause Analysis

The most effective risk identification techniques focus on root cause identification and analysis. Risk identification along with root cause identification empowers risk practitioner with the knowledge of why a risk event occurs. Identifying the root cause of a risk provides information about what triggers a loss or opportunity and where an organization is vulnerable. Using root cause category provides a meaningful feedback to the Boards/Management teams on the steps to be taken to most effectively mitigate risk. Identifying risk solely based on the effect or outcome

often leads to ineffective mitigation activities.

Risk identification is followed by Risk Assessment which involves evaluating risks for probability, cost implications, prioritisation and impact assessment. Risk Mitigation activities are aimed at eliminating the risk root cause and will depend on the nature and source of risk.

Example - If illness is causing us headaches, seeing a doctor is the appropriate mitigation activity. However, if headaches are caused by excessive use of mobile phone, we should try to reduce the usage of mobile phone.

In order to prevent a headache, we need to know why we have one. Armed with the knowledge of the source of a risk, we can proactively manage risk and avoid future risk events.

3.5 Use of Specific Tools to Identify Risks

PESTLE denotes P for Political, E for Economic, S for Social, T for Technological, L for Legal and E for Environmental. It gives a bird's eye view of the whole environment and eco-system in which an entity operates. This concept is used as a tool by companies to track the environment they're operating in or are planning to launch a new project/product/service etc.

Amanda Dcosta's paper on the subject of PESTLE analysis highlights several merits and demerits of adopting PESTLE, relevant extracts are re-produced hereunder:-

PESTLE Analysis is a tool that is used to identify and analyze the key drivers of change in the strategic or business environment. The abbreviation stands for Political, Economic, Social, Technological, Legal, and Environmental factors. The tool allows the assessing of the current environment and potential changes. The idea is, if the project is better placed than its competitors, it would be able to respond to changes more effectively. The term has been widely used and the earliest reference can date back to a book by Aguilar in 1967 who discussed ETPS (Economic, Technical, Political, and Social) in his book Scanning the Business Environment. After this publication, came the work of Brown who modified the theory and named it STEP (Strategic Trend Evaluation Process). This was further modified and became known as the STEPE analysis (Social, Economic, Political, and Ecological factors). Post 1980, the word PESTLE originated along with its variations like PEST, STEEPLE (includes Ethical factors), PESTLIED (includes Demographic and International factors), STEEPLED (includes Demographic and Education factors), etc.

The PESTLE analysis alongside SWOT can be used as a basis for analysing the business and environmental factors of a project or business.

3.6 Risk Treatment Options

A risk mitigation strategy is an organization's plan for 'how it will address its identified risks'. Creating and implementing mitigation strategies is one of the most effective ways to protect an organization's information assets, and is nearly always more cost effective than repairing the damage after a security incident. Mitigation and measurement techniques are applied according to the event's losses, and are measured and classified according to the loss type.

The primary objective of risk treatment is:-

- To contain the risks 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).

Broadly, the risk responses are categorized into the following buckets:

Sr. No	*Risk action*	*Description*
1	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.
2	Reduce/ Manage	Action is taken to reduce the risk likelihood or impact, or both. This, typically, involves any of the myriad of everyday business decisions. This is involves addressing the root cause of the risk factor.
3	Transfer/ Share	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.
4	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.

In addition to establishing causal relationship, other risk mitigation measures are:-

- Control Self-assessments;
- Calculating reserves and capital requirements;
- Creating culture supportive of risk mitigation;
- Strengthening internal controls, including internal and external audit of systems, processes and controls, including IS audit and assurance;
- Setting up operational risks limits (so business will have to reduce one or more of frequency of loss, severity of loss or size of operations);
- Setting up independent operational risk management departments;
- Establishing a disaster recovery plan and backup systems;
- Insurance; and
- Outsourcing operations with strict service level agreements so operational risk is transferred.

Out of these aforementioned techniques, some of the common risk mitigation techniques are briefly discussed below:

- **Insurance:** An organization may buy insurance to mitigate such risk. Under the scheme of the insurance, the loss is transferred from the insured entity to the insurance company in exchange of a premium. However while selecting such an insurance policy one has to look into the exclusion clause to assess the effective coverage of the policy. Under the Advanced Management Approach under Basel II norms (AMA), a bank will be allowed to recognize the risk mitigating impact of insurance in the measures of operational risk used for regulatory minimum capital requirements. The recognition of insurance mitigation is limited to 20% of the total operational risk capital charge calculated under the AMA.
- **Outsourcing:** The organization may transfer some of the functions to an outside agency and transfer some of the associated risks to the agency. One must make careful assessment of whether such outsourcing is transferring the risk or is merely transferring the management process. For example, outsourcing of telecommunication line viz. subscribing to a leased line does not transfer the risk. The organization remains liable for failure to provide service because of a failed telecommunication line. Consider the same example where the organization has outsourced supply and maintenance of a dedicated leased line communication channel with an agreement that states the minimum service level performance and a compensation clause in the event failure to provide the minimum service level results in to a loss. In this case, the organization has successfully mitigated the risk.
- **Service Level Agreements (SLAs):** Some of risks can be mitigated by designing the service level agreement. This may be entered into with the external suppliers as well as with the customers and users. The service agreement with the customers and users may clearly exclude or limit responsibility of the organization for any loss suffered by the customer and user consequent to the technological failure. Thus a bank may state that services at ATM are subject to availability of service there and customers need to recognize that such availability cannot be presumed before claiming the service. The delivery of service is conditional upon the system functionality. Whereas the service is guaranteed if the customer visits the bank premises within the banking hours.

It must be recognized that the organization should not be so obsessed with mitigating the risk that it seeks to reduce the systematic risk - the risk of being in business. The risk mitigation tools available should not eat so much into the economics of business that the organization may find itself in a position where it is not earning adequate against the efforts and investments made.

4. IMPACT OF BUSINESS RISK

Risk identification and assessment empowers us and prepares us for the effects of the risks that the organisation is exposed to. Knowing the risks that the business could face can make mitigation easier. From external to internal, the nature of the risk and its severity can vary.

There are risks associated with running any business that could have short term or long-term consequences. Understanding the various types of risks can help in creating a risk management

plan for the organisation.

Risks can vary greatly, depending on industry, locale, and other business variables. The impact a risk could have on an organisation is multi-dimensional in nature. The levels of risk impact can be assessed across following levels:-

Sr. No.	*Impact Areas*	*Nature of Impact*
1	Strategy and business objectives	Delays, change management, failure to achieve objectives
2	Financial	Direct or indirect financial loss
3	Customer	Loyalty, relationship, payment terms, attrition
4	Employee	Morale, engagement, attrition
5	Vendor/supplier	Loyalty, relationship, payment terms, attrition
6	Compliance	Delays, penalties, offences, defaults, imprisonment
7	Reputation/ Brand equity	Loss of confidence, public exposures, litigation, etc

As seen from above table the impact of risk is all pervasive and organisations are rarely able to document the full and complete impact of risks across their business value chains. The impact is dependent on the severity or magnitude of the risk event.

Example –

- The impact from a high magnitude earthquake could be catastrophic; however, from a low magnitude it could be minimal.
- The impact from loss of a single customer could be insignificant, however, loss of a business segment comprising of a bunch of customers could be material.

Few more examples on the nature of impact that risks pose to a business

- Criminals can pose a threat to the security of a business's sensitive data. If trade secrets are revealed to competitors or client financial data is stolen, the results can be disastrous.
- Online reviews, blogs and social media can make it easier to spread negative information; a negative review or post on social media can sometimes impact a company's earnings, in a single day.
- Employee injuries can be disastrous for a business.
- Internal fraud can be another major risk factor, and one that is an all-too-common reality.
- Customer payment defaults represent a financial risk to the company with a direct financial loss/ exposure.
- Operational risks can disrupt a business, if proper precautions are not taken. For instance, in the event of a fire, flood, or chemical leak, a business may be unable to operate as usual, resulting in a loss of revenue.

- Supply chain disruptions caused by vendors who aren't able to deliver reliably can also result in business interruption.
- In case a key business asset is damaged by vandalism, misuse, or accidental damage, the cost of repairing or replacing it can put substantial stress on a business's cash flow.

Once businesses have identified the risks, they will assess the possible impact of those risks. Depending on the results of the risk assessment and impact analysis exercise, organisations can classify and separate minor risks from major risks that must be managed immediately.

Risks can be classified on the basis of their impacts into following rating buckets:-

- Severe
- Major
- Moderate
- Minor
- Insignificant

Organisations conduct Business Impact Analysis (BIA) which is a similar process like Risk Impact Analysis. The BIA is primarily performed while organisations chalk out their business continuity plans. To conduct a business impact analysis for the business, managers carry out following activities:

- Understand and document the daily activities conducted in each area of business.
- Understand and document the long-term or on-going activities performed by each area of business.
- Understand and document the potential losses if these business activities could not be provided.
- Understand and document the outage time meaning how long could each business activity be unavailable for (either completely or partially) before the business would suffer.
- Understand and document whether the business activities activities are dependent on any outside services or products.
- Understand and document the activities important to the business for example, on a scale of 1 to 5 (1 being the most important and 5 being the least important), where would each activity fall in relation to the rest of the business?

The BIA (business impact analysis) should identify the operational and financial impacts resulting from the disruption of business functions and processes. Impacts to consider include:-

- Loss of life
- Lost sales and income

- Delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay of new business plans

As the business risks change, so too will their potential impacts. Therefore, risks assessment and impact analysis should be performed continuously.

Analysing the Level of Risk

To analyse risks, we need to work out the likelihood of its happening (frequency or probability) and the consequences it would have (the impact) of the risks that are identified. This is referred to as the level of risk, and can be calculated using this formula:-

Level of risk = consequence x likelihood

Level of risk is often described as low, medium, high or very high. It should be analysed in relation to what is currently being done to control it. Control measures decrease the level of risk, but do not always eliminate it.

Example

A risk analysis can be presented in the form a matrix, such as this

Likelihood scale example

Level	*Likelihood*	*Description*
4	Very likely	Happens more than once a year in the industry
3	Likely	Happens about once a year in the industry
2	Unlikely	Happens every 10 years or more in the industry
1	Very unlikely	Has only happened once in the industry

Consequences scale example

Level	*Consequence*	*Description*
4	Severe	Financial losses greater than ₹ 5 Crores
3	High	Financial losses between ₹ 1 to 5 Crores
2	Moderate	Financial losses between ₹ 10 Lacs to 1 Crore
1	Low	Financial losses less than Financial losses between ₹ 10 Lacs

Ratings vary for different types of businesses. The scale above uses 4 Levels; however, one can

use as many levels as deemed fit for the business/sector. Also use descriptors that suit the purpose (e.g. you might measure consequences in terms of human health, rather than rupee value).

Evaluating risks

Once the level of risk is completed, we then need to create a rating table for evaluating the risk. Evaluating a risk means making a decision about its severity and ways to manage it.

For example, one may decide the likelihood of a fire is 'unlikely' (a score of 2) but the consequences are 'severe' (a score of 4). Using the tables and formula above, a fire therefore has a risk rating of 8 (i.e. 2 x 4 = 8).

Risk rating table example

Risk rating	*Description*	*Risk Management Action*
12-16	Severe	Needs immediate corrective action
8-12	High	Needs corrective action within 1 week
4-8	Moderate	Needs corrective action within 1 month
1-4	Low	Does not currently require corrective action

Risk evaluation should consider:

- The importance of the activity to the business
- The amount of control we have over the risk
- Potential losses to the business
- Benefits or opportunities presented by the risk.

Once we have identified, analysed and evaluated the risks, the next step is to rank them in order of priority. Effective risk management involves prioritization and thorough analysis of the risk factors based on probabilistic models which can be directly related to the extent of impact of the risk. Likewise, prioritizing stakeholders by authority and degrees of involvement and levels of risk threats are necessary. This analysis will provide valuable input to a risk mitigation plan so that more resources and attention are paid to the stakeholders who pose or face the greatest risk to the project.

5. IDENTIFY AND ASSESS THE IMPACT UPON THE STAKEHOLDERS INVOLVED IN BUSINESS RISK

Every organization whether for-profit or not, exists to create value for its stakeholders. Value is created (or destroyed) by management decisions in all activities, ranging from setting strategy to managing the daily operations of the enterprise. But value is constantly at risk, and risks need to be managed in order to be able to create value.

Businesses are responsible to several stakeholders as they function in an eco-system. The first stakeholders can be the owners of the company who own equity in the company and therefore the business has a duty towards them. This duty is primarily protect the value of investment and generate more value to provide returns on investments to the shareholders. A modern view on this subject is that a business converts inputs such as capital of investors, labour of employees and materials from suppliers into outputs such as goods and services which customers buy, thereby returning capital plus profits to the firm.

Therefore, a business has not only to take into account the primary interest of the owners or shareholders, but it also has to create sustainable value for other key stakeholders such as employees, its suppliers and its customers. This is further expanded by considering society, community, government and other stakeholders who are impacted by the operations of the business.

Stakeholders can be classified into two categories viz., internal stakeholders and external stakeholders.

Internal stakeholders are entities within a business (e.g., employees, managers, the board of directors, investors). Employees want to earn money and stay employed. Owners are interested in maximizing the profit the business makes. Investors are concerned about earning income from their investment.

External stakeholders are entities not within a business itself but who care about or are affected by its performance (e.g., consumers, regulators, investors, suppliers). The government wants the business to pay taxes, employ more people, follow laws, and truthfully report its financial conditions. Customers want the business to provide high-quality goods or services at low cost. Suppliers want the business to continue to purchase from them. Creditors want to be repaid on time and in full. The community wants the business to contribute positively to its local environment and population.

As John Greijmans states that - A corporate stakeholder is a party that can affect or can be affected by the actions of an organization. Stakeholders are those groups without whose support the organization would cease to exist. The stakeholder concept has been broadened to include everyone with an interest (or “stake”) in what the entity does. Examples of stakeholders and their stakes are:

- Government: taxation, legislation, low unemployment and truthful reporting.
- Employees: pay rates, job security, compensation, respect and truthful communication.
- Customers: quality, customer care and ethical products.
- Suppliers: equitable business opportunities.
- Creditors: credit score, new contracts and liquidity.
- Community: jobs, involvement, environmental protection, shares and truthful communication.

- Trade Unions: quality, staff protection and jobs.
- Owner(s): success of the business.

All or each category of stakeholders has the capacity to strongly influence the business, its strategy and objectives. Therefore, they can play a key role in risk management exercise of the business. Engagement of stakeholders in the risk management exercise will enable the management to create a comprehensive and sustainable risk management framework.

Risk Analysis

The organization must identify the stakeholders, determine their requirements and expectations, and identify and evaluate the levels of risks of each one of them and successfully manage the risk factors. A stakeholder risk analysis is essential so that each stakeholder – be it an individual or organization - is aware of the risk perception. Stakeholder risk analysis means identifying the stakeholders, types of risks, extent of risks, levels of stakeholder commitment, and degree of influence.

Risk impacts varied stakeholders and are multi-dimensional. Common belief is that risk only has financial consequences, however, risk has non-financial consequences as well and primary non-financial consequence is loss of confidence. The levels of risk impact can be assessed across following stakeholder levels:-

S. No.	Stakeholders	Nature of Impact
1	Owners, Boards & Management	Failure to achieve objectives, Delays, Change management, disruption, financial losses, etc.
2	Society	Loss of confidence, health hazards, direct or indirect financial losses, disruption in life style, etc.
3	Consumer	Health, financial losses, loss of confidence, etc.
4	Employee	Life, health, morale, engagement, attrition
5	Vendor/supplier	Loyalty, relationship, payment terms, attrition
6	Government, Regulators	Revenue loss, delays in project implementations, loss of public confidence, etc.
7	Investors	Loss of confidence, lower returns, litigation, financial losses, etc.

As seen from above table the impact of risk is pervasive and organisations are rarely able to document the full and complete impact of risks across their business value chains. The impact is dependent on the severity or magnitude of the risk event.

Advanced technologies can be put to meaningful use only if one is clear which stakeholder needs what information and in what manner to manage risks effectively. One also needs to understand how often the information needs to be shared with stakeholders.

Stakeholder Value Creation by Enterprise Risk Management

Effective implementation of Enterprise risk management leads to number of benefits to the business and society. The full value of payoff is realised over a period of time. It is similar to a business entity implementing an Enterprise Resource Planning Package where the return on investment is achieved over a period of time. Likewise when ERM is implemented the payoff is realised over few years of the business life-cycle. The gains from ERM implementation are realised in two stages intermediate/ short term and long term.

The Risk Management Payoff Model of Epstein and Rejc, 2005, demonstrates how improved risk measurement and management provides benefits throughout the organization. Benefits extend to

(a) enhanced working environment,

(b) improved allocation of resources to the risks that really matter,

(c) Sustained or improved corporate reputation, and

(d) Other gains, all of which lead to prevention of loss, better performance and profitability, and increased shareholder value.

Successful Stakeholder Risk Management

It is necessary to evaluate all types of risks impacting all categories of stakeholders and find solutions to pre-empt the threats before the risk occurs. The more one knows about the stakeholders and their levels of importance, the more effective and purposeful the risk management strategy will be. The risk management program should look at the big picture and identify not only short term risk factors but also long term factors impacting the entire value chain of business activities and connected communities.

6. ROLE OF RISK MANAGER AND RISK COMMITTEE IN IDENTIFYING RISK

The Companies Act, 2013 and Listing guidelines issued by the Securities and Exchange Board of India lay great emphasis on the subject of identification and management of risks including development of robust internal control system for mitigating risks. The legal framework in India requires the top listed entities to constitute Risk Committee and casts onerous responsibilities on the Boards and Audit Committees to discharge their risk related responsibilities in terms of annual responsibility statements and oversight of the risk management function. Therefore, it is obligatory for listed entities to design and implement comprehensive risk management frameworks and the architecture for doing so can be through people.

Managing risk is all about engaging people and creating a risk aware culture therefore a Risk Leader has to be someone who exercises good influence and authority on the organisation. Risk Management Committee should comprise of people who have authority and influence over the organisational activities.

6.1 The Role of the Risk Manager

The role of the Risk Manager includes following tasks:-

1. Manage the implementation of all aspects of the risk function, including implementation of processes, tools and systems to identify, assess, measure, manage, monitor and report risks.
2. Select the most suited risk identification techniques and approaches.
3. Manage the process for developing risk policies and procedures, risk limits and approval authorities.
4. Monitor major, critical and minor risk issues.
5. Manage the process for elevating control risks to more senior levels when appropriate.
6. Management of risk reporting, including reporting to senior management.
7. Prepare high-level user requirements to assist in preparation of Project Initiation documents.
8. Liaison with Business users to prepare Functional risk specifications. Translate business requirements and functional needs into business / reporting and system specifications. Ensure technical specifications meet the stated needs of the business.
9. Generate project management documents.
10. Provide User Training for in-house developed risk management systems.
11. Conduct compliance & risk assessments.
12. Conduct and document audits of risk related compliance to industry standards
13. Define & develop risk policies, procedures, processes & other documentation as required.
14. Implement the risk management program and risk strategy. Ensure the risk management program is effectively integrated into product development and delivery methodology.
15. Participate in local and global discussions to formulate new or enhance existing risk management processes, policies and standards.

6.2 Role and Responsibility of Risk Management Committee

Role

1. To assess the company's risk profile, risk appetite and key areas of risk in particular.
2. To recommend to the board and adoption of risk assessment and rating procedures.
3. To articulate the company's policy for the oversight and management of business risks.

4. To examine and determine the sufficiency of company's internal processes for reporting and managing key risk areas.
5. To access and recommend board acceptable levels of risk.
6. To facilitate development and implementation of a risk management framework and internal control system.
7. To review the nature and level of insurance coverage.
8. To have special investigation into the area of corporate risk and break downs in internal control.
9. To review management response to the company auditor's recommendations.
10. To report the trends on the company's risk profile, reports on specific risk and the status of risk management process.

Responsibility

1. To define the risk appetite of the organization.
2. To exercise oversight of managements responsibilities, and review the risk profile of the organization to ensure that risk is not higher than the risk appetite decided by the board.
3. To ensure that the company is taking appropriate measures to achieve prudent balance between risk and reward in both on-going and new business activities.
4. To assist the board in setting risk strategies, policies, framework, models and procedures in liaison with the management and in discharge of its duties related to corporate accountability and associated risk in terms of management assurance and reporting.
5. To review and assess the quality, integrity and effectiveness of the risk management systems and ensure that the risk policies and strategies are effectively managed.
6. To review and assess the nature, role, responsibility and authority of risk management function with the company and outline the scope of risk management work.
7. To ensure the company has implemented an effective on-going process to identify risk, to measure its potential impact against a broad set of assumptions and then to act pro-actively to manage these risks, and to decide the company's appetite or tolerance for risks.
8. To ensure that a systematic, documented assessment of the processes and the outcome surrounding key risk is undertaken at least annually for the purpose of making its public statement on risk management including internal control.
9. To oversee the formal review of activities associated with effectiveness of risk management

and internal control process. A comprehensive system of control should be established to ensure that the risk are mitigated and the company's objective are attained.

10. To review process and procedure to ensure the effectiveness of the internal control systems so that decision making capability, accuracy of reporting and financial results are always maintained at an optimal level.
11. To monitor external development related to practice of corporate accountability and the reporting of specifically associated risk, including emerging and prospective impacts.
12. To provide an independent and objective oversight and view of the information presented by the management on corporate accountability and specifically associated risk, also taking account of the report by the audit committee to the board on all categories of identified risk being faced by the company.
13. To review the risk bearing capacity of the company in light of its reserves, insurance coverage, guarantee funds or other such financial structures.
14. To fulfill its statutory, fiduciary and regulatory responsibilities.
15. To ensure that risk management culture is pervasive throughout the organization.
16. To review issues raised by internal audit that impact the risk management framework.
17. To ensure that infrastructure, resources and systems which are in place for risk management is adequate to maintain a satisfactory level of risk management discipline.
18. The board shall review the performance of risk management committee annually.
19. Perform other activities related to risk management as requested by the board of directors or to address issues related to significant subject within its term of reference.

6.3 IBM Case Study – Role of Risk Management Function

IBM has been managing risk since its founding, in 1911, but in 2006, it created an enterprise risk management function to help its 380,000 employees become more "risk aware." Harvard Business Review has published details about the Risk Management Program of IBM.

The role of the Enterprise Risk Management function at IBM

IBM has risk leaders throughout the company — without recruiting lot of people in a new risk department. IBM philosophy is that risk management should be centered in the businesses, which need to understand risk and make trade-offs in pursuit of strategic gains. Risk management is the responsibility of every IBMer. The Risk team at IBM plays the role of supporting senior managers, risk leaders, and all employees with targeted resources, education, and training.

IBM has about 30 online courses available to all employees. IBM has introduced risk gaming and using simulation in which a business leader developing a customer proposal has to consider different risks i.e. how to account for them, how to mitigate and control them. People find it funny and engaging.

IBM's risk team spends more time on the strategic side, engaging with risk leaders and ensuring that they're thinking about things like technology shifts, industry disruptions, and the risks of mergers and acquisitions. The more fun part of their job is when they focus on value creation. IBM's risk team's mission is that risk management must be engrained in the fabric of the business, not a separate check-the-box process.

6.4 Principles for Effective Implementation of Risk Management Recommended By OECD

While discharging the roles and responsibilities associated with the risk function, the Risk Managers and Risk Committees should refer to the principles recommended by OECD. The principles are re-produced hereunder:-

Perhaps one of the greatest shocks from the financial crisis has been the widespread failure of risk management. In many cases risk was not managed on an enterprise basis and not adjusted to corporate strategy. Risk managers were often separated from management and not regarded as an essential part of implementing the company's strategy. Most important of all, boards were in a number of cases ignorant of the risk facing the company.

1. It should be fully understood by regulators and other standard setters that effective risk management is not about eliminating risk taking, which is a fundamental driving force in business and entrepreneurship. The aim is to ensure that risks are understood, managed and, when appropriate, communicated.

2. Effective implementation of risk management requires an enterprise-wide approach rather than treating each business unit individually. It should be considered good practice to involve the board in both establishing and overseeing the risk management structure.

3. The board should also review and provide guidance about the alignment of corporate strategy with risk-appetite and the internal risk management structure.

4. To assist the board in its work, it should also be considered good practice that risk management and control functions be independent of profit centers and the "chief risk officer" or equivalent should report directly to the board of directors along the lines already advocated in the OECD Principles for internal control functions reporting to the audit committee or equivalent.

5. The process of risk management and the results of risk assessments should be appropriately

disclosed. Without revealing any trade secrets, the board should make sure that the firm communicates to the market material risk factors in a transparent and clear fashion. Disclosure of risk factors should be focused on those identified as more relevant and/or should rank material risk factors in order of importance on the basis of a qualitative selection whose criteria should also be disclosed.

6. With few exceptions, risk management is typically not covered, or is insufficiently covered, by existing corporate governance standards or codes. Corporate governance standard setters should be encouraged to include or improve references to risk management in order to raise awareness and improve implementation.

CHAPTER 3

RISK MANAGEMENT

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

- Concept of Risk Management
- Objective and Process of Risk Management
- Importance of Risk Management
- Risk Management Techniques

1. CONCEPT OF RISK MANAGEMENT

The term “Risk” as a noun means a situation involving exposure or danger and as a verb means expose to danger, harm or loss. It is said that the word Risk is derived from the early Italian word “risco” which means danger or “risicare,” which means “to dare” or French word “risqué”. Risk is known or unknown but is always inherent in individual or business actions therefore it is more of a “choice” rather than a fate accompli.

Risk and reward are two sides of the same coin. Good Risk leaders select their actions well or take calculated risks. They evaluate risks carefully and take actions with full cognizance of consequences. They integrate decisions with corporate strategy, and strike a healthy balance between risk management as an opportunity and a protection shield.

According to "Risk Management: History, Definition, and Critique," the modern terms for managing risk rose after World War II, but the discipline mostly began as a study of using insurance to manage risk. Later, from the 1950s to the 1970s, risk managers began to realize that it was too expensive to manage every risk with insurance, so the discipline began to expand to alternatives to insurance. For example, training and safety programs might be considered insurance

alternatives. Regulators started recognising the relevance and significance of the subject of risk management and started prescribing advisories from 1980s; however, the awakening and intensity of detailed regulatory interventions came about greatly post the global financial crisis in the year 2007.

Each strategy and business action is accompanied with its expected risk and reward. Good risk management therefore does not imply avoiding all actions and associated, rather it implies making informed and coherent choices. The risks that the organization wants to take in pursuit of its objectives and in particular choices it makes to manage and mitigate those risks.

Let us study few important views on the subject of Risk and Risk Management:-

Source	*Views*
Warren Buffet	Risk comes from not knowing what you are doing
Theodore Roosevelt.	Risk management is about people and processes and not about models and technology
The Risk Management Standard, The Institute of Risk Management	Risk management is a central part of any organisation's strategic management. It is the process whereby organizations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities. Risk management should be a continuous and developing process which runs throughout the organisation's strategy and the implementation of that strategy. It should address methodically all the risks surrounding the organisation's activities past, present and in particular, future. It must be integrated into the culture of the organization with an effective policy and a programme led by the most senior management. It must translate the strategy into tactical and operational objectives, assigning responsibility throughout the organization with each manager and employee responsible for the management of risk as part of their job description. It supports accountability, performance measurement and reward, thus promoting operational efficiency at all levels.
Thomas S. Coleman, Practical Guide Risk Management, CFA Institute	Risk management is the art of using lessons from the past to mitigate misfortune and exploit future opportunities—in other words, the art of avoiding the stupid mistakes of yesterday while recognizing that nature can always create new ways for things to go wrong. We cannot lose sight of the most important aspect of risk management—managing risk. That means making the tactical and strategic decisions to control those risks that should be controlled and to exploit those opportunities that should be exploited. Managing risk cannot be divorced from managing profits; modern portfolio theory tells us that investment decisions are the result of trading off return for risk, and managing risk is simply part of managing returns and profits. Managing risk must be a core competence for any financial firm. The ability to effectively manage

	risk is the single most important characteristic separating financial firms that are successful and survive over the long run from firms that are not successful. At successful firms, managing risk always has been and continues to be the responsibility of line managers—from the board through the CEO and down to individual trading units or portfolio managers. Managers have always known that this is their role, and good managers take their responsibilities seriously. The only thing that has changed in the past 10–20 years is the development of more sophisticated analytical tools to measure and quantify risk. One result has been that the technical skills and knowledge required of line managers have gone up.

1.1 Risk Attitude, Appetite, and Tolerance

The terms risk attitude, appetite, and tolerance are often used similarly to describe an organization's or individual's attitude towards risk-taking. One's attitude may be described as risk-averse, risk-neutral, or risk-seeking. Risk tolerance in the context of investing is defined by Investopedia "as the degree of variability in investment returns that an investor is willing to withstand. Risk tolerance is an important component in investing. You should have a realistic understanding of your ability and willingness to stomach large swings in the value of your investments; if you take on too much risk, you might panic and sell at the wrong time". Therefore, the subject of Risk Tolerance deals with understanding one's ability to accept or reject deviations from the expected results.

Risk appetite is the risk taking capacity and looks at how much risk one is willing to take. There can still be deviations that are within a risk appetite. For example, recent research finds that insured individuals are significantly likely to divest from risky asset holdings in response to a decline in health, controlling for variables such as income, age, and out-of-pocket medical expenses.

1.2 Determining Risk "Appetite"

The board of directors has the primary oversight responsibility for developing and implementing the organization's mission, values, strategy, and must carefully review corporate processes of risk identification, monitoring, and management. The board also originates risk philosophy, risk appetite, and risk tolerances. Specific reviews of financial objectives, plans, major capital expenditures, and other significant material transactions also typically fall within a board's responsibility. These responsibilities require broad and transparent reporting on the various organizational risks—strategic, operational, reporting, and compliance risks.

When the Board sets the organisation's vision, strategy, goals and targets into motion it is aware of the potential business risks the organisation is exposed to and thereby can broadly estimate the extent of potential losses that the business shall be exposed to in the event the plans and management actions don't bear the desired fruits. Risk capacity is the overall ability and financial boundary within which the Board can play their business bets; whereas Risk Appetite is the hard

stop limit within which the Board would like to restrict its business actions. For example an entity with a networth of ₹ 500 Crores may have a capacity of risk taking upto ₹ 500 Crores while the Board may still articulate a philosophy that the risk appetite of the entity would be limited to ₹ 100 Crores only or upto 20% of the networth of the entity. On account of such policy statement on the risk appetite, the Business managers would not be allowed to take decisions that have the potential to go beyond the risk appetite limits of the entity. Therefore, Business managers would have to drop choices that have the potential to impair the financial stability of the company beyond the boundary set up by the Board.

In determining the risk appetite of the company, the Board should engage with the executive/ management team and provide clear directions on the contours and definition of the risk capacity, appetite and tolerance levels. For example, when does a company become uncomfortable if the percentage of its revenues generated by just top four or five clients rises continually or even becomes dominant? Another example 'X' company which experiences 10% growth (and still growing) in product returns from customers. At what point does this become too big a risk to overall customer satisfaction, company costs or general reputation? In both of these cases, one company may have a completely different tolerance of risk to another but this needs to be explicitly understood and capable of change when circumstances require it to do so.

1.3 Risks Appetite – Principles and Approach

The key question for all companies is how much risk do they need to take? And yet taking risks without consciously managing those risks can lead to the downfall of organizations. This is the challenge that has been highlighted by the UK Corporate Governance Code issued by the Financial Reporting Council in 2010.

The following key principles have underpinned risk appetite:

1. *Risk appetite can be complex.* Excessive simplicity, while superficially attractive, leads to dangerous waters: far better to acknowledge the complexity and deal with it, rather than ignoring it.
2. *Risk appetite needs to be measurable.* Otherwise there is a risk that a statement may become empty and vacuous.
3. *Risk appetite is not a single, fixed concept.* There will be a range of appetites or ranges for different risks which need to be aligned and these appetites may vary over time. Like in sourcing decisions, the Board may set vendor business share limits as they would be make the entity dependent on few vendor companies that could eventually impact business continuity or range of quality defects.
4. Risk appetite should be developed in the context of an organization's risk management capability, which is a function of risk capacity and risk management maturity. Risk management remains an emerging discipline and some organizations, irrespective of size or complexity, do it much better than others. This is in part due to their risk management culture

(a subset of the overall culture), partly due to their systems and processes, and partly due to the nature of their business. However, until an organization has a clear view of both its risk capacity and its risk management maturity, it cannot be clear as to what approach would work or how it should be implemented.

5. Risk appetite must be integrated with the control culture of the organization. The Risk Management framework explores this by looking at both the propensity to take risk and the propensity to exercise control. The framework promotes the idea that the strategic level is proportionately more about risk taking than exercising control, while at the operational level the proportions are broadly reversed. Clearly the relative proportions will depend on the organization itself, the nature of the risks it faces and the regulatory environment within which it operates.

2. OBJECTIVES AND PROCESS OF RISK MANAGEMENT

2.1 Objective of risk management

The first step to defining risk management goals and risk management objectives is to define the organization's shared vision. Once the shared vision is articulated, overall risk management goals and objectives must be defined.

While a vision statement is often aspirational, the goals and objectives should ordinarily describe in simple terms what is to be accomplished. They should be actionable by the organization. They should be defined in the context of the organization's business strategy.

For example, some common risk management objectives chosen by companies to frame their risk management approach include the following:

- Develop a common understanding of risk across multiple functions and business units so as to manage risk cost-effectively on an enterprise wide basis.
- Achieve a better understanding of risk for competitive advantage.
- Build safeguards against earnings-related surprises.
- Build and improve capabilities to respond effectively to low probability, critical, catastrophic risks.
- Achieve cost savings through better management of internal resources.
- Allocate capital more efficiently.

The Risk Management Cycle

It is a process, involving the following steps:

- identifying business functions, assets, vulnerabilities and threats;
- assessing the risks;

- developing a risk management plan;
- implementing risk management actions, and
- re-evaluating the risks.

These steps are categorized into three primary functions -

(i) Risk Identification,

(ii) Risk Assessment and

(iii) Risk Mitigation.

In a nutshell, Risk Management is all about "Identifying, Measuring, and Managing Organizational Risks for Improving Organizational Performance".

According to the standard ISO 31000 "Risk management – Principles and guidelines on implementation, the process of risk management consists of several steps as follows :—

This involves:

1. Identification of risk in a selected domain of interest.
2. Planning the remainder of the process.
3. Mapping out the following:
   (i) the social scope of risk management.
   (ii) the identity and objectives of stakeholders.
   (iii) the basis upon which risks will be evaluated, constraints.
4. Defining a framework for the activity and an agenda for identification.
5. Developing an analysis of risks involved in the process.
6. Mitigation or solution of risks using available technological, human and organizational resource.

2.2 Step by Step Process of Risk Management

All risk management processes follow the same basic steps, although sometimes different description may be used to describe these steps. Together these 5 risk management process steps combine to deliver a simple and effective risk management process.

Steps	*Action*	*Principles*
Step 1: Identify the Risk	Uncover, recognize and describe risks that might affect your project or its outcomes. There are a number of techniques one can use to find	*Risk identification* – What can go wrong?

	business risks. During this step you start to prepare your Risk Register.	
Step 2: Analyze the risk.	Once risks are identified thereafter determine the likelihood and consequence of each risk. Develop an understanding of the nature of the risk and its potential to affect business goals and objectives. This information is also entered in the Risk Register.	*Risk analysis* – How will it affect us? (Consider probability and impact to operations – is it high or low?)
Step 3: Evaluate or Rank the Risk.	Evaluate or rank the risk by determining the risk magnitude, which is the combination of likelihood and consequence. Make decisions about whether the risk is acceptable or whether it is serious enough to warrant treatment. These risk rankings are also added to the Risk Register.	*Risk control* – What should we do? (to prevent the loss from occurring or to recover if the loss does occur)
Step 4: Treat the Risk.	This is also referred to as Risk Response Planning. During this step assess the highest ranked risks and set out a plan to treat or modify these risks to achieve acceptable risk levels. Minimize the probability of the negative risks as well as enhancing the opportunities by creating risk mitigation strategies, preventive plans and contingency plans.	*Risk treatment* – If something does happen, how will you pay for it? • Avoidance (eliminate, withdraw from or not become involved) • Reduction (optimize – mitigate) • Sharing (transfer – outsource or insure) • Retention (accept and budget)
Step 5: Monitor and Review the risk.	Review the Risk Register and use it to monitor, track and update risks.	*Risk Monitoring* – How can we continuously look at foresight and hindsight?

If one designs a framework around that uncertainty, then you effectively de-risk the business. And that means one can move much more confidently to achieve your goals. By identifying and managing a comprehensive list of business risks, unpleasant surprises and barriers can be reduced and golden opportunities discovered. The risk management process also helps to resolve problems when they occur, because those problems have been envisaged, and plans to treat them

have already been developed and agreed. One can avoid impulsive reactions and going into "fire-fighting" mode to rectify problems that could have been anticipated. This makes for happier, less stressed business teams and stakeholders. The end result is that we minimize the impacts of threats and capture the opportunities that occur.

Risk Management Checklist (ISO 31000)

Risk architecture
• Statement produced that sets out risk responsibilities and lists the risk-based matters reserved for the Board
• Risk management responsibilities allocated to an appropriate management committee
• Arrangements are in place to ensure the availability of appropriate competent advice on risks and controls
• Risk aware culture exists within the organization and actions are in hand to enhance the level of risk maturity
• Sources of risk assurance for the Board have been identified and validated
Risk strategy
• Risk management policy produced that describes risk appetite, risk culture and philosophy
• Key dependencies for success identified, together with the matters that should be avoided
• Business objectives validated and the assumptions underpinning those objectives tested
• Significant risks faced by the organization identified, together with the critical controls required
• Risk management action plan established that includes the use of key risk indicators, as appropriate
• Necessary resources identified and provided to support the risk management activities
Risk protocols
• Appropriate risk management framework identified and adopted, with modifications as appropriate
• Suitable and sufficient risk assessments completed and the results recorded in an appropriate manner
• Procedures to include risk as part of business decision-making established and implemented
• Details of required risk responses recorded, together with arrangements to track risk improvement recommendations
• Incident reporting procedures established to facilitate identification of risk trends, together with risk escalation procedures
• Business continuity plans and disaster recovery plans established and regularly tested
• Arrangements in place to audit the efficiency and effectiveness of the controls in place for

significant risks

• Arrangements in place for mandatory reporting on risk, including reports on at least the following:
  • Risk appetite, tolerance and constraints
  • Risk architecture and risk escalation procedures
  • Risk aware culture currently in place
  • Risk assessment arrangements and protocols
  • Significant risks and key risk indicators
  • Critical controls and control weaknesses
  • Sources of assurance available to the Board

3. IMPORTANCE OF RISK MANAGEMENT

Governance functions include planning and budgeting, performance measurement, assurance and auditing, procurement, hiring, assessing staff as well as control over all day-to-day operations. The management of an organization, enabled by its governance arrangements, can be described as "coordinated activities to direct and control an organization". Risk management is defined as "coordinated activities to direct and control an organization with regard to risk". The parallels between these two statements demonstrate how closely risk management and governance are linked.

Risk Management is one of the important pillars of Governance and arguably the only tool to deal with business uncertainty. Risk Management is used most successfully by Fortune 500 and other large companies to sustain and grow their businesses. Risk management is recognised as an integral component of good management and governance. It is an iterative process consisting of steps, which, when undertaken in sequence, enable continual improvement in decision making.

Risk management is the term applied to a logical and systematic method of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organisations to minimise losses and maximize opportunities.

Risk management is as much about identifying opportunities as avoiding or mitigating losses.

Risk consequences can be fatal to any business. The expenditure of fixing damage and/or the loss of valued assets or even customers to competition after a catastrophe can have a significant impact on the bottom line of a business. By identifying and managing risks entities are able to actively protect value from any potential catastrophes and save valuable time and money. A risk management plan and system is there to do more than identify risk, a good system should also quantify the risk, predict the impact, and put procedures in place to mitigate the risk, or even eliminate it to the extent possible.

The benefits of risk management plan

What are the benefits of a risk management plan?

- Saving valuable resources: time, income, assets, people and property can be saved if fewer claims occur
- Creating a safe and secure environment for staff, visitors, and customers
- Reducing legal liability and increasing the stability of your operations
- Protecting people and assets from harm
- Protecting the environment
- Reducing your threat of possible litigation
- Defining your insurance needs to save on unnecessary premiums

The absence of effective risk management participation at the Board level encourages herd mentality and the acceptance of status quo. Effectively defining and managing risks that matter is a key element for survival and sustained growth. It empowers the Boards to build business resilience and the maturity to manage risk priorities. This ultimately results in greater predictability of performance and higher value creation for shareholders. A holistic risk management framework would empower Boards to:

- Identify top threats to entity and asset protection measures.
- Link risks to more efficient capital allocations and business strategy.
- Develop a common language in the organisation for problem solving.
- Effectively respond to an evolving business environment.

It is wise to learn from history and risk scenarios than experience business catastrophe. Boards may be better prepared by reviewing the risk profit & loss statement along with the financial profit & loss statement to determine the health of their entities.

Insurance and risk management systems

Purchasing the appropriate insurance coverage for the business is an important element of the risk management plan, but it's not enough by itself. Organisation must have policies and procedures in place to reduce risks to ensure your assets, reputation, financial security and operations can continue without interruption.

Insurance companies may view an organization more favourably if there is a stable risk management plan in place to minimize the impact of potential claims. It could even help in qualifying for reduced insurance premiums.

Risk management is an essential business activity for enterprises of all sizes. Enterprises that manage risks effectively will thrive and produce high quality products or services.

4. RISK MANAGEMENT TECHNIQUES

Enterprises both small and large need to identify, understand and manage the uncertainties of risks that are critical to achieving success.

Risk treatment is the activity of selecting and implementing appropriate control measures to treat or modify the risk. Risk treatment includes as its major element, risk control (or mitigation), but extends further to, for example, risk avoidance, risk transfer and risk financing. Any system of risk treatment should provide efficient and effective internal controls. Effectiveness of internal control is the degree to which the risk will either be eliminated or reduced by the proposed control measures. The cost effectiveness of internal control relates to the cost of implementing the control compared to the risk reduction benefits achieved.

Risk Management techniques and options include:-

(i) **Tolerate:** The exposure may be tolerable without any further action being taken. Even if it is not tolerable, ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained.

In these cases, the response may be to tolerate the existing level of risk. This option, of course, may be supplemented by contingency planning for handling the impact that will arise if the risk actually takes place in future.

(ii) **Transfer:** For some risks, the best response may be to transfer them. This might be done by conventional insurance or by paying a third party to take the risk.

This option is particularly good for mitigating financial risks or risks to assets. The transfer of risks may be considered to either reduce the exposure of the organization or because some other organization is more capable of effectively managing the risk.

It is important to note that some risks are not (fully) transferable in particular; it is generally not possible to transfer reputation risk even if the delivery of a service is contracted out.

(iii) **Terminate:** Some risks can only be treatable, or containable to acceptable levels, by terminating the activity itself. This option can be particularly important in project management if it becomes clear that the projected cost-benefit relationship is in jeopardy as the cost of treating the risk does not make the activity viable. For example, land acquisition for a project whose feasibility is based on that particular land may be risky and the cost of treating it in terms of legal fees is so high, that it may be better to terminate the project.

(iv) **Treat:** By far, a large number of risks will be addressed in this way. The purpose of treatment is to continue with the activity giving rise to the risk and action (internal control) is taken to contain the risk to an acceptable level.

Some of the Risk Enabled and Managed organisations used the following techniques.

Technique	*Description*
Risk Questionnaires	Designed to identify the relevant risks and create risk history
Flow Charts with Risk Flags	Designed to identify operational risks embedded in the processes
Identify Controls to manage risks	Recognize controls and test their adequacy and operative effectiveness
Risk Event Maps	Identify potential events that can have a significant impact on business to avoid negative surprises
Risk Scorecards	A Monitoring tool to track progress of risk management
Capital Budgeting	A financial analysis tool to evaluate the future cash flow benefits arising from risk management actions against the costs of risk consequences
Value at Risk	A financial analysis tool to evaluate the impact of the worst case scenario of a risk event
Risk Heat Maps	A Monitoring tool to track progress of risk management using qualitative assessment of probability and impact of risk

5. RISK MANAGEMENT CASE STUDIES

Case Study 1

An inappropriate risk culture isn't always about taking too much risk. Eastman Kodak was a trusted leading brand for over a hundred years. But its strategic failure to reinvent itself and exploit digital technology led to a descent into Chapter 11 bankruptcy.

Its culture meant that Kodak avoided risky decisions, and instead developed procedures and policies to maintain the status quo rather than adapting to the changing external environment.

(Mendes, 2007)

Case Study 2

In May 2012 JP Morgan Chase disclosed a multi-billion-dollar trading loss on its "synthetic trading portfolio". By its own admission the events that led to the company's losses included inadequate understanding by the traders of the risks they were taking; ineffective challenge of the traders' judgment by risk control functions; weak risk governance and inadequate scrutiny (Dimon, 2012). According to the New York Times, individuals amassing huge trading positions were not effectively challenged, there were regular shouting matches and difficult personality issues.

(New York Times, 2012)

Case Study 3

Staff at Barclays repeatedly filed misleading figures for interbank borrowings. First, between 2005 and 2008 – and sometimes working with traders at other banks - they tried to influence the Libor rate, in order to boost their profits. Then between 2007 and 2009, at the peak of the global banking crisis, Barclays filed artificially low figures. This tactic sought to hide the level to which Barclays was under financial stress at a point where their peers were being forced to accept state funding. When the scandal came to light it led to the resignation of the bank's chief executive Bob Diamond, along with Barclays chairman Marcus Agius. Barclays was fined €290m by UK and US regulators for rigging Libor and investigations are continuing. Barclays have set up an independent review to assess the bank's current values, principles and standard of operation and determine to what extent those need to change. It will also test how well current decision-making processes incorporate the bank's values, standard and principles and outline any changes required.

(BCC Website, 2012) (Barclays Press Release, 2012)

Case Study 4

Improving Cross Organizational Processes through Risk Management Working Group – A Carrier Team One Case Study

An aircraft carrier is a floating city with power plants, satellite telecommunications, convenience stores, and medical, dental, and hotel facilities. Maintaining and modernizing these ships can involve up to fifty different organizations simultaneously conducting all sorts of work, from painting to structural repair to electronic, electrical, and mechanical system upgrades. As an added project management challenge, the ship's crew typically lives on board during a major overhaul, which means that work cannot be conducted day and night, and services such as telecommunications, heating, ventilation, air conditioning, electricity, sanitation, and fresh water supply must remain intact as much as possible. With up to 500,000 man-days of work scheduled during an eleven-month dry docking period, you can imagine the tremendous amount of activity that must be carried out in a confined space and on a tight schedule.

The Naval Sea Systems Command (NAVSEA) established Carrier Team One (CT1) in 1997 to define, champion, and improve cross-organizational processes for planning and executing these complex aircraft carrier overhauls, known as "availabilities." CT1 provides the structure for managing and systematically improving cost, schedule, and quality performance by focusing on key planning and execution processes. They also integrate the efforts of numerous contributing organizations into an effective total-maintenance process.

CT1 took notice when two aircraft carrier availabilities were completed a number of weeks late in 2006. The team identified many factors that contributed to the delays, including large work packages with a number of high-risk items, critical path work with minimal margin, significant new and expanded work, and project team inexperience and turnover. All these issues affected both projects, yet project managers lacked an effective means of identifying, assessing, mitigating, and communicating the risks they posed to their project's timely completion. As a result, the carrier

maintenance community was unaware that help was needed until it was too late to take steps to avoid or limit delays. In response to the problems encountered on those projects, CT1's Executive Steering Committee formed a Risk Management Working Group (RMWG) and tasked them to (1) develop a standard process for comprehensive availability of risk management that could be applied consistently across all aircraft carrier shipyards and (2) support and monitor a risk management pilot project to be implemented on nine carrier availabilities at five different locations. CT1 used the existing Northrop Grumman Shipbuilding Newport News Operations (NGSB-NN) Risk Management Program (already in compliance with Department of Defence guidance) to develop a formal process for all aircraft carrier availabilities.

NGSB-NN based their 1998 risk program on a NASA-proven practice. NASA's Goddard Space Flight Center conducted a number of risk management training sessions at NGSB-NN and provided copies of their risk management procedures. Building on this knowledge transfer from NASA, NGSB-NN developed a risk management process designed specifically for ship construction and repair. This process included the development of a risk management strategy; developing and conducting risk management training; identifying program risks; analysing potential technical, quality, cost, schedule, and human-capital impacts; determining likelihood of problem occurrence; developing plans to mitigate risks; developing and maintaining a risk tool for capturing and updating project and shipyard risks; capturing risk management lessons learned; and continually improving the process to reflect customer feedback. To indicate the probability and impact of risks, the process uses the red/yellow/green risk cube described in the Defence Acquisition University Risk Management Guide for Department of Defence Acquisition. It adds environmental and safety risks to cost, schedule, and technical /quality risks. Proving its value over time, NGSB-NN's risk management program is now used company wide.

The CT1 risk management pilot project focused on the cultural journey required to convince naval shipyard aircraft carrier project teams of the value of a formal risk management process and to actively engage in it. That journey included the following essential elements.

Catalyst: As in any cultural journey, a catalyst for change is essential. In this case, the catalyst was the late completion of the two 2006 aircraft carrier overhauls in an environment that lacked a formal risk management process.

Infrastructure: The Executive Steering Committee formed the RMWG to establish a formal risk management program and associated training tools.

Initial Buy-In: Once the infrastructure was in place, the RMWG leader met with key stakeholders to share risk management background and procedures and develop their implementation plan and customer expectations.

Launch: As Executive Steering Committee chairman, Captain Daniel Seigenthaler, United State Navy (assistant chief of staff for carrier maintenance at Commander, Naval Air Forces Pacific Fleet), signed a letter directing the implementation of a risk management pilot program for nine aircraft carrier availabilities over a one-year period. This was followed by the RMWG leader

meeting with project leaders at the headquarters of all three aircraft carrier shipyards to discuss ideas for implementation.

During the pilot project, the RMWG leader provided peer assistance and training for each project's assigned risk manager to support skills development and team acceptance.

Integration into the Organization's Culture: From the outset, each project team's leadership needed to perceive the value of risk management to encourage their engagement. The initial direction and expectations set by CT1 provided the "push;" the challenge was to create a "pull" from the project teams. This was done by integrating risk management into command briefings, progress briefings, meeting agendas, team training, awards and recognition, newsletter articles, project strategies, retrospects, and the "hot wash" meeting at project completion. ("Hot wash" is a military term for a meeting used to capture learning and develop related recommendations at the end of a major activity or engagement.) CT1 thinks of a hot wash as a carrier-overhaul project team's "gift" to future project teams. Establishing a cross-project risk manager community of practice for knowledge sharing and comparison was the key to the pilot's accelerated adoption. This community provides a peer-assist environment for the risk managers to communicate and collaborate. It is also a forum for risk managers to discuss their challenges and share experiences and learning.

Retrospect and Process Maturity: The one-year pilot involved eight different overhaul projects that were either planned and less than a year from starting or in the process of executing four- to six-month-long repair projects. The pilot work proved to be process easy, but the implementation was hard. Early in the project, team leaders wanted to see value before engaging, but the best way to see risk management's value for their project team was to engage in it. At the conclusion of the risk management pilot, project leadership interviews captured what went well and what could be improved. A risk management process retrospect was held to capture lessons learned and recommendations from the one carrier project whose risk implementation extended from the start of planning to availability completion. Resistance occurred on all projects, but the quickest adoption came from the one that was furthest from their start date (ten months of planning remaining). As one would expect, the team that was a month into their six-month overhaul and focused on executing the work that was already under way saw the least value in the risk program. Data gathered during the pilot showed that project teams who embraced the formal risk management process quickly achieved risk-exposure reductions similar to those NGSB-NN teams that had been using it for years. These metrics helped convince other project teams of the value of the process and encouraged their engagement. Captured risks were shared via CT1's portal. The commonality of risks gave valuable insights to shipyard and program leadership personnel. Some examples of frequent risk categories were material availability, work package size and changes, constraints from shipyards or naval bases, planning performance, key event management, unidentified work and weather impacts, scheduling conflicts, worker availability, funding, ship's crew readiness, and project team turnover.

Following the pilot project, feedback from leadership showed that they were all fully engaged and appreciative of this tool's ability to help communicate and mitigate their biggest concerns. Matt Durkin, Norfolk Naval Shipyard's project superintendent for United State Ship Harry S. Truman's (CVN 75) 2009 overhaul, commented, "Risk management provided me with more visibility of our project's key issues. I'm not sure we would have completed our last availability on time without the Risk Management process." And Tim Ferguson, Puget Sound Naval Shipyard and Intermediate Maintenance Facility's project superintendent for USS Abraham Lincoln's (CVN 72) 2009 overhaul, said, "Our project team leveraged the risk management program to support open and honest discussion of issues that could have impacted delivering the ship on time." Pilot participant suggestions for taking the risk management program to the next level included:

- Adapting the process to address potential problems that were beyond the program manager's scope of influence.
- Using the risk management process to identify and communicate potential shipyard and ship's crew work distribution conflicts.
- Integrating risk management into a work package's development process during planning.

Captain Kevin Terry, USN, CT1's chairman, summed up the work so far: "The Risk Management Working Group has been a true success story. The pilot project was a home run. Aircraft carrier public and private shipyards are using the same language and risk cube to mitigate and communicate their issues." The U.S. Navy's Ship Maintenance Enterprise is currently building on the success of CT1's risk management pilot project. A NAVSEA instruction is being issued to formalize the process for all the U.S. Navy's ship and submarine overhauls. Over the next few years, NAVSEA will expand from individual project teams to the entire shipyard enterprise. As Cleve Butts, NAVSEA's director for Carrier Support, notes, "It is absolutely essential that we complete our maintenance periods on time and within cost, not only for aircraft carriers but for all our ships. Risk management is a great communication and management tool for ensuring that the right actions are being applied effectively and early. The RM [risk management] process has now been successfully implemented at all aircraft carrier shipyards.

CHAPTER 4

EVALUATION OF RISK MANAGEMENT STRATEGIES

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

- Risk Management Strategy alignment with Business Strategy
- Internal Control environment and linkages with Risk Management
- Risk Culture and attitudes to Risk Management
- Integrated Risk Reporting and Stakeholder responsibilities
- IT Risk Management – Disaster Recovery

1. RISK MANAGEMENT STRATEGY ALIGNMENT WITH BUSINESS STRATEGY

Primary goals and objectives of successful businesses are to make profits in an ethical and fair manner, fulfill social responsibilities, tax obligations and sustain the business for a longer duration. Organizations may have short, medium- and long-term strategic objectives. Business strategies are crafted keeping in mind the risk and opportunities, competitive landscape, regulatory regime, consumer preferences and business differentiators to meet such goals and objectives. Enterprise Risk Management (ERM) is a tool that assists organizations in meeting its business objectives. ERM is initiated by the Board of directors in a strategic context and implemented by senior executives of the organisation. Strategic context is Strategic objectives together with the strategies to achieve them. The strategic objectives of the organisation drive the risk management objectives. One of the key strategic objective and outcome of ERM is to improve the performance of the

organisation. The term "strategic context" is relevant as it indicates alignment with business strategy. Further, as ERM deals with risk mitigation it is natural that any event that prevents an organisation from meeting its objectives would be managed effectively through an Internal Control (IC) measure designed for this purpose; thereby improving the performance of the organisation. ERM is closely linked to business strategy and performance of the organisation. ERM and IC are also inter-connected subjects that compliment each other.

Empires or Businesses that survived over 100 years practiced risk management effectively by anticipating events that could threaten their very existence. Over the years the art of anticipation has been mastered through use of smart risk management strategies that are aligned to business objectives. These smart risk management strategies have revolved around –

- Collecting signals for potential events,
- Acquiring data to learn more about such potential events,
- Detecting patterns of change in the environment and acquired data,
- Imagining event outcomes, using intuition and taking precautionary actions such as designing internal controls.

Whether it is the golden era of India or the current digital era; substance or core of risk management strategies remain the same. The primary design of any risk management strategy is focused on de-risking the organisation from sudden surprise, emerging crisis, ability to adapt to changing consumer needs, altered circumstances, rare large shock events such as natural disasters, terrorism, collapse risk of business model and insulating from a contagion risk.

Contemporary Risk management strategies that are linked to business strategy and performance outline the ERM vision on "how risks can be effectively managed" in addition to "what risks need to be managed". Further, risk management strategies focus on how to identify "Key Risk Indicators" by describing "what measures need to be tracked or monitored" for monitoring emergence of a risk factor.

For example: -

Risk Factor - Threat of a disaster at an off-shore service centre

Key Risk Indicator - Tracking the threat levels from emergency response teams/ weather bureaus

1.1 Alignment of risk with strategy

Global statistics suggest that 80% of companies suffered business losses as a result of strategic blunders. Such strategic blunders are often caused on account of inability of the businesses to learn from history or past events, lack of sufficient planning for the short and long term, ignoring customer needs, pre-mature scaling, on-boarding costly capital, etc. Entrepreneurs end up with wrong strategic choices leading to strategic blunders or business failures. On the other hand, successful Companies incorporate Enterprise Risk Management into strategy setting sessions to a large, or very large extent foster a growth and performance-oriented culture. Involves appropriate levels of management;

For example

Strategic Objective	Strategic Measure	Risk Factor	Control Measure
Flawless Operations Provide flawless implementation and operations at competitive cost	Reliability (number of faults/ unit time) Serviceability (mean time to repair)	Machine break down	Use of specified material (quality and quantity) Preventive inspection (daily) and maintenance (scheduled)

Boards and entrepreneurs should understand the Risk Profile of the "Strategic Choice" that they are making and also the "Strategy Execution Risks" involved.

For example: -

Strategic Objective	Strategic Measure	Risk Factor	Control Measure
Product development Reduce product introduction cycle time	Product development cycle time	Delay in legal clearances	Planned product filings that are comprehensive, pre-audited for accuracy and complete. Product acceptance testing by retired or ex-regulators to incorporate improvements at test stage.

Boards foster an environment of performance, outcome orientation and quick risk responses to manage emerging risk events. In emerging risk situations responses are "action oriented" rather than focused on analyzing the "reason" of occurrence. Reasons and root causes are either pre or post analyzed for preventive actions.

In order to align risk with strategy a goal alignment must exist from top to bottom. This is possible by creating education and awareness of the significance of ERM in achieving strategic objectives, open communication about strategic business objectives and events that could prevent achievement of strategic business objectives, employee empowerment towards positive contributions/ suggestions on introducing control measures that could prevent risk event occurrences and finally linking employee compensation to risk management outcomes.

To align risk to business strategies – Corporate Boards invest time and resources in ERM implementation exercises. Such exercises are a combination of top down and bottom up approach where the Boards are setting the strategic context and executive management are identifying, assessing and reporting risks. Regulators such as SEBI, RBI, IRDA in India are issuing enhanced prescriptions to companies to develop robust ERM models and prepare their organisations to address emerging challenges and opportunities. Indian companies that have evolved risk monitoring practices are using Dashboards, Business Intelligence tools and enterprise wide pictorial maps to monitor risk indicators on a real-time basis and take corrective action to prevent

crisis and resultant losses. The financial services industry in India is heading towards a risk-based supervision regime involving real-time risk monitoring through automatic data transfer to the regulator with respect to key risk indicator position for the purpose of centralised risk monitoring.

1.2 Case Example – Risk Management at core of Business Strategy – Unilever Code of Business Principles

Risk management is integral to Unilever's strategy and to the achievement of Unilever's long-term goals. Our success as an organisation depends on our ability to identify and exploit the opportunities generated by our business and the markets Unilever operates in.

Unilever takes an embedded approach to risk management which puts risk and opportunity assessment at the core of the leadership team agenda. Unilever defines risks as actions or events that have the potential to impact our ability to achieve our objectives. Unilever identifies and mitigates downside risks such as loss of money, reputation or talent as well as upside risks such as failure to deliver strategy if it does not strengthen brand equities or growth in growing channels.

Unilever's Risk Management approach is embedded in the normal course of business. Its structural elements include: -

- Governance of Unilever, organizational structure and delegation of authority
- Vision, Strategy and Objectives
- Risk and Control Frameworks
- Performance management and operational processes execution
- Compliance and assurance activities.

1.3 Integrating Risk in the Strategic Planning Process

Strategic risks impact an organization's ability to deliver its goal - that is generally articulated in the strategic plan or intent document of the organisation. At the annual or early stage of strategic planning organization can identify and respond to strategic risks. Given the velocity with which threats and risk events strike organizations find it useful to integrate significant risk factors in the strategic planning process.

For example: -

- An organisation with an on-line selling business model may identify a cyber-attack threat at the stage of business plan preparation and respond by investing in a suitable internal control such as a best in class Firewall device.
- Strategic risks affect the organizations' s strategic plan can arise from internal operations or external factors. More often from external forces that shape its business environment such as - political, demographic, economic—and the dynamics of the industries where the organisation plays a role.

- New legislation that curtails the selling price of a medical device. This would significantly curtail the margins of the company.
- Company's strategic objective may require launch of a new sophisticated product, however, a specific set of skills required for installing the product may not be available with the company
- A new strategic initiative to implement cloud computing solutions may make the company more vulnerable to information security breaches

The strategy of an organisation should make it clear as to how it intends to mitigate or manage risks and maximize opportunities. It should develop objectives and the strategies to fulfil them. Further, these can be implemented through resource allocation plans.

1.4 Integrating Risk with Performance

Organisations can evaluate the level of risk they are exposed to while they pursue their growth goals. Knowledge of the level of risks that the organisation can take or accept at each stage of progression or growth enables the organisation to make informed decisions while pursuing their growth/ performance goals. Management's confidence enhances with risk awareness, understanding the risk profile of a strategic choice, risks associated with a desired performance. Existence of Internal controls and internal control assurance programs such as internal control evaluations or internal audits provide confidence to the management that they are ready to accept greater risks in pursuing their growth/ performance goals.

Certain business performance indicators may also disclose the associated risk profile –

Examples: -

- % of Customer attrition (loss of customer is a risk event for the company)
- % of Employee turnover (loss of employee is a risk event for the company)
- Profitability of customer by regional segments (unprofitable customers in certain regions may be a risk for the company)
- % of mission critical business processes with tested contingency plans (lack of contingency testing for mission critical processes represents a risk for the company)

2. INTERNAL CONTROL ENVIRONMENT AND LINKAGES WITH RISK MANAGEMENT

The subject of ERM is a sub-set of Corporate Governance. ERM is mandatory under the Companies Act, 2013 for large and listed entities therefore a matter of compliance as well. IC is a sub-set of ERM, basically internal control is the strategy or tool for the purpose of managing or mitigating the identified risk factor under the ERM. Internal Control Environment (ICE) is an intangible concept that represents the ethical, moral and governance climate of the organisation. It is difficult to measure the effectiveness of the ICE in simplistic terms, however, it can be assessed by surveying the culture of

the organisation. Such surveys to ascertain the ICE effectiveness are referred to as "Ethical Climate Surveys" or "Culture Monitoring Surveys". ICE can be evaluated through company-wide or entity level controls as well. These are high level controls that set the direction for other operating controls, example policy for financial closure or budgeting. We can observe a clear linkage between the concepts of ERM, IC and ICE as they have similar objectives of: -

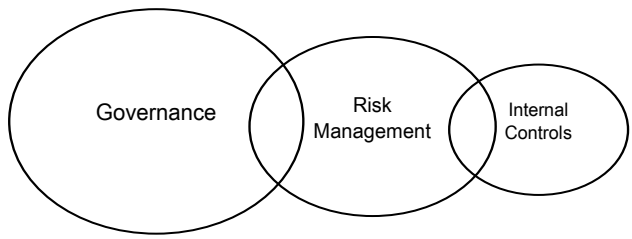
- Ensuring reliable financial reporting
- Efficient use of resources
- Compliance with the laws
- Improving performance

ERM is business strategy aligned whereas IC is operational and transactional driven. ERM is generally driven by the highest level whereas IC is implemented by the operating management.

ERM exercise requires the risk teams to study the business environment, eco-system of the company in terms of vendors, customers, employees, etc to identify relevant business risks and develop risk response action plans.

ICE and IC exercises requires the executive management to develop entity and process specific control strategies say for example internal control checklists, authorisation matrix, compliance procedures, standard operating procedures, etc.

Risk Management is a larger concept and internal control is a sub-set of Risk Management. Both subjects fall under the mega-concept of Governance. The pictorial depiction of the three concepts is as under: -



Generally, organizations face a wide range of uncertain internal and external uncertainties that may affect achievement of their objectives which can be strategic, operational, financial or otherwise and effect of these uncertainties on their objectives can be a Positive or a Negative Risks. While Positive Risks are opportunities the Negative Risks are threats to the achievement of objectives.

Both Risk Management and IC works together as on one hand the Risk Management mainly focuses on identification of threats and opportunities, on the other hand IC assist in countering threats and taking advantage of opportunities.

Proper Risk Management and IC hand in hand assist organizations in to effectively pursue their objectives by making informed decisions about the level of risk that they want to take and

implementing the necessary controls.

Accordingly, it can be said that both Risk management and IC are important pillars for governance, management, and operations of an organization's. Further to be a successful organization it is essential to integrate effective governance structures and processes along with performance-focused risk management and internal control at every level as well as across all operations of an organization.

It should be noted that though both Risk Management and IC should always be considered when setting and achieving organizational objectives and creating, enhancing, and protecting stakeholder value but are not objectives in themselves.

Since Risk Management and IC form an integral part of an organization's governance system with an integrated, organization-wide approach Risk Manager can treat risks in a more holistic, comprehensive way, ensuring that all business decisions are based on proper risk assessment and management considering the overall effect of uncertainties on the organization's objectives.

It is pertinent from above that internal control is an important sub-set of ERM. ERM is applied by the Board or highest executive from strategy through execution, while placing reliance on internal control at various stages. The two concepts of ERM and IC are interconnected, but not interchangeable. Both are used together, as powerful complementary tools in supporting management.

The task of IC is to help organisations achieve compliance, reporting and operations goals and objectives. So, IC is basically a component of risk management. And, internal control complements ERM. The ERM is basically a top down approach to Risk Management. It's focus is broader and aims at reducing risks that affect the entire enterprise. On the other hand, internal control provides a bottom up approach and it complements ERM by doing an in-depth assessment of agency's business processes, its specific risks, and how those risks are being controlled.

IC includes activities designed to help organizations achieve compliance, reporting and operations goals and objectives. Part of doing so requires that management consider the risk to those objectives – so it is inherently a component of risk management. But IC complements ERM; each raises the value of the other. For example, ERM helps in developing the objective used as a basis for developing controls, while IC makes ERM more effective when control activities are in place over risk responses and other ERM processes.

3. RISK CULTURE AND ATTITUDES TO RISK MANAGEMENT

3.1 Risk Culture

People are the cornerstone for effective Risk Management in any organisation or society. Risk aware culture and pro-active attitude ensure quick risk responses and containment of damages. Risk culture means that all levels of the organisation from the junior most to the Chief Executive understand and appreciate the positive and negative results that a risk event can bring.

Risk culture takes a long time to evolve, it requires continuous efforts of communication, building of corporate memory so that people can learn from previous mistakes, shaping the right risk actions, etc.

Basel's Principles for the Sound Management of Operational Risk defines Risk culture as "the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a firm's commitment to and style of Operational Risk Management."

Organisations are integrating Risk management into strategic planning, performance measurement, budgeting, projects and operational activities to create Risk Culture and reap benefits of sustainable business practices.

Various definitions of risk culture are available. The 2009 International Institute of Finance report "Reform in the financial services industry: Strengthening Practices for a More Stable System" defines Risk culture as the norms of behaviour for individuals and groups within an organisation that determine the collective ability to identify and understand, openly discuss and act on the organisations current and future risk.

Guidance on Supervisory Interaction with Financial Institutions on Risk Culture - A Framework for Assessing Risk Culture (April 2014) states that: -

A sound risk culture should emphasise throughout the institution the importance of ensuring that:

(i) an appropriate risk-reward balance consistent with the institution's risk appetite is achieved when taking on risks;

(ii) an effective system of controls commensurate with the scale and complexity of the financial institution is properly put in place;

(iii) the quality of risk models, data accuracy, capability of available tools to accurately measure risks, and justifications for risk taking can be challenged, and

(iv) all limit breaches, deviations from established policies, and operational incidents are thoroughly followed up with proportionate disciplinary actions when necessary.

3.2 Case Example – Risk Culture Development – Risk Focus Integrity

One of the leading Corporates operating in the Energy Sector has disclosed its policy on "Supporting our Culture of Integrity". Let us study the policy disclosure for prevention of improper payments: -

3.2.1 Supporting our Culture of Integrity

CNOOC International's culture and processes support our commitment to integrity. Our Prevention of Improper Payments Standard requires that all employees comply with applicable laws everywhere we operate. This Standard is periodically reviewed for best practices, vetted by external counsel and reviewed by our Compliance Committee.

The Compliance Committee is comprised of members of our executive management team and provides oversight on potential high-risk payments. Approvals required under the Prevention of Improper Payments Standard are dealt with by this Committee, which also receives a report on high risk payments. As an additional control, our internal audit department assesses corruption risk on a periodic basis and conducts investigations if necessary.

Risk-based Prevention of Improper Payments training has been developed that provides employees in high risk positions with guidance on avoiding improper payments.

3.2.2 Integrity Leaders

A network of Integrity Leaders has been established to promote the organization's culture of integrity, facilitate integrity education and awareness, as well as act as a divisional resource for employees and internal stakeholders faced with an ethical dilemma or seeking guidance. Integrity Leaders regularly liaise between the Integrity and Compliance group in Calgary, Canada and employees working in our global locations.

4. INTEGRATED RISK REPORTING AND STAKEHOLDER RESPONSIBILITIES

Business models are being constantly challenged with volatile economic cycles, wide fluctuations in fuel and commodity prices, ballooning of debts; as a result, instances of business failures are rising. There is a growing demand for better and comprehensive risk disclosures. Stakeholders, investors, societies, communities and special interest groups believe that existing risk management disclosures are not enough, and they lack:

- Transparency
- Timeliness
- Depth
- Quality

They also believe that the disclosures are Strait jacketed.

Regulators have realised that corporates are reporting risks in a standardised manner as they do not like to disclose the true risk and opportunities. Therefore, regulators are deepening the risk disclosure norms applicable to listed and regulated entities.

Globally, there is a movement that has been initiated by the International Integrated Reporting Council (IIRC) on Integrated Reporting. IIRC is a global coalition of regulators, investors, companies, standard setters, the accounting profession and NGOs. The coalition is promoting communication about value creation as the next step in the evolution of corporate reporting. IIRC has promoted the concept of Integrated thinking and integrated report. The IIRC's vision is to align capital allocation and corporate behaviour to wider goals of financial stability and sustainable

development through the cycle of integrated reporting and thinking.

The main aim of an Integrated Report is to highlight by way of explaining to the investors who have contributed financial capital about the organisation's value creation over time. Further, an integrated report proves advantageous to all the stakeholders of the company including employees, customers, suppliers, business partners, regulators, policy makers etc.

An Integrated Report's primary purpose is to explain to providers of financial capital how an organization creates value over time. An integrated report benefits all stakeholders interested in an organization's ability to create value over time, including employees, customers, suppliers, business partners, local communities, legislators, regulators and policy-makers.

An integrated report includes the eight Content Elements. The Content Elements are fundamentally linked to each other and are not mutually exclusive. The order of the Content Elements is not the only way they could be sequenced.

The Content Elements are not intended to serve as a standard structure for an integrated report with information about them appearing in a set sequence or as isolated, standalone sections. Rather, information in an integrated report is presented in a way that makes the connections between the Content Elements apparent.

The content of an organization's integrated report will depend on the individual circumstances of the organization. The Content Elements are therefore stated in the form of questions rather than as checklists of specific disclosures. Accordingly, judgement needs to be exercised in applying the Guiding Principles to determine what information is reported, as well as how it is reported.

There are eight content elements of Integrated Report suggested by the Framework which include answering the Questions raised.

4.1 Organisational Overview and External Environment

Question: "What does the organisation do and what are the circumstances under which it operates?"

(I) Organisational Overview

An integrated report identifies the organization's mission and vision, and provides essential context by identifying matters such as:

(a) The organization's:

- Culture, ethics and values
- Ownership and operating structure
- Principal activities and markets

- Competitive landscape and market positioning (considering factors such as the threat of new competition and substitute products or services, the bargaining power of customers and suppliers, and the intensity of competitive rivalry)
- Position within the value chain

(b) Key Quantitative Information (KQI)

- Number of employees
- Revenue
- Number of countries in which the organization operates
- Highlighting, in particular, significant changes from prior periods

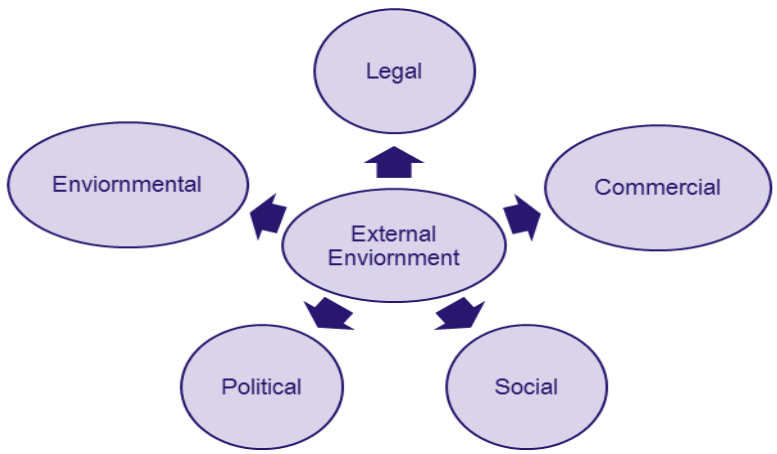
(c) Significant factors

- Significant factors affecting the external environment and the organization's response

(II) External Environment

External Environment can affect the organization directly or indirectly (e.g., by influencing the availability, quality and affordability of a capital that the organization uses or affects). Significant factors affecting the external environment that affects the organization's ability to create value in the short, medium or long term include aspects of:

- Legal
- Commercial
- Social
- Environmental
- Political context



4.2 Governance

Question: "How does the organisation's governance structure support its ability to create value in the short, medium and long term?"

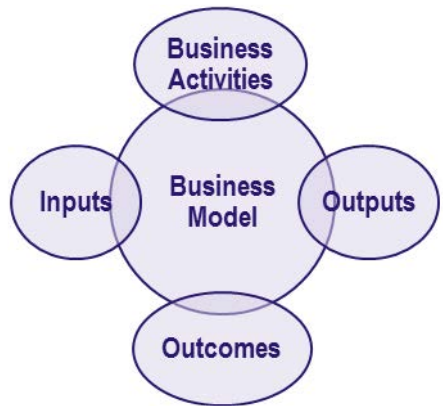
An integrated report provides insight about how such matters as the following are linked to its **ability to create value:**

- The **organization's leadership structure**, including the skills and diversity (e.g., range of backgrounds, gender, competence and experience) of those charged with governance and whether regulatory requirements influence the design of the governance structure.
- **Specific processes** used to make strategic decisions and to establish and monitor the culture of the organization, including its attitude to risk and mechanisms for addressing integrity and ethical issues
- **Particular actions** those charged with governance have taken to influence and monitor the strategic direction of the organization and its approach to risk management
- How the **organization's culture, ethics and values** are reflected in its use of and effects on the capitals, including its relationships with key stakeholders
- Whether the organization is **implementing governance practices** that exceed legal requirements
- The **responsibility** those charged with governance take for promoting and enabling innovation
- How **remuneration and incentives are linked to value creation** in the short, medium and long term, including how they are linked to the organization's use of and effects on the capitals.

4.3 Business Model

Question: "What is the organisation's business model?"

Basically Business Model is a system of transforming inputs into output or outcomes using business activities that fulfil organization's strategic purposes and creating value.



(I) **Inputs:** An integrated report shows how key inputs relate to the capitals on which the organization depends, or that provide a source of differentiation for the organization, to the extent they are material to understanding the robustness and resilience of the business model.

(II) **Business Activities:** An integrated report describes key business activities. This can include:

- How the organization differentiates itself in the market place? – For example through product differentiation, market segmentation, delivery channels and marketing
- The extent to which the business model relies on revenue generation after the initial point of sale – For example extended warranty arrangements or network usage charges
- How the organization approaches the need to innovate? – For example, growing demand less pollutant vehicles.
- How the business model has been designed to adapt to change – For example, producing electric vehicles.

(III) **Outputs:** An integrated report identifies an organization's key products and services. There might be other outputs, such as by-products and waste (including emissions), that need to be discussed within the business model disclosure depending on their materiality.

(IV) **Outcomes:** An integrated report describes key outcomes, including:

- Both internal outcomes (e.g., employee morale, organizational reputation, revenue and cash flows) and external outcomes (e.g., customer satisfaction, tax payments, brand loyalty, and social and environmental effects)
- Both positive outcomes (i.e., those that result in a net increase in the capitals and thereby create value) and negative outcomes (i.e., those that result in a net decrease in the capitals and thereby diminish value).

4.4 Risks and Opportunities

Question to be answered through this element in the integrated reporting is "What are the specific risks and opportunities that affect the organisation's ability to create value over the short, medium and long-term, and how is the organisation dealing with them?"

An integrated report identifies the key risks and opportunities that are specific to the organization, including those that relate to the organization's effects on, and the continued availability, quality and affordability of, relevant capitals in the short, medium and long term.

This can include identifying:

- The specific source of risks and opportunities, which can be internal, external or, commonly, a mix of the two. External sources include those stemming from the external environment. Internal sources include those stemming from the organization's business activities.
- The organization's assessment of the likelihood that the risk or opportunity will come to

fruition and the magnitude of its effect if it does. This includes consideration of the specific circumstances that would cause the risk or opportunity to come to fruition. Such disclosure will invariably involve a degree of uncertainty such as:

- ♦ an explanation of the uncertainty
- ♦ the range of possible outcomes, associated assumptions, and how the
- ♦ information could change if the assumptions do not occur as described
- ♦ the volatility, certainty range or confidence interval associated with the information provided

- The specific steps being taken to mitigate or manage key risks or to create value from key opportunities, including the identification of the associated strategic objectives, strategies, policies, targets and KPIs.

4.5 Strategy and Resource Allocation

Question: "Where does the organisation want to go and how does it intend to get there?"

An integrated report ordinarily identifies:

- The organization's short, medium and long term strategic objectives
- The strategies it has in place, or intends to implement, to achieve those strategic objectives
- The resource allocation plans it has to implement its strategy
- How it will measure achievements and target outcomes for the short, medium and long term.

This can include describing:

- The linkage between the organization's strategy and resource allocation plans, and the information covered by other Content Elements, including how its strategy and resource allocation plans.
- What differentiates the organization to give it competitive advantage and enable it to create value.
- Key features and findings of stakeholder engagement that were used in formulating its strategy and resource allocation plans.

4.6 Performance

Question: "To what extent has the organisation achieved its strategic objectives for the period and what are its outcomes in terms of effects on the capitals?"

An integrated report contains qualitative and quantitative information about performance that may include matters such as:

- **Quantitative indicators** with respect to targets and risks and opportunities, explaining their significance, their implications, and the methods and assumptions used in compiling them

- The **organization's effects (both positive and negative) on the capitals**, including material effects on capitals up and down the value chain
- The **state of key stakeholder relationships** and how the organization has responded to key stakeholders' legitimate needs and interests
- The **linkages between past and current performance**, and between current performance and the organization's outlook

4.7 Outlook

Question: "What challenges and uncertainties is the organisation likely to encounter in pursuing its strategy, and what are the potential implications for its business model and future performance?"

An integrated report ordinarily highlights anticipated changes over time and provides information, built on sound and transparent analysis, about:

- The **organization's expectations** about the external environment the organization is likely to face in the short, medium and long term
- How that will **affect** the organization
- How the **organization is currently equipped** to respond to the critical challenges and uncertainties that are likely to arise.

4.8 Basis of Preparation and Presentation

Question: "How does the organization determine what matters to include in the integrated report and how are such matters quantified or evaluated?"

An integrated report describes its basis of preparation and presentation, including:

- A summary of the organization's Materiality determination process
- A description of Reporting boundary and how it has been determined
- A summary of Significant frameworks and methods used to quantify or evaluate material matters

[Source: International <IR> Framework, The International Integrated Reporting Council (IIRC)]

5. RISK & OPPORTUNITY REPORTING

As per the IIRC - Continuous monitoring and analysis of the external environment in the context of the organization's mission and vision identifies risks and opportunities relevant to the organization, its strategy and its business model.

Most of the guidance and regulatory requirements for risk reporting were developed after the global financial crisis of 2007-08, but few nations have a better record than others, historically, of

mandating or encouraging companies to report on risk. The US, for example, has required companies listed with the Securities and Exchange Commission (SEC) to describe the risks faced by the business (in some form or another) since the 1970s. The EU Accounts Modernisation Directive of 2003 said that companies should describe the risks they face, in both annual and interim reports.

Two countries have gone further than the Europe-wide requirements – Germany has its own Risk Reporting Standard (GAS 5), while the UK's Corporate Governance Code states that companies should report at least annually on the effectiveness of their risk-management procedures. The UK's Corporate Governance Code still goes further where a more integrated approach to risk reporting, linking risk management to internal controls and going concern.

The Management Discussions & Analysis (MD & A) section that is popular in Annual Report disclosures was prescribed by the US Securities & Exchange Commission in the 1980s to meet the growing demand of enhanced risk disclosures. The MD & A section requires has specific disclosures on the trends, economic uncertainties that the business is exposed to and the likely positive or negative impact of such trends and economic uncertainties on the revenues of the company. In the US, large unexpected losses on derivatives incurred by several firms in the early to mid-1990s reinforced demands that had already begun to emerge for better information on firms' derivative positions and market risks. This led to risk disclosure requirements in Disclosures about Derivative Financial Instruments and Fair Value of Financial Instruments and Accounting for Derivative Instruments and Hedging Activities, and Disclosure of Accounting Policies for Derivative Financial Instruments etc. These include Germany's requirement for companies to disclose all material risks, subsequently supplemented by an accounting standard on risk reporting, and the EU's requirement that a company's annual report to include description of principal risks and uncertainties that it is exposed to.

Global developments about risk reporting encompass following contemporary aspects to provide a holistic risk reporting disclosure to stakeholders and investors: -

- Reporting of principal or material risk factors and responsibility for mitigating such risk factors
- Clear categorisation of risks into company specific or general/ industry related
- Ordering or numbering the risks so that investor understand the risk priorities
- Movement of risks from previous reporting periods showing the context and cause for such changes
- Risk linkages to financial statements, other important parts of the Annual Report
- Impact of risks on financial and non-financial matters
- Indictive risk appetite of the company as it may be difficult to quantify
- Short term Liquidity and Long-term Business Viability reporting
- Stress and Sensitivity analysis with specific scenarios linking back to principal risk factors

In India, as per the SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015: -

(i) Under responsibility of Directors - Ensuring the integrity of the listed entity's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.

(ii) The Board of Directors shall ensure that, while rightly encouraging positive thinking, these do not result in over-optimism that either leads to significant risks not being recognised or exposes the listed entity to excessive risk.

(iii) The Board of Directors shall have ability to "step back" to assist executive management by challenging the assumptions underlying: strategy, strategic initiatives (such as acquisitions), risk appetite, exposures and the key areas of the listed entity's focus.

(iv) The listed entity shall lay down procedures to inform members of board of directors about risk assessment and minimization procedures.

(v) The Board of Directors shall be responsible for framing, implementing and monitoring the risk management plan for the listed entity.

(vi) Risk Management Committee: - The board of directors shall constitute a Risk Management Committee. Majority members of Risk Management Committee shall consist of members of the board of directors. The Chairperson of the Risk management committee shall be a member of the board of directors and senior executives of the listed entity may be members of the committee.

The board of directors shall define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit. The provisions of this regulation shall be applicable to top 100 listed entities, determined based on market capitalisation, as at the end of the immediately preceding financial year.

(vii) Under minimum information to be placed before the Board on a quarterly basis- Quarterly details of foreign exchange exposures and the steps taken by management to limit the risks of adverse exchange rate movement, if material.

(viii) Under disclosures in Annual Reports applicable to all listed entities except banks - Management Discussion and Analysis: This section shall include discussion on the following matters within the limits set by the listed entity's competitive position:

(a) Industry structure and developments

(b) Opportunities and Threats

(c) Segment–wise or product-wise performance

(d) Outlook, (e) Risks and concerns,

(f) Internal control systems and their adequacy

(g) Discussion on financial performance with respect to operational performance,

(h) Material developments in Human Resources / Industrial Relations front, including number of people employed and General information to shareholders: Commodity price risk or foreign exchange risk and hedging activities.

6. IT RISK MANAGEMENT – DISASTER RECOVERY

6.1 Disaster Recovery Plan

Information is said to be the currency of the 21st century and it is considered the most valuable asset of an organisation. This is more so in case of organisations which use and are heavily dependent on Information Technology (IT). Organisations in this modern era run their business based on information which are processed using Information and Communication Technology (ICT). The ICT plays a central role in the operation of the business activities. For example, the stock market is virtually paperless. Banks and financial institutions have become online, where the customers rarely need to set foot in the branch premises. There is a heavy dependence on real time information from information technology assets for conducting business. Information is a critical factor for continued success of the business. This dependence on Information is more explicit in the most organisations which are now dependent on IT for performing their regular business operations. We can understand the criticality of IT by imagining impact of failure or non-availability of IT in case of following types of organisations:

(i) Bank using Core banking solution with a million accounts, credit cards, loans and customers.

(ii) Companies using centralised ERP software having operations in multiple locations.

(iii) An airline serving customers on flights daily using IT for all operations.

(iv) Pharmacy system filling millions of prescriptions per year (some of the prescriptions are life-saving).

(v) Automobile factory producing/manufacturing hundreds of vehicles daily using automated solution.

(vi) Railways managing thousands of train routes and passengers through automated ticketing and reservation.

The above situations clearly demonstrate the heavy dependence on IT systems. IT can fail due to multiple factors. Hence, organisations should have appropriate disaster recovery and/ or contingency plans for resuming operations from disruption. The disruption of business operation can be due to unforeseen manmade or natural disaster and this may lead to loss of productivity, revenue and market share among many other impacts. Hence, organisations have to take necessary steps to ensure that the impact from such disasters is minimised and build resilience which ensures continuity of critical operation in the event of disruptions. Modern organisations

cannot think of running their business operations without IT. IT is prone to increased risks which can lead to failure of IT thus impacting operations. Hence, it is becoming increasingly important for organisations to have a business contingency plan for their Information Systems. The criticality of the plan can be determined based on the level of impact on critical business operations due to failure or non-availability of IT impacting service delivery. The failure of IT could be caused due to any or more of the following: -

(i) Server or network failure

(ii) Disk system failure

(iii) Hacker break-in

(iv) Denial of Service attack

(v) Electrical or extended power failure

(vi) Snow storm, earthquake, tornado, tsunami or fire

(vii) Spyware, malevolent virus or worm

(viii) Employee error or revenge

(ix) Sabotage or theft

(x) Terrorist cyber attack

(xi) Communication link break down

(xii) Civil disturbance

Disaster is a physical event which interrupts business processes sufficiently to threaten the viability of the organisation. The basic objective of a Disaster Recovery Plan (DRP) is to document a set of procedures which can be used to protect a business IT infrastructure if any disaster takes place. DRP includes tasks like plan for disaster recovery, crisis management, recovery operations etc. Disaster Recovery Plan is the set of plans which are to be executed initially at the moment of crisis. These plans include measures to control the disaster, mitigate them and to initiate the recovery of the resources that is needed for the continuity of business. These plans are targeted to initiate/recover the resources that have been affected by a disaster. These are the first plans that would be executed at the time of disaster. There are three basic strategies that encompass a disaster recovery plan:

- preventive measures,
- detective measures, and
- corrective measures.

As the name indicates, the job of preventive measures is to prevent a disaster from taking place. The purpose of these measures is proper identification and reduction of risks. They are designed to mitigate or prevent an event from turning into a disaster.

These measures may include keeping data backed up and off site, using surge protectors, installing generators and conducting routine inspections. Further, these measures may be bifurcate into Detective or Corrective measures. For example: -

- Installing Fire alarms – detective
- Employee DR related trainings – detective
- Insurance Policies – Corrective
- Restoring systems post disaster - Corrective

A disaster can be defined as an unplanned interruption of normal business process. It can be said to be a disruption of business operations that stops an organisation from providing critical services caused by the absence of critical resources. An occurrence of disaster cannot always be foreseen; hence we need to be prepared for all the types of disasters that can arise, handle them effectively in the shortest time.

Business Continuity Plan (BCP) includes tasks like establishing continuity strategies, planning for continuity of critical operations, continuity management etc. BCP is a plan that contains the steps that would be taken by an entity to resume its business functions during its period of disruption. These plans are executed in parallel with the disaster recovery plans depending on the impact of the disaster. BCPs on a whole is about re-establishing existing business processes and functions, communications with the business contacts and resuming business processes at the primary business location.

6.2 Testing the Disaster Recovery Plan

The Disaster Recovery Co-ordinator is responsible for testing of the disaster recovery plan at least annually to ensure the viability of the plan. Special Disaster Recovery testing is undertaken whenever there are changes in the software and technology or business environments. Objectives of testing the Disaster Recovery plan/ procedures are outlined under: -

(i) To simulate the conditions of an actual Business recovery situation

(ii) Determine the time consumed and feasibility of the recovery process

(iii) Identify deficiencies in the existing procedures for improvement and take note of the physical / practical constraints

(iv) Test the completeness of the business recovery information stored at the Offsite Storage Location.

(v) Train members of the Disaster Recovery teams the initial test of the plan will be in the form of a structured walk-through and should occur within two months of the Disaster Recovery plan's acceptance. Subsequent tests should be to the extent determined by the Business continuity co-ordinator that are cost effective and meet the benefits and objectives desired.

(vi) Test the state of resilience of the organisation and associated service providers

(vii) Provide assurance to the Board and regulators that Disaster Recovery plan is operational and effective

CHAPTER 5

RISK MODEL

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

- VAR
- Stress Testing
- Scenario Analysis
- Country and Sovereign Risk Models and Management

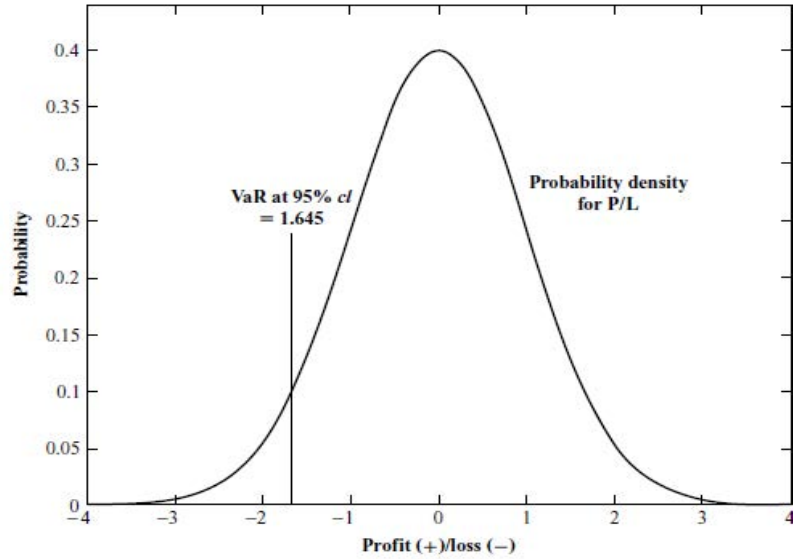
1. VALUE AT RISK (VAR)

VaR is a method of measuring the loss in the value of the portfolio over a given time period and for a distribution of historical returns. It is the percentage loss in the asset or portfolio value that will be exceeded or can be equal to only X percent of the time. A 1%, 5% and 10% VaR would be denoted as VaR (1%), VaR (5%) and VaR (10%) respectively. X percent probability of interest and the time period over which the VaR is calculated will be selected. Generally, the time period selected is one day. VaR can measure broader measures of calculating potential losses.

For example, a risk manager calculates the daily 5% VaR as $15000. The VaR (5%) of $15000 indicates that there is 5% chance that on any day, the portfolio will experience a loss of $15000 or more. Also, there is 95% chance that on any given day the portfolio will experience either a loss less than $15000 or a gain.

1.1 Calculating VaR

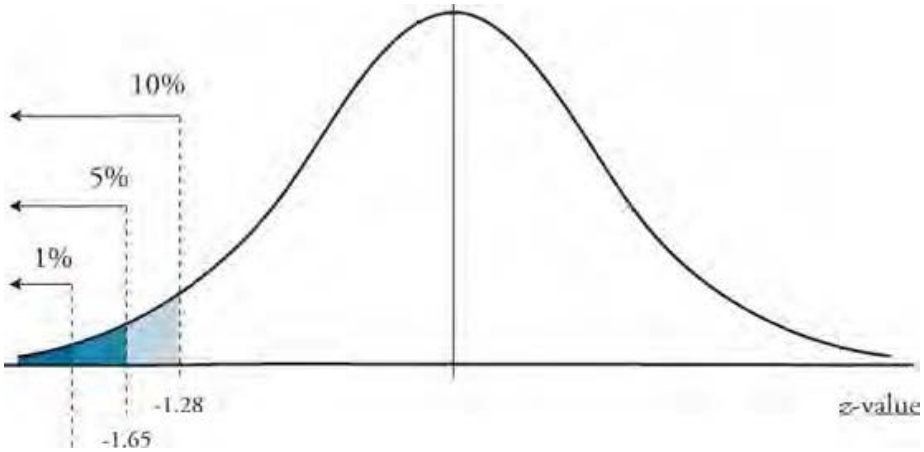
If we are calculating VaR using delta-normal method, we need to assume that it follows a standard normal distribution in which mean ($\mu = 0$) and standard deviation ($\sigma = 1$). It can be used to measure broader measures of the distribution of potential losses.



The VaR is dependent on two parameters which is holding period which is the time interval in which we measure our profit/loss and second is the confidence level which indicates the likelihood that we will get an outcome no worse than our VaR which might be 90%, 95% , 99% or indeed any fraction between 0 and 1.

The figure above shows a common probability density function over a chosen holding period. Positive P/L means profits and negative observations means losses. For VaR calculation, we need to specify the confidence levels. If the confidence interval is 95%, then the VaR will be given by the negative of the point on the X-axis that cuts offs the top 95% of P/L observations from the bottom 5% of tail observations. So corresponding to that the x-axis value is -1.645 so the VaR is 1.645. The negative P/L value corresponds to a positive VaR which indicates the worst outcome at this confidence level is 1.645. So the worst outcome at this level of confidence is a loss of 1.645. If the worst outcome at this confidence level is a particular profit rather than a loss then the likely loss must be negative. If we take corresponding VaR at 99% level of confidence so it is determined by the cut-off between the top 99% and bottom 1% of the observations, so we are dealing with 1% tail rather than the earlier 5% tail. So the cut off point is -2.326 and the VaR is 2.326. The higher the confidence level, smaller the tail which leads to higher VaR.

VaR not only rises with the confidence level, but also rises at the rate which is increasing. Also, VaR depends on the choice of the holding period. It rises with the square root of the holding period. But we should recognise that VaR might rise in a different way or even fall, as the holding period rises.



In the above chart, we have the following observations i.e. probability of observing a value more than 1.28 standard deviations below the mean is 10%, the probability of observing a value more than 1.65 standard deviations below the mean is 5%; and the probability of observing a value more than 2.33 standard deviations below the mean is 1%. Thus, we have critical z-values of-1.28, -1.65, and -2.33 for 10%, 5%, and 1% lower tail probabilities, respectively. We can define VaR as:-

$$VaR\ (X\ \%) = z_{X\%} * \sigma$$

where VaR(X %) = X% probability at risk

Zx% = the critical Z value based on normal distribution and the X% probability

σ (sigma) = standard deviation of daily returns on percentage basis

VaR is a one tailed test so the level of significance is entirely in one tail of the distribution

To calculate VaR on dollar basis, we multiply the percent VaR by the asset value:

$$VaR(X\ \%)_{\text{dollar basis}} = VaR(X\ \%)_{\text{decimal basis}} * \text{asset value}$$

$$= (zx\%\ \sigma) * \text{asset value}$$

(a) VaR Conversions: Finance Professionals and Risk Managers may be interested in measuring risk over long time periods such as month, quarter or year. VaR can be converted from one day basis to longer basis by multiplying daily VaR by square root of no. of days e.g to convert into monthly VaR, multiply daily VaR by square root of 20(i.e. 20 business days)

$$VaR(X\ \%)_{\text{X-days}} = VaR(X\ \%)_{1\ \text{day}} * \sqrt{X}$$

VaR can also be converted to different confidence intervals.

For example, if you want to convert VaR with 95% confidence interval to VaR with 99% confidence interval. The formula will be

$$VaR\ (1\%) = VaR\ (5\%) * \frac{z_{1\%}}{z_{5\%}}$$

(b) VaR Parameters : VaR involves two parameters i.e. the holding period and the confidence level. The usual holding periods are one day or one month but institutions can operate on other holding periods. As per Capital adequacy rules, banks should operate with a holding period of two weeks. The factor that determines the length of the holding period is the liquidity of the markets in which institution operates. A short holding period is preferable for model validation or back testing purposes, reliable validation requires a large data set and a large data set requires a short holding period.

In case of backtesting, we would usually want low confidence levels to get a proportion of excess loss observations. For example, we might want a high confidence level if we were using our risk measures to set capital requirements. If we wish to estimate VaR, we would probably wish to use confidence levels and holding periods that are comparable to those used by other institutions which are in the range of 95%-99%.

1.2 VaR Methods

1.2.1 Delta – Normal Method (Linear Method)

In the delta normal approach, the linear approximation is assumed on the risk factor which is assumed to follow normal distribution e.g. when looking at positions in options, the linear exposure used will be delta. Also, in case of positions in bonds, the linear exposure will be duration. Both are first derivatives. In case of options, the underlying factor is the stock price and we assume that the stock price is normally distributed. In case of a bond, we would assume the yield is normally distributed. This method is best used in portfolios which has a linear position.

Change in portfolio value with respect to change in risk factor is described as:

$$dp = \Delta * dr$$

where Δ is the sensitivity of the portfolio value with respect to risk factor

dp is change in the portfolio value

dr is change in risk factor

Limitations of the delta-normal method

It is only accurate for linear exposures, non – linear exposures are not correctly captured by this VaR method. E.g. Non linear exposures like convexity, mortgage backed securities and fixed income securities with embedded options are not adequately captured by this method. For measuring non-linear exposures, delta-gamma method can be used.

1.2.2 Full Revaluation Method

It is the full re-pricing of the portfolio with the assumption that the underlying risk factors are shocked to experience a loss. This method shocks the risk factor. VaR for this method calculates the worst expected change in the risk factor given some confidence and time horizon. It prices the portfolio under the changed risk factors and for wide range of price levels. The values can be generated by:

(a) Historical Simulation

(b) Bootstrap Simulation

(c) Monte Carlo Simulation

(a) Historical Simulation – In this method, the portfolio is revalued using risk factors taken from historical data. E.g. Calculation of 5% daily VaR using the historical method for the past daily returns. First we need to rank the returns from highest to lowest and then identify lowest 5% of the returns. The highest value of the lowest 5% of the returns will give 1 day 5% VaR. This method is easiest to implement and it is easy to calculate. The limitation of this method is that there may not be enough historical data. Also, the variation of risk in the past may not represent the variation of risk in the future. This method is quite slow in case of adapting to new correlations and volatilities.

(b) Bootstrap Simulation – Bootstrap Simulation is an extension of historical simulation. It draws a sample from the dataset and records its VaR. Then again it will draw another new sample and record its VaR. This procedure is repeated over and over again using various samples and from all the samples, VaR is recorded. This procedure is similar to sampling with replacement. The best VaR estimate from the data is the average of all sample VaR.

(c) Monte Carlo Simulation – This method is similar to bootstrap simulation except the movements in various risk factors are generated from distributions which are estimated. It basically refers to computer software that generates thousands of possible outcomes from the distribution of inputs which are specified by a user, e.g. distribution of monthly returns of hundreds of stocks in a portfolio. The computer will select one monthly return from each stock's distribution of returns and calculate weighted average portfolio returns. The number of runs is specified by the user. Thousands of weighted average portfolio returns are formulated which will form the normal distribution.

VaR will be calculated the same as delta normal method. The main advantage of the use of Monte Carlo simulation is that we can generate correlated scenarios based on a statistical distribution. Due to which it models multiple risk factors. Thus this approach is very powerful in understanding the risk factors. Moreover, we can specifically focus on the tails of extreme loss scenarios. So, Monte Carlo Simulation method can be used both to calculate VaR as well as to complement it. Also, it can work both for linear and non linear risks. As unlimited number of scenarios is generated, this helps in creating correct distributions.

The drawback of this method is that it may generate red flags, that it is highly subjective and that generated scenarios may not be relevant going forward. The computation time is quite high and this method is expensive due to the requirement of advanced technological skills.

1.3 Coherent Risk Measures

We want risk measures to correctly reflect diversification effects and should facilitate effective decision making. The answer to this will be found in the theory of coherent risk measures. If X and Y are the future values of two risky positions, a risk measure ρ(rho) is said to be coherent if it satisfies the following properties:

- **Subadditivity** – The risk of the portfolio is at most equal to the risk of the assets within the portfolio.

$$\rho(X) + \rho(Y) \leq \rho(X + Y)$$

- **Homogeneity** – Size of the portfolio, t will impact the size of its risk

$$\rho(t X) = t \rho(X)$$

- **Monotonicity** – Portfolio with greater future returns will likely have less risk

$$\rho(X) \geq \rho(Y) , X \leq Y$$

- **Risk free condition** - The risk of a portfolio is dependent on the assets within the portfolio for all constants n

$$\rho(X + n) = \rho(X) – n$$

The second, third & fourth properties imply well behaved distributions. Homogeneity says risk of a position is always proportional to its size. Monotonicity suggests that if one risk always has greater losses than the other risk, the capital requirements should be greater. Risk free condition means that there is no additional capital requirement for an additional risk for which there is no uncertainty.

Subadditivity is the most important property for a coherent risk measure. It states that portfolios will have equal or less risk than the sum of the individual portfolios.

1.4 Expected Shortfall

It is the most attractive coherent risk measure. This measure often has different names including expected tail loss, conditional VaR, tail VaR, all of which are the same. It is the expected value of our losses if we get a loss in excess of VaR. The VaR tells us the most we can expect to lose if a bad or tail event does not occur whereas Expected Shortfall tells us what we can expect to lose if a tail event does occur.

It is a more robust risk measure that satisfies all the properties of a coherent risk measure with less restrictive assumptions. Expected Shortfall is defined as the average loss conditional on being beyond a given percentile. E.g. the expected tail loss at the 99^{th} percentile is the probability weighted average of all losses greater than the VaR at the 99^{th} percentile.

Despite the VaR measure being better known than the expected shortfall, the latter has more advantages:

- Expected shortfall is sensitive to the entire tail of the distribution, whereas VaR will not change even if there are large increases in some of the losses beyond the cut-off percentile at which the VaR is being measured.
- Expected Shortfall is a more stable measure than VaR in showing less sensitivity to data errors and less day to day movement due to irrelevant changes in the input data.

- With VaR, negative diversification effects can arise whereas expected shortfall never displays negative diversification effects.

1.5 Limitations of VaR

VaR has its drawbacks as a risk measure. VaR estimates can be subject to errors, model risk and implementation risk. However, such problems are common to all risk measurement systems.

(a) VaR uninformative of tail losses – VaR tells us the most we can lose if a tail event does not occur. It tells us the most we can lose 95% of the time but tells us nothing about what we can lose on the remaining 5% of the occasions. If a tail event (i.e. loss in excess of VaR) does occur, we can expect to lose more than the VaR but VaR itself does not give any indication of how much that might be.

(b) VaR can create perverse Incentives Structures – It is not feasible to use information about VaR at multiple confidence levels and where it is not, the failure of VaR to take account of losses in excess of itself can create some perverse outcomes. For example, an investor using a VaR risk measure can easily end up with perverse positions because a VaR based risk return analysis fails to take account of the magnitude of the losses in excess of VaR. If a particular investment has a higher expected return at the expense of the possibility of a higher loss, a VaR based decision will suggest that we should make that investment if the higher loss does not affect the VaR regardless of the size of the higher expected return and the size of higher expected loss. Such acceptance of any investment that increases expected return regardless of the possible loss and the investor who makes decisions in this way is asking for trouble.

(c) VaR can discourage diversification – Another drawback is that VaR can discourage diversification. The VaR of the diversified portfolio is much larger than the VaR of the undiversified one. So, a VaR measure can discourage diversification of risks because it fails to take into account the magnitude of losses in excess of VaR.

(d) VaR not sub-additive – Sub–additivity means that aggregating individual risks does not increase overall risk. Sub-additivity matters for a number of reasons. If the risks are sub-additive then adding risks together would give us an overestimate of combined risk. This facilitates decentralised decision making within a firm as we can always use the sum of the risks of the units as a conservative measure. But if the risks are not sub-additive, adding them together gives us an underestimate of combined risks, and this makes the sum of risks effectively useless as a risk measure. In risk management, we want our risk estimates to be biased or unbiased conservatively.

2. STRESS TESTING

Stress testing as a formal discipline for risk and capital management was born out of financial crises. Stress tests had previously been carried out for certain types of risk or for specific portfolios, but rarely for all the risks faced by an entire enterprise. For example, market risk stress testing was widely adopted in 1990s to supplement VaR measures, whose calculations tend to underestimate

extreme losses. While these narrow stress tests were useful for managing specific risks or portfolios, they shed light on the overall effect that a stress event would have on an institution.

2.1 Role of Enterprise wide Stress Testing

The impetus for setting up enterprise-wide stress testing in most jurisdictions was a regulatory requirement around capital adequacy assessment. As a result, the early use of stress testing was narrow, focusing on whether there was sufficient capital to survive a stress event and what capital actions such as dividend payments etc. were possible. However, financial institutions have since built up their stress testing capabilities and explored ways of using it to the meet broader risk management and business objectives, specifically, for which applications or decisions will stress testing, will be a key input or a driver? Should risk appetite be articulated based upon tolerances in a stress environment? Should capital requirements from stress testing be used for performance management or loan pricing?

Various Reasons for incorporating stress testing results into a broader set of such risk and business applications.

- **Binding Constraint** – Stress test results have become the binding constraint for evaluating capital adequacy and the key driver of dividend policy for many institutions.
- **Management attention** – Given its linkage to dividend payments, as well as the governance requirements demanded by regulators, stress testing has the attention of senior management and the board of directors.
- **Intuition** – Many users find stress results to be more intuitive than other risk metrics because they are presented in an accounting framework, similar to other external communications regarding the institution's financial condition.
- **Transparency** – As outcomes are linked to casual factors in stress testing, such results are also more transparent and easier to understand than other risk metrics (such as economic capital).
- **Consistency** – The enterprise wide stress testing usually piggybacks the budgeting and planning process, which gives a degree of consistency with the inputs and approaches accepted already in a well established process.

2.2 Applications of Stress Testing

Almost all surveyed institutions use stress testing to measure capital adequacy. However, half or more also use it for risk reporting, risk appetite, limit setting and management, and various planning exercises (e.g. financial, strategic and contingency)

Examples of such extended uses of stress testing are:

- **Risk Reporting** – Stress testing results are often used to report levels of risk in business activities – for example, by reporting the credit losses by portfolio in various stress

scenarios would cause in specific portfolios, or by showing a business unit's contribution to the P&L in a stress scenario.

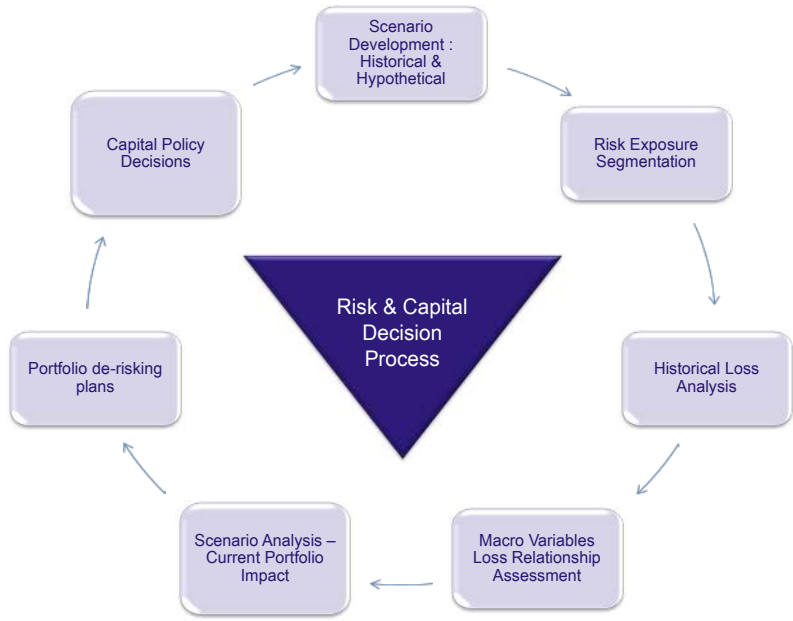
- **Strategic Planning** – These results are increasingly integrated into business planning as institutions look to understand the impact of stress scenarios on alternative strategies and especially on the ability to pay dividends.
- **Risk Appetite** – Stress testing is increasingly being integrated into risk appetite, using tolerance for outcome in a stress to set risk appetite and cascade it down to risk appetite/ tolerance to individual products/ businesses.
- **Limits** – Stress testing expressions of risk appetite are often cascaded into limits at the enterprise level.

To a lesser extent, banks are using stress testing to inform capital allocation, credit portfolio structuring, performance measurement and management, pricing and original strategy.

Uses	*Description*	*Key Challenges*
Capital Adequacy	Ensuring Institution maintains sufficient capital in line with risk appetite	Managing between regulatory stress testing based and economic capital views of required capital and risk
Risk Measurement and Reporting	Communicating risk exposure across the organisation	
Risk Appetite Statement	Definition of the institution's high level, risk related objectives and constraints	
Contingency Planning	Contingency measures such as capital raising and balance sheet reduction	NA
Strategic Planning	Medium term planning of strategy and targets around business units, geographies and products	Cultural shift in some cases to incorporate stress scenarios as a planning scenarios
Financial Planning and Budgeting	Annual exercise to forecast revenues and expenses, and allocate budget across businesses	Organizational challenge to achieve financial buy in on risk metrics
Limit Setting	Setting risk limits at business, product & portfolio level	Scenario severity used for establishing limits and measuring risk against limits is difficult to define objectively
Risk Measurement	Measuring and monitoring usage	

against limits	of risk limits	
Capital Allocation	Allocation of economic and regulatory capital at granular portfolio and business line level	Stress testing produces a narrow view of risk that may not be well suited to allocation and achieving consistency across exposures
Performance measurement and management	Measurement of risk/return of portfolios and business lines	Stress results are less accurate at granular levels at which capital allocation is needed for performance measurement
Pricing	Transaction level pricing and decision support	Stress results are less accurate at granular levels at which capital allocation is needed for pricing purposes

2.3 Stress Test Process



The above exhibit clearly provides a step-by-step process by which stress testing can be integrated into the decision-making system of a typical financial institution. The first step in the process is the generation of various scenarios. The scenario development incorporates both historical and hypothetical states of macroeconomic variables. It is important to select scenarios that appropriately reflect the idiosyncratic business profile of a particular financial institution.

The second step involves the segmentation of the current risk exposures with particular focus on risk concentration. It is essential to have detailed record of historical losses that correspond to the same level of granularity as the current exposure to enable temporal analysis. Historical losses in

the form of defaults, loss severities, and exposure details are explained by macroeconomic scenarios using regression based techniques.

The consequent relationships are then applied to the current portfolio to generate current assessments of income and expenses, losses and capital ratios etc. These results are then compared to the desired risk appetite of the financial institution. In case of a mismatch between actual and potential risk appetite, de-risking options could have an impact on the capital policy decisions of the financial institutions especially decisions involving dividends, share buybacks and compensation policies. The entire process is subjected to governance oversight at every level, beginning with scenario and model validation, to internal controls over data, and finally ending with clear communication and review by senior executives and the various board committees.

3. SCENARIO ANALYSIS

Scenario analysis helps firms to look at their businesses and portfolios downside movement which can either be because of a stress event or a downturn scenario. This analysis helps firms to analyse any stressful situation which may or may not have happened in the past. It has been used for years in many areas (e.g. health, economics etc.). Scenarios are basically sequence or development of events which start from one set of assumptions in order to evaluate or map various outcomes of a particular situation.

Generating scenarios can either be event based or portfolio based. In case of event based scenarios, the scenario is generated from events that will cause movements in the relative risk factors. In case of a portfolio driven scenario, first step is to evaluate the portfolio risk vulnerability. It is then translated into adverse risk factor movements.

3.1 Categories of Stress Scenarios

In scenarios, we take into account the impact of adverse and external conditions which can be a big threat to the survival of a company. There are four main categories of scenarios:

- **Normal Stress Scenarios** – The occurrence of these scenarios can be once or twice in ten-year period. This type of scenarios should be manageable within the normal structure of roles and responsibilities for daily decisions. In this scenario, the credit criteria can be made more vigorous and guidelines might need to be tightened, but these fall within the normal scope of regular policy adjustments. These types of events lead to increased loan losses and reduced earnings but they usually do not present a serious threat to the survival of a financial institution.
- **Severe Stress Scenarios** – These are scenarios that one would expect only once or twice in a professional lifetime. The two oil shocks in 1970s triggered unusually severe economic consequences. These episodes represent severe stress scenarios for many institutions. It is normally included in regular stress testing exercises and it will definitely result in declines

in earnings and some period of losses. With proper early warning indicators and timely action, institutions should be able to avoid serious risk of default in this environment.

- **Near-Default Stress Scenarios** – The global financial crises that began in late 2008 falls into this category for many institutions especially those that were involved in the creation and sale of the subprime mortgage securities. Because of this event, some institutions came close to default but were able to weather the storm without assistance from the Government. These types of stress scenarios form the basis for the development of a detailed recovery plan. Such a plan represents an institution's response to extraordinary conditions during which extraordinary actions are required.
- **Stress to Default Scenarios (Reverse Stress Test Scenarios)** – Some institutions failed during global financial crises, this period represented stress to default scenario. It involves extremely unlikely events which force the companies to think about the firm's most serious vulnerabilities and design stress to default scenarios accordingly. Broad organizational involvement is essential when defining appropriate events like failure of a major counterparty, rogue trading losses, internal fraud etc. which might contribute to institutional failure.

3.2 Scenario Selection

The identification of relevant stress events requires the opinions of all relevant experts such as risk managers, economists, business managers, and traders. Stress Testing should include business cycle stresses as well as event specific tail risks. For example, markets with low historical volatility may experience large discrete movements, the scenario in such a case should reflect the potential interaction of market risk, trading liquidity risk, and credit risk for corporate bonds. Effective scenario analysis should take into account how events unfold over time. Scenarios should also address correlations between risk factors and distinguish between static and dynamic scenarios—i.e., one-period versus multi period frameworks. Forward looking stress and scenario tests must specify length, speed and magnitudes of events and should describe dynamics between transactions. If the scenarios are well developed, they can form an integral part of the management culture and have a meaningful impact on business decisions.

3.3 Drawbacks of Scenario Analysis

With a small number of risk factors, the number of alternative scenarios is manageable. As the number of risk factors increases, the number of alternative scenarios could easily become unmanageable.

Another drawback of Scenario Analysis is that it assumes that the scenarios are equally probable. This ignores the correlations between the risk factors. Although stress testing does allow risk managers to identify major risks, it is subjective in deciding how serious the risks are. The risk manager could generate an ever larger number of scenarios and uncover more extreme events. But

these potential losses might not be significant. Implausible losses might be considered and plausible losses might not be discovered.

3.4 Basel Committee on Banking Supervision (BCBS) Principles for Sound Stress Testing Practices and Supervision*

**Source: Basel Committee on Banking Supervision*

1. Stress testing should form an integral part of the overall governance and risk management culture of the bank. Stress testing should be actionable, with the results from stress testing analyses impacting business decisions of the board and senior management. Board and senior management involvement in the stress testing programme is essential for its effective operation
2. A bank should operate a stress testing programme that promotes risk identification and control; provides a complementary risk perspective to other risk management tools; improves capital and liquidity management; and enhances internal and external communication.
3. Stress testing programmes should take into account of views from across the organization and should cover a range of perspectives and techniques.
4. A bank should have written policies and procedures governing the stress testing programme. The operation of the programme should be appropriately documented.
5. A bank should have a suitably robust infrastructure in place, which is sufficiently flexible to accommodate different and possibly challenging stress tests at an appropriate level of granularity.
6. A bank should regularly maintain and update its stress testing framework. The effectiveness of the stress testing programme, as well as the robustness of major individual components, should be assessed regularly and independently.
7. Stress tests should cover a range of risks and business areas, including at the firm-wide level. A bank should be able to integrate effectively, in a meaningful fashion, across the range of its stress testing activities to deliver a complete picture of firm-wide risk.
8. Stress testing programmes should cover a range of scenarios, including forward-looking scenarios, and aim to take into account system-wide interactions and feedback effects.
9. Stress tests should feature a range of severities, including events capable of generating the most damage whether through size of loss or through loss of reputation. A stress testing programme should also determine what scenarios could challenge the viability of the bank (reverse stress tests) and thereby uncover hidden risks and interactions among risks.
10. As part of an overall stress testing programme, a bank should aim to take account of simultaneous pressures in funding and asset markets, and the impact of a reduction in market liquidity on exposure valuation.
11. The effectiveness of risk mitigation techniques should be systematically challenged.

12. The stress testing programme should explicitly cover complex and bespoke products such as securitized exposures. Stress tests for securitized assets should consider the underlying assets, their exposure to systematic market factors, relevant contractual arrangements and embedded triggers, and the impact of leverage, particularly as it relates to the subordination level in the issue structure.
13. The stress testing programme should cover pipeline and warehousing risks. A bank should include such exposures in its stress tests regardless of their probability of being securitized.
14. A bank should enhance its stress testing methodologies to capture the effect of reputational risk. The bank should integrate risks arising from off-balance sheet vehicles and other related entities in its stress testing programme.
15. A bank should enhance its stress testing approaches for highly leveraged counterparties in considering its vulnerability to specific asset categories or market movements and in assessing potential wrong-way risk related to risk mitigation techniques.
16. Supervisors should make regular and comprehensive assessments of a bank's stress testing programme.
17. Supervisors should require management to take corrective action if material deficiencies in the stress testing programme are identified or if the results of stress tests are not adequately taken into consideration in the decision-making process.
18. Supervisors should assess and if necessary challenge the scope and severity of firm-wide scenarios. Supervisors may ask banks to perform sensitivity analysis with respect to specific portfolios or parameters, use specific scenarios or to evaluate scenarios under which their viability is threatened (reverse stress testing scenarios).
19. Under Pillar 2 (supervisory review process) of the Basel II framework, supervisors should examine a bank's stress testing results as part of a supervisory review of both the bank's internal capital assessment and its liquidity risk management. In particular, supervisors should consider the results of forward-looking stress testing for assessing the adequacy of capital and liquidity.
20. Supervisors should consider implementing stress test exercises based on common scenarios.
21. Supervisors should engage in a constructive dialogue with other public authorities and the industry to identify systemic vulnerabilities. Supervisors should also ensure that they have the capacity and skills to assess a bank's stress testing programme.

4. COUNTRY RISK

Country Risk is broader concept which covers the adverse impact of host country's economic, financial and political environment. This risk is most important in case of Multinational National

Corporations (MNCs) which establishes their business in different countries away from the country where they are registered.

4.1 Types of Country Risk

The analysis of Country Risk is not important not only because it impacts the profitability of MNCs but also important for the investors who invest their money through FPI, FDI etc. Let us now discuss the major types of Country Risk.

4.1.1 Political Risk

This risk mainly arises out of the changes in the political scenarios as well as adverse decisions by the ruling Government. The various types of political risk which ultimately affect the profit of the MNCs from the operations in the host country can be described as follows:

(i) *Nationalisation or Expropriation Risk*: This is most common form of risk wherein host country takes over the business of MNCs without or with inadequate compensation.

(ii) *Exchange Control Risk*: This form of risk prevents the MNCs to get converted their earning from local currency to foreign currency to repatriate the same to home country of MNCs. Due to this restrictions even investors in MNCs business also suffer a lot.

(iii) *Taxes, Rule and Regulation Risk*: This risk arises mainly due to a sudden or dramatic change in Rule and Regulations governing the host country. These sudden changes can be in any of following type of forms:

- Unanticipated increase tax rates applicable for MNCs operating in the host country.
- Compulsion to hire local workforce.
- Compliances of stricter environmental standards.

(iv) *Inefficient Legal System:* High level of red tapism and corruption at local and higher level pose a serious risk for MNCs operating in the host country as it leads to uncertainty and high cost of operation.

(v) *Repudiation of Contracts*: This type of risk arises on account revocation of earlier awarded turnkey projects by the Government of host country without adequate consideration and damages. This risk is also called indirect expropriation risk.

4.1.2 Financial and Economic Risk

The main risk covered in this category is the Sovereign Risk i.e. default in repayment of borrowing by the Government of host country.

Although Government of host country can easily repay the loan by printing more currency notes but it will depreciate value of its currency. The sovereign risk hamper the reputation of the country severely from investment point of view but it saves a lot of foreign exchange of the Government.

To identify such types of risk well in advance following economic variables can be used:

- Ratio of country's Import to its Official Reserve
- Ratio of Import to its Export
- Balance of Payment Surplus/ Deficit on current account.
- Country's Debt Service Ratio
- Country's external debt to its GDP

4.2 Country Risk Management Process

As discussed above Country Risk is a major issue of concern in overall management of business. Broadly speaking the country risk management process involves the following steps:

(i) *Identification of Risk:* First and foremost, step in country risk management is identification of risk. The various quantitative and qualitative techniques can be used to identify the risks.

(ii) *Analysis of Risk:* Once the risk is identified the next step is analyse the same from various angles.

(iii) *Evaluation of Risk Management Techniques:* Evaluation of various techniques to manage the risk is carried out.

(iv) *Selection of suitable techniques:* Once various techniques have been evaluated next steps comes of selection of most suitable technique to manage the risk.

(v) Implementation of Techniques: The techniques to manage the risk are implemented.

(vi) *Control:* Once the selected techniques are implemented they need to be reviewed on periodic and if required they are revised.

4.3 Country Risk Assessment Tools

Broadly Country Risk Assessment tools can be divided into following two categories:

(1) Qualitative Tools (2) Quantitative Tools

Now let us discuss each of these tools one by one.

4.3.1 Qualitative Tools

This is one of the simplest techniques for country risk assessment to rank the countries. The methods employed are:

(i) **Numeral Coding:** In this method, after considering various factors, a number is assigned to a country. While the highest number indicates lesser risk, the lowest number indicates higher risk.

(ii) **Colour Coding:** Different colours can be used to indicate the level of country risk. While Red Color indicates higher risk, Green Colour indicates a risk free zone.

(iii) **Combination of Numeral and Colour:** A combination of colour and numeral is also used to indicate relative level of country risk.

(iv) **Other Methods:** In addition to above, other methods can also be used which are as follows:

(a) *Grade Based Rating* – The grade can be assigned such as S & P, Moody's and Fitch assigns rating. For example, while USA been assigned rating of Aaa, AA+ and AAA by these agencies respectively of safer zone, Venezuela has been assigned rating Caa, B- and C indicating riskier zone.

(b) *Event Driven* – A very specific negative event such as removal of current government by military or sovereign default etc. assessed with the probability of happening.

For example, for India, due to its democratic system, the possibility of taking over of Government by military is rare and hence 0% probability can be assigned for this happening. On the other hand for same event, 70% probability can be assigned in case of Pakistan.

4.3.2 Quantitative Tools

Generally, quantitative tools are related to economic measures such as GDP, Forex rates and services, FDI etc. Other numbers include Growth in Industrial Production, Population Growth, etc. Some of the indices that can be used for Country Risk Analysis are following:

S. No.	*Index*	*Basis*
1	Corruption Perception Index	It is one of the most popular indicator published by Transparency International. The ranking is numeral based ranging from 0-10. While 0 indicate least corrupt, 10 indicate highly corrupt.
2.	Democracy Index	Published by Economic Intelligent, countries are classified into following four groups. • Full democracy (8 to 10) • Flawed Democracy (6 to 10) • Hybrid Regime (4 to 5.9) • Authoritarian Regime (0 to 3.9) This index is based on following 5 categories : ❖ Electoral process pluralism ❖ Civil liberties ❖ Functioning of Government ❖ Political Participation ❖ Political Culture
3.	Freedom in the world	This survey is conducted by Freedom House and provides on the basis of study of Political rights and civil liberties. It uses rating based on 1-7 scale indicating 1 being most free and 7 being least free.
4.	Gini Coefficient	It is one of the most popular index to gauge the rich-n-poor income countries. It measures inequality in income

		distribution. It uses scales 0 to 1, where 0 indicates total equality and 1 indicates total inequality.
5.	Global Peace Index	This index is published by Vision of Humanity and derived from key information such level of crimes, violence, military expenditure etc.
6.	Human Development Index	Published by UN rates, the countries on the basis of following factors: ❖ Education level ❖ Literacy Rate ❖ Year of Schooling ❖ Income ❖ Life Expectancy and ❖ Standard of Living It uses the scale of 0 to 1, where 0 being the least developed while 1 being the highest developed.

CHAPTER 6

CREDIT RISK MEASUREMENT AND MANAGEMENT

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

- Understanding the component of credit risk
- Evaluating credit risk
- Mitigating Credit risk
- Qualitative and Quantitative techniques to manage risk
- Credit scoring models

1. UNDERSTANDING CREDIT RISK

Credit is the basis of business though it is difficult to define but it can be termed as amount of money that will be paid later in exchange of some goods or services received earlier.

Since, it involves a commitment to pay in future period and future is uncertain it involves the risk. Hence, credit risk can be defined as refusal or inability of credit customer to pay the owed sum partially or in full or in time.

Credit Risk is also known as counterparty risk.

While in non-banking businesses the credit risk is related to promised payment for goods and services supplied, in the context of banking business it means failure or refusal to refund the loan account by the borrower in full or partially in time.

1.1 Two Way Risk

The definition of credit risk can also be viewed from other angle or other side i.e. receiver of goods or borrower in case of banking. This risk lies in not supplying the committed supply of goods by the seller leading to production halt or other results for the buyer.

Similarly in banking business the borrower faces the risk of withdrawing of lending facilities by the bank.

1.2 Risk – Return Trade Off

As discussed earlier credit is the basis of business and accordingly, while decision to give credit to be taken there should be a tradeoff between the risk and return (reward) for the supplier or lender. In case of banking business risk is greater when larger amount of credit is granted or when credit is granted for longer periods.

The optimal credit decision would maximize return. The trade-off between risk and return in the context of Credit Risk calls for following decisions:

i) How much Credit Risk should be accepted in return of increase in sale or business in case of banking?

ii) How much compensation should be added while pricing the product?

iii) Placing of Credit Cap or limit for each customer.

iv) Acceptance or rejection of customer's request.

1.3 Credit Risk in Capital Market

Credit Risk analysis from Bank's point of view will be an umbrella covering credit risk of other financial institutions. A bank acts as intermediate between provider of funds and seeker of funds. Bank accepts deposits from one group and provides funds to other group. Since bank grants credit it accepts the risk on regular basis. Hence, banks evaluate their experience and incorporate lessons from failure in a routine manner.

Banks caters both segments wholesale as well as retail segments. The main distinction between these two segments is complexities of financial products involved. For example, in case of retail segments the banking product may generally range from credit card to housing loans, in case of whole sale segment there are 'n' number of financial products. Main sources of seeker of bank's fund are corporates, ranging from small to large capitalization.

2. COMPONENTS OF CREDIT RISK

Broadly, credit risk can be divided into following components:

(i) Default Risk – This risk means the missing a payment obligation (of principal or interest or both). Default Risk can be measured by probability of default. It depends on credit worthiness of a borrower which in turn depends upon various factors such as management of organization, size of business, strength and reputation of promoters etc.

(ii) **Exposure Risk –** This implies the uncertainty associated with future level or amount of risk. In other words, this risk is mainly associated with unexpected action of other party say prepayment of loan before due date or request for refund of deposit before due date.

In some cases, say for amortized credit such risks does not exists as period of receipt is known with greater certainty. Due to uncertainty generally off balance sheet items create such risks. However, in such cases, the exposure is not associated with client's behavior rather behaviors of market which keeps on changing constantly. In case value of derivative position turns out to be positive there is credit risk as it will lose money, if other party defaults. To overcome such risk normally derivative instrument are used.

(iii) **Recovery Risk –** This risk is related to recoveries in the event of default, which in turn depends upon various factors such as quality of guarantee provided by borrower, and other surrounding circumstances. This risk can be minimized through Collateral and Third Party Guarantee. However, existence of these two risk management tool also carries risk.

(a) **Collateral Risk:** Although collateral reduces the credit risk but it happens only if collateral can be sold at a significant value. The quickness in realization of collateral depends upon its nature and prevailing market conditions. In normal course, fixed asset collateral normally carries low realizable value than cash collateral. However, if in buoyant market say in case of a property even a fixed asset in the form of a house property carries a higher value. With the use of collateral, the credit risk becomes twofold:

(i) Uncertainty related to access it and disposing encumbrances which may be legal in some cases.

(ii) Uncertainty related to the value realizable from the collateral which may be subject to various factors. To some extent the 2008 crisis was due to overvaluation of collateral against which borrowers were granted hefty loan and at the time of realisation the collateral value was very less.

(b) **Third Party Guarantee Risk:** This collateral is a kind of simple transfer of risk on Guarantor and in case guarantor defaults then risk again comes back to lender.

3. MEASUREMENT OF CREDIT RISK IN BANKING TRANSACTIONS AND FACTORS AFFECTING THE CREDIT RISK

3.1 Measurement of Credit Risk in Banking Transactions

To measure random loss, following formula can be used:

D X A X (1 – r)

D = Default %

A = Amount of Exposure

R = Recovery Rate %

This default % can also be computed through probability.

3.2 Factors Affecting the Credit Risk

The factors affecting the credit risk of a bank can be divided into following two categories:

(i) ***Internal Factors:*** These factors are internal to the bank, some of these are as follows:

(a) Concentration of credit in particular geographical locations or business segments.

(b) Excessive lending to particular industry is subject to cyclical fluctuations.

(c) Ignoring the purpose for which loan was sought by the customer.

(d) Poor Quality or Liberal Credit Appraisal while granting the loan.

(e) Absence of efficient recovery mechanism.

(ii) ***External Factors:*** These factors are external to the bank and beyond its controls. These factors not only impact the profitability of borrower but also effects their repayment capability. Some of such external factors are as follows:

(a) Fluctuation in Exchange Rate.

(b) Change in Govt. Policies.

(c) Fluctuation in Interest Rates.

(d) Change in Political Environment of the own country.

(e) In case of Foreign project change in Country Risk profile.

4. TYPES OF CREDIT FACILITIES

Banks may offer different types of credit facilities / loans to an individual or companies / corporate depending on the purpose of taking the loan / end use. The tenor of the loan and the security offered would depend on the credit worthiness and nature of credit facility / loan. Loans are typically classified into two types:

(a) Retail Financing – refers to the consumer oriented services offered by banks to individuals rather than companies / institutions. These include mortgages, personal loans, debit cards, credit cards, small equipment loans like farm loans, commercial vehicle loan etc. This is usually called as the B2C type of funding – Business to Consumer.

(b) Wholesale Financing – this is offered by banks to organizations such as large corporate of various sectors, real estate developers, international trade finance businesses, institutions etc. These include term loans, project loans, demand loans, working capital loans etc. This is usually called as the B2B (business to business)

Retail & wholesale financing could either be fund based or non fund based. Different types of loans / credit facilities are enumerated below:

4.1 Fund Based Facilities

Fund based facilities are limits where the borrower gets the money in cash from banks / financial institutions. Few fund based facilities / loans are enumerated below

(a) Personal Loan – also called as consumer loans, these loans are unsecured in nature and are advanced on the basis of borrower's credit history and ability of repay the loan from personal income. Repayment is usually through fixed amount installments over a fixed term. These loans are generally unsecured in nature.

(b) Mortgage loan / Home Loan – a loan that is secured by property or real estate is called a mortgage loan. In exchange of funds received by the borrower to buy a home or property, a lender gets a promise from the borrower to repay the loan within a certain time frame for a certain cost.

(c) Working Capital loans – These loans are for the purpose of financing the everyday operations of a company. Working capital loans are not used to buy long term assets or investments and are instead used to cover short term needs of the business like funding the creditors, accounts payable, wages etc.

Maximum Permissible Banking finance (MPBF) – This is mainly a method of working capital assessment. As per the recommendations of Tandon Committee, the corporates are discouraged from accumulating too much of stocks of current assets and are recommended to move towards very lean inventories and receivable levels. There are 3 methods of working out the maximum amount that a company / borrower may expect from the bank:

- Method 1 – MPBF = 75% of (Current Assets – Current Liabilities other than bank borrowings). The borrower should provide the remaining 25% from long – term sources. The minimum current ratio under this method works out to 1:1
- Method 2 – MPBF = (75% of Current assets) – Current liabilities other than bank borrowings. The borrower should provide the raise finance to the extent of 25% of current assets from long term assets. The minimum current ratio under this method works out to 1.33:1.
- Method 3 – MPBF = 75% of (Current Assets – Core Current Assets) – Current Liabilities other than bank borrowings. The borrower should contribute 100% core current assets and 25% of balance current assets from long term sources. A minimum current ratio under this method works out to above 1.5:1

Various types of working capital loans include Bank Overdraft, Cash Credit, Factoring etc

(i) Overdraft - is a type of fund based lending. It occurs when money is withdrawn from a bank account and the available balance becomes nil. In this situation the account is said to be overdrawn. Thus under this facility, the account holder (individual or corporate) is allowed to withdraw in excess of the balance standing in bank account. Bank fixes a limit beyond which the

account holder will not be able to overdraw the account. Legally, overdraft is a demand assistance given by the bank. It is given for a very short period of time, at the end of which the account holder is supposed to repay the amount. Interest is payable on the actual amount drawn.

(ii) Cash Credit - Cash credit is a short term cash loan to a company. It is just like overdraft facility except there is no need to open a formal current account. Also, this type of funding requires security deposit to secure the loan given by the bank. Legally, cash credit is a demand facility. Interest is payable on actual amount drawn.

(iii) Bill Discounting- Bills purchased / discounted facility - enables the company to get the immediate payment against credit invoices raised by the company. The bank holds the invoices till the customer has actually made the payment. While granting this facility, the bank first satisfies itself about the credit worthiness of the customer and the genuineness of the bill. A limit is fixed in case of the company beyond which the bills are not purchased or discounted by the bank.

(iv) Packing Credit – This is the type of assistance given by the bank to enable the company to buy the goods to be exported. This type of facility is included as short term loan and is in two forms:

(a) Pre shipment packing credit – loan / advance granted to an exporter for financing the purchase, processing, manufacturing or packing of goods prior to shipment.

(b) Post shipment packing credit – loan / advance granted to an exporter after shipment of goods to the date of realization of export proceeds.

(v) Factoring – This is a financial transaction and a type of debtor financing in which a company sells its accounts receivable to a third party (called a factor) at a discount. There are 3 parties involved; the factor who purchases the receivable, the one who sells the receivable and the debtor who has a financial liability that requires him / her to make the payment to the owner of the invoice.

(d) Demand Loan – A demand loan is a rare form of loan that can be called for complete / partial repayment by the lender without any prior notice to the borrower. In other words, when the lender demands the money, the borrower must pay it.

(e) Term Loans – A term loan is repaid in regular payments over a fixed tenor. They usually are of tenor between one to 10 years, but may last as long as 30 years in some cases. These loans are typically extended to mid and large corporate and usually have a unfixed (fixed / floating) rate of interest. They are usually secured in nature. The security could be in the form of movable or immovable assets like plant & machinery, land, building, shares, guarantees etc.

(f) Project / Infrastructure Loans – Project finance / loans are financing of long term infrastructure, industrial projects and public services in which project debt and equity used to finance the project are paid back from the cash flow generated from the project with the project's assets, rights and interests held as secondary security or collateral. These loans are long term in nature and usually have a tenor of 15-20 years. Usually, project financing structure involves a number of equity investors known as 'sponsors' and multiple banks / financial institutions / lenders

called a syndication or consortium of banks. Generally, a special purpose entity called a Special Purpose Vehicle (SPV) is created for each project, thereby shielding other assets owned by the project sponsor for the detrimental effects of a project failure. As a special purpose entity, the project company has no assets other than the project.

(g) Micro finance loans – These loans are extended to individuals / entrepreneurs having small businesses who lack access to banking and related services. The two main mechanisms for the delivery of financial services to such borrowers are (1) relationship – based banking for individuals entrepreneurs and small businesses, and (2) group based models where several entrepreneurs come together to apply for loans and other services as a group.

(h) Real Estate Construction Loans – These loans are extended to developers / builders for construction of residential / commercial buildings including and real estate development. These are large ticket loans and have a long tenor ~ 10 to 20 years.

(i) Agriculture and Allied Services Loans – These are advances given to farmers for purchasing farm equipment's like tractors, harvesters etc. These are small ticket retail loans where the underlying asset is hypothecated to the lender. The tenor of the loan usually matches the life of the underlying assets ~ 4-5 years. The repayment of these loans is aligned to the harvesting cycle usually bi annually.

4.2 Non Fund Facilities

Non fund facilities are where the banks / financial institutions do not commit any physical outflow of funds. It is a nature of promise made by a bank / financial institution in favour of a third party to provide monetary compensation on behalf of their clients. The fund position of the lending bank remains intact. Types of non-fund facilities are as given below:

(a) Bank Guarantee – a bank guarantee is a guarantee from a lending institution / bank ensuring the liabilities of a debtor will be met. In order words, if the debtor fails to settle a debt, the bank covers it. A bank guarantee enables the customer, or debtor, to acquire goods, buy equipment, or draw down loans.

(b) Letter of Credit - Letter of Credit is a non-fund based lending which is very regularly found in international trade.

This facility is given when the exporter and importer are unknown to each other. In this case, the importer applies to his bank (Issuing Bank) in his country to open a letter of credit in favour of exporter whereby the importers' bank undertakes to pay the exporter on fulfilling the terms and conditions specified in the letter of credit.

5. CLASSIFICATION OF ASSETS

Every bank / FI after taking into account the degree of well – defined credit weaknesses and extent of dependence on collateral security for realization, classify its loans & advances into various

classes. RBI in its Master Circular for Banks – Prudential Norms and asset classification have spelled out the following classes:

- Standard Assets – shall mean the asset in respect of which, no default in repayment of principal or payment of interest is perceived and which does not disclose any problem or carry more than normal risk attached to the business.
- Sub – standard assets – shall mean an asset which has been classified as non – performing asset for the period not exceeding 12 months.
- Doubtful assets – an asset which remains sub standard for a period not exceeding 12 months.
- Loss Assets – an asset which is adversely affected by a potential threat of non recoverability due to either erosion in the value of security or non availability of security or sue to fraudulent act or omission on the part of the borrower. Loss asset could be identified as such by the bank / FI or its internal or external auditor

Non Performing Asset (NPA) shall mean an asset, in respect of which, interest has remained overdue for a period of 3 months or more.

Banks write off assets which are non collectable removing it from their balance sheets. A reduction in the value of an asset or earnings by the amount of an expense or loss is called write off.

6. EVALUATING CREDIT RISK

Companies who are in lending business must understand the importance of the credit risk and they should take a note of what sort of credit risk its customers are exposed to. Especially during the hard time, customer or the lender can affect badly due to in accurate credit risk management. This is very important as we need to evaluate the credit risk associated with the customers. Companies and consumers alike who are hit by hard economic times will either try to stretch out their payments or, worse, fail to pay at all – something that can be disastrous for a small, growing business.

In this section, let's understand what are the ground rules to assess credit risks of the customer.

(1) **Understand the reality:** As a lender you need to ensure that you made your customer aware of all the charges and fees associated with the credit which you are planning to extend to the customer. This is critical as customer might be at negotiation stance to have maximum benefit from your line of credit. Longer time he takes to negotiate, there is high possibility that pay off will be late. So communicate the implicit and non-implicit costs that associated with it. Even administrative aspects are also important as they sometime drive the business decision to have line of credit or not.

(2) **Check the credibility:** It may be possible that customer externally looks reliable to the organization, but that does not mean that the customer has full ability to pay off appropriately

and regularly. You need to understand the credibility that the customer possesses. And for that purpose, lender organization should rely on the reports which are available. Or they can consider going through the credit scoring agencies to ensure the customer has the paying ability. Even asking for the basic information will provide you a rough idea about the credit history of the customer. It always better to take the help of professionals during this step. Engage the professional and rely on their expertise. During this stage, credit evaluation is very critical.

(3) **Ask and Check the references:** It's absolutely ok to ask customer for the references, List of creditable clients are much more reliable source than anything else. It's important to ask for the lender organization to understand who all have been given trade credit from in the past and how old are the relationship with such counterparty. This will establish a pattern to understand if the customer has a tendency to maintain the business relation or it's just a pure business. Also, asking reference from the third party proves to be independent source to verify the commitment made by the customers.

(4) **Due Diligence:** When a lender is convince to provide a line of credit to the customer, it is his duty to have proper due diligence in place to ensure the line of credit is being placed in safe pair of hands. Irrespective of the professionals involvement in due diligence process, lender still has the moral responsibility to perform the due diligence on its own. This can be achieved by simply visiting the website, assessing the market creditability etc. Basically, publically sourced information is pretty useful in such cases.

(5) **Recovery:** Lender organization or its employee must understand that every single rupee invested in the customer has cost involved in it. An effort should be made to ensure that this minimal cost of capital should be recovered from the customer. This can be achieved by simply asking your prospect for a deposit or the collateral.

(6) **Nature of business**: Once should not hesitate to ask for the nature of business in which borrower is dealing with. This will give a fair bit item on risk exposure and also provide adequate comfort to the lender.

7. MITIGATING CREDIT RISK

7.1 Identification of Credit Risks

Identifying the credit risk is the first step in credit risk management. This is the step where the potential risks are identified for a business. All the risks identified may not have major impact on the organization. But this, broaden way helps to identify the realistic view and develop cost effective strategies for them. Financial institutions have the major credit risk in the form of loan, advances, debt given. Hence, it is necessary to study the borrower's profile to understand borrower's financial stability, regularity in payments (from CIBIL), default ting nature, if any, education, source of income.

Apart from this major risk other minor risks such as foreign exchange risk, inter-bank transactions, letter of credit, derivative transactions like future, options , swaps and likewise. Financial Institutions also needs to resolve the following issues: Magnitude of risk arising from large complex organization structure, Geographical spread of the operations of the above organizations, and borrowing pattern of large organizations.

The historical method of risk identification involves the identification of types of risk credit, market, operational and liquidity. This approach is based on traditional method of measuring risk and capital adequacy. However, the new approach to risk identification involves testing of the organizations to stressful situations. This helps the institutions to test, develop their own vulnerability to stress.

7.2 How Credit risk is Mitigated

We all know that credit risk is inevitable. But - mitigating the credit risk is a way where one can lessen; reduce the impact of credit risk. This is one of the steps in credit risk management. There are different ways and means to mitigate the credit risk. Banks may use various techniques which reduce their exposure to individual customers and transactions. The taking of guarantees and security to support the obligations of the primary borrower pre-dates capital adequacy rules by many centuries. The desire to avoid loss is simply a feature of prudent banking and is by no means intimately associated with the lender's capital position.

Basel II has suggested the two broad categories of risk mitigation. These are funded and non – funded risk mitigation. As the name suggests, funded credit risk mitigation is that way of risk mitigation where a bank has recourse to cash or buyers asset in order to money owing to it. The concept of funded credit protection refers to the nature of the asset which forms the available security.

As per Basel II norms, following are the different types of funded credit risk mitigation methods:

(a) On Balance Sheet Netting. On balance sheet netting of mutual claims/reciprocal cash balances between the bank and the counterparty creates effective security and collaterals. This norm accordingly be recognised as an acceptable form of credit risk; in order take in account a funded credit risk mitigation, the underlying arrangement has to go through the legal test.

(b) Collateral: The assets/security which are retained or deposited with bank against grant of any loan advances, debt or credit lines. The typical examples are

- Cash or cash equivalents – Cash or Hand loans
- Gold Pledging
- Corporal Debt Securities
- Debt securities issued by banks, local authorities and certain other entities which meet stated credit quality criteria;

- ♦ Short term debt securities with an acceptable rating;
- ♦ Equities or convertible bonds listed on the various indices
- ♦ Units in a collective investment scheme such as mutual funds, provided that they have a daily price quotation and invest only in instruments which are themselves eligible for recognition under (i) - (vi) above or as specified under the by-laws.

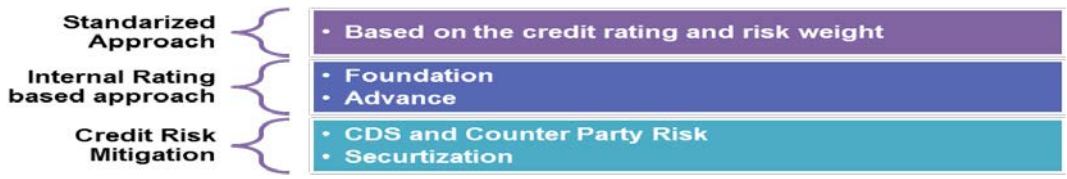
On the other hand, Unfunded credit risk mitigation process, involves an unsecured obligation of a third party. It is implicit in this concept that the entity providing the credit protection is more creditworthy than the primary borrower, thus allowing a reduction in the capital which the bank must ascribe to the transaction at hand.

Since no specific asset is available by way of security in the context of unfunded credit protection, it follows that the rules focus on (i) the creditworthiness and reliability of the provider and (ii) the validity and enforceability of that party's obligations.

As a result, credit protection is only "eligible" for these purposes if it is provided by an appropriate counterparty. These include:

- National Governments/Central Banks;
- Regional Or Local Governments;
- Multilateral Development Banks;
- Certain International Organisations;
- Banks;
- Other corporate which meet stipulated credit requirements

BASEL II is the most recognized and modern norms in the financial market. Basel II was pillar model which provides the guidance and the recommendation on the banking rule and the regulations. The norms was initially published in year 2004. BASEL II has made the concision effort to ensure that a bank has adequate capital for the risk the bank exposes itself to through its lending, investment and trading activities. Out of three main pillars in Basel II norms, very first pillar is more focus on Credit risk. Per the Basel II norms, The credit risk component can be calculated in three different ways of varying degree of sophistication and as prescribed by Basel II.



Basel II has forced financial institution to comply with the requirements including the stringent guidance and assessment by credit risk by private players. Detailed documentation is available at (http://www.bis.org/publ/bcbsca.htm)

Other techniques or methods of credit risk mitigation include the following:

(a) **Risk-based pricing:** Where the lender feels that borrower is more likely to do default, the lender may increase the interest rate. This is called as risk-based –pricing. In the method the probability of default is hedge with the incremental interest rate. This type of method may not provide good worth in today market considering the competitiveness.

(b) **Credit insurance:** The lender may purchase the credit insurance under which the risk is transferred from lender to the issuer on payment of certain amount. The best example is the housing loan insurance. Where the lender asks the borrower to purchase the requisite insurance to ensure the mortgage is secured. This will ensure that the in case of borrower becomes as a default party, lender can re-coupe the loan by way such insurance

(c) **Tightening:** Under this method, lender may tighten the norms of lending including the amount to be lend. For an example, the lender may mitigate the credit risk by reducing the payment period from 45 to 30 days. Reducing the credit period will provide the early warning indicators to the lender to analyse and act upon the situation.

(d) **Diversification:** Lenders may lend to number of small borrowers instead (kinds of borrower) to diversify the lending pool. This approach will help lender to diversify the risk associated with each credit line extended. For example, high credit rating borrower ultimately funds the low credit risks.

(e) **Covenants:** The lender may put some covenants like periodic review of financial position, repay the loan in full in case of certain events like debt coverage ratio shows improvement. Sometimes, lender also perform an independent audit on the business operation with the proper consent and according to the contractual agreements.

8. QUALITATIVE TECHNIQUES OF CREDIT RISK MANAGEMENT

Credit Risk is the most critical of all risk for a bank / financial institutions and the management of it is the most crucial for survival of any banks / FIs.

8.1 Borrower / Transaction specific risk management

Financial institutions / banks attempt to mitigate the risk of lending to unworthy borrowers by performing a credit analysis on individuals and businesses. This process is based on a review of borrowers five C's of Credit viz; Capacity, Capital, Character, Collateral and Conditions. Although each financial institution (FIs) / bank employs it own process of determining the credit worthiness, most FIs / banks pay greater emphasis on borrower's Capacity.

(a) Capacity – This refers to the borrower's ability to repay the loan. The lenders / banks will consider the cash flows generated from the underlying business, timing of repayment and the probability of successful payment of the loan under various stressed scenarios.

(b) Capital – It is the promoters / borrower money invested in the business and is an indicator of how much of promoters / borrowers money is at risk should the business fail. FIs / banks will generally consider the borrowers debt to equity ratio to understand how much money the lender is being asked to lend as against the money invested by the promoters / borrower in the business. High debt to equity ratio indicates that the promoters / borrower already have high levels of debt / loans and could be higher financial risk.

(c) Character – Is the obligation that the borrower feels to repay the loan. Emphasis is given on the past loan repayment track record, credit history, credit bureau score. This analysis pertains to the softer aspect of the borrower's intent to pay rather emphasis on financials, ratios and cash flows.

(d) Collateral – Is a form of security for the lender in case there is default on the loan. In case of default, the lender will take possession of the collateral in place of debt. Collateral can be in the form of tangible assets like land, building, plant, machinery, cash flows, receivables, project assets etc and also in the form of intangible assets like patents, trademarks etc. The loan agreement should be suitably drafted to include all the relevant details of the collateral. The lender would ideally want the term of the loan to match the useful life of the collateral.

(e) Conditions – Additionally, apart from the borrower specific criteria's, lenders may also consider external factors which may affect borrower's financials, cash flows and its underlying ability to repay the loan obligations. End use of the loan / purpose for taking the loan / debt will also be carefully assessed and the transaction will be suitably structured.

Further, a well defined credit approval matrix / delegation need to be in place for approving transactions. For the sake of good order, the approval matrix / responsibility should be joint in nature. Each bank / financial institutions will have an internal credit rating / score card model factoring the parameters enumerated above. Once the loan is approved as per the credit criteria's defined and the same is disbursed, it needs to be monitored in terms of security, cover, repayment track, sector updates etc.

8.1.1 Credit Due Diligence for Retail Financing

Credit due diligence for a retail financing is different from the wholesale financing since the quantum of loan and the complexity of transaction is different. Retail finance credit due diligence is parameterised / score card driven wherein if the borrower fits into a pre defined credit matrix / parameters and gets a score which is above the threshold, loan is approved / sanctioned. The scorecard parameter would be suitably deliberated and considered based on historical experience and keeping in view the dynamic environment. The scorecard based approved portfolio is closely monitored at regular frequency and the parameters are suitably modified based on portfolio's performance.

For e.g: For Farm / tractor loan, parameters / factors like soil fertility, area under cultivation, produce per acre, rainfall / reservoirs levels, make model of the tractor, geography are pre defined and weightages are assigned to each parameter depending on the criticality which will throw up a score for each borrower. These models / score cards are embedded in the loan management system of the banks which result into auto approval of the loan. While the quantum of the loan is small, number of retail borrowers is significantly large and therefore it is time consuming for banks / FIs to evaluate credit for each borrower. Hence credit loan approval for retail financing is primarily score card driven. Parameters could be qualitative and quantitative in nature.

8.1.2 Credit Due Diligence for Wholesale Financing

Credit risk management for wholesale financing is done on case to case basis with greater emphasis on each of the 5C's of credit and in –depth due diligence on account of large amounts and complexities. As part of due diligence process, a detailed appraisal note / information memorandum which captures all the key information of the borrower and the proposed facility / transaction is enumerated. Suitable appraisal / proposal formats are specified for different customer segments like small & mid corporate, large corporate, project finance etc.

For wholesale credits, the detailed appraisal would inter alia cover the following aspects:

- Assessment of project sponsor(s)/ borrower and the group;
- Integrity and reputation of the borrower;
- Track record in the relevant sector, market position and its sensitivity to economic and market developments,
- Sector perspective;
- Technical feasibility evaluation including opinion of external experts if necessary;
- Commercial and economic viability evaluation;
- Debt servicing capability;
- Credit reference from the existing lenders/bankers
- Credit reference checks from credit bureaus;

- Cash flows from the project and its adequacy
- Nature of Security and its enforceability
- Credit rating rationales (if rated by any external agency)
- Whether name of any of the directors of the borrower appear in the list of defaulters by way of reference to DIN/PAN. In case of any doubt arising on account of identical names, business/ credit person will use independent source of confirmation of identity of the director. In no case, declaration to the effect from the borrower will suffice for the purpose
- Adherence to Know Your Customer – Anti Money Laundering (KYC-AML) Policy and guidelines issued by RBI in this regard and review of promoter's status as Politically Exposed Persons (PEPs);
- Interaction with the key management personnel & sponsors to understand their perspective about the project and sectoral business dynamics;
- Site visits
- Risk identification, risk allocation and risk mitigation;
- Security requirements including adequacy and enforceability;
- Put/call options, prepayment etc. backed by assessment of feasibility;
- Ability to infuse capital by the promoters/ shareholders to be ascertained and noted, (Multiple leveraging may camouflage debt-equity ratio, leading to adverse selection of borrowers)
- Adherence to standards, credit framework or guidelines
- Covenants / conditions to be stipulated
- Risk adjusted Returns and Yield management

8.2 Credit Rating Scales

Few leading credit rating agencies in India are as follows:

- Credit Rating Information Services of India Limited (CRISIL)
- Indian Credit Rating Agency (ICRA)
- Credit Analysis and Research Ltd (CARE)
- Fitch Ratings India Private Limited (Fitch)
- Equifax
- Credit Information Bureau India Limited (CIBIL)
- High Mark Credit Information Services
- SME Rating Agency of India Ltd (SMERA)

- Brickwork Rating India Private Limited (Brickwork)

  Rating Scale for Long term instruments is as follows:

AAA (Highest Safety)	Instruments with this rating are considered to have the highest degree of safety regarding timely servicing of financial obligations. Such instruments carry lowest credit risk.
AA (High Safety)	Instruments with this rating are considered to have high degree of safety regarding timely servicing of financial obligations. Such instruments carry very low credit risk.
A (Adequate Safety)	Instruments with this rating are considered to have adequate degree of safety regarding timely servicing of financial obligations. Such instruments carry low credit risk.
BBB (Moderate Safety)	Instruments with this rating are considered to have moderate degree of safety regarding timely servicing of financial obligations. Such instruments carry moderate credit risk
BB (Moderate Risk)	Instruments with this rating are considered to have moderate risk of default regarding timely servicing of financial obligations
B (High Risk)	Instruments with this rating are considered to have high risk of default regarding timely servicing of financial obligations
C (Very High Risk)	Instruments with this rating are considered to have very high risk of default regarding timely servicing of financial obligations
D (Default)	Instruments with this rating are in default or are expected to be in default soon.

A1	Instruments with this rating are considered to have very strong degree of safety regarding timely payment of financial obligations. Such instruments carry lowest credit risk
A2	Instruments with this rating are considered to have strong degree of safety regarding timely payment of financial obligations. Such instruments carry low credit risk
A3	Instruments with this rating are considered to have moderate degree of safety regarding timely payment of financial obligations. Such instruments carry higher credit risk as compared to instruments rated in the two higher categories
A4	Instruments with this rating are considered to have minimal degree of safety regarding timely payment of financial obligations. Such instruments carry very high credit risk and are susceptible to default
D	Instruments with this rating are in default or expected to be in default on maturity.

- Additionally, the rating agencies may apply '+' (plus) or '-' (minus) signs for ratings from AA to C to reflect the comparative standing within the company

The rating agency may also assign outlooks for ratings from AAA to B. Ratings on rating watch will not carry outlooks. A rating outlook indicates the direction in which a rating may move over the medium term horizon on one to two years. A rating outlook can be 'Positive', 'Stable' or 'Negative'. A positive or negative rating outlook is not necessarily a precursor of a rating change.

8.3 Portfolio Risk Management

Once the funds are disbursed, periodic reviews on the portfolio/borrowers/assets are conducted by the relevant Business and Credit Departments. Notwithstanding sound appraisal processes and risk management, some portfolios / accounts may develop weakness on account of changes in internal or external conditions. Mechanisms for monitoring and identifying early warning signals (EWS) should be in place to review the portfolio and identify such weak accounts before they turn NPA. These monitoring mechanisms will help take remedial measures and limit losses. Such monitoring / review can be undertaken through a mix of portfolio and borrower level EWS matrix (indicative parameters and not exhaustive list):

Retail Financing

- Roll forward / roll back rates – (deterioration on days past due / improvement in days past due)
- Infant / Early delinquencies – non payment of first EMI / instalments.
- Performance review across at branch / scheme / program / Relationship Manager etc
- Scorecard parameter reviews

Wholesale Financing

- Early Default Alerts (EDA) in the form of adverse deviations in operational performance and cash inflows vis-a-vis projections.
- Site visit reports.
- Progress report of the project through internal / external agencies including Lenders Engineers vis-a-vis the envisaged / projected performance at the initial appraisal/previous review stage.
- Security margin cover.
- Movement in internal / external rating including suspension/ withdrawal, more specially downward revision in ratings.
- Covenant monitoring.
- Overdue monitoring.

- Credit concentration risk analysis.
- Stress Asset / Watchlist asset monitoring.
- Any other factors / MIS as deemed necessary for effective monitoring and control.
- Special Mention Account classification (SMA accounts) – As per the RBIs framework for "Revitalising Distressed Assets in the Economy" issued in January 2014 has outlined a corrective plan that will incentivize early identification of problem account, timely restructuring of accounts which are considered to be viable, and taking prompt steps by lenders for recovery or sale of unviable accounts. The Corrective action plan includes early recognition of stress and reporting the same to Central Repository of Information on Large Credits (CRILC). Before the loan turns non performing, banks / FIs will be required to indentify incipient stress in the account by creating a sub – asset category viz: Special Mention Account with the three sub categories as given below

SMA sub categories	*Basis of classification*
SMA – 0	Principal or interest payment not overdue for more than 30 days but account showing signs of incipient stress as illustrated in the annex to the framework of Jan 30, 2014
SMA-1	Principal or interest payment overdue between 31-60 days
SMA-2	Principal or interest payment overdue between 61-90 days

Portfolio risk management emanates from a clearly spelled out risk appetite of the organization to meet its strategic objectives. Portfolio Risk Management is predominantly driven through "Concentration Risk Management". Concentration risk in banking term denoting the overall spread of bank's outstanding loan accounts over the number or variety of debtors to whom the bank has lent money. Concentration risk can be in terms of overexposure against a particular borrower / group of borrowers or being over exposed to a particular industry / sector / regions / geography etc. Concentration risk could be managed by setting limits on exposure per borrower or group of borrowers belonging to the same management or limits on industry / sector / geography.

8.4 Credit Risk Rating Process

Credit Risk Rating or Credit Rating is an important tool to manage large ticket exposures credit risk. The rating provides a consistent and common scale for measurement of credit risk of a loan asset in terms of Probability of Default (PD) across products and sectors. Coupled with estimation of Loss Given Default (LGD), it enables the organisation to make an estimate of credit cost for the loan assets and thus, helps to differentiate among loan assets as objectively as possible. PD is measured by the internal rating assigned to the Borrower and assesses the likelihood that the Borrower will default on its debt obligations. LGD is measured by the value of the security/ collateral / cash flow cover (project finance)/ DSRA/other credit enhancements for the particular

facility provided by the Borrower, after applying haircut to each assets sub class, which will form a cover for the outstanding facility, once a default has occurred.

Each Bank / FI would have an internal credit rating model which takes into account critical success parameters relevant for each industry, competitive forces within the industry, regulatory issues while capturing financial parameters, management strengths, project parameters, etc. and the LGD models take into consideration the cover expected to be available for recovery based on asset or cash flows that could be accessed after a default has happened. The LGD model also factors in the estimated time to invoke different types of securities for applying suitable discounting factors.

Each proposed debt commitment is rated before taking a sanction decision and all such ratings of assets in the portfolio are periodically reviewed by banks / FIs. Revised ratings are awarded for the borrower if there is deterioration in the financial parameters from the originally assessed and projected, adverse changes in industry / sector, changes in government regulations etc. Each corporate loan is then assessed for rating migration (upward or downward movement) through out the loan life cycle.

8.5 Credit Loss Estimation

Credit risk being the most prominent risk for banks and FIs and subject of strict regulatory oversight and policy debate needs to be carefully estimated / assessed.

Credit risk management is the practice of mitigating those losses by understanding the adequacy of both capital and loan loss reserves at any given time – a process that has long been a challenge for financial institutions. Various quantification and modelling techniques are being applied in practice for credit risk measurement and management. The estimation around credit risk management necessitates the following measures to be quantified for capital and provisioning purposes:

- **Expected Loss:** The average loss that the organisation expects from an exposure over a fixed time period, usually a year
- **Unexpected Loss:** The loss that the organisation incurs over and above the average loss expected from an exposure over a certain time period, usually a year. It is also known as the variation in Expected Loss and includes the possibility of large losses

There are 3 integral components (known as **risk components**) that are required to be estimated for credit risk quantification.

I. **Probability of Default (PD):** It refers to the probability / risk / chance of a borrower defaulting* on the payment of the credit obligations, within a given time horizon, usually one year.

II. **Loss Given Default (LGD):** It refers to the loss likely to be suffered in the event of a default occurring in an exposure. It takes into account the amount of recoveries likely to be made post default.

III. **Exposure at Default (EAD):** It refers to the amount that is exposed to the default risk. It is usually the amount outstanding as well as undrawn commitment that is expected to be drawn by the time of default.

A range of statistical or expert judgement techniques are used to estimate risk components (PD, LGD, EAD) for both funded and non-funded exposures.

*Default definition as per Bank for International Settlement (BIS) - A default is considered to have occurred with regard to a particular obligor when either or both of the two following events have taken place: (i) The bank considers that the obligor is unlikely to pay its credit obligations to the banking group in full, without recourse by the bank to actions such as realising security (if held). (ii) The obligor is past due more than 90 days on any material credit obligation to the banking group.

8.5.1 Estimation of Probability of Default (PD)

Given the requirement or constraints, PD can be calculated for a single obligor or a group of obligors with similar credit risk features. The former method is more prevalent in corporate book and the latter in retail book.

Types of PD Estimation

1. **Pooling Method:** This method relies on the historical data and assumes that past defaults are a reasonable predictor for future likelihood of losses. Historical PD is calculated by taking the ratio of the facilities that have defaulted to the total facilities that existed in the concerned time frame, usually a year. In this method, the facilities are divided into different categories/pools based on their risk drivers.

2. **Statistical Method:** Data on characteristics of retail obligors and corporate obligors can be used to estimate their respective probability of defaults. Various statistical techniques can be employed on the data to estimate PD for defined time horizons. The statistical model specifies the relationship between the inputs and the outcome – PD. The parameters determined depend on the data used to develop the model.

One of the most recommended statistical techniques to estimate PD is logistic regression. This method of regression is applicable when the dependent variable is binary i.e. takes one of the two available values i.e. default & non default. This variable indicates whether or not the loan/debt has gone into default over a certain time horizon, usually a year. Some of the common variable sources used to estimate the PD of a corporate are financial statements, owner's data, type of loan, size of loan, and industry of the company. Similarly, for retail obligors, variable sources could be customer demographics, income statistics, age of loan, and number of late payments etc.

3. **Structural Method:** This method is generally applicable for listed corporate entities wherein structural models are used to calculate the probability of default for a corporate based on the value of its assets and liabilities. This technique is a sophisticated approach and requires valuation models to be applied for firm valuation.

Over a period of time, we propose to collate other statistical relevant inputs to explore possibilities of using statistical method for PD calculation as well as to improve portfolio quality.

8.5.2 Estimation of Loss Given Default

A bank / financial institution incur a loss when a company to which it has lent money, or entered into a contract with, defaults on its payments. Loss Given Default (LGD) is defined as the percentage loss rate on EAD, given the obligor defaults. It provides the loss that a bank is bound to incur when a default occurs. The components of the loss that will be incurred, given the obligor defaults are Loss of principal, Carrying costs and Workout expenses

Value of LGD varies with the economic cycle, so the following variations in LGD are defined:

- Cyclical LGD (Point-in-Time LGD) - Cyclical LGD is calculated based on the recent data and its value depends on the economic cycle
- Long-run LGD (Through-the-Cycle LGD) - Long-run LGD represents the average long-term LGD, corresponding to a non-cyclical scenario that is not dependent on the time the LGD is calculated
- Downturn LGD - Downturn LGD represents the LGD at the worst time of the economic cycle

The current document is based on cyclical LGD calculation for our portfolio. As the data gets enriched over time, the long run LGD would be gradually adopted.

8.6 Credit Default Swaps

A Credit Default Swap (CDS) is a financial swap agreement that the seller of the CDS will compensate the buyer (usually the creditor of the reference loan) in the event of a loan default (by the debtor) or other credit event. That is, the seller of the CDS insures the buyer against some reference loan defaulting. The buyer of the CDS makes a series of payments (the CDS "fee" or "spread") to the seller and, in exchange, receives a payoff if the loan defaults. It was invented by Blythe Masters from JP Morgan in 1994.

In the event of default, the buyer of the CDS receives compensation (usually the face value of the loan), and the seller of the CDS takes possession of the defaulted loan. However, anyone can purchase a CDS, even buyers who do not hold the loan instrument and who have no direct insurable interest in the loan (these are called "naked" CDSs). If there are more CDS contracts outstanding than bonds in existence, a protocol exists to hold a credit event auction; the payment received is usually substantially less than the face value of the loan.

Credit default swaps have existed since 1994, and increased in use in the early 2000s. CDSs are not traded on an exchange and there is no required reporting of transactions to a government agency. During the 2007–2010 financial crisis the lack of transparency in this large market became a concern to regulators as it could pose a systemic risk.

As an example, imagine that an investor buys a CDS from AAA-Bank, where the reference entity is Risky Corp. The investor—the buyer of protection—will make regular payments to AAA-Bank—the

seller of protection. If Risky Corp defaults on its debt, the investor receives a one-time payment from AAA-Bank, and the CDS contract is terminated.

If the investor actually owns Risky Corp's debt (i.e., is owed money by Risky Corp), a CDS can act as a hedge. But investors can also buy CDS contracts referencing Risky Corp debt without actually owning any Risky Corp debt. This may be done for speculative purposes, to bet against the solvency of Risky Corp in a gamble to make money, or to hedge investments in other companies whose fortunes are expected to be similar to those of Risky Corp.

If the reference entity (i.e., Risky Corp) defaults, one of two kinds of settlement can occur:

- the investor delivers a defaulted asset to Bank for payment of the par value, which is known as physical settlement;
- AAA-Bank pays the investor the difference between the par value and the market price of a specified debt obligation (even if Risky Corp defaults there is usually some recovery, i.e., not all the investor's money is lost), which is known as cash settlement.

The "spread" of a CDS is the annual amount the protection buyer must pay the protection seller over the length of the contract, expressed as a percentage of the notional amount. For example, if the CDS spread of Risky Corp is 50 basis points, or 0.5% (1 basis point = 0.01%), then an investor buying $10 million worth of protection from AAA-Bank must pay the bank $50,000. Payments are usually made on a quarterly basis, in arrears. These payments continue until either the CDS contract expires or Risky Corp defaults.

All things being equal, at any given time, if the maturity of two credit default swaps is the same, then the CDS associated with a company with a higher CDS spread is considered more likely to default by the market, since a higher fee is being charged to protect against this happening. However, factors such as liquidity and estimated loss given default can affect the comparison. Credit spread rates and credit ratings of the underlying or reference obligations are considered among money managers to be the best indicators of the likelihood of sellers of CDSs having to perform under these contracts.

Key features of RBI guidelines on CDS

- Participants in the CDS market are classified as either users or market makers. User entities are permitted to buy credit protection (buy CDS contracts) only to hedge their underlying credit risk on corporate bonds. Such entities are not permitted to hold credit protection without having eligible underlying as a hedged item. The users cannot buy CDS for amounts higher than the face value of corporate bonds. This is the most important point of difference, as there was no such limitation in United States of America prior to 2008, and hence many Institutional players had taken huge long positions (in CDS) without having any exposure to reference asset.
- Since the users are envisaged to use the CDS only for hedging their credit risks, assumed due to their investment in corporate bonds, they shall not, at any point of time, maintain

naked CDS protection i.e. CDS purchase position without having an eligible underlying bonds held by them and for periods longer than the tenor of corporate bonds held by them.

- The eligible entities under user's category would be Commercial Banks, PDs, NBFCs, Mutual Funds, Insurance Companies, Housing Finance Companies, Provident Funds, Listed Corporates, Foreign Institutional Investors (FIIs) and any other institution specifically permitted by the Reserve Bank of India.
- CDS will be allowed only on listed corporate bonds as reference obligations. However, CDS can also be written on unlisted but rated bonds of infrastructure companies. This is another major area of difference between the US markets and RBI guidelines. In United States of America, the CDS were written on various pass through securities like Mortgage Backed Security (MBS), Collateralized Debt Obligation (CDO) etc, whereas as per the RBI guidelines, the CDS are specifically restricted for listed corporate bonds, the obvious reason being that there is no big market of pass through securities in India as it is in US.
- The credit events specified in the CDS contract may cover: Bankruptcy, Failure to pay, Repudiation/moratorium, Obligation acceleration, Obligation default, Restructuring approved under Board for Industrial and Financial Reconstruction (BIFR) and Corporate Debt Restructuring (CDR) mechanism and corporate bond restructuring.
- Since, CDS are traded mainly over-the-counter (OTC), the contracting parties therefore have to agree upon the terms and conditions of the CDS individually. In order to facilitate documentation, and to avoid disputes as to whether a credit event had actually occurred and how a contract should best be settled, CDS contracting parties (in the international and US market) generally refer to the International Swaps and Derivatives Association (ISDA) Master Agreement. In India, the RBI guidelines specifically states that Fixed Income Money Market and Derivatives Association of India (FIMMDA) shall devise a Master Agreement for Indian CDS
- Regarding the Settlement procedures, the RBI Guideline states that the parties to the CDS transaction shall determine upfront, the procedure and method of settlement (cash/physical/auction) to be followed in the event of occurrence of a credit event and document the same in the CDS documentation. However it further adds that for transactions involving users, physical settlement is mandatory. For all other transactions, market-makers have been permitted to opt for any of the three settlement methods (physical, cash and auction), provided the CDS documentation envisages such settlement
- Further, the guidelines specifically provide norms for Prevention of mis-selling and market abuse, wherein it requires protection sellers to ensure that CDS transactions shall be undertaken only on obtaining from the counterparty, a copy of a resolution passed by their Board of Directors, authorizing the counterparty to transact in CDS.
- RBI has also incorporated certain reporting requirements in the guidelines which would require market makers to report their CDS trades with both users and other market makers on

the reporting platform of CDS trade repository within 30 minutes from the deal time. The users would be required to affirm or reject their trade already reported by the market- maker by the end of the day. In addition to these reporting requirements the participants are also required to report to respective regulators (e.g. IRDA for Insurance companies) information as required by them such as risk positions of the participants vis-à-vis their net worth and adherence to risk limits, etc.

8.7 Credit Insurance

Trade credit insurance, business credit insurance, export credit insurance, or credit insurance is an insurance policy and a risk management product offered by private insurance companies and governmental export credit agencies to business entities wishing to protect their accounts receivable from loss due to credit risks such as protracted default, insolvency or bankruptcy. This insurance product is a type of property and casualty insurance and should not be confused with such products as credit life or credit disability insurance, which individuals obtain to protect against the risk of loss of income needed to pay debts. Trade credit insurance can include a component of political risk insurance which is offered by the same insurers to insure the risk of non-payment by foreign buyers due to currency issues, political unrest, expropriation etc.

8.8 Difference between Credit Insurance and Credit Default Swaps

CDS contracts have obvious similarities with insurance, because the buyer pays a premium and, in return, receives a sum of money if an adverse event occurs.

However, there are also many differences, the most important being that an insurance contract provides an indemnity against the losses actually suffered by the policy holder on an asset in which it holds an insurable interest. By contrast a CDS provides an equal payout to all holders, calculated using an agreed, market-wide method. The holder does not need to own the underlying security and does not even have to suffer a loss from the default event. The CDS can therefore be used to speculate on debt objects.

The other differences include:

- The seller might in principle not be a regulated entity (though in practice most are banks);
- The seller is not required to maintain reserves to cover the protection sold (this was a principal cause of AIG's financial distress in 2008; it had insufficient reserves to meet the "run" of expected payouts caused by the collapse of the housing bubble);
- Insurance requires the buyer to disclose all known risks, while CDSs do not (the CDS seller can in many cases still determine potential risk, as the debt instrument being "insured" is a market commodity available for inspection, but in the case of certain instruments like CDOs made up of "slices" of debt packages, it can be difficult to tell exactly what is being insured);
- Insurers manage risk primarily by setting loss reserves based on the Law of large numbers and actuarial analysis. Dealers in CDSs manage risk primarily by means of hedging with

other CDS deals and in the underlying bond markets;

- CDS contracts are generally subject to mark-to-market accounting, introducing income statement and balance sheet volatility while insurance contracts are not;
- To cancel the insurance contract the buyer can typically stop paying premiums, while for CDS the contract needs to be unwound

8.9 Other Qualitative Techniques of Credit Risk Management

Some other qualitative techniques which are generally taken care of while managing the credit risk are discussed as below:

8.9.1 Stipulation of Covenants

Conditions imposed by the lender on the borrower that certain activities will or will not be carried out are called 'Covenants'. Covenants can be affirmative or negative in nature. Covenants are stipulated by the lenders to protect themselves from borrowers defaulting on their obligations due to financial actions detrimental to themselves or the business. Covenants are stipulated at the time of sanction / approval of limits or at the time of review of facilities. Covenants are most often represented in terms of financial ratios such a maximum debt – equity ratio, debt to EBIDTA, minimum debt service coverage ratio etc. Banks / FIs periodically review the covenants to ensure that the same are adhered by the borrower and necessary actions taken in case of breach. Any breach in covenants stipulated could be an indication / early warning for stress in the borrower's repayment capacity.

8.9.2 Collateral / Security

Banks / FIs seek security / collateral for the transactions to adequately secure themselves should the borrower default. RBI has not stipulated any minimum cover for security except for listed shares where the cover should be minimum 2x. Various types of securities depending upon the nature of facilities are:

- Pledge of Shares (listed / unlisted)
- Hypothecation of Movable goods and Receivables
- Mortgage of Immovable assets
- Guarantees
- Lien on Deposits
- Assignment of Insurance policies, Book Debts etc.

8.9.3 Structuring of the transaction

Banks structure large ticket / complex transactions in such a way that complete recourse is available to the lender in case of default by the borrower. Some examples of good structuring are:

- Direct control over escrows / cashflows

- Ring fencing of cashflows
- Identified / cash flows carved out for banks loan repayment hence giving visibility to the repayments
- Board representation / voting rights to the lender
- Priority of repayments over other lenders / creditors
- Exclusive charge or Pari-passu charge on the security with other lenders

8.9.4 Sell Down / syndication / Co- participating / Securitization

All these risk mitigation techniques to prevent one lender from taking exponentially large exposure against a single borrower. Sell down is a technique wherein a large loan is underwritten by a single lender and then down-sold to other investors / banks / FIs for a fixed fee / income. Down-selling could be before or after the loan is disbursed to the borrower. A syndicated loan is a loan offered by a group of lenders that work together to provide funds to a single borrower. Securitization is a financial practice of pooling various types of contractual debt such as residential mortgages, commercial mortgages, auto loans or credit card debt obligations and selling their related cash flows to third party investors as securities.

9. QUANTITATIVE TECHNIQUES OF CREDIT RISK MANAGEMENT

9.1 Altman Z Score

The Z-score formula for predicting bankruptcy was published in 1968 by Edward I. Altman, who was, at the time, an Assistant Professor of Finance at New York University. The formula is used to predict the probability that a firm will go into bankruptcy within two years. Z-scores are used to predict corporate defaults and an easy-to-calculate control measure for the financial distress status of companies in academic studies. The Z-score uses multiple corporate income and balance sheet values to measure the financial health of a company.

The Z-score is a linear combination of four or five common business ratios, weighted by coefficients. The coefficients were estimated by identifying a set of firms which had declared bankruptcy and then collecting a matched sample of firms which had survived, with matching by industry and approximate size (assets).

Altman applied the statistical method of discriminant analysis to a dataset of publicly held manufacturers. The estimation was originally based on data from publicly held manufacturers, but has since been re-estimated based on other datasets for private manufacturing, non-manufacturing and service companies.

The original data sample consisted of 66 firms, half of which had filed for bankruptcy under Chapter 7. All businesses in the database were manufacturers, and small firms with assets of < $1 million were eliminated.

The original Z-score formula was as follows:

Z = 1.2X1 + 1.4X2 + 3.3X3 + 0.6X4 + 1.0X5.

X1 = working capital / total assets. Measures liquid assets in relation to the size of the company.

X2 = retained earnings / total assets. Measures profitability that reflects the company's age and earning power.

X3 = earnings before interest and taxes / total assets. Measures operating efficiency apart from tax and leveraging factors. It recognizes operating earnings as being important to long-term viability.

X4 = market value of equity / book value of total liabilities. Adds market dimension that can show up security price fluctuation as a possible red flag.

X5 = sales / total assets. Standard measure for total asset turnover (varies greatly from industry to industry).

Altman found that the ratio profile for the bankrupt group fell at −0.25 avg, and for the non-bankrupt group at +4.48 avg.

In its initial test, the Altman Z-Score was found to be 72% accurate in predicting bankruptcy two years before the event, with a Type II error (false negatives) of 6% (Altman, 1968). In a series of subsequent tests covering three periods over the next 31 years (up until 1999), the model was found to be approximately 80%–90% accurate in predicting bankruptcy one year before the event, with a Type II error (classifying the firm as bankrupt when it does not go bankrupt) of approximately 15% –20% (Altman, 2000).

From about 1985 onwards, the Z-scores gained wide acceptance by auditors, management accountants, courts, and database systems used for loan evaluation (Eidleman). The formula's approach has been used in a variety of contexts and countries, although it was designed originally for publicly held manufacturing companies with assets of more than $1 million. Later variations by Altman were designed to be applicable to privately held companies (the Altman Z'-Score) and non-manufacturing companies (the Altman Z"-Score).

Neither the Altman models nor other balance sheet-based models are recommended for use with financial companies. This is because of the opacity of financial companies' balance sheets and their frequent use of off-balance sheet items. There are market-based formulas used to predict the default of financial firms (such as the Merton Model), but these have limited predictive value because they rely on market data (fluctuations of share and options prices to imply fluctuations in asset values) to predict a market event (default, i.e., the decline in asset values below the value of a firm's liabilities).

9.2 Risk Adjusted Returns / Capital

Risk-adjusted return refines an investment's return by measuring how much risk is involved in producing that return, which is generally expressed as a number or rating. Risk-adjusted returns are applied to individual securities, investment funds and portfolios. Some common risk measures include alpha, beta, R-squared, standard deviation and the Sharpe ratio. When comparing two or more potential investments, an investor should always compare the same risk measures to each different investment to get a relative performance perspective.

Alpha, often considered the active return on an investment, gauges the performance of an investment against a market index used as a benchmark, since they are often considered to represent the market's movement as a whole. The excess returns of a fund relative to the return of a benchmark index is the fund's alpha. Alpha is most often used for mutual funds and other similar investment types. alpha is often known as the "Jensen index. Because of the intricacies of large funds and portfolios, as well as of these forms of investing in general, comparing alpha values is only useful when the investments contain assets in the same asset class. Additionally, since alpha is calculated relative to a benchmark deemed appropriate for the fund or portfolio, when calculating alpha it is imperative that an appropriate benchmark is chosen.

Beta, is a measure of the volatility or a systematic risk of security or a portfolio in comparison to the market as whole. A beta of 1 indicates that the security's price moves with the market. A beta of less than 1 means that the security is theoretically less volatile than the market. A beta of greater than 1 indicates that the security's price is theoretically more volatile than the market. For example, if a stock's beta is 1.2, it's theoretically 20% more volatile than the market. Conversely, if an ETF's beta is 0.65, it is theoretically 35% less volatile than the market. Therefore, the fund's excess return is expected to underperform the benchmark by 35% in up markets and outperform by 35% during down markets.

Sharpe Ratio, is a measure of an investment's excess return, above the risk free return, per unit of standard deviation. It is calculated by taking the return of the investment, subtracting the risk free rate, and dividing this result by the investment's standard deviation. All else equal, a higher Sharpe ratio is better. e.g: Mutual fund A returns 12% over the past year and had a standard deviation of 10%. Mutual Fund B returns 10% and had a standard deviation of 7%. The risk free return over the time period was 3%. The Sharpe ratio would be calculated as follows:

Mutual fund A (12%-3%) / 10% = 0.9

Mutual fund B (10%-3%)/7% = 1.

Even though Mutual fund A had a higher return, Mutual fund B had a higher risk adjusted return, meaning that it gained more pre unit of total risk than Mutual fund A.

R Squared, is a statistical measurement that determines the proportion of a security's return, or the return on a specific portfolio of securities, that can be explained by variations in the stock market as measured by a benchmark index. R-squared values range from 0 to 1 and are

commonly stated as percentages from 0 to 100%. An R-squared of 100% means all movements of a security are completely explained by movements in the index. A high R-squared, between 85% and 100%, indicates the fund's performance patterns have been in line with the index. A fund with a low R-squared, at 70% or less, indicates the security does not act much like the index. A higher R-squared value indicates a more useful beta figure. For example, if a fund has an R-squared value of close to 100% but has a beta below 1, it is most likely offering higher risk-adjusted returns.

9.2.1 Return on Risk Adjusted Capital (RORAC)

The return on risk-adjusted capital (RORAC) is a rate of return statistic commonly used in financial analysis, where varying projects, endeavours and investments are evaluated based on capital at risk. Projects with different risk profiles are easier to compare to each other once their individual RORAC values have been calculated.

RORAC = Net income / Allocated Risk Capital

Allocated risk capital is the firm's capital, adjusted for a maximum potential loss based on estimated future earnings distributions or the volatility of earnings. Companies use RORAC to place greater emphasis on firm-wide risk management. For example, different corporate divisions with unique managers can use RORAC to quantify and maintain acceptable risk-exposure levels. With RORAC, however, the capital is adjusted for risk, not the rate of return. RORAC is used when the risk varies depending on the capital asset being analyzed.

For example, assume a firm is evaluating two projects it has engaged in over the previous year and needs to decide which one to eliminate. Project A had total revenues of ₹ 100,000 and total expenses of ₹ 50,000. The total risk-weighted assets involved in the project are ₹ 400,000. Project B had total revenues of ₹ 200,000 and total expenses of ₹ 100,000. The total risk-weighted assets involved in Project B are ₹ 900,000. The RORACs are calculated as below:

Project A RORAC = ₹ 1,00,000 – ₹ 50,000 / ₹ 4,00,000 = 12.5%

Project B RAROC = ₹ 2,00,000 – ₹ 100000 / ₹ 9,00,000 = 11.1%

Even though Project B had twice as much revenue as Project A, once the risk-weighted capital of the projects are taken into account, it is clear that Project A has a better RORAC.

9.2.2 Economic Capital

Economic capital is the amount of capital that a firm, usually in financial services, needs to ensure that the company stays solvent given its risk profile. Economic capital is calculated internally, sometimes using proprietary models, and is the amount of capital that the firm should have to support any risks that it takes

Calculations of economic capital and their use in risk/reward ratios reveal which business lines a bank should pursue that maximize the risk-reward trade-off. Performance measures that utilize economic capital include return on risk adjusted capital (RORAC), risk adjusted return on capital

(RAROC) and economic value added (EVA). Business units that perform better on measures like these can receive more of the firm's capital in order to optimize risk. Value-at-risk (VaR) and similar measures are also based on economic capital and are used by financial institutions for risk management.

9.2.3 Value at Risk (VaR)

Value at risk (VaR) is a statistical technique used to measure and quantify the level of financial risk within a firm or investment portfolio over a specific time frame. This metric is most commonly used by investment and commercial banks to determine the extent and occurrence ratio of potential losses in their institutional portfolios. VaR calculations can be applied to specific positions or portfolios as a whole or to measure firm-wide risk exposure. VaR modelling determines the potential for loss in the entity being assessed, as well as the probability of occurrence for the defined loss. VaR is measured by assessing the amount of potential loss, the probability of occurrence for the amount of loss and the time frame. For example, a financial firm may determine an asset has a 3% one-month VaR of 2%, representing a 3% chance of the asset declining in value by 2% during the one-month time frame. The conversion of the 3% chance of occurrence to a daily ratio places the odds of a 2% loss at one day per month.

9.2.4 Risk – adjusted Return on Capital (RAROC)

Risk-adjusted return on capital (RAROC) is a risk-based profitability measurement framework for analysing risk-adjusted financial performance and providing a consistent view of profitability across businesses. The concept was developed by Bankers Trust and principal designer Dan Borge in the late 1970s. Note, however, that more and more return on risk adjusted capital (RORAC) is used as a measure, whereby the risk adjustment of Capital is based on the capital adequacy guidelines as outlined by the Basel Committee, currently Basel III.

RAROC = Expected return / Economic Capital OR RAROC = Expected Return / Value at Risk

Broadly speaking, in business enterprises, risk is traded off against benefit. RAROC is defined as the ratio of risk adjusted return to economic capital. The economic capital is the amount of money which is needed to secure the survival in a worst-case scenario, it is a buffer against unexpected shocks in market values. Economic capital is a function of market risk, credit risk, and operational risk, and is often calculated by VaR. This use of capital based on risk improves the capital allocation across different functional areas of banks, insurance companies, or any business in which capital is placed at risk for an expected return above the risk-free rate.

RAROC system allocates capital for two basic reasons:

(a) Risk management

(b) Performance evaluation

For risk management purposes, the main goal of allocating capital to individual business units is to determine the bank's optimal capital structure—that is economic capital allocation is closely

correlated with individual business risk. As a performance evaluation tool, it allows banks to assign capital to business units based on the economic value added of each unit.

9.3 Ratios and Financial Assessment

For any Credit or Finance professional, it is critical to examine and analyze the Audited Financials of the past 5 years of the company / borrower, in detail. They should additionally require to seek and assess the latest audited or provisional quarterly / semi-annual financial data of the company. Once the financial information has been gathered, the analysis should include the following critical ratios:

9.3.1 Financial Statement analysis

(a) Sales Growth Rate – This ratio gives us a trend whether the growth / decline in topline is consistent and hence sustainable over the projected period or it's a spurt in one of the years. The ratio is : ((Yr2 Sales – Yr1 Sales) / Yr1 Sales)*100

(b) EBITDA% - EBIDTA refers to Earnings before interest, depreciation and tax. This gives us a fair idea how much profit the borrower is making from its business at operating level. This eliminates the effects of financing and accounting decisions thus giving profitability purely from operations. Ratio is (EBIDTA / Net Sales)*100

(c) PAT% - This is the net earnings after all the expenses before appropriation to reserves and distribution to shareholders in the form of dividend. Ratio is (PAT / Net Sales)*100

(d) EBIDTA / Interest – This ratio gives us the measure of company's ability to meet its interest expenses through operating profits.

(e) Net Fixed asset turnover ratio – This ratio indicates how well the borrower is using its fixed assets to generate sales. If a company has a higher fixed asset turnover ratio than its competitors it is using its assets well to generate the topline.

(f) Total Debt / TNW – Tangible Networth (TNW) is most commonly a calculation of the networth of a company that excludes any value derived from intangible assets such as copyrights, patents, intellectual property etc.

Tangible Networth = Total Assets – Total Liabilities – Intangible Assets

The ratio Total Debt / TNW – this measures the proportions of company's borrowed funds to equity. The ratio indicates the financial risk to which a business is subjected, since excessive debt can lead to financial difficulties. A high gearing ratio is indicative of high debt, which in business downturn may pose trouble on the borrower in meeting its debt repayment schedules.

(g) Debt Service Coverage ratio (DSCR) – is a measure of the cash flow available to pay current debt obligations. The ratio states net operating income as a multiple of debt obligations due within one year, including interest, principal. Ratio is (PAT + Dep + Interest) / (Current portion

of long term debt + Interest).

(h) ROCE / ROE / ROA

(i) Return on Capital employed (ROCE) - is a financial ratio that measures a company's profitability and the efficiency with which its capital is employed. ROCE is calculated as: ROCE = Earnings before Interest and Tax (EBIT) / Capital Employed.

(ii) Return on Equity (ROE) - is the amount of net income returned as a percentage of shareholders equity. Return on equity measures a corporation's profitability by revealing how much profit a company generates with the money shareholders have invested. ROE = PAT / Shareholders Equity

(iii) Return on Assets (ROA) - Return on assets (ROA) is an indicator of how profitable a company is relative to its total assets. ROA gives an idea as to how efficient management is at using its assets to generate earnings. Calculated by dividing a company's annual earnings by its total assets, ROA is displayed as a percentage. Sometimes this is referred to as "return on investment". ROA = Net Income / Total Assets.

9.3.2 Cash Flow analysis

(a) Operating Cash flow - The first set of cash flow transactions is from operational business activities. Cash flows from operations starts with net income and then reconciles all noncash items to cash items within business operations. For example, accounts receivable is a noncash account. If accounts receivables go up, it means sales are up, but no cash was received at the time of sale. The cash flow statement deducts receivables from net income because it is not cash. Also included in cash flows from operations are accounts payable, depreciation, amortization and numerous prepaid items booked as revenue or expenses but with no associated cash flow

(b) Investment cash flow - Cash flows from investing activities includes cash spent on property, plant and equipment. This is where analysts look to find changes in capital expenditures (CAPEX). While positive cash flows from investing activities is a good thing, investors prefer companies that generate cash flows primarily from business operations, not investing and financing activities.

(c) Financing cash flow - Cash flows from financing is the last business activity detailed on the cash flow statement. The section provides an overview of cash used in business financing. Analysts use the cash flows from financing section to find the amount paid out in dividends or share buybacks. Cash obtained or paid back from capital fundraising efforts, such as equity or debt, is also listed.

9.3.3 Working capital analysis

(a) Account receivable days - Accounts receivable days is the number of days that a customer invoice is outstanding before it is collected. The point of the measurement is to determine the

effectiveness of a company's credit and collection efforts in allowing credit to reputable customers, as well as its ability to collect cash from them in a timely manner.

Formula : Account receivable turnover (days) = (Debtors / Sales)*365

(b) Inventory days - The inventory turnover ratio is an efficiency ratio that shows how effectively inventory is managed by comparing cost of goods sold with average inventory for a period. This measures how many times average inventory is "turned" or sold during a period. Formula: (Inventory / Sales) * 365

(c) Payable days - The accounts payable turnover ratio is a short-term liquidity measure used to quantify the rate at which a company pays off its suppliers. Accounts payable turnover ratio is calculated by taking the total purchases made from suppliers, or cost of sales, and dividing it by the average accounts payable amount during the same period.

Formula: (Creditors / Purchases) * 365

(d) Current Ratio and Quick ratio - The current ratio is a liquidity ratio that measures a company's ability to pay short-term and long-term obligations. To gauge this ability, the current ratio considers the current total assets of a company (both liquid and illiquid) relative to that company's current total liabilities. Quick Ratio is a measure of how well a company can meet its short-term financial liabilities. Also known as the acid-test ratio, it can be calculated as follows: (Cash + Marketable Securities + Accounts Receivable) / Current Liabilities.

While conducting credit risk due diligence on a borrower, it is also important to formulate suitable assumptions for projections basis the business model / historical experience and industry / sector the borrower belongs to. Ideally, the projections should cover the tenor of the loan. This will indicate whether the borrower has the ability / capacity to pay the lenders debt as per the terms & conditions of the loan. All the ratios indicated above should be suitably calculated to understand the financial viability of the borrower under consideration. Further, the projections should also be assessed basis two or three stressed scenarios by modifying the assumptions. Eg: Drop in turnover by 5%. No Growth in EBIDTA margins or drop in volumes etc. The proof of the pudding lies in the fact that Debt service coverage ratio should be above 1 in all the projected years which indicates the borrower's ability. This is a very important exercise in the wholesale financing including project finance wherein the loan tenor is usually long ~ 15-20 yrs.

10. CREDIT SCORING MODELS

10.1 What is a Credit Scoring Model?

As per "Investopedia", credit score is a statistical analysis performed by lenders and financial institutions to access a person's credit worthiness. Lenders use credit scoring, among other things, to arrive at a decision on whether to extend credit. A person's credit score is a number between 300 and 850, 850 being the highest credit rating possible. The methods which are used in understanding this credit related with the customer are called credit scoring models.

Credit scoring models which are alternatively called as scorecards are primarily used to inform management for decision making and to provide predictive analysis or the information on the potential delinquency of the loan approved or credit line extended. Adoption of the credit scoring model is vital for the organization as it's a base to determine the credit management policy. Erroneous, misused, misunderstood, or poorly developed and managed scoring models may lead to lost revenues through poor customer selection (credit risk) or collections management.

The usage of credit models are as follows but not limited to:

- Controlling risk selection
- Translating the risk of default into appropriate pricing
- Managing credit losses
- Evaluating new loan programs.
- Reducing loan approval processing time

Most likely, scoring and modeling will increasingly guide risk management program in an organization through end to end. The increasing regulatory requirements are the guide to use scoring and modeling to be embedded in management's lending decisions and risk management processes which accentuates the importance of understanding scoring model concepts and underlying risks.

10.2 Types of Credit Scoring Model

Credit scoring models are mainly used by the credit rating agency to determine the credit worthiness of an individual. The degree of creditworthiness is denoted by the credit scores for each individual. Now a days, many financial institutions are using credit scores to evaluate the potential risks exposure by lending the money to consumers and to mitigate the losses organization may suffer by the default risk. To determine the credit score various credit scoring models are available through the agencies or credit bureaus.

In this section lets understand the different models predominantly used across the world. These are mix of statistical or behavioral scoring models.

FICO Score

It imperative to have knowledge about the credit. Bad credit history has the impact on borrower's future. If you want to be better versed about your credit, resorting to FICO Score could be a great place to start.

A FICO Score is a powerful measure of the creditworthiness as a lender might refer. FICO Scores are used in 90% of credit decisions, so they're a very good barometer of how your credit can look to potential lenders. Credit score ranges between 300 – 850 points

Scoring ranges are just one of the tools lenders can use to link ranges of values with associated characteristics and metrics at-a-glance, allowing

them to make more informed lending decisions quickly and fairly.

Under this credit scoring model following ranges and associated credit ratings are as follows:

1) 800 & + ➔ Very Well above average : 1% chance of default
2) 740 – 799 ➔ Very good : 2% chance of default
3) 670 – 639 ➔ Median Credit Score : 8% chance of default
4) 580 - 669 ➔ Below average : 28% chance of default
5) 570 & - ➔ Poor : 61% chance of default

Under FICO model credit scores are calculated based on following

35% - Payment History

30% - Debt or Credit

15% - Length of the Credit History

10% - New Credit

10% - Type of Credit Used

Vantage Score

Vantage score are based on the credit reporting agencies. Vantage calculate the credit scores based on the three credit reporting agencies that are Equifax, Experian and TransUnion. As per the latest Vantage Score model the credit scores are being rated between 300 – 850

The level of credits scores follows similar brackets as that of FICO. However the rating is based on A to F alphabets. A being the best and F being the poor.

The credit score range was redefined with new version of Vantage score model due to the credit behavior as well as change in economy. Accurate results will lead to appropriate level of credits to the borrowers.

Vantage score is being calculated based on the one month's credit history of the consumer. This is useful for those consumer who are new to the credit market. Further negative vantage discourages the late mortgage payments etc. and this will have direct impact on the credit rating. Vantage score disregards the payment collection accounts if any maintained by the consumer. This means no credits being given against any line of credit.

PLUS Score

Plus score is developed by Experian credit reporting agency. The scoring model is based on the mathematical calculation and represents in the range of 330 – 830 points.

The most important and noteworthy point is that the PLUS score is very much consumer focussed. That means the credit score depends upon the

consumer behavior. Like FICO, PLUS score is also calculated based on the payment history, debt used and nature of credit history.

As referred above, the PLUS Score range runs from 330 to 830. Consumers with a low PLUS Score are considered to be "high risk", while those with higher scores are considered to be "low risk".

The score under this model is compared with the other consumer in the similar lines and across the segment. This will ensure that the credit score will be ranked based on the percentile.

For instance, your score may be noted as in the "87th percentile" the "56th percentile" or the "67th" percentile. This simply means that your score is better than 87%, 56% or 67% of the public, respectively.

Experian National Equivalency Score

Experian's National Equivalency Score (ENES) is also called as FAKO credit score. This scoring model aims at to estimate the credit worthiness of an individual customer. The score range is 360-840. It has been claimed by the Experian, institution who owns the ENES system, that it is quite similar to the FICO scoring model. The exact basis of the mathematical calculation is not publicized by the model owners. But considering the facts that the it's a replica of FICO model, one cannot expect drastic dissimilarity between these two models.

The model has a lower range with marginal reduction of 10 point on either ends.

However, since this score is free of cost to the individual this may not be considered by the lending organization. It's up to the organization to use the scoring model. The usage is typically based on the user risk profile.

Equifax

Like Experian, Equifax is one of the major credit-reporting bureau and produces credit reports similar to those from Experian.

Equifax offers numerical credit scores that range from 280 to 850. The criteria used by the Equifax is similar to the FICO. A high Equifax credit score typically indicates a high FICO score.

The advantages of Equifax

1. Detailed Reported as compared to other reports.
2. Establishes and presents the consumers borrowing pattern.
3. Borrower need a real good credit history to ensure line of credit is being extended appropriately.

CHAPTER 7

RISK ASSOCIATED WITH CORPORATE GOVERNANCE

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

- Evaluation of Risk Associated with Governance
- Description and evaluation of framework for Board level consideration of risk
- OECD Guidelines for Corporate Governance

1. EVALUATION OF RISK ASSOCIATED WITH GOVERNANCE

Governance risks mean significant deficiencies that can impact the reputation, existence and continuity of the organisation. These arise on account of failure of the Board to direct and control the organisation or inappropriate practices adopted by the Board or collusion of management to override significant internal control mechanism causing financial losses or inability of the Board to identify principal risk factors that can impact business continuity.

Often these failures are facilitated by corporate governance failures, where boards do not fully appreciate the risks that the companies are taking (if they are not engaging in reckless risk-taking themselves), and/or deficient risk management systems.

Governance Risks
• Absence of effective corporate governance framework and documented governance policies
• The rights of shareholders and key ownership functions are not defined and communicated
• There is no equitable treatment of shareholders

- The role of stakeholders in corporate governance is not defined, communicated and monitored
- Disclosure and transparency norms are not articulated
- The responsibilities of the Board of directors are not defined, documented and reviewed annually
- Board has not defined risk capacity, appetite and risk response strategies
- Risk not managed on an enterprise basis and not adjusted to corporate strategy.
- Risk managers separated from management and not regarded as an essential part of implementing the company's strategy. Most important of all, boards were in a number of cases ignorant of the risk facing the company.
- Risk management and control functions be independent of profit centres and the "Chief Risk Officer" (CRO) or equivalent should report directly to the board of directors along the lines
- Corporations developing their risk management and oversight practices face challenges, such as linking risks to strategy; better defining risks; developing corporate responses to risks that manage to address all five key dimensions (strategy, people, detail, tasks, and drivers); effectively considering stakeholders' and gatekeepers' concerns; and addressing all these issues from a whole-enterprise perspective. These challenges are faced by both financial and non-financial companies.
- Boards simply review and approve management's proposed strategies.
- Insignificant Board time spent on business risk management
- Boards have incomplete understanding of the risks faced by the company.
- Boards receive information that is short-term.
- The process of risk management and the results of risk assessments should be appropriately disclosed. Disclosure of risk factors should be focused on those identified as more relevant and/or should rank material risk factors in order of importance on the basis of a qualitative selection whose criteria should also be disclosed.
- Whistle blower matters
- Negative media reports
- Shareholder activism
- Unauthorised related party transactions
- Ownership /Shareholder disputes

To evaluate and assess Governance Risks it is highly recommended to study the **Sound Risk Governance Practices recommended by the Financial Stability Board in 2013**. The list extracts some of the better practices exemplified by national authorities and firms. The sound practices also build on some of the principles and recommendations published by other organisations and standard setters, drawing together those that are relevant for risk governance.

This integrated and coherent list of sound practices aims to help national authorities and firms continue to improve their risk governance. This list is summarized as below:

(i) The Board of Directors

a) avoids conflicts of interest arising from the concentration of power at the board (e.g., by having separate persons as board chairman and CEO or having a lead independent director where the board chairman and CEO are the same person);

b) comprises members who collectively bring a balance of expertise (e.g., risk management and financial industry expertise), skills, experience and perspectives;

c) comprises largely independent directors and there is a clear definition of independence that distinguishes between independent directors and non-executive directors;

d) sets out clear terms of references for itself and its sub-committees (including tenure limits for committee members and the chairs), and establishes a regular and transparent communication mechanism to ensure continuous and robust dialogue and information sharing between the board and its sub-committees;

e) conducts periodic reviews of performance of the board and its sub-committees (by the board nomination or governance committee, the board themselves, or an external party); this includes reviewing, at a minimum annually, the qualifications of directors and their collective skills (including financial and risk expertise), their time commitment and capacity to review information and understand the firm's business model, and the specialised training required to identify desired skills for the board or for director recruitment or renewal;

f) sets the tone from the top, and seeks to effectively inculcate an appropriate risk culture throughout the firm;

g) is responsible for overseeing management's effective implementation of a firm-wide risk management framework and policies within the firm;

h) approves the risk appetite framework and ensures it is directly linked to the business strategy, capital plan, financial plan and compensation;

i) has access to any information requested and receives information from its committees at least quarterly;

j) meets with national authorities, at least quarterly, either individually or as a group.

(ii) The risk committee

a) is required to be a stand-alone committee, distinct from the audit committee;

b) has a chair who is an independent director and avoids "dual-hatting" with the chair of the board, or any other committee;

c) includes members who are independent;

d) includes members who have experience with regard to risk management issues and practices;

e) discusses all risk strategies on both an aggregated basis and by type of risk;

f) is required to review and approve the firm's risk policies at least annually;

g) oversees that management has in place processes to ensure the firm's adherence to the approved risk policies.

(iii) The audit committee

a) is required to be a stand-alone committee, distinct from the risk committee;

b) has a chair who is an independent director and avoids "dual-hatting" with the chair of the board, or any other committee;

c) includes members who are independent;

d) includes members who have experience with regard to audit practices and financial literacy at a financial institution;

e) reviews the audits of internal controls over the risk governance framework established by management to confirm that they operate as intended;

f) reviews the third party opinion of the design and effectiveness of the overall risk governance framework on an annual basis.

(iv) The CRO

a) has the organisational stature, skill set, authority, and character needed to oversee and monitor the firm's risk management and related processes and to ensure that key management and board constituents are apprised of the firm's risk profile and relevant risk issues on a timely and regular basis; the CRO should have a direct reporting line to the CEO and a distinct role from other executive functions and business line responsibilities as well as a direct reporting line to the board and/or risk committee;

b) meets periodically with the board and risk committee without executive directors or management present;

c) is appointed and dismissed with input or approval from the risk committee or the board and such appointments and dismissals are disclosed publicly;

d) is independent of business lines and has the appropriate stature in the firm as his/her performance, compensation and budget is reviewed and approved by the risk committee;

e) is responsible for ensuring that the risk management function is adequately resourced,

taking into account the complexity and risks of the firm as well as its Risk Assessment Framework (RAF) and strategic business plans;

f) is actively involved in key decision-making processes from a risk perspective (e.g., the review of the business strategy/strategic planning, new product approvals, stress testing, recovery and resolution planning, mergers and acquisitions, funding and liquidity management planning) and can challenge management's decisions and recommendations;

g) is involved in the setting of risk-related performance indicators for business units;

h) meets, at a minimum quarterly, with the firm's supervisor to discuss the scope and coverage of the work of the risk management function.

2. THE RISK MANAGEMENT FUNCTION

a) It is independent of business lines (i.e., is not involved in revenue generation) and reports to the CRO;

b) It has authority to influence decisions that affect the firm's risk exposures;

c) It is responsible for establishing and periodically reviewing the enterprise risk governance framework which incorporates the Risk Appetite Framework (RAF), Risk Appetite Statement (RAS) and risk limits.

i) The RAF incorporates an RAS that is forward-looking as well as information on the types of risks that the firm is willing or not willing to undertake and under what circumstances. It contains an outline of the roles and responsibilities of the parties involved, the risk limits established to ensure that the framework is adhered to, and the escalation process where breaches occur.

ii) The RAS is linked to the firm's strategic, capital, and financial plans and includes both qualitative and quantitative measures that can be aggregated and disaggregated such as measures of loss or negative events (e.g., earnings, capital, and liquidity) that the board and senior management are willing to accept in normal and stressed scenarios.

iii) Risk limits are linked to the firm's RAS and allocated by risk types, business units, business lines or product level. Risk limits are used by management to control the risk profile and linked to compensation programmes and assessment.

d) It has access to relevant affiliates, subsidiaries, and concise and complete risk information on a consolidated basis; risk-bearing affiliates and subsidiaries are captured by the firm wide risk management system and are a part of the overall risk governance framework;

e) It provides risk information to the board and senior management that is accurate and reliable and periodically reviewed by a third party (internal audit) to ensure completeness and integrity;

f) It conducts stress tests (including reverse stress tests) periodically and by demand. Stress test programs and results (group-wide stress tests, risk categories and stress test metrics) are adequately reviewed and updated to the board or risk committee. Where stress limits are breached or unexpected losses are incurred, proposed management actions are discussed at the board or risk committee. Results of stress tests are incorporated in the review of budgets, RAF and ICAAP processes, and in the establishment of contingency plans against stressed conditions.

3. INDEPENDENT ASSESSMENT OF THE RISK GOVERNANCE FRAMEWORK

A Risk Management Framework (RMF) sets the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management capability. Undertaking a periodic review to assess the effectiveness of an entity's risk management framework is necessary to ensure that the framework continues to evolve and meet the needs of the entity. The RMF should define a policy statement on the following matters:-

(i) Determining when to review the RMF and the frequency for undertaking the review.

(ii) Deciding who is responsible for the review. The RMF is generally reviewed by the Audit Committee or a team of Directors. Once in few years the RMF can be reviewed with external facilitation this would provide fresh insights and benchmarking information to the Board.

(iii) Selecting the scope and method for a review. The scope and boundary of the RMF review can be clearly set out along with the most suited method for review.

(iv) Manner of circulation of results.

The Board requires a periodic independent assessment of the firm's overall risk governance framework and provides direct oversight to the process.

The Board should assess whether the organisation has the required stature, talent, and character needed to provide a reliable independent assessment of the firm's risk governance framework and internal controls and not be unduly influenced by the CEO and other members of management;

Organisations may develop an entity level control framework on the basis of the Sound Risk Governance Principles prescribed by the Financial Stability Board for evaluating Governance Risks. The results and findings from the said entity level control assessment may be submitted to the Board of the company on an annual basis and suitably disclosed as part of its risk disclosures.

3.1 Entity's Risk Assessment Process with respect to Financial Reporting

The **ICAI Guidance note on Internal Financial Controls** over financial reporting states that for financial reporting purposes, the entity's risk assessment process includes how management

identifies business risks relevant to the preparation of financial statements in accordance with the entity's applicable financial reporting framework, estimates their significance, assesses the likelihood of their occurrence, and decides upon actions to respond to and manage them and the results thereof.

For example, the entity's risk assessment process may address how the entity considers the possibility of unrecorded transactions or identifies and analyses significant estimates recorded in the financial statements. Risks relevant to reliable financial reporting include external and internal events, transactions or circumstances that may occur and adversely affect an entity's ability to initiate, record, process, and report financial data consistent with the assertions of management in the financial statements. Management may initiate plans, programs, or actions to address specific risks or it may decide to accept a risk because of cost or other considerations.

Risks can arise or change due to the following circumstances:

a) **Changes in operating environment.** Changes in the regulatory or operating environment can result in changes in competitive pressures and significantly different risks.

b) **New personnel.** New personnel may have a different focus on or understanding of internal control.

c) **New or revamped information systems.** Significant and rapid changes in information systems can change the risk relating to internal control.

d) **Rapid growth.** Significant and rapid expansion of operations can strain controls and increase the risk of a breakdown in controls.

e) **New technology.** Incorporating new technologies into production processes or information systems may change the risk associated with internal control.

f) **New business models, products, or activities.** Entering into business areas or transactions with which an entity has little experience may introduce new risks associated with internal control.

g) **Corporate restructurings.** Restructurings may be accompanied by staff reductions and changes in supervision and segregation of duties that may change the risk associated with internal control.

h) **Expanded foreign operations.** The expansion or acquisition of foreign operations carries new and often unique risks that may affect internal control, for example, additional or changed risks from foreign currency transactions.

i) **New accounting pronouncements.** Adoption of new accounting principles or changing accounting principles may affect risks in preparing financial statements.

3.2 Role of Risk Assessment with respect to Financial Reporting

Risk assessment underlines the entire audit process described by the ICAI guidance note, including the determination of significant accounts and disclosures and relevant assertions, the selection of controls to test, and the determination of the evidence necessary for a given control. A direct relationship exists between the degrees of risk that a significant deficiency or material weakness could exist in a particular area of the company's internal financial controls over financial

reporting and the amount of audit attention that should be devoted to that area. In addition, the risk that a company's internal financial controls over financial reporting will fail to prevent or detect a misstatement caused by fraud usually is higher than the risk of failure to prevent or detect error. The auditor should focus more of his or her attention on the areas of highest risk. On the other hand, it is not necessary to test controls that, even if deficient, would not present a reasonable possibility of material misstatement to the financial statements. The complexity of the organisation, business unit, or process, will play an important role in the auditor's risk assessment and the determination of the necessary procedures.

3.3 Risk Based Internal Auditing (RBIA)

The definition of internal audit, as described in the Preface to the Standards on Internal Audit, issued by the Institute of Chartered Accountants of India, amply reflects the current thinking as to what is an internal audit: Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity's strategic risk management and internal control system.

Internal auditors can carry out their job in a more focused manner by directing their efforts in the areas where there is a greater risk, thereby enhancing the overall efficiency of the process and adding greater value with the same set of resources.

Internal audit is a management function, thus, it has the high-level objective of serving management's needs through constructive recommendations in areas such as, internal control, risk, utilisation of resources, compliance with laws, management information system, etc.

Risk management enables management to effectively deal with risk, associated uncertainty and enhancing the capacity to build value to the entity or enterprise and its stakeholders. Internal auditor plays an important role in providing assurance to management on the effectiveness of risk management.

Boards of Directors are increasingly becoming risk aware and risk focused. Expectations from internal auditors are increasing from providing an assurance on the adequacy and effectiveness of internal controls to an assurance on whether risks are being managed within acceptable limits as defined by the Board of Directors. This has given to birth Risk Based Audit Methodologies that are pursued by Auditors.

The business environment is increasingly throwing up newer challenges and opportunities with globalisation, disruptive technologies and rules being continuously rewritten. New risks are hence coming up frequently. Risk management is the process of measuring or assessing risk and developing strategies to manage it. The 21st century internal auditors have the following vital areas of responsibility in the field of risk management:

- Review operations, policies, and procedures.
- Help ensure that goals and objectives are met.

- Understanding the “big picture” and diverse operations.
- Make recommendations to improve economy and efficiency.

Therefore, the internal audit report is on the management of significant risks of the organisation and the assurance is on these risks being managed within the acceptable limits as laid down by the Board of Directors. To give this assurance, the internal auditor conducts a process audit on risk management processes at all levels of the organisation, viz., corporate, divisional, business unit, business process level, etc., put in place by line management so as to assess the adequacy of their design and compliance

3.4 Audit Risk & Sampling

Some degree of uncertainty is implicit in the concept of "a reasonable basis for an auditor’s opinion". The justification for accepting some uncertainty arises from the relationship between factors such as cost and time required for examining all of the data and the adverse consequences of possible erroneous decisions based on the conclusions resulting from examining only a sample of the data.

Audit risk includes both uncertainties due to sampling and uncertainties due to factors other than sampling. These aspects of audit risk are sampling risk and non-sampling risk, respectively. Sampling risk arises from the possibility that, when a test of controls or a substantive test is restricted to a sample, the auditor's conclusions may be different from the conclusions he would reach if the test were applied in the same way to all items in the account balance or class of transactions. That is, a particular sample may contain proportionately more or less monetary misstatements or deviations from prescribed controls than exist in the balance or class as a whole. For a sample of a specific design, sampling risk varies inversely with sample size: the smaller the sample size, the greater the sampling risk.

Non-sampling risk includes all the aspects of audit risk that are not due to sampling. An auditor may apply a procedure to all transactions or balances and still fail to detect a material misstatement. Non-sampling risk includes the possibility of selecting audit procedures that are not appropriate to achieve the specific objective. For example, confirming recorded receivables cannot be relied on to reveal unrecorded receivables. Non-sampling risk also arises because the auditor may fail to recognize misstatements included in documents that he examines, which would make that procedure ineffective even if he were to examine all items. Non-sampling risk can be reduced to a negligible level through such factors as adequate planning and supervision and proper conduct of a firm's audit practice.

4. RISK MANAGEMENT DISCLOSURES IN INDIA

4.1 Indian Scenario

4.1.1 Provisions of the Indian Companies Act, 2013

In recognition of the risk realities, the Indian Companies Act, 2013 has mandated provisions that

the Annual Report of the Board of Directors must include a statement indicating the development and implementation of a risk management policy for the company. This should include the identification of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company.

The audit committee is directed to act in accordance with the terms of reference specified in writing by the Board, which shall, inter alia, include evaluation of risk management systems. The code of conduct prescribes that the Independent Directors should satisfy themselves that systems of risk management are robust and defensible.

4.1.2 Provisions of the SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015

SEBI Listing Requirements as applicable to listed entities in India is a comprehensive set of guidelines that are prepared on the lines of international practices. As per SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015 following risk management disclosures are mandatory for listed entities in India.

i) Under responsibility of *Directors* - Ensuring the integrity of the listed entity's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.

ii) The board of directors shall ensure that, while rightly encouraging positive thinking, these do not result in over-optimism that either leads to significant risks not being recognised or exposes the listed entity to excessive risk.

iii) The board of directors shall have ability to "step back" to assist executive management by challenging the assumptions underlying: strategy, strategic initiatives (such as acquisitions), risk appetite, exposures and the key areas of the listed entity's focus.

iv) The listed entity shall lay down procedures to inform members of board of directors about risk assessment and minimization procedures.

v) The board of directors shall be responsible for framing, implementing and monitoring the risk management plan for the listed entity.

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

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

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

The board of directors shall define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit.

The provisions of this regulation shall be applicable to top 100 listed entities, determined on the basis of market capitalisation, as at the end of the immediate previous financial year.

vii) Under minimum information to be placed before the Board on a quarterly basis- Quarterly details of foreign exchange exposures and the steps taken by management to limit the risks of adverse exchange rate movement, if material.

viii) Under disclosures in Annual Reports applicable to all listed entities except banks-

Management Discussion and Analysis: This section shall include discussion on the following matters within the limits set by the listed entity's competitive position:

(a) Industry structure and developments.

(b) Opportunities and Threats.

(c) Segment–wise or product-wise performance.

(d) Outlook

(e) Risks and concerns.

(f) Internal control systems and their adequacy.

(g) Discussion on financial performance with respect to operational performance.

(h) Material developments in Human Resources / Industrial Relations front, including number of people employed.

(i) Details of significant changes (i.e. change of 25% or more as compared to the immediately previous financial year) in key financial ratios, along with detailed explanations therefor, including:

(i) Debtors Turnover

(ii) Inventory Turnover

(iii) Interest Coverage Ratio

(iv) Current Ratio

(v) Debt Equity Ratio

(vi) Operating Profit Margin (%)

(vii) Net Profit Margin (%) or sector-specific equivalent ratios, as applicable.

(j) Details of any change in Return on Net Worth as compared to the immediately previous financial year along with a detailed explanation thereof.]

General information to shareholders: Under this head the information related to Commodity Price Risk or Foreign Exchange Risk and related Hedging activities are covered.

4.2 Risk Management Disclosures – Global Scenario

In US, the Companies listed with the Securities and Exchange Commission (SEC), have to describe the risks faced by the business (in some form or another) since the 1970s. In Europe, the EU Accounts Modernisation Directive of 2003 said that companies should describe the risks they face, in both annual and interim reports. Two countries have gone further than the Europe-wide requirements – Germany has its own risk reporting standard (GAS 5), while the UK's Corporate Governance Code says that companies should report at least annually on the effectiveness of their risk-management procedures. The UK's Corporate Governance Code still goes further where a more integrated approach to risk reporting, linking risk management to internal controls and going concern is included.

The first important attempt to meet the demand for increased risk disclosures was the 1980 remodelling of the rules of the US securities and Exchange Commission (SEC) for a management discussion and analysis (MD&A). The MD&A rules include a requirement to 'Describe any known trends or uncertainties that the company reasonably expects will have a material favourable or unfavourable impact on net sales or revenues or income from continuing operations', and similar requirements in relation to capital and liquidity.

In many jurisdictions, risk management principles are dealt with (in one way or another) in national corporate governance codes, as is the case with the New York Stock Exchange (NYSE) listed company rules, the UK's combined code, the French AFEP-MEDEF code and several other county regimes. Internationally, professional institutes and associations also offer their prescriptions. In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published an internal control – integrated framework guide, and in 2004 an enterprise risk management (ERM) – integrated framework guide. A report prepared for the OECD in 2010 concluded, however, "none of the existing guidance on risk management is adequate for the purpose. Most of the guidance is extremely high-level, is process-oriented and gives scant guidance on how to create an effective risk management and assurance framework." More recently, COSO published guidance on risk assessments and on risk appetite (2012), which provides more specific guidance on certain issues. In 2009, the International Organization for Standardization issued its standard for implementation of risk management principles, ISO 31000, which has de facto become the world standard. The purpose of ISO 31000 is to provide principles and generic guidelines on risk management that could achieve convergence from a variety of standards, methodologies and procedures that differ between industries, subject matters, and countries. In 2016 (year-end), the revised ERM standard of COSO has been released.

Enhancing Organizational Reporting: Integrated Reporting Key

There is emergence of Integrated Reporting Framework (IRF) on the global landscape. It is fast emerging as holistic framework of corporate reporting that goes beyond the traditional financial reporting frameworks. The key objective of the IRF is to align capital allocation and corporate behaviour to wider goals of financial stability and sustainable development through the cycle of integrated reporting and thinking.

International Federation of Accountants (IFAC) states that Integrated Reporting is the way to achieve a more coherent corporate reporting system, fulfilling a need for a single report that provides a fuller picture of organizations' ability to create value. Integrated reporting can be used as an "umbrella" report for an organization's broad suite of reports and communications, enabling greater interconnectedness between different reports. IFAC also strongly supports the International Integrated Reporting Council and the implementation of its Framework.

IFAC's position paper No. 8 addresses reporting that provides decision-useful information to organizational stakeholders beyond that which is provided in traditional financial reporting and financial statements, and may provide important links between that financial reporting and other organizational reporting.

Risk & Opportunity Reporting (ROR) is a key component in the IRF. The details of the ROR as part of the IRF are as under:-

a. Key risks impacting ability to create value in short term, medium term and long term- these could be from:-

   i) Internal sources – business related risks

   ii) External sources-from external environment

b. Key opportunities like those related to process improvement, employee training and relationships management.

c. Organisation assessment of likelihood that the risk or opportunity will fructify and probability or certainty of same.

d. Steps taken to mitigate or manage key risks or create value from key opportunities including identification of associated strategic objectives, policies, targets and KPIs.

4.3 Risk Management Disclosures – A Global Case Study

Let us study the annual report of Global major operating in the retail sector in 2016; Principal Risk and Uncertainties Disclosure in a summarised manner describes all the Principal Risk Factors covering Customer Proposition, Transformation of economic model, Liquidity, Competition and Markets, Brand, Reputation and Trust, Technology, Data Security and Privacy, Regulatory and Compliance, Safety, People, etc. Further, the Board discloses that three scenarios have been modelled, considered severe but plausible, that encompass these identified risks. None of these scenarios individually threaten the viability of the Company; therefore the compound impact of these scenarios has been evaluated as the most severe stress scenario.

Scenario	*Associated principal risks*	*Description*
Competitive pressure	• Brand, reputation and trust • Competition and markets • Customer	Failure to respond to fierce competition and changes in the retail market drives sustained significant like-for-like volume

		decline in core food categories with no offsetting price inflation, putting pressure on margins.
Data security or regulatory breach	• Brand, reputation and trust • Data security and data privacy • Political, regulatory and compliance	A serious data security or regulatory breach results in a significant monetary penalty and a loss of reputation among customers.
Brexit impact	• Competition and markets • Political, regulatory and compliance	Brexit continues to drive high UK domestic inflation and increased import costs from a weaker Sterling, compounded by new import duties and tariffs, with a consequential economic impact.

These scenarios assumed that external debt is repaid as it becomes due and also considered the results with and without the proposed Booker merger which is still subject to regulatory and shareholder approval and other conditions to a merger. The scenarios above are hypothetical and purposefully severe for the purpose of creating outcomes that have the ability to threaten the viability of the Group. In the case of these scenarios arising, various options are available to the Group in order to maintain liquidity so as to continue in operation such as: accessing new external funding early; more radical short-term cost reduction actions; and reducing capital expenditure. None of these actions are assumed in our current scenario modelling. Based on these severe but plausible scenarios, the Directors have a reasonable expectation that the Company will continue in operation and meet its liabilities as they fall due over the three-year period considered.

4.4 Risk & Opportunity Disclosures – An Indian Example

Let us study the annual report of a leading manufacturing company in India operating in the steel sector;

Risk & Opportunity Disclosure in the Annual Report (2017) is as under:

Risks and Opportunities

Risks

We are exposed to risks arising out of the dynamic macroeconomic environment as well as from internal business environment. These could adversely affect our ability to create value for our stakeholders.

Macroeconomic

- Over capacity and over-supply in steel industry
- High levels of imports
- Consolidation among competitors

- Local circumstances of geographies we operate in

Financial

- Volatility in financial markets and fluctuations in exchange rates
- Downgrading of credit rating of Company's securities
- Substantial amount of debt
- Restrictive covenants in financing agreements

Regulatory

- Predatory pricing
- Non-renewal of mining leases
- Non-availability of protective trade measures
- Regulatory and judicial actions

Climate Change

- International and domestic regulations relating to Green House Gas emissions

Operational

- Highly cyclical industry
- Inability to implement growth strategies
- Inherently hazardous industry
- Volatility in raw material prices
- Hostilities, terrorist attack or social unrest
- Failure of Information Technology Systems

Market Related

- Competition from alternate materials
- Product liability claims

People

- Continued services of Senior Management
- Unanticipated labour unrest

Opportunities

Setting benchmarks in the sector, we monitor and leverage opportunities presented by the external and internal environment.

- Capitalising the demand growth, due to urbanisation and needs of a young demography in

India, and developmental needs of other emerging economies

- Leveraging Supportive schemes of the Government such as the "Make in India" initiative
- Securing raw-material supplies by investing in mines which are in close proximity
- Innovating and adopting new technologies through Company-wide mobilisation of resources, implementation of pilots and capacity development
- Value realisation of by-products by exploring new areas of application, collaboration and potential customers
- Creating differentiation through acceleration of new product development, growing revenue from services & solutions and the B2C segment

5. DESCRIPTION AND EVALUATION OF FRAMEWORK FOR BOARD LEVEL CONSIDERATION OF RISK

Directors and boards need to ensure that policies, frameworks and governance arrangements are in place to ensue ethical conduct and decision making and effective risk governance and management. They must also make sure that their own conduct and the vision, mission, values, goals, objectives and priorities they set are conducive of them and do not undermine them.

The failure to address certain risks can prove catastrophic. Yet the taking of reasonable and calculated risks is at the heart of entrepreneurship. The courage to venture and explore is necessary for innovation if a company wants to progress. Hence, in relation to risk governance, directors need to achieve a balance between contending factors and there may be difficult choices to be made.

The following are some of the issues that directors may have to consider and the questions they should ask:

A degree of risk is inevitable in business operations. To obtain higher returns, innovate and secure market leadership one may need to adopt a higher risk strategy. Not innovating and being risk averse can result in the stagnation of the enterprise. A Board should establish and communicate its risk appetite and agree to the level of risk it is prepared to accept in different areas of corporate operation. Which stakeholder should be involved and how should they be engaged? Does the risk culture of the board match to that of the organization and its aspirations? If not, what changes are required and how might they be brought about?

What are the risk oversight functions of the board and how effectively are they being discharged? For example, is annual reporting of risk to shareholders fair and balanced? Would confidence accounting present a clearer picture? Within the governance structure, what arrangements have been made for risk governance which involves setting a strategy and policies for the management of risks and monitoring the performance of those to whom risk and security responsibilities are delegated?

Policies could cover the transfer of risk, such as whether or not to hedge or insure against certain risks, depending upon the costs and practicalities involved. They could establish criteria and thresholds for reporting and guiding management responses. Directors need to ensure effective processes and practices are in place for the identification and management of risks. How complex and comprehensive do these needs to be once the most likely and significant risks have been addressed?

Assumptions and business models should be periodically challenged. An assessment of the implications, consequences and dependencies of certain corporate strategies, policies and projects might reveal exposure and vulnerability. Corporate systems and processes need to be sufficiently resilient to be able to withstand the simultaneous materialization of multiple risks.

For example,

- Should an interruption in certain supplies occur, might just in time approaches result in shortages?
- What external and objective advice does the board receive in relation to risk?
- Overall, from the board perspective, what more needs to be done to build a risk resilient enterprise?

5.1 Corporate Risk Management

Are people within the organization and its supply chain aware of the diversity, incidence and severity of some categories of risk? For example, while overall relationships with customers might seem acceptable, what about particular relationships with key customers that are especially at risk? When addressing questions read the road ahead. A small account might have growth potential and could become strategically significant in the future.

Directors need to make sure that a management team and executives are not so focused upon listing and addressing individual risks that they overlook the interrelationship of different risk factors. An incident or development in one area can often have consequences elsewhere. For example, too many errors and exceptions can lead to overload and may bring down a system.

How well positioned is a company in respect of certain risks? Is the risk culture of the organization appropriate in relation to its activities, its operations and the opportunities it faces? A degree of balance is required. An excessively risk averse culture could prevent progress, but a step change increase in risk might be unsettling for some investors. High risk in certain areas can sometimes be balanced within a portfolio of activities and products by other items with lower risk profiles.

Processes and systems need to be adaptive as well as resilient. The nature and source of risks can change. As old ones are addressed so new ones may emerge. Are risk registers and management reports relating to risk over generalized? How realistic are they in relation to assessments of risk and planned corporate responses? Do they provide sufficient evidence and explanation to inform the board's own reporting of risk to shareholders?

5.2 Risk Management Frameworks, Approaches and Techniques

The following are the points to be considered by the Board :

- Has the management team established an effective risk prevention, management and control framework?
- Are people equipped with the skills, tools, techniques and other support they need to effectively operate it?
- Are the techniques used adequate in the situation and circumstances? How outward looking and inclusive does risk management need to be?
- Are the risks of major and strategic customers and business partners understood?
- Are business opportunities being identified for how the company might use its capabilities to help customers and others to mitigate, prevent or manage the risks they face? Does the company's risk management framework, policies and practices extend to its supply chain? In particular, are supplier risks and the risks of activities such as outsourcing and joint ventures assessed and managed? Does this involve collaborative action where relevant?
- Is the risk registering a living document? Are the prioritization of risks, mitigation measures, responsibilities and residual risks regularly reviewed? Are risk reports color coded to reflect likelihood of occurrence and impact?
- Is the direction of travel given?
- Are movements in relation to high priority "red rated" risks monitored by the board? Are there trigger points at which additional advice is sought and/or further resources deployed or other action taken? Are risk factors understood, appropriately categorized and mapped? Are the risk assessment criteria used reasonably and fair in the circumstances? Do the results of risk analysis inform business and management decisions? Are they inhibiting or supporting innovation and entrepreneurship?
- To whom should risk management responsibilities be delegated? Is there a Chief Risk Officer (CRO)? If so, how is the role of the CRO changing? What skills and experience are required by risk management professionals? What steps are taken to ensure that other people do not abdicate their responsibilities in relation to risk by leaving too much to the CRO and his or her team?
- Responsibilities for risk prevention, mitigation and management need to be delegated with care. Allocating them to particular individuals can sometimes led to others assuming that risks are "taken care of "and not themselves being alert to risks. A healthier approach may be to both delegate and ensure all staff reflect upon and help to address risks inherent in their roles and any corporate operations they are involved in. Any risk concerns they might have should be reported.
- What should be done to ensure that adopted approaches to risk management are current and that knowledge of changing risks and how they might best be addressed is up-to-date? Within the governance structure, how does the CRO relate to and collaborate with the audit, compliance, finance and legal teams? Are regular formal and/or informal meetings held to identify and discuss patterns, trends and common root causes?

Some boards regularly review schedules of risks notified by management, but rarely consider less predictable and external risks such as natural disasters, an act of terrorism or political instability. Does issue monitoring and management involve identifying and ranking developments in the eternal business environment and assessing their impact upon a company and its customers and supply chain? Do the results feed into risk management processes? Is the risk management team involved in deciding what action a company needs to take in response?

Certain unpredictable events might potentially have huge implications for companies and their activities. Corporations have had their assets and operations nationalized as a result of regime change. How resistant would offices and plants be to gales, floods or a tsunami or earthquake? How should a company cope with a terrorist attack, a pandemic, a sudden interruption to its supply chain, the loss of key staff, or a breakdown of law and order? Are contingency arrangements and backup and recovery plan in place? How resilient area company's finances and business model?

Companies that operate internationally sometimes find that the risk profiles of their local activities vary significantly. Particular involvements might expose them to geopolitical, economic, trade and other risks. These could range from a repudiation of debts to the sudden devaluation of currencies.

Some risks might be insurable at a cost, while others may need to be borne. How does a company assess unpredictable and/or uninsurable risks? Are these spread across a range of activities, or is there disproportionate exposure in certain markets? Are such risks and a distinctive risk management perspective taken into account in related and strategic decision making? For example, a strategy of focusing upon a core business has resulted in many companies being less diversified and having "more of their eggs in a single basket."

The continuing operation of many businesses as going concerns is dependent upon the effective operation of the utilities, the banking and financial system and the activities of governments, regulators and the legal system in the major markets within which they operate even in advanced countries, one cannot assume a banking and financial system will remain free of the challenges and loss of confidence that occurred in the period 2008-09 and which led to bank failures and bailouts.

A company's defenses are only as strong as the weakest link across the various networks to which its people and operations are connected. The internet of things is a frontier of opportunity for hackers. The issue is not whether a breach will occur, but how to limit the damage and recover quickly when a breach occurs.

Monitoring of emerging and mutating threats in relation to cyber security and fraud, is important., such as sharing of information about identified threats, breaches and responses with other organizations, regular review of cyber security and information governance policies, testing of threat scenarios and planned responses and contingency arrangements.

Checks to avoid money laundering, to avoid the loss of strategically significant intellectual property and unapproved access to personal information when data thefts occur/ means of information when in case of corporate data breach and compensation to those who suffer losses.

The speed with which defensive and anti-malware software, and data and system security, can be updated quickly as and when the need arises, is also a key question.

Further, whether adequate security, measures to a company's supply chain, corporate data that is held externally and corporate systems that are operated by thief parties? How secure are "working from home" equipment, customer support facilities and portable devices? What advice and assistance is given to staff and business partners in these areas?

The management/Board should also consider and review the usefulness of International frameworks and standards such as COSO's ERM framework, ISO 31000 standards, in enterprise risk management, in effective internal control and fraud deterrence and prevention, mitigation and management of risk.

5.3 Striking the Right Balance in Action and Reaction

Today, companies operate in an uncertain world. Management and Boards face multiple challenges and confront sensitive issues. Circumstances demand difficult decisions.

An organization that is prepared is able to respond quickly and aptly when unwelcome risks materialize. Having a moral compass and reacting in a proportionate, fair and responsible way can help a company and its board to restore confidence, maintain trust and build relationships with stakeholders. This can be achieved by listening to peers and learning, thereby building resilience and a balanced perspective. It is important to both recover and move forward while responding to incidents.

In a globally competitive market transition and with intense digitization taking place in the country, it is but necessary that risk appetite and risk mitigation measures are fully integrated with the business plans and policies so that the companies can benefit by correctly assessing their risk appetite and identifying and mitigating risk in time. Cyber Security has taken a new dimension and is important not only for the financial sector but for all sectors of the society. The majority of the cases reported so far under cyber security refer to financial institutions, alone, whereas cyber security for infrastructure sectors is equally important.

Today, Companies from different sectors of activities are seriously trying to put the risk management system in place as per the international standard. What is now needed is an emphasis on the effective implementation, thereby ensuring maximum benefits to the companies and "Enterprise risk management" emerging as the "Business differentiator".

6. OECD GUIDELINES (PRINCIPLES) FOR CORPORATE GOVERNANCE

The Organization for Economic Corporation and Development (OECD) emphasized the importance of corporate governance and has developed set of principles for better corporate governance. The principles are intended to assist and improve the overall economic efficiency and bring more stability to the markets.

6.1 Ensuring the basis for an effective corporate governance framework

The corporate governance framework should be developed keeping in mind the macroeconomic changes, market situation and legislation requirements. Companies implementing corporate governance need to have a method of regularly reviewing and monitoring the objectives set as part of the framework. It should be ensured there is proper distribution of responsibilities among the authorities and it is clearly articulated. The management along with the responsibilities should be vested with the powers to take timely, transparent and correct decisions which are in line with the strategy defined by the company.

6.2 The rights and equitable treatment of shareholders and key ownership functions

Under the Companies Act, shareholders are classified under different categories like equity shareholders, preference shareholders etc. Shareholders can influence an organization's core functioning as they have right to participate and vote in general shareholders meeting, elect the board member, make amendments to company's organic documents, approval of extraordinary transactions, etc.

The Corporate governance framework ensures the equitable treatment of all the minority and foreign shareholders. Also, shareholders should have the appropriate redressal mechanism for any violation of their rights.

The acquisition of corporate control in the capital markets, mergers, and sales of substantial portions of corporate assets, should be clearly articulated and disclosed so that investors understand their rights and recourse.

6.3 Institutional investors, stock markets, and other intermediaries

The corporate governance framework should provide sound incentives throughout the investment chain and provide for stock markets to function in a way that contributes to good corporate governance.

6.4 The role of stakeholders in corporate governance

The corporate governance framework should recognize the rights of stakeholders established by law or through mutual agreements and encourage active co-operation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises. Further, the mechanism for employee participation should be encouraged. Also, stakeholders should have access to regular flow of information.

6.5 Disclosures and Transparency

An organization should have adequate disclosures regarding the following:

- The financial and operating results of the company.

- Company objectives and non-financial information.
- Major share ownership, including beneficial owners, and voting rights.
- Remuneration of members of the board and key executives, Information about board members, including their qualifications, the selection process, other company directorships and whether they are regarded as independent by the board.
- Related party transactions.
- Foreseeable risk factors.
- Issues regarding employees and other stakeholders.
- Governance structures and policies, including the content of any corporate governance code or policy and the process by which it is implemented.

A strong disclosure regime can help to attract capital and maintain confidence in the capital markets.

An annual audit should be conducted by an independent, competent and qualified auditor in order to provide an external and objective assurance to the board and shareholders that the financial statements fairly represent the financial position and performance of the company in all material respects.

6.6 The responsibilities of the board

- The Board members should act in good faith, diligently and in the best interest of the company and the shareholders.
- The Board should also adopt high ethical standards.
- The Board should also review and guide corporate strategy, action plans, management policies and procedures etc.
- The Board should also monitor the company's governing practices and make required changes as and when required.
- Monitoring and executing the selection, remuneration and replacement of key executives.
- Ensuring a formal and transparent board nomination and election process.
- Monitor and manage conflicts of interest of management, misuse of corporate assets and abuse in related party transactions.
- Ensure the integrity of the company's accounting and financial reporting systems and make sure that appropriate systems are in place for risk management, financial and operating control.
- The Board should oversee the process of disclosure and communications.

(Source : OECD Website)

CHAPTER 8

ENTERPRISE RISK MANAGEMENT

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

- Definition
- Scope
- Techniques

1. DEFINITION AND SCOPE OF ENTERPRISE RISK MANAGEMENT

Fast-changing business scenario, uncertainty arising from global events, disruptive competition, and protectionist agenda of cultural majorities and volatility of commodity and currency prices creates stress and complexity in managing businesses. Gradually, these events start playing on the minds of stakeholders. The occurrence of risk events coupled with their poor handling impacts organisational performance. Enterprise Risk Management (ERM)/ Business Risk Management (BRM) is a structured form to assists organisations in preparing for the worst-case scenario, while aspiring to be "better, faster and cheaper". ERM is arguably the only effective tool in contemporary times that assists in the evaluation and bridging of the gap between uncertainty and performance in organisations; also a simplified approach to problem solving and making the organisation nimble footed. Iconic entities that feature in the top global rankings consistently practice integrated risk management.

Enterprise risk management (ERM) is a leading best practice approach to effectively manage and optimize business events that have the potential to impact business objectives or risks, enabling a company to determine how much uncertainty and risk are acceptable to an organization. Various definitions of risk management are enumerated as below :

CIMA Official Terminology, 2005

'A process of understanding and managing the risks that the entity is inevitably subject to in attempting to achieve its corporate objectives. For management purposes, risks are usually divided into categories such as operational, financial, legal compliance, information and personnel. One example of an integrated solution to risk management is enterprise risk management.'

Webster's New World Law Dictionary

The process of assessing risk and acting in such a manner, or prescribing policies and procedures, so as to avoid or minimize loss associated with such risk.

With a company-wide span, ERM serves as a strategic analysis tool, cutting across business units and departments, and considering end-to-end processes. In adopting an ERM approach, companies gain the ability to align their risk criteria to business strategy by identifying events that could have an adverse effect on their organizations and then developing an action plan to mitigate them.

By applying ERM in conjunction with other operational elements in the current business environment, companies can also accomplish many of their governance-related tasks.

Specifically, ERM can help organizations:

1. Identify strategic risk opportunities that, if undertaken, can facilitate achieving organizational goals.
2. Introduce a common language within the organization where people recognize problems and adopt a problem solving approach by developing risk treatment actions.
3. Provide senior management with the most up-to-date information regarding risk that may be used in the decision-making process.
4. Establish linkage between the ERM initiative and adherence to capital market reporting disclosures and other corporate laws and regulations.
5. Align annual performance goals with risk identification and management.
6. Encourage and reward upstream reporting of business-risk opportunities and challenges.
7. Align other risk monitoring initiatives such as self-appraisals, internal auditing activities, control assessments, continuous control monitoring, to organizational objectives.
8. Imagining key Risk Scenarios that could potentially result in a stress on the financial position of the company.
9. Financial Risk monitoring a part of the ERM initiative can balance the financial stability equation of the company

Among the more widely known frameworks and/or standard, and the related ERM definitions that they promulgate are:

- **ISO 31000 Risk Management Standard:** provides a set of principles, a framework and a process for managing risk.
- **COSO ERM Framework:** This framework defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management.

Enterprise risk management (ERM) is a plan-based business strategy that aims to identify, assess and prepare for any dangers, hazards and other potentials for disaster – both physical and figurative – that may interfere with an organization's operations and objectives. Relatively new (it's less than a decade old), the discipline not only calls for corporations to identify all the risks they face and to decide which risks to manage actively; it also involves making that plan of action available to all stakeholders, shareholders and potential investors, as part of their annual reports. Industries as varied as aviation, construction, public health, international development, energy, finance and insurance all utilize ERM. *(Source : Investopedia)*

Risk management in an organization minimizes the impact of risk on the business with the help of a chief risk officer or a risk committee but it does not give a guarantee that the organization will become risk free.

2. IMPLEMENTING ERM

COSO framework states that Enterprise Risk Management (ERM) is defined as a process, affected by an entity's board of directors, management, and other personal, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. ERM includes the following activities:

- Determining the risk appetite.
- Establishing an appropriate internal environment, including a risk management policy and framework.
- 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 assurance on the effectiveness with which risks are managed.

The term 'risk appetite' used in the above definition refers to the extent of risk that the Board is 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, and 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.

While risk appetite is to be set lower than the risk capacity; however, with an aggressive Board, the risk appetite can be higher than the risk capacity. For example, the Board may decide on utilizing the cash flow for operational purposes in the short term for earmarked funds meant for payment of quarterly installment of taxes. This could result in default of payment on due date and hence becomes a significant risk which needs to be covered by the internal auditor and reported upon even though the risk may be within the risk appetite. However, in the normal course, internal auditors are expected to take the risk appetite as a given and evaluating the risk appetite is out of audit scope. Internal auditors can, however, do a consulting activity of assisting the Board in fixing the risk appetite and its documentation.

ERM is a new approach in the ways organizations are assessing, managing and communicating business risks. By assisting organizations climb up on the risk maturity scale, ERM makes a major contribution towards helping an organization manage risks to achieve its objectives. ERM helps an organization become a risk managed business.

An ERM policy is first put in place which defines the guiding principles showing 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.

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

Risk Register

- Risk register is a record of risk, risk assessments; risk mitigation and action plans prepared by the responsible parties that help to support overall ERM and controls disclosures reporting process.
- Risk register is continuously updated and has columns for risk, causes, consequences, ownership, inherent risk score, controls, residual risk score, process, action for further mitigation, action owner, due date, etc.

3. TECHNIQUES OF ENTERPRISE RISK MANAGEMENT (ISO 31000 SUGGESTS KEYS TO ERM IMPLEMENTATION)

It starts with themes to provide management with a strong foundation for an effective ERM program as they develop and tailor their specific approach to implementing ERM. These themes "Keys to Success" for organizations that are starting ERM initiatives and provide a useful

foundation for specific actions detailed. These keys also help company's board to address some of the recognized barriers and resistance points to ERM adoption.

Key 1: Winning support and sponsorship from the Top management is a pre-cursor

The Board of directors should sponsor the ERM function and activities by providing the right focus, resources and attention for ERM. ERM must be truly enterprise wide, and understood and embraced by all personnel, and driven from the top through clear and consistent communication and messaging from the company's board to senior management and to the organization as a whole.

The Board needs to put in place an effective ERM leader who is widely respected across the organization and who has accepted responsibility for overall ERM leadership, resources and support to accomplish the effort.

Key 2: Building ERM using small but solid steps

Organisation can start with a simple process and build from there using incremental steps rather than trying to make a quantum leap to fully implement a complete ERM process.

By doing so, they are able to:

- Identify and implement key practices to achieve immediate, tangible results.
- Provide an opportunity to change and further tailor ERM processes.

Key 3: Focus on a simple Risk model with Small Number of Top Risks

The ERM team should identify small number of critical and strategic risks that can be managed, and then evolve from this start.

Focusing initially on a smaller, manageable number of key risks would also be beneficial in developing related processes such as monitoring and reporting for those specific risks. This focused approach also keeps the developing ERM processes simple and lends itself to subsequent incremental steps to expand the risk universe and ERM processes.

Key 4: Leverage Existing Resources

Organizations often discover that they can rely on their existing staffs, with the knowledge and capabilities relating to risks and risk management that can be effectively used to start the ERM process. For example, some organizations have used their Chief Audit Executive or their Chief Financial Officer as the catalyst to begin an ERM initiative. In other instances, organizations have appointed a management committee, sometimes headed by their Chief Finance Officer (CFO), to bring together a wide array of personnel from across the entity that collectively have sufficient knowledge of the organization's core business model and related risks and risk management practices to get ERM moving.

In addition, most organizations start their ERM effort without any specific enabling technology or automated tools other than basic spreadsheets and word-processing capabilities.

Key 5: Build on Existing Risk Management Activities

Existing functions such as internal audit, compliance, ethics and other support function could be leveraged to build on the ERM blocks and activities.

Key 6: Embed ERM into the Business Fabric of the Organization

ERM is a management process, ultimately owned by the board of directors and involves people at every level of the organization. The comprehensive nature of the ERM process and its pervasiveness across the organization and its people provides the basis for its effectiveness.

ERM cannot be viewed or implemented as a stand-alone staff function or unit outside of the organization's core business processes. In some companies and industries, such as large banks, it is common to see a dedicated enterprise risk management unit to support the overall ERM effort including establishing ERM policies and practices for their business units.

Key 7: Provide On-going ERM Updates and Continuing Education for Directors and Senior Management

ERM practices, processes and information continue to evolve. Thus, it is important for directors and senior executives to ensure that they are receiving appropriate updates, new releases and continuing education on ERM, including information about regulatory requirements and best practices.

This information provides the opportunity for directors and senior management to update their risk management processes as they become aware of new or developing practices. This ongoing improvement process is particularly important with the increased focus on ERM by regulators, rating agencies, and the capital market authorities.

4. RISK MATURITY OF AN ORGANIZATION

Some organizations especially those in a fast growth mode have an organizational culture which promotes operational managers to remain at the risk naïve/ risk aware level. This means that the line managers are not expected to identify risks and if they do, it is confined to their personal knowledge or within their functional team. The internal control environment may be well defined but again it is to be operated by the staff management (such as the accounts manager), the logic being that line managers need to spend maximum time in operations and not be defocused by 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 wherein the organization sells whatever it produces but flounders in a competitive and dynamic 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.

A risk naïve/risk aware organization in today's dynamic environment exhibits inefficiencies as a continuous long list of pending issues at all times with the line manager or even mundane issues

as goods received but unreconciled with Purchase Orders, delayed supplier payments resulting in line managers chasing accounts department for release of payment, etc., wherein the root cause is usually a risk which has not been addressed. In a risk aware organization, the silo approach culture wherein the manager tracks and addresses new risks related to his department only rather than in the business process usually throws up big losses arising out of customer dissatisfaction or failure of an enterprise wide activity such as implementing ERP.

The audit strategy depends upon the organization's risk-maturity. Organizations at low risk maturity levels may require internal auditors to consult by promoting and advising on identification of and response to risks. For organisations with high risk maturity, the internal auditor would need to concentrate more on carrying out process audits of the risk management processes and especially reviewing the risk assessment process wherein the inherent risk (untreated) are identified, estimated (scored) and evaluated (compared with risk appetite).

Risk Maturity Levels

The following aspects in the organisation indicate its risk maturity. Internal auditors should refer to the same for concluding on the organisation's risk maturity:-

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

The table given below shows the levels of risk maturity. Key Characteristics at Different Levels of Risk Maturity:-

Risk Maturity	*Key Characteristics*
Risk Naive	No formal approach developed for risk management.
Risk Aware	Scattered silo based approach to risk management. Risks identified within functions and not across processes. Also risks not communicated across enterprise.
Risk Defined	Strategy and policy in place and communicated. Risk appetite defined.
Risk Managed	Enterprise wide approach to risk management developed and communicated. Risk register in place.
Risk Enabled	Risk management and internal control fully embedded into operations. Organization in readiness to convert market uncertainties into opportunities.

5. PROCESS OF ENTERPRISE RISK MANAGEMENT AND INTERNAL AUDIT

Enterprise Risk Management is a structured, consistent and continuous process of measuring or assessing risk and developing strategies to manage risk within the risk appetite. It involves identification, assessment, mitigation, planning and implementation of risk and developing an appropriate risk response policy. Management is responsible for establishing and operating the risk management framework. The Enterprise Risk Management process consists of Risk identification, prioritization and reporting, Risk mitigation, Risk monitoring and assurance. Internal audit is a key part of the lifecycle of risk management. The corporate risk function establishes the policies and procedures, and the assurance phase is accomplished by internal audit.

6. STAKEHOLDER VALUE CREATION BY ENTERPRISE RISK MANAGEMENT

Effective implementation of Enterprise risk management leads to number of benefits to the business and society. The full value of payoff is realised over a period of time. It is similar to a business entity implementing and Enterprise Resource Planning Package where the return on investment in over a period of time likewise when ERM is implemented the payoff is realised over few years of the business life-cycle. The gains from ERM implementation are realised in two stages intermediate/ short term and long term.

The Risk Management Payoff Model of Epstein and Rejc, 2005, demonstrates how improved risk measurement and management provides benefits throughout the organization. Benefits extend to

(a) enhanced working environment,

(b) improved allocation of resources to the risks that really matter,

(c) Sustained or improved corporate reputation, and

(d) Other gains, all of which lead to prevention of loss, better performance and profitability, and increased shareholder value.

Successful Stakeholder Risk Management

It is necessary to evaluate all types of risks impacting all categories of stakeholders and find solutions to pre-empt the threats before the risk occurs. The more one knows about the stakeholders and their levels of importance, the more effective and purposeful the risk management strategy will be. The risk management program should look at the big picture and identify not only short term risk factors but also long term factors impacting the entire value chain of business activities and connected communities.

CHAPTER 9

OPERATIONAL RISK MANAGEMENT

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

- Operational Risk Management
  - (a) Definition,
  - (b) Scope and
  - (c) Techniques

1. INTRODUCTION

1.1 What is Operational Risk?

The most commonly used and accepted definition of operational Risk is from Basel II which states that Operational Risk is the risk of loss resulting from inadequate or failed processes, people and systems and from external events.

This definition includes legal risk, but excludes strategic risk and reputational risk.

Basel II is the common name used to refer to the "International Convergence of Capital Measurement and Capital Standards: A Revised Framework," which was published by the Bank for International Settlements in Europe in 2004, and the framework is broadly adopted, with country level customisation as required by the countries that have been party to the accord. While this was specific only for the regulated financial institutions industry, the overall concept of operational risk remains the same irrespective of the industry.

Each and every industry, whether manufacturing, trading or in service sector, is subject to a degree of operational risk though the level of risks may differ between industry sectors,

companies, the nature of products and services offered, and the actual management control over these risks.

Operational risk is an overarching concept interrelated with several other types of risks, and cannot be viewed in isolation. The most important risks linked to operational risk are risk of non-compliance to applicable laws and regulations, risk of fraud losses due to an internal or external event that takes advantage of gaps in the processes to make an unlawful gain, risk of financial losses, risk of incorrect financial reporting, and in several organisations, reputational risk is also part of the areas touched by operational risk.

1.2. Why does operational risk originate?

(a) Inadequately defined products and services which may not be compliant to industry regulations, and/or may be exposed to risk of misspelling;

(b) Inadequately defined policies and processes which would directly adversely impact quality of controls like checks and balances, segregation of duties as may be required;

(c) Inadequate technology functionality, or infrastructure that exists in any technology supported environment, which organisations use in respective business operations;

(d) Internal or external crime that takes advantage of gaps in processes for unlawful gain, i.e. fraud;

(e) External events like terrorist attacks or natural disasters that disrupt business or cause financial losses;

(f) Change in the environment of the industry sector (including significant regulatory changes) that impacts the operational risk profile of an organisation.

Thus, Operational Risk Management (ORM) is primarily an exercise in mitigating potential losses, i.e. possible losses, through a well-laid out mechanism of identifying the inherent risks in a business process and reviewing / testing the efficacy of the controls related to each risk.

Additionally, an important part of ORM is also to identify and report operational risk events, including their financial impact (losses and recoveries) if any. Thus, an adequate governance framework is expected to cover both the preventive and the lag aspects of operational risks.

In coming sections, we shall also elaborate on the concepts outlined above, in terms of how policies, processes and technology failures can cause possible risks and losses.

2. RELEVANCE OF OPERATIONAL RISK

Why is operational risk relevant for accountants, auditors and management professionals?

(a) The Companies Act 2013 (Sections 134 and 177) lays down clear expectations from Boards of organisations in assessing the robustness of risk management framework implemented by the company. Section 134 instructs that Board of Directors should include a statement on

development and implementation of risk management framework for the company, including identification of risks, which as per Board's opinion could threaten the very existence of the company.

Clause (e) of Sub-section 5 of Section 134 explains the meaning of the term 'internal financial controls' as "the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information."

Section 177 instructs that the Audit Committee shall review the risk management procedures implemented by the management.

Schedule IV instructs that Independent Directors are required to get assurance that systems of risk management are robust and defensible.

(b) Paragraph 4(c) of the Standard on Auditing (SA) 315 "Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment" defines the term 'internal control' as "the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, safeguarding of assets, and compliance with applicable laws and regulations. The term "controls" refers to any aspects of one or more of the components of internal control."

(c) Clause 49 of the Listing Agreement, indicates that disclosures are to be made to the Board of Directors on risk management, on whether the company has laid down any procedures to inform Board members about the risk assessment and mitigation procedures.

(d) The ICAI Guidance Note on Audit of Internal Financial Controls over Financial Reporting has several sections pertinent to the understanding of operational controls underlying in the processes;

While the Guidance Note does not explicitly dwell on operational risk per se, the overall approach and methodologies mentioned in the Note rest on, and derive from an implied understanding of the auditor's understanding of operational risks and the mitigating controls of the organisation; for instance, the auditor is expected to have a thorough understanding of the automated and manual controls that lie in each of the processes that have a direct bearing on the financials of the organisation.

The following section on auditor's responsibility is broadly paraphrased from the Guidance Note, and it is recommended that the student read it in entirety for a holistic understanding:

- Assessing risks across the organisation that could lead to a material misstatement in the financial statement;

- Segregation of duties in processes;
- Addressing compliance requirements, fraud risk mitigation and implementation of meaningful control strategies;
- Assessment of Control environment, including the use of technology to automate control activities, to ensure timeliness, accurate and reliability of the information used in the financial control are dependent on underlying application systems that are used to generate, process, store and report the information in a manner that adequately addresses effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability;
- Testing of Information Provided by Entity (IPE), and EUC (End Use Computation tool);
- The auditor should test the design effectiveness of controls by determining whether the company's controls, if operated as prescribed by those authorised to perform the controls, satisfy the company's control objectives and can effectively prevent or detect frauds that could result in material misstatements in the financial statements.
- A review of control is to be done with regard to appropriateness of the purpose of the control and its correlation to the risk/assertion; appropriateness of control considering the nature and significance of the risk; competence of authority performing the control (especially if it is of a nature of supervisory review); frequency and consistency with which the review control is performed, including clarity of the exact steps of performance of the review control;
- An assessment of the regulatory compliance framework in highly regulated industries also is part of the exercise, and any significant weakness in internal controls related to implementing compliance requirements may result in a material weakness highlighted in the report.

(e) Moreover, Indian companies eligible to be covered under compliances of Sarbanes Oxley ("SOX") regulations have to adhere to a comprehensive framework of documentation and testing of risks and control framework, and these necessitate that the management personnel, consultant or auditor be highly proficient in assessing operational risk that impacts all categories of risk such as regulatory risk, financial loss risk, financial reporting risk, legal and contractual risk, fraud risk and reputational risk etc. The companies where SOX stipulations are applied, have to adhere to internationally established practices of risk management.

(f) The Internal Audit processes also establish a direct connection between risk management and audit methodology; currently most internal audit firms practice a Risk Based Audit approach, which necessitates an understanding of all risks including a comprehensive understanding of operational risks since it overarches on several other areas of risk.

(g) Operational risk forms a significant part of the ERM framework. Several organisations that are

complying to the Companies Act 2013 stipulation on implementing a risk management framework.

(h) Several organisations adopt standards like ISO 31000 (risk management), ISO 9000 (quality), and ISO 31000 (cyber security) for better management of risks. Professional managers working on these are also required to have an understanding of operational risk.

(i) For highly regulated entities such as banking that come under RBI regulation, there are very comprehensive requirements on operational risk management. Banks are also required to provide capital under regulatory norms, for which specific calculation methods are also prescribed.

Hence there is a strong convergence of audit and operational risk in current context of corporate governance responsibilities of management, Board and the role of the auditors.

3. OPERATIONAL RISK MANAGEMENT GOVERNANCE

As outlined in section 1, as part of the overall responsibilities of the Board of Directors, an oversight on the operational risk profile of the organisation is also included. The nature and intensity of Board oversight may differ from organisation to organisation, depending on its constitution, any specific requirements from a regulatory angle, the industry and the nature of business etc.

For banks it is mandatory to have an Operational Risk policy approved by the Board, and the RBI guidelines have clearly described roles and responsibilities of the ORM Committee, the Chief Risk Officer and other roles that are expected to engage in the implementation of the framework. For other industries where a Board approved policy may not be mandatory as per regulatory environment, it is still strongly advisable to have a comprehensive policy documenting the governance mechanism of operational risk.

3.1 Operational Risk Management Policy

The following areas are advised to be addressed in the Policy; the list is indicative and not comprehensive; the organisation depending on the priorities and readiness level can evolve new areas to be covered.

- Role of the Board and the Risk Management Committee of the Board in driving the implementation of the framework;
- Setting up an Operational Risk Management Committee comprising of senior management with an outline of the membership, quorum and frequency of meetings;
    - ♦ The review of the Risk and Control Self Assessment (RCSA) results, Operational risk events, Loss reports, and breaches of Key Risk Indicators;
    - ♦ Risk assessment of new products and services;

- ♦ Risk assessment of existing and new Technology platforms;
- ♦ Review of Cyber risk (Information security);
- ♦ Review of Business Continuity and Disaster Recovery framework;
- ♦ Review of any regulatory development or external events that may impact the operational risk profile of the organisation;
- ♦ Management functions may highlight identified process gaps and potential issues discovered by way of routine business or reviews, and include the action being taken on them. The self-awareness of the management functions on highlighting such issues is an evolving process.

- The broad methodology of setting up the Risk & Control Self-Assessment library, the roles and responsibilities of those engaged in performing the control testing, the collation of results and review process need to be outlined in the Policy.
- The constituents of the framework, like RCSAs, KRIs, Loss-Data to be described in detail followed by a brief on roles designated to perform the necessary activities. Each of the policy stipulations is to be ideally backed up with corresponding process notes to detail the granular steps in implementation.
- Operating linkages with the other units such as those manage the policy and process documentation of the organisation, product development, internal audit, regulatory compliance unit, information security officer, business continuity plan etc. need to be outlined since operational risk impacts all these areas.
- Capital computation methodology if applicable, needs to be described in the Policy.

3.2 Operational Risk Management Committee (ORMC)

The ORMC must conduct its business basis a Charter / Terms of Reference and the proceedings and discussions are advised to be documented for future reference and follow-up on agreed actionables. The regular updates to the Board (or the Risk Management Committee of the Board if the task is assigned to it by the Board) have to be provided by the management, covering key highlights of all the constituents.

The Operational Risk framework is effective only if imbibed at all relevant linkages who are managing the monitoring process at the departmental level. Hence it is advised that the Committee instruct and/or arrange regular trainings and awareness camps for the departmental staff, including giving them sufficient understanding of process of identifying new risks and adding them to the RCSA library from time to time, a process duly assisted and facilitated by the Operational Risk unit.

3.3 Lines of Defence

Basel II norms indicate the recommended governance of operational risk in an organisation by three lines of defence model. This is followed by banks in India too as part of regulatory guidance on operational risk management. However, this concept can be used by any industry with some customisation on basis of the organisational structure, the complexity of the business processes and evolving capability of the control awareness.

The ***First line of defence*** is the function/department/role that owns the process. They are supposed to have sufficient governance on the operational risks pertaining to their areas of responsibility, such as

- Set up required policies govern the area of work,
- Establish process notes, control-steps in the process notes, and methods to measure the efficacy of the controls,
- Perform the self-assessments and monitoring of risk indicators, etc.
- Examples are, in a financial organisation, the Operations department often has a detailed set of process notes that assign control steps to designated individuals, and also a method of measuring / tracking if the controls were exercised properly.

These tracking / measuring tools could be at varying frequency, being built into a formal RCSA (Risk Control Self-Assessment) where risks and control efficiency are highlighted. This line functions closely with the Second line in a collaborative method which could be formalised in any governance process established by the ORM Committee.

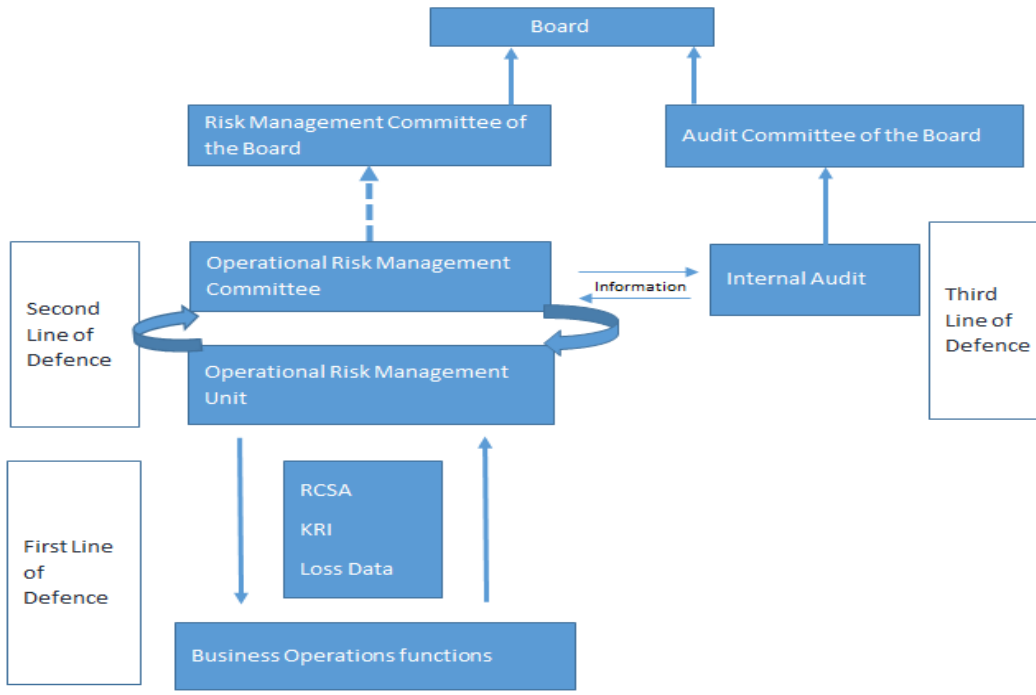
The ***Second line of defence*** is the Operational Risk department, which while being part of the management framework, sets up, oversees the operational risk management of the first line of defence. The typical roles played by the second line of defence are:

- Working with the process owners (first line of defence) to set up the risk and control matrix.
- Advise / recommend the method and frequency of testing of controls to the first line of defence, thereby setting up a self-assessment process based on the RCM.
- Perform risk assessment of new products, services and processes, especially in instances where new technology is being deployed.
- Review and publish results of the RCSAs and risk assessments, and any exception reports / Key risk indicators set up in the framework.
- Convene, and report to the ORMC, and report to the Board / Risk Committee of the Board as well with the necessary updates.

The ***Third line of defence*** is Internal Audit; it is independent of management control and reports to the Audit Committee of the Board.

- An effective internal audit would highlight issues and potential gaps in processes, which were missed by the first two lines of defence as well. As an independent vertical, their value addition provides a better insight into the process from a holistic perspective since they are not directly involved in managing the process.
- Checking on efficacy of controls that mitigate operational risk, is a key deliverable of Internal Audit.
- Over last few decades, internal audit has evolved into a concept of Risk Based Auditing. The term itself refers to an approach where the audit function identified risks and controls in a very similar fashion as the operational risk methodology, and then choose to focus their attention and deploy resources on checking the areas of choice.

All three lines of defence are expected to work in a professionally collaborative manner, respecting each other's views and concerns. ORMC of an organisation must include the Internal Audit head too, in addition to senior management, so that a holistic view of the risks and controls is obtained.



For an effective Operational Risk Management Framework, the following focus areas are recommended; though they fall outside the direct management of the Operational Risk

department, these are prime drivers of operational risk, and hence frequently either the cause of higher operational risks and/or its remedial measure.

3.4 Effective policy framework

- **Entity level policies:** Depending on nature of the industry and applicable regulations, it is necessary for an organisation to have certain high-level policies that are applicable to the organisation, irrespective of lines of businesses or departments. These are typically owned at the highest levels of management and set the tone at the top. Examples are Code of Conduct for employees, Whistleblower policy, Expense Delegation Policy, Procurement Policy, Information Security Policy etc.
- **Line of business / Departmental policies:** Depending on nature of the business an organisation is engaged in each business activity or department may need suitable Policies to govern and direct its functioning. Inadequate definition of the policy statement and responsibilities thereof are often a cause of operational risk events. Examples are Credit policy in a lending institution, product specific policies in a manufacturing industry, Human Resources policies, and Operational policies. Policies often include a "standard" too, which outlines the specific deliverables and a minimum expected level of performance in it. In some organisations, the Standards could be maintained outside the Policy documentation, nevertheless, it is an advisable item to have in overall governance process.

Policies have to be made in a manner that they are compliant all existing applicable laws and regulations, and enable the organisation meet the business objective.

3.5 Process notes / Standard Operating Procedures (SOP)

Process notes are detailed instructions that address the specific responsibilities given in the policy documents; process notes detail the roles and responsibilities of each department / responsible person in executing a process/ transaction; it is expected that process notes have fair granularity, on how exactly a process is executed, including the controls to be exercised. In an advanced operational risk management environment, the process notes tend to be very articulate and define the processes granularly and leave no scope for ambiguity or misinterpretation by those responsible for execution.

Taking the same example as in policies, in a lending institution, a credit process note would detail the exact steps that an organisation is to follow, in lending money to a customer and all the checks and controls expected to be done in the process. A manufacturing process manual may describe in detail aspects like the factory specifications, technology used in the process or the sub-process, the assembly line, the specific departmental, and individual roles and technical tasks, output, productivity and the quality expected.

4. RISK IDENTIFICATION AND RISK-TYPES

4.1 Definition of RCM and RCSA

The acronym RCM stands for Risk and Control Matrix. To understand the Risk and Control concepts we need to understand the various terms that are commonly used in assessing them, as is elucidated in this section.

The acronym RCSA stands for Risk & Control Self-Assessment; when a test step is tagged to each of the controls and the management function performs that test, the exercise is known as a Risk and Control Self-Assessment.

This is the basic platform on which an ORM framework is built. It has these critical constituents: Risk, Control, Risk grading, Control Owner

4.2 Description of the Inherent Risk

RCSA is built on identification of all risks that could lead to an operational risk event. This is built on an inherent risk concept. Inherent risks mean the risk as it stands assuming there is no control to mitigate it. In creating a risk register, the process, the sub-process, and the inherent risk is described. To arrive at the inherent risk, one may use judgement of the impact category that a failure in the particular process/sub-process can lead to. For example, in a finance lending business, an error in data entry of a bank account of a customer, can lead to a disbursement going to the wrong account and hence cause financial loss to the organisation. Or, in case of an inadequate check on KYC of customer before approving a loan facility, it is possible that a regulatory violation is committed, leading to regulatory risk.

This exercise is a comprehensive one and can take an organisation a few months or years to effectively document all identified inherent risks, and at any point in time, there would always be some new learnings to modify and enhance the list.

The Risk description is then followed by an assessment of the impact that a failure can have. Some failures will have a minor impact on the organisation while some may cause a higher level of impact. It is up to each organisation what it considers major and medium and any intermediate grading it may have in between these two, basis the risk appetite of the management and shareholders.

Example of a major impact are regulatory licence suspension, or a class action legal indemnity that can throw all or most of the financial profits in jeopardy; a financial loss due to excess payment or short recoveries of dues, that can wash away the projected revenues; loss of life of employees or significant part of physical assets;

Example of minor impact are violation of regulation but not likely to invite penal action by regulator; financial loss up to a small portion of the projected revenues to an extent that can be easily absorbed; litigation losses on individual cases that can be easily absorbed without significant

impact to the revenues, injury to employees or loss or property that can be recuperated with a small expense or effort.

Broadly, **risk types** that often overlap or are caused by operational failures, used commonly are:

(a) **Regulatory risk:** When the risk of a failure may lead to a violation of the regulatory requirements that the organisation is supposed to comply with, the risk is termed as regulatory risk. An inter-related term, often used in conjunction with regulatory risk, is statutory risk. Statutory risk refers to violation of applicable law. Essentially, in common parlance they often refer to the same group of potential risk, though, most organisations use the word statutory risk to refer to violation of law, and regulatory risk to refer to violation of norms issued by the specific regulator they fall under. KYC-AML is a common example of being a statutory and regulatory risk (since Prevention of Money Laundering is an Act), and since all regulated industries have norms on KYC, it is commonly tagged as regulatory risk.

(b) **Financial risk:** Risk of possible financial loss to the organisation.

(c) **Financial reporting:** Risk of misstatement of financials due to a failure, is termed risk of financial reporting. This may be linked to financial risk in some specific risks, but not always. For example, an excess payment made to a vendor may qualify for being categorised as financial loss, but if it is accounted for properly it may not lead to risk of financial reporting. Some organisations choose to include a description of financial assertions in the RCSAs, so as to indicate the nature of impact a failure may have on the financial reporting from an audit perspective.

(d) **Legal risk:** Risk of the organisation being at a risk of facing lawsuits, litigation, or a risk of inadequate legal enforceability. Often, contractual risk is clubbed with legal risk, since lack of due diligence in contractual agreements is inter-related to legal risks, given the chance of disputes between parties, or the incapability to enforce terms of the agreement due to a poorly defined contract.

(e) **Reputation risk:** Risk of the organisation's reputation in public view is a key concern in current age of an active and engaged media and social media. The related aspects like a lower credit rating for the organisation, higher borrowing costs, reduction in credit terms extended to organisation, fall in share price leading to overall market capitalisation fall, and disruption due to vendors/suppliers/service providers refusing to do business due to reputational risk are all real risks that a business faces. Quite often, a failed operational transaction leading to a customer dispute/complaint may lead to an enhanced reputation risk.

(f) **Fraud risk:** Fraud risk is basically one that can lead to an unlawful gain by an internal employee or an external person / entity by exploiting a gap in a process that fails to catch the deliberately created scenarios by the perpetuator of the fraud; Examples are falsifying identity for taking a loan, or raising an inflated bill, deliberate excess payment to a customer / vendor etc. With the enhancement of COSO framework to ensure highest degree of accuracy and completeness in financial statements, fraud risk in financial reporting assumes greatest

importance. Operational control failures, such as those that allow an employee to deliberately tamper data (on systems or manually) leading to financial misstatement is a typical fraud risk, linked to operational risk (poorly designed process of reporting of data).

(g) **External risk:** External risk are essentially those on which the organisation has no control, like terrorist attacks, natural disasters etc. But these are real risks and the losses of loss of employee lives or damage to physical assets incurred on these events do fall under operational losses.

4.3 Risk Grading / Rating

Table of examples below indicate an assessment of impact into high, medium and low. These are purely indicative and a hypothetical example; each organisation has to create this grid basis a mix of qualitative and quantitative parameters and keep improving upon it with ongoing learnings with reference to the risk appetite.

A purely illustrative table is given below, containing hypothetical thresholds.

A lot of it is subjective to the perception of the organisation and basis the risk appetite of each operational risk framework. These are only examples, and parameters are to be set by the ORMC and evolved.

Parameter	*High*	*Medium*	*Low*
Financial loss	Over 10 lacs (due to any event falling under any Loss category)	5 to 10 lacs (due to any event falling under any Loss category)	Below 5 lacs (due to any event falling under any Loss category)
Regulatory violation	Design level error, over 1% violation in key regulatory compliance; May lead to regulatory reprimand / license suspension / penalty etc.	Transaction level errors, above 0.2% and below 1% of transactions ; May lead to regulatory reprimand/ penalty	Below 0.2% of transactions Minor violations, but overall the process design is in place
Statutory violation	Design level error, leading to serious non-compliance of applicable laws, may lead to penalties, reprimand, withdrawal of licence etc.	Transaction level errors, not leading to serious penalty / withdrawal of licence etc., but may lead to issues with statutory authorities	Minor transgressions, not leading to statutory penalty etc. Overall process being in place, only transactional errors occur.
Financial reporting error	Significant error that may lead to material misstatement of financial information and/or material	Minor error but overall could lead to a misstatement in financials and an adverse comment from	Minor error in financial reporting, leading to a material misstatement or a qualified statement

	misstatement of financial information and/or qualified statement from auditors. May be impacting regulatory reporting and impact on investor and lender relationships; Fraudulent misstatements	auditors; May lead to external adverse impact on investor / lender relationships.	from auditors.
Reputational loss	Reputational risk event inviting regulatory and media attention, Significant Investor and lender impact Attrition of employees due to reputational loss	Reputation risk event inviting moderate media attention, but no significant impact on investor / lender relationship or regulatory aspects.	Minor event with short term impact only.
Cyber risk	Loss of data of more than 1% of accounts / Failure of firewall vulnerability control of over a defined threshold that could threaten entire network	Minor loss of data / Failure of firewall vulnerability control to limited impact on network, or limited to some part of it	Minor issues not amounting to any significant impact on network security
Fraud risk	Fraud in financial statement leading to misstatement; Significant fraud in core business process of organisation with a fraud loss of over 10 lacs, May invite media, regulatory ire, legal suits, law enforcement action etc. on company/officials.	Fraud impacting financial statement but not material misstatement; Fraud in peripheral processes of an organisation not its core business process; Will not invite regulatory or law enforcement / legal action on company/ officials Impact of less than 10 lacs loss	Transactional events of fraud with negligible impact on the overall financial statements; Events not impacting regulatory, investor, or law enforcement / legal aspects

- **Impact /Severity:** Impact category has to be ascribed to each risk. Impact category may fall under one or more heads; for example, a fraud risk may also result in financial loss; or a regulatory violation may lead to a reputational risk; or, wrong product configuration sold to a customer and inability to service it, may lead to regulatory, reputational and financial losses in combination; thus, it is possible to tag multiple heads of impact as well as use only the primary impact category, that is a flexible judgement of the organisation.
- **Probability / Frequency:** Probability, simply put, is the chance of the transaction / process going wrong due to a failure. Probability of failures are often expressed in percentage terms of the total volume of transactions in a process if it is a high volume transaction process; in processes where the universe of transactions is of lower volumes or of lower frequency, a qualitative judgement on probability is often required to be taken. Probability can be arrived at in high-volume processes by analysing past data on failures in the process. It is important to note that this is often a subjective assessment in instances where no past data is available.

This brings us to a very important concept of bucketing the risk profile of the processes into four basic categories:

- High Impact – High Probability
- High Impact- Low Probability
- Low Impact – High Probability
- Low Impact – Low Probability

While the first and third categories tend to get sufficient attention by management, the high impact low probability often skips the management decision purely because these incidents are either not foreseen at all in reality or even if they are, they are so rare but with severe impact that putting a risk mitigation plan for them is very difficult. However, wherever possible the management must consider them on an evolving basis.

While it is easier for an operational risk practitioner to work on four buckets, it is often enhanced by introducing an additional factor of Medium Probability and Medium Impact, depending on the organisation's view on risk grading.

4.4 Residual risk and Rating/Grading

Identified inherent risks in processes, are expected to be mitigated by using suitably designed controls. In any organisation that has a view on managing operational risks, all or most of the identified risks in a process would be controlled through a process that reduces, or eliminates the risk of a failure taking place in that process.

Residual risk is thus the remaining risk in a process assuming the control designed is operating properly. Thus, all companies strive to have a low level of residual risk.

Higher the control effectiveness, the lower the residual risk. Lower the control effectiveness, the residual risk would be same or similar to level of inherent risk. We shall study more about the concept of controls in the subsequent section.

5. UNDERSTANDING OF CONTROLS

Controls are activities that are intended to prevent the inherent risk from materialising into a real failure of the process / transaction. These activities are designed keeping in mind the overall process objective, the inherent risks in the process, and the impact of the risk if the failure were to materialise in reality. Given that this concept applies to all industries we have attempted to broadly categorise the types of controls into the following.

There are several different, but closely related or similar categorisations used in different kinds of control framework, organisations, but mostly they would fall under these categories, thus this is an indicative list and is subject to evolution.

(a) **Verification:** Refers to a control where a control step necessitates the transaction is verified by either the same individual or a different individual before it is completed. For example, in a financial lending institution, a department may process an application along with the customer documents, and carry out a verification at the end of the process within the department, before passing the file to the other department for further processing that relies on the accuracy of the earlier department's processing.

(b) **Reconciliations:** Refers to a control where an output of a process step is reconciled against other known, established sources of information. For example, before publishing a report, the responsible person may use the primary data, and reconcile it with other existing sources from multiple systems / departments before finalising it.

(c) **Segregation of duties:** Refers to a control where part of the transaction is executed across two segregated departments / functions / verticals thereby eliminating the risk of the originating department to carry out the entire transaction on its own. For example, in a finance lending organisation, the process of sourcing an application is owned by Sales department, while the credit process is completely segregated into the Risk department, and further, the entire operational process of checking the accuracy and completeness of the processed application documentation may lie with Operations who would actually set up the account and make the disbursement.

(d) **Physical control:** Refers to a control type where physical custody of an asset is the control. For example, cash and blank cheque books are stored in a vault or safe to prevent misuse. Original critical documents, legal agreements etc. are also stored safely in safe keeping vaults. In certain cases, organisations may further add a control of authorisation thereby creating a process where an individual holding a key has to operate it first, and additionally the manager would use a different key in his position and open the vault to be accessed.

(e) **Supervisory control:** Refers to a control where the primary transaction / process is executed at a particular level in an organisation, but before finalising it, the supervisor is required to review it and accord an approval. Sometimes this is also classified as Authorisation if the authorisation is given by an authority superior to the one originating the transaction. Often, where the primary control is MIS (Management Information System) such review based controls fall under supervisory control category.

(f) **Exception triggers:** Refers to a control where a system, or a responsible individual, throws up regular reports of transactions which are deviant from the accepted, established process. These reports are expected to be actioned upon by designated individuals. This control type is effective only when the process has achieved a stability and scale that only deviations are reviewed by authorities. For example, reporting of error rate in an operational process is an exception trigger. Or, reporting of a high balance in a suspense account beyond the usual acceptable levels can be an exceptional report item.

(g) **Authorisation/ approval:** Refers to a control step where, after a processing of a transaction basis built in controls is almost complete, a final authority reviews it and approves it. For example, there are several organisations use automated or semi-automated credit decision tools in a financial lending process. However, as per selected parameters, a credit officer may be designated to review the system based processing and approve it as well.

Classification of controls is also required to be classified in two more ways, considering whether the control is exercise manually or is built into an automated system; and if the control is intended to prevent a potential failure in the process, or detect a failure if it has happened.

(i) **Preventive controls** are those which attempt to prevent the inherent risk from materialising into a failure.

(ii) **Detective controls** are built in to analyse the process / transactions post-facto and throw up issues and exceptions. Preventive control in a transaction intensive process may be verification and authorisation; a detective control may be MIS on errors that falls under supervisory review.

For example, two people being required to count cash before making a cash payment, is a common preventive control. If there is a cash reconciliation process at end of day, that detects whether the correct amounts of cash was paid out, it is termed detective control.

(iii) **Manual controls** are those which are exercised by a designated role in a manual fashion. For example, a verification of customer documents in a credit application, done manually, is a manual control.

(iv) **Automated controls** are dependent on a predefined system check, it is called an automated control. For example credit application data is fed into an automated system and data supporting the process is done by a system, giving the recommended investment decision and/or next steps in processing as the output. For example, a complex credit decision involving several parameters and input data, if done manually, is subject to error if done manually; using a system would be an optimal control and hence an automated control is set

up. There may be controls that are partly automated and use manual steps to synergize / verify data from automated controls, these are termed hybrid controls. A MIS process that uses automated data, and involves manual collation from different sources and checked manually by a verifier is a hybrid control.

6. RISK CONTROL SELF-ASSESSMENT (RCSA)

A Risk Control Self Assessment (RCSA) activity is to be done through an objective, quantitative review. Some assessment checks may involve sampling, some may involve specific affirmative / negative answers, or some other test Steps. It is imperative to define the test step of each check in each row item of the RCSA so that objectivity is maintained in the exercise irrespective of the person conducting the activity. If the check involves sampling, it is ideally recommended to follow an established standard or practice; for example, the ICAI guidelines on sampling logic used in audits can be used. The residual risk rating is important to derive after the test results are populated on each check, thereby indicating to the management any areas requiring attention.

RCSA: indicative details

Process	*Sub-process*	*Inherent risk description*	*Probability rating*	*Impact rating*	*Risk type*	*Control description*	*Control type*	*Control owner*	*Control Test steps*	*Test results*	*Residual risk rating*

Additional information may include, financial assertion impact (if any), the name of system used (if any), Sample description of test done etc.

7. TECHNOLOGY RISK

As we saw in the very fundamental definition of operational risk, a key constituent is technology risk. In the current environment of increasing automation in business processes, and evolved technology platforms for accounting, the operational risk practitioner and the auditor must both understand the exact nuances of technology risk in any organisation.

All organisations nowadays use some kind of systems, technology platforms depending on the nature of business. For large complex business processes, there would be several systems, either in isolation or interrelated with each other, working to deliver the business outputs required.

From an auditor's perspective or the operational risk professional perspective, the main issues that can surface from technology risk are:

(a) Unscheduled system downtime or a system malfunctioning due to which a business process is disrupted, due to which the necessary work output suffers a setback. This could result in financial loss, loss of opportunity of business, customer issues and loss of raw material. For

example, a system failure in a financial lending organisation may lead to critical customer commitments like disbursements not happening due to which customer may suffer losses; or inability to post incoming payments on account leading to liquidity issues; or inability to service a customer account leading to customer attrition. Organisations have backup servers, systems, databases, and disaster recovery procedures to ensure work disruption is minimized in such circumstances. The operational risk manager is expected to have an overview of the specific facilities available to the technology department, to service the organisation's critical needs at such times of failure.

(b) System failure pertaining to incorrect programming: This is by far the most common cause of operational risk events in an organisation, since each system can only function in the manner it is set up. Organisations either build their own systems or buy them from specialised service providers, and customise them. In either case, depending on the nature of transactions required to be processed, a very detailed business requirement document is required to be given to the technology department by the business user groups. Often, either due to incapability or poor co-ordination between the business user groups, the requirement document does not capture the entire detailing and the extremely granular details that are required by the technical teams doing the coding, customisation or the deployment. The result is a poorly executed system that causes errors in processing, which may have financial, regulatory, fraud risks, depending on kind of error in the system.

For example, taking an example of a lending institution that processes loan applications on a particular Loan Originating System and a Loan Management System the following scenarios indicate how errors of programming can cause severe operational risk failures:

- Processing fees or interest not being charged correctly to the loan account correctly, resulting in financial loss and / or customer disputes;
- Hands-off between different control owners may be compromised if the system workflow is not properly defined on the system; for example, an application that requires specific fraud risk checks on documents supplied by customer, may totally bypass the required check and go from sales to credit department, thus exposing the organisation to fraud risk. Or, an application may get processed with incorrect customer data, credit bureau information basis the credit parameters set in the system. The coding of acquisition scorecards in the financial lending industry is a typical example of a very sensitive area where technology risk is the cause of operational risk.

Taking an example from manufacturing,

- A software error in parameterizing the right quantity of one raw material to flow into an automated assembly line may result in a completely wasted production output thereby causing an operational loss;
- Another industry-agnostic example is wrong master maintenance of taxation rates in any business charging its customers can lead to a non-compliance in taxation requirements.

(c) Master maintenance: All systems, besides the basic coding, need a set of Masters which are user-defined parameters that enable the processing of the data. Master configuration is in itself a key risk that technology users face, since the linkages between products or service programs as defined by the business users can be ambiguous, or at times contradictory instructions go to the technology team resulting in erroneous set up of Masters.

(d) User access control: This is by far the most key control in driving controls in an automated controls environment. For example, in a lending institution, a credit officer if allowed to process operational activities beyond his job role may result in compromise of the segregation of duties that the process is designed with; or, if an user may have a higher level of access to changing customer data by one modification, while the process may require an authorisation which was bypassed due to inadequate user access control maintenance. User access control requires the user profiles to be set up properly upfront in the initial basic programming, followed by correct assignment of user profiles upon employee requests as per their permissible authorities basis their job role. Organisations are required to delete or modify user IDs once employees move out from their roles or the organisation itself.

(e) Accounting systems: From an audit and accounting perspective, the most intensive focus area is the technology platform that is used for accounting. There are obvious operational risks of misstatements in financial reporting if the accounting software is not configured properly. In complex organisations with several types of transactions that have a financial impact are performed in various systems, the feed in from other production systems (i.e. outside of the main accounting system) are very important to check for accuracy since they are used in financial reporting. The feeds, if manual have their own risk of incorrect manual processing; in automated feed process also, there are risks of incorrect data inflows that could lead to financial misstatements. In lending institutions, the loan management systems are different from the main accounting system; a huge amount of data, at various frequencies, flows into the accounting system. The linkage of the source system to the correct GLs in accounting system, and appropriate reconciliations, the exception reports, analysis and ongoing supervisory reviews can prevent the data from being inconsistent in final reporting. Any regular exceptions in the data in two systems, need to be analysed to find out the root cause of the technological reason, and any incorrect programming. Examples are the data of customers like interest due, principal outstanding, overdue amounts etc. which flow from loan management systems to accounting systems.

(f) Change management is a key area of Information Technology General Controls (ITGC). It simply means that any change to the systems can cause a risk of incorrect change being developed or deployed. This can be a result of multiple causes:

- Change being carried out without approvals of authorised roles,
- Change being wrongly conceived by the user groups, without adequate analysis of pros and cons for the change, and getting deployed by the technology unit under approvals

- Change, though conceived correctly and communicated correctly under adequate approvals to the technology team, is wrongly executed
- The preventive control around all these issues, is to ensure only authorised roles, whether internal or external, have access to making changes in the system; these changes have to be approved by all the departments that the change impacts so that the impact of change is well understood before approvals are accorded; and, a proper user acceptance testing is conceived and conducted before deploying the change. Often the design of the User Acceptance Testing (UAT) script is found defective, and sufficient combinations of test data is not put through the system resulting in some functionalities not being adequately tested.
- A database of such changes, such as audit trail reports have to be judiciously maintained as to what changes were carried out, including the issue tracker related to the changes. This helps track back any changes, to ensure that appropriate change management control and review was exercised.

(g) Migration risk is a subset of change management ITGC to the extent that the controls over an end-to-end migration from one system to another, can bring upon significant operational risk if not carried out perfectly. A significantly high effort is required to ideate before the deployment as to the exact manner of migration; migration has to cover:

- Data, both dynamic and static
- Functionality mapping from old to new system, and any changes to be adequately familiarised within user groups
- Exception reports that could help track any incorrect migration points
- User acceptance test scripts to be intelligent enough to enable the usage of the new system after adequate granular review
- An emergency roll back plan in case some significant unpredictable issue comes up in migration deployment.
- An auditor or operational risk manager is required to carry out a review of the data integrity and the functionality of the systems that have an impact on the financials of the organisation. This risk is not only restricted to financial reporting, but any risk that could jeopardise the business process, including regulatory, financial and other risks.

(h) Technology outsourcing risk: In many organisations the technology platform, or the servicing / maintenance of the platform is outsourced. Outsourcing while has its inherent efficiency benefits comes with operational risks of running a system through a service provider that has no or little understanding of the actual business process the system supports in the organisation; such relationships of principal and service provider have to be carefully defined both contractually as

well as from an operational perspective otherwise the seamless functioning of the systems can be disrupted.

8. KEY RISK INDICATORS AND SCENARIO ANALYSIS

As an organisation evolves from an elementary level of operational risk management to the next level, there is a need to monitor certain areas on continuous basis, by way of regular reports and exception triggers. While an RCSA hinges on the self-assessment at a point in time, the Key Risk Indicator (KRI) concept is more focused on continuous monitoring.

They are actually interrelated concepts. For example, in a manufacturing process, a half yearly RCSA check may be built on checking for number of batches failed in quality check; however a KRI may be a better method being a lead indicator, where batch failure numbers are reviewed every week rather than at longer intervals. Conversely, if a KRI exists for a process, an RCSA can be built using the KRI.

In an evolved internal control framework, there would be a robust KRI monitoring process.

In initial stage of an operational risk management implementation, when either a KRI or RCSA is not possible due to paucity of objective data or capability to analyse it, an organisation can use Scenario analysis as a surrogate mode. In a scenario analysis, the risk scenarios are described and a subjective assessment of the risk materialising is described, using whatever available data and reviews are possible to collate. Over time, this method has been gradually overshadowed by more objective methods like KRI monitoring (which is based on MIS), and RCSA (which is based on actual testing and/or uses the KRI as a base).

9. BUSINESS CONTINUITY PLAN

Business continuity refers to a concept that encompasses technology and business process framework that ensures that in times of unscheduled disruption of the routine process, an alternative mode of management of priorities, technology solutions, and business processes is undertaken.

Business Continuity is now an integral part of Operational Risk Management. Any of the risks we enumerated above, can be triggered as part of an overall disruption that is caused by any or a combination of the following reasons:

(a) Natural disaster affecting services of either technology solutions and/or the business process itself; to elaborate, a situation to invoke BCP may exist in a case of natural disaster like flood, where staff of a company are unable to go to office; or, it may be a combination of situation where the technology solutions of the company that is required for daily functioning of the organisation is also not working;

(b) Civic infrastructural failures like essential services of electricity or transport being brought down due to terrorist attacks or natural disasters;

(c) Keyman risk due to death or incapacitation of key decision makers in a company leading to chaos in management of the company;

(d) Failure of one department or function to do their assigned tasks in a case of disruption may cause the entire process to delivery of the organisation;

(e) In current business scenario, several organisations concentrate their operational activities in one major operational hub; these organisations are at a higher BCP risk than the ones with operations in several hubs if they are geared to support each other in a moment of crisis.

Common examples of critical disruption in business process are:

- Raw material in process being lost or spoilt due to one of the processes being disrupted due to system, people or process failure, i.e. operational reasons;
- Contractual financial obligations such as repayment of loans, or vendor payments, salaries,
- Payment of taxes;
- Inability to disbursement of loans that causes customer dissatisfaction;
- In an ITES company, the principal (i.e. the main organisation that hires an ITES company) may have complete disruption of their services to their customers in case of failure in the ITES service provider's services;
- In fact in highly developed economies, the risk of customer's dissatisfaction, the highest form of which takes class lawsuits, is high in case of large scale business process failures;

Hence a Business Continuity Plan ("BCP") is required to be adopted.

BCP is now an evolved, objective framework and involves a large section of the organisation, including the operational risk management framework.

Now we shall discuss the key constituents of a BCP one by one.

9.1 Business Impact Analysis (BIA)

This refers to the impact that a business disruption has on all activities in an organisation; this is the base line from which an organisation can build its BCP.

All departments of the organisation are required to list all their processes (including sub-processes) and grade them in order of priority. This is a difficult task, since most organisations like to believe all their processes are critical; but in reality, with limited resources in a disruption situation, the best that can be done are the most important activities; hence parameters of prioritisation are to be fixed; these could be as follows:

Impact: Critical, Important, Routine; the classification into each of these could be done on the basis of some objective parameters such as whether it affects regulatory violations, or can cause financial loss, or loss to lives or property; for instance, in a lending institution, a process that does

due diligence on customer identity and address (KYC checks) may be very critical and indispensable without which a sanction cannot happen since it is a regulatory risk; or a case where a secondary check on the sanction is dispensed with in given sanctions, where a financial loss can happen. These are carefully evaluated parameters that the management has to consider and take a decision on what processes to keep running in disruption situation and what to stop.

Also, what is considered as important but not critical for a department, may be critical for another department; for instance, treasury may feel making payment to external lenders as most critical while making payments to operations or finance departments for making disbursements to loan customers or vendors as not critical; however, the operations or finance departments may be severely inconvenienced if the money to service their obligations is not made available in a disruptive situation. Thus, a categorisation of Impact is done with collaborative approach of all departments that a process impacts.

In summary,

A BIA must ideally cover following aspects:

- Minimum % that the process must continue to run in BCP scenario (say 10 %, 50 % etc. of original volume / workload),
- Minimum resourcing required to carry it out,
- Maximum permissible time to allow a task to be not performed (Recovery Time)
- Category of impact due to disruption (customer impact, regulatory impact, financial loss or risk to employee health and life),
- Deriving the criticality from these parameters (including consideration for normal days and month-ends),
- Minimum technological and infrastructural requirements in the BCP site.
- This exercise will lead to decisions on which processes / activities need to be covered under BCP on priority, and which can be scoped out (and for how long).

9.2 Functional Recovery Plan (FRP)

Here, once the BIA is approved at management level, a detailed plan as to alternate functioning of the selected processes / sub-processes has to be made. This by far is the most challenging phase since it involves alternative resources, staffing, infrastructure and maybe technology systems as well. Depending on the complexity and nature of services provided by an organisation, each organisation must decide the steps to be taken;

For example: an operations intensive company may decide to use an alternative, smaller hub to process all key transactions; a customer service centric company may have an alternative customer service centre if the main one is down due to disruption;

Roles identified as key in running a FRP in execution, are required to have formal backups in case they cannot move locations or carry out the required operation from their base location or site. Companies resort to several tech savvy solutions such as work-from-home facilitated by remote logging in to systems, webinars, video conference, telephonic conference bridges, and use of secured-data-storage such as cloud.

An FRP has to consider the key elements involved in the alternate plan; whether it is movement of goods, or movements of information, or paper-based files; any plan is successful only if the practical constraints of the Plan are clearly elucidated, thereby objectively listing the conditions in which the FRP would function, and when it cannot.

A FRP is a very detailed document that would list the following at a minimum:

- Site in which the process would be carried out (called the Alternate Site), the role/s who would carry it out, the back-up to the roles if the primary one is unable to perform in disruptive circumstances; the minimum resources such as telephones, internet, printers or access to intranet, internal systems etc. as an indicative list.
- This needs to be documented and circulated, and reiterated to each employee and/or service provider who is involved in the FRP. Operational risk managers are required to oversee whether the framework is composite and integrated sufficiently to ensure the framework is real and practically implementable, not a drawing board theory document.
- The names and contacts of all key members in each process need to be listed and available to all others involved in FRP , in a domain other than the primary office domain so that the communication lines are not disrupted when it is required to invoke a FRP. This communication plan is commonly known as a Call Tree.
- The FRP is useful and practical only if tested regularly, maybe at predefined periodic intervals, as well as unannounced situations to mirror a real disruption. This is the critical stage where theory is tested in practice, and the ensuring failures and successes have to be documented to improve the Plan in future. An organisation has to ensure this is a recurring process to be able to give confidence to investors/promoters/owners, management, and customers that the FRP is practical and genuinely addresses the critical tasks.

In an effective BCP, the concern on outsourced activities need to be addressed too; in current scenario where several organisations use outsourced vendors, the vendor's BCP has to reviewed periodically to ensure the whole process works. In fact the choice of a vendor should ideally cover the BCP aspects too.

An auditor / consultant working on internal controls or an operational risk manager needs to review the efficacy of the organisation's BCP, in context of the services it provides. For example, even a small scale audit firm may need a BCP to ensure its services to the clients are not disrupted. In

large complex manufacturing organisations the BCP needs to be a major framework that co-ordinates the interrelationships of various business units, locations, business processes etc.

It is highly advisable to have a formal decision making committee of management functions to oversee the entire chain of activities from formation of BCP policy, Business Impact Analysis, Functional Recovery Plan and to review Test results.

10. OUTSOURCING RISK

There are several specific aspects that need to be looked into Outsourcing Risk. Hiring of an outsourced vendor/service provider must cover the following aspects:

- Clearly defined objective of outsourcing; this has to be brought into the scope of work;
- Contractual documentation to be adequate to ensure the service provider does only what is assigned and to the standard mutually agreed to by all parties involved;
- Legal indemnities to the organisation to be assessed while hiring a service provider;
- In agreements where the client and the service provider are in different states or in different countries, the respective countries' or states' laws have to be complied with;
- The BCP of the service provider has to be reviewed.
- The operational risk assessment covering regulatory risks, financial risk, financial reporting risk and other risks as delivery to end customers of the client in case the service provider fails to deliver for whatever reason.
- If technology or its disaster recovery itself is outsourced, all the attention is required to ensure the business operations work as designed and agreed.

It is advisable for an operational risk manager to have an oversight of different department's adherence to the management of their respective outsourcing risks, and have it covered in their respective RCMs.

11. CYBER RISK AND INFORMATION SECURITY CONTROLS

Cyber risk is a vast and complex technical subject by itself; however we shall outline some of the key points that is relevant from an operational risk perspective. Information Security and Cyber risk by themselves are studied under specialised courses as CISA by those aspiring for professional certification in information security management domain.

Cyber risk term broadly refers to the risks an organisation / individual is exposed to, due to a situation where its data, or network systems, or its transactions are disrupted, compromised or damaged/destroyed by an intrusive access from an external entity.

This broadly covers scenarios like this, for example:

- Confidential data of customers' demographics, personal financials, collaterals, bank account data etc. stolen from a lending institution's database by an external entity having made unauthorised access to the system of the organisation; this can cause customer disputes, class lawsuits, breach of confidentiality law, and loss of business.
- Trade secret software programs, like acquisition scorecards or manufacturing formulae, stolen from the systems of an institution and causing significant loss of competitive business; this is also covered in a broad term called Intellectual Property risk. This is a result of corporate espionage, or simply, an employee quitting a job with a view to take up a career in a competitor organisation may take away account data or other information that may help his unlawful benefits.
- Malevolent attack on system of an institution that can lead to complete or partial data loss, of customers, accounts and of past financial transactions; this can lead to serious regulatory violation, financial reporting issues, and /or financial losses;
- Ransomware can lock or encrypt the entire data on an individual or entity's computer systems and thereby completely ruin the business; the retrieval of such data may not be possible or would come at significantly high cost and at compromised quality; ransomware originators demand money, often through illegal channels for release of such data.
- The financial transactions that an organisation performs outside its own network can also be compromised due to cyber risk; organisations involved in e-commerce where a large chain of activities is performed on internet, and, since multiple parties are connected with each other and a compromise on one entity's network may lead to issues for anyone in the entire chain. A lot of customer data, credit card numbers, bank account numbers, details of the goods and services being transacted, all are being transmitted over the internet. An increasingly digitized business environment does put all parties involved in such transactions, at a higher risk.
- An entity intending to create fraudulent transactions and benefit financially may send emails to individuals or organisations, pretending to be from an organisation that the other one is already engaged with; this happens on an email that looks identical to the ones from the actual organisation, and it may ask for money to be transferred to a bank account.
- Phishing is a very common fraud technique, whereby there is a link sent to the targeted victim and upon clicking it, the intruder gets access to the victim's computer system/s; and, in cases, if asked for personal data of credit card, passwords etc. on such dubious links, the victim may also incur immediate financial losses because the link is a malevolent one and the perpetuator of the fraud gets access to credit card details or bank account detail of the victim.

Mitigation of such risks is done through the following measures:

An organisation, depending on its nature of business, complexity of business operations, and the kind of system network/s used, need to take adequate measures on cyber risk.

The key aspects in consideration are:

- Identification of risk areas: whether it is own or outsourced network, internet, individual computers, mobile devices etc. Prioritization of resources and effort can be managed accordingly.
- Adequately restricting access to systems is the common way to prevent cyber risk; this is done by password protection at various levels, from common user to administrator level.
- Encryption solutions on individual computers is also done in a manner that if lost, the unauthorised entity cannot download the data into an external storage device.
- There are several technology solutions that create an adequate firewall of the organisation's systems to protect them from hacking from outside.
- A regular vulnerability testing of the firewall and periodic review to upgrade it is one of the main tasks of the information security manager. Detection of a test-attack is very important part of the preventive mechanism; an attacker may attempt to cause a minor violation to test the organisation's network security before causing a major incident.
- A response strategy to a cyber-attack incident is also important as part of risk management. The measures to prevent or mitigate customer disputes, legal indemnities, assess and minimize the financial impact of a cyber-attack, and governance over decision making and investments to restore the system functionalities to its secure state, are all important considerations. The root cause of these incidents and the impact have to be adequately documented.

Examples in recent times are the ransomware attacks (for example WannaCry Ransomware) that led to several reputed organisations both in public and private services to be adversely impacted.

It is highly advisable to maintain adequate documentation on technical standards followed and aspired to be followed by the organisation, and that is driven by policy and senior management governance. For example, the RBI has issued information security and IT governance related circular that enables the organisations regulated by it, to follow adequate security measures and to ensure that the highest level of attention from the Board level is also accorded to information security.

Different sets of employees depending on whether they are users / custodians of data or are part of governance of the systems network need different kind of awareness and training to maintain information security. It is recommended that the senior management is guided by a professional Chief Information Security Officer (or a role that carries these responsibilities) in carrying out these responsibilities.

It is recommended to have an internal audit scoped for technology and information security by teams that have technology assessment competence.

Most organisations do have a Code of Conduct that has a significant section on confidentiality and protection of data, broadly covering information security aspects. This is further enabled by mandatory training by the employees depending on their roles and exposure.

12. OPERATIONAL LOSS DATA MANAGEMENT

While an effective operational risk management framework drives to bring preventive measures as elucidated above, there is every possibility that some loss events do occur in an organisation. It is imperative to identify the losses as and when they happen, quantify them (both in financial and non-financial terms), and assess their short term and long term impact. This is normally followed by an assessment of the controls of the specific process / sub-process in which the event occurred.

Basel II has already indicated a comprehensive list of operational loss event categories. While these were introduced for financial organisations, they are, with minor customisations, equally valid for all organisations measuring operational loss data with an objective methodology. A slightly modified description from the one in Basel II norms is presented in table below:

Identification of an operational loss event is the primary challenge an organisation faces, because a loss may occur and its discovery may takes place after a long time. Some very common scenarios are elaborated in the description of three levels of activity examples in Basel norms itself. A slightly modified extract is thus:

Event type Category (Level 1)	*Description*	*Categories (Level 2)*	*Activity examples (Level 3)*
Internal fraud	Losses due to intentional fraud, misappropriation of property, violate law or company rules, by an internal party/in collusion with an internal party	Unauthorised activity	Unauthorised transaction with monetary loss; Transaction not reported intentionally; Mismarking of position intentionally.
		Theft and Fraud	Fraud/Credit fraud, theft/extortion/embezzlement/robbery, Misappropriation of assets, malicious destruction of assets, forgery, smuggling, account impersonation,

			tax non-compliance intentional; bribes/kickbacks, insider trading (not on company's account)
External fraud	Losses due to an intentional fraud, misappropriation, violation of law or company rules by an external party	Theft and Fraud	Theft/robbery Forgery
		Systems Security	Hacking damage Theft of information with financial loss
Employment Practices and Workplace Safety	Losses due to activity inconsistent with employment, health and physical safety of employees, claims, or from discrimination events.	Employee relations	Compensation, benefit, termination issues Organized labour activity
		Safe environment	General liabilities (slip and fall etc.) Employee health and safety rules events
		Diversity and discrimination	Losses or issues arising out of diversity and discrimination
Clients, Products, and Business Practices		Suitability, disclosure and fiduciary	Fiduciary breaches/guideline violations Suitability/disclosure issues (KYC etc.) Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender liability
		Improper Business and market practices	Antitrust Improper trade / market practices Market manipulation Insider trading on firm's account

			Unlicensed activity Money laundering
		Product Flaws	Product defects (unauthorised etc.) Model errors
		Selection, Sponsorship, and Exposure	Failure to investigate client as per guidelines Exceeding client exposure limits
		Advisory activities	Disputes over performance of advisory activities
Damage to physical assets	Losses from physical assets damage either intentional or from natural disaster	Disasters and other events	Natural disaster losses, human losses from external events like terrorism
Business Disruption and System Failures	Losses arising from disruption of business or system failures	Systems	Hardware, software, telecommunications, utility disruptions/outage
Execution, Delivery and Process Management	Losses from failed transactions processing or process management	Transaction capture, execution, and maintenance	Miscommunication, Data entry, maintenance or loading error, Missed deadline/ responsibility Model/ system mis-operation Accounting error Delivery failure Collateral management failure Reference data maintenance, Other task mis-performance
		Monitoring and reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)
		Customer intake and documentation	Client permissions/disclaimers missing; Legal documents missing/incomplete
		Customer/client account management	Unapproved access given to accounts Incorrect client records leading to loss Negligent loss or damage of client assets
		Trade counterparties	Non-client counterparty mis-performance / disputes

		Vendors and suppliers	Outsourcing, Vendor disputes

The process for identification and reporting of operational losses are recommended to be laid down in an internal process note approved by the competent authorities in the organisation, or the ORMC itself.

12.1 Identification

The organisation may identify an operational loss event by any or more of the following triggers:

- Regular reconciliations or other internal control checks
- RCSA process
- Customer complaint
- Vendor complaint/ dispute
- Regulatory inspection / audit / reviews
- Concurrent / management audits
- Internal and/or Statutory audits that identify an issue that uncovers operational loss events

As and when an event that falls under the above scenarios occurs, the following steps are recommended:

12.2 Quantification

The quantification of the event is to be done next;

It may have a direct financial loss impact (like excess payment to external party, or compensation to customers etc.) or not having an immediate direct financial impact (like a few instances of KYC due diligence failures, or a process failures not leading to compensation to customers etc.)

From a reporting perspective, it is necessary to enumerate all Operational risk events, since these are the failures in which the organisation needs to take some remedial action.

Only in those cases where direct financial loss is involved, an operational loss is booked.

While RBI, following the direction of Basel II norms, has detailed instructions applicable to banks on the handling of loss data and its impact on capital computation, other industries do not have such guidelines currently.

It is advisable to have an Operational Loss GL in the organisation where all financial loss instances can be booked. In case, a different GL has already taken in the loss by routine course of business, or inadvertently due to the loss not having been discovered earlier, it is advisable to book a credit in the original GL and the debit in the Operational Loss GL.

For example, an excess full and final settlement payment to an exiting employee, would have been booked under Salaries by normal course. But once the error is discovered, it is advisable to book it in a separate Operational Loss GL and credit the Salaries GL so that the financial reporting is appropriate. Further in a lending institution, if a loan is closed erroneously, the entire principal and other heads' outstanding is a real financial loss to the organisation; these need to be booked in the operational loss GL and the respective other GLs be credited with the amounts.

Some organisations book Fraud Losses in the Operational Loss GL (since fraud losses are also part of operational losses as per categorisation elaborated above), but some organisations maintain a separate GL for Fraud losses, so as to enable efficient reconciliation with other reporting requirements like Fraud reports to regulators and to track action taken against them.

In instances where a recovery of the loss is expected, the management is expected to track the event till its logical end by recovering whatever is possible thereby reducing the net operational loss.

12.3 Reporting

A report to the ORMC (and to the Board / Board Committee as may be necessary by regulation or by company policy) is recommended to include the following:

Date of incident	*Date of reporting*	*Event description including root causes*	*Financial loss*	*Event category*	*Recovery if any*	*Action taken*	*Event closed / further action due*

12.4 Corrective action

Any event has to be correlated with the respective RCSA to evaluate whether it was covered in the RCSA. If yes, then assess the sampling or test frequency adequacy. If not covered, it needs to be included in future.

The most important corrective activity after an event is to review the scenario for further happening of such risks. If that is possible then, the organisation may even set aside a financial provision for the same for estimated future events.

13. BUSINESS ANALYTICS AND ARTIFICIAL INTELLIGENCE

The increasing penetration of information technology in everyday life has meant that global data size has increased in exponential terms in velocity, variety, and volume. It is now available almost instantaneously, creating possibilities for near real-time analysis.

The convergence of the secular trends of exponential growth in data volume, concomitant geometric increase in computational capacity and the resultant development of sophisticated algorithms is fuelling rapid technology advances and business disruptions. The field of risk management is not immune to these changes and we are witnessing significant changes in the discipline.

13.1 Machine Learning

A standard software code is characterized by explicit rules that a computer is supposed to perform. In case, there is a change in the data / situation, a programmer needs to change these explicit rules. In contrast, a machine learning program dynamically responds to change in data / situation by changing the rules that govern the behaviour.

Machine learning, meanwhile, uses an inductive approach to form a representation of the world based on the data it sees. It is able to tweak and improve its representation as new data arrive. In that sense, the algorithm "learns" from new data inputs and gets better over time.

Techniques such as regression, support vector machines, and k-means clustering have been in use for decades. Others, while developed previously, have become viable only now that vast quantities of data and unprecedented processing power are available. Deep Learning and Reinforcement learning are good example of newly developed machine learning techniques.

At the most basic level, machine learning techniques can be divided into two primary groups:

- Supervised Learning
- Unsupervised Learning

Supervised Learning refers to the statistical analysis that aims to map the behaviour of a certain variable on the basis of some other variables. The principal aim of these methods is to fit a model that relates the set of independent variables to the dependent variable. The model in turn is largely used for future prediction of better understanding of the relationship between the independent and dependent variables. Bulk of the machine learning methods such as linear regression, logistic regression, boosting, and support vector machines operate in the supervised learning domain.

Unsupervised Learning, as the name suggests, refers to statistical methods that aim to delve into the challenging realm of data that has no dependent or response variable i.e. there is no variable that supervises the behaviour of the algorithm. The primary aim of this kind of analysis is to understand the relationships between the variables or between the observations. One statistical learning tool that we may use in this setting is cluster analysis, or clustering.

Machine Learning methods can also be categorized on the basis of the nature of the variables handled. Regression methods primarily deal with variables that are quantitative in nature e.g. a person's age, height, or income, the value of a house, and the price of a stock. In contrast, Classification methods deal with qualitative variables i.e. variables that take on values in one of K

different classes, or categories. Examples of qualitative class variables include a person's gender (male or female), the brand of product purchased (brand A, B, or C), whether a person defaults on a debt (yes or no), or a cancer diagnosis (Acute Myelogenous Leukemia, Acute Lymphoblastic Leukemia, or No Leukemia).

13.2 Analytics – Risk Management Applications

Risk management faces new demands and challenges. In response to the crisis, regulators are requiring more detailed data and increasingly sophisticated reports. Banks are expected to conduct regular and comprehensive bottom-up stress tests for a number of scenarios across all asset classes. Big Data technologies present fresh opportunities to address these challenges.

Vast, comprehensive and near real-time data has the potential to improve monitoring of risk, risk coverage, and the stability and predictive power of risk models. In a number of key domains – particularly operational and compliance risk – Big Data technologies will allow the development of models that will support every day.

Post-crisis, financial institutions are now expected to have thorough knowledge of their clients. Increasingly, forward-thinking banks harness Big Data to develop more robust predictive indicators in the credit risk domain. New data sources - including social media and marketing databases – are being used to gain greater visibility into customer behaviour. This information can augment traditional data sources including financial, socio-demographic, internal payments and externals loss data.

Together, the data sets can produce a highly robust, comprehensive risk indicator. Rather than waiting to review loan clients' financial reports to discover loan-servicing problems, firms can utilise Big Data technologies to detect early warning signals by observing clients' on-going behaviours, and act in time.

The high cost of money laundering cases has prompted banks to seek new ways to address the severe limitations in current anti-money laundering risk management. Traditional approaches to anti money laundering remain dependent on rule-based, descriptive analytics to process structured data. This system clearly has limitations - without automated algorithms, detecting information within the wealth of data requires laborious keyword searches and manual sifting through reports.

Big Data analytics can improve the existing processes in AML operations. Its approaches allow for the advanced statistical analysis of structured data, and advanced visualisation and statistical text mining of unstructured data. These approaches can provide a means to quickly draw out hidden links between transactions and accounts, and uncover suspicious transaction patterns. Advanced analytics can generate real-time actionable insights, stopping potential money laundering in its tracks, whilst still allowing fund transfers for crucial economic and human aid to troubled regions. Big data technologies can identify incidents, help draw a wider picture, and allow a bank to raise the alarm before it's too late.

Business Analytics is heavily used in Liquidity Forecasting, Asset Liability Management, Operational & Compliance Risk as well as in Credit Risk model.

13.3 Artificial Intelligence

Artificial Intelligence is the science that makes intelligent machines especially computer programs. It is a way of making a computer in a similar manner the intelligent humans think.

It works by studying how human brain thinks and how humans learn, decide and work while trying to solve a problem, and then the outcomes of this study is used in developing intelligent software and systems. It has been dominant in many fields such as:

Gaming – It plays a crucial role in strategic games such as chess, poker etc.

Natural Language Processing – It is possible to interact with the computer that understands natural language spoken by humans.

Expert Systems - There are some applications which integrate machine, software, and special information to impart reasoning and advising. They provide explanation and advice to the users.

Vision Systems - These systems understand, interpret, and comprehend visual input on the computer.

For example,

- Doctors use clinical expert system to diagnose the patient.
- Police use computer software that can recognize the face of criminal with the stored portrait made by forensic artist.

AI is also used in Speech Recognition, Handwriting Recognition, and Intelligent Robots etc.

Artificial Intelligence is dependent on large amounts of data. So proper big data architecture needs to be set up for AI that involves architecture like Hadoop clusters, Spark Clusters etc. So that the processing of the data is faster and smooth.

13.4 Distributed Ledger Technology

Distributed Ledger Technology (DLT) is the generic name of advanced technologies that allow nodes in a decentralized information technology network to securely propose validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's nodes.

This technology is perceived by many commentators to have significant potential to disrupt payment, clearing, settlement and related activities. DLT is expected to radically redefine the payment and settlement landscape and is expected to produce the following benefits:

- Significant reduction in operational complexity
- Major increase in processing speeds and consequent asset availability
- Higher operating efficiency due to lowered reconciliation requirements

- Transparency and immutability in transaction record keeping
- Network security and safety due to distributed architecture
- Overall reduction in credit and operational risk

14. INSURANCE

Insurance is used by organisations to mitigate operational risks that can be insured. Insurance coverage is commonly available for risks arising out of fire, for instance. Depending on the cover available and opted for, other losses due to terrorist attacks, natural disasters etc. can also be covered. Cash transit insurance and fidelity insurance are off quoted examples.

These three examples are based on loss categories of Damage to Assets, External fraud and Internal fraud. Recently a new concept of Cyber risk insurance has also come up, and there are companies offering cover against the risk of damages due to lawsuits / compensation on account of being a victim of cyber-attack, due to which data of customers, vendors or any other counter-party can be leaked to an unauthorised, malevolent entity.