INTRODUCTION TO RISK

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

LEARNING OUTCOMES

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 organizational cultures, heavy regulatory interventions, creates stress and complexity in managing life and businesses. Black seven 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: "danger or possibility of danger, loss, injury or other adverse consequences" and the definition of risk is "exposed to danger". In the 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 risks resulting from a green action or inaction, foresight or unforeseen. In business and monetary terms, the value of risk outcomes shall be on employees, suppliers, customers, strategy, objectives, profile, assets, etc.

Examples
- 1. A fisherman starting a sea voyage on a fishing expedition may result in loss of life.
- 2. A home alone infant climbing on a window pane.
- 3. A family of fishermen starting a sea voyage on a fishing expedition may result in loss of life.
- 4. A homeowner taking a risk by buying a house in an earthquake-prone area.
- 5. A fast food restaurant opening a new branch in a high-crime area.

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 irrespective of uncertainty. The degree of uncertainty or likelihood of occurrence and impact of the risk outcome combined together forms the magnitude of the risk.

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 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 full promises made to stakeholders. Absence of risk management means failing "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 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 organizational cultures, heavy regulatory interventions, creates stress and complexity in managing life and businesses. Black seven 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: "danger or possibility of danger, loss, injury or other adverse consequences" and the definition of risk is "exposed to danger". In the 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 risks resulting from a green action or inaction, foresight or unforeseen. In business and monetary terms, the value of risk outcomes shall be on employees, suppliers, customers, strategy, objectives, profile, assets, etc.

Examples
- 1. A fisherman starting a sea voyage on a fishing expedition may result in loss of life.
- 2. A home alone infant climbing on a window pane.
- 3. A family of fishermen starting a sea voyage on a fishing expedition may result in loss of life.
- 4. A homeowner taking a risk by buying a house in an earthquake-prone area.
- 5. A fast food restaurant opening a new branch in a high-crime area.

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 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 full promises made to stakeholders. Absence of risk management means failing "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 the only world and nothing beyond it exists.
RISK MANAGEMENT

1.2 Occupational Health & Safety Advisory Services (OHSAS)

OHSAS 18001 is a standard that helps organizations improve occupational health and safety performance and achieve business objectives.

Environmental risks, for example, can lead to the possibility of loss, injury, or other adverse or unintended consequences, which include economic losses, environmental damage, and human health effects.

Table 1.1: Definition of Risk

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>An occurrence that may happen or not happen, and whose outcome is uncertain.</td>
</tr>
<tr>
<td>Condition</td>
<td>A state or situation that may or may not occur, and whose outcome is uncertain.</td>
</tr>
<tr>
<td>Activity</td>
<td>An action or a process that has the potential to cause harm.</td>
</tr>
</tbody>
</table>

ISO Guide 73 (ISO 31000) defines risk as the "effect of uncertainty on objectives." In this definition, uncertainties include events (which may or may not happen) and their consequences. Consequences can range from positive to negative.

Oxford English Dictionary defines risk as "the possibility of loss, injury, or other adverse or unintended consequence, which includes economic loss, environmental damage, and human health effects."
arise from events taking place within the business enterprise. Such risks arise specifically to the processes, techniques and instruments utilized due to events occurring outside the business organization. Such events are associated with the management and protection of knowledge and affect the company, whether directly or indirectly.

The Open Group suggests classifying risks with respect to effectiveness of operations, financial reporting, and compliance. This categorization is illustrated below:

1.4 Risk Categories by COSO

- Efficiency and effectiveness of operations grow.
- The company does not meet strategic objectives.
- The processes do not operate efficiently.
- Customers are not satisfied with services received, etc.
- Financial reporting, the absence of a key financial control causes a material error in the financial statements.
- Compliance with laws and regulations, etc., 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 ‘low’ understanding 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.) indicates 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.

INTRODUCTION TO RISK

1.3

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

Positive and negative feedback about past risk taking affect future risk taking. In an experiment, people who were led to believe they were 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 fewer opportunities 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 tension, they pay close attention to potential threats in the environment and are highly vigilant so as to preserve themselves and their resources (Eysenck, 1997; Pressman, 1997, Auti, Gallois, & Lupintz, 2010). This attention to threat and vigilance leads people to avoid risk (Coxwellen et al., 201)

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 space 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 cars 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 fulfillment of corporate objectives. Corporate objectives are usually not fully stated or well-defined by most corporations. Where the objectives have been established, they tend to be stated as internal, annual, and change objectives. This particular true of the operational 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 1 for illustrative risks that Corporates are exposed to while navigating the business environment.

TABLE 1 Illustrative Corporate Risks

<table>
<thead>
<tr>
<th>Corporate Functions</th>
<th>Risk Areas</th>
<th>Sales &amp; Marketing</th>
<th>Human Resources</th>
<th>IT &amp; Technology</th>
<th>Finance &amp; Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor employee morale</td>
<td>Poor customer loyalty &amp; retention</td>
<td>Poor morale &amp; talent retention</td>
<td>Poor employee morale</td>
<td>Poor customer loyalty &amp; retention</td>
<td>Poor morale &amp; talent retention</td>
</tr>
</tbody>
</table>

1.6 ICAI’s Standard of Internal Audit

1.6.1 Strategic Risks

- 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 utilized to manage the finances of the enterprise, as well as the 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 based on the impact to the business (contingency plan). For example, if the risk of a recession would severely affect the company, it is important to classify the risk as High or Critical.

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 significantly. Internal factors giving rise to such risks include:

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

External factors giving rise to such risks include:

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

1.1 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 ‘low’ understanding 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.) indicates 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.

INTRODUCTION TO RISK

1.3

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

Positive and negative feedback about past risk taking affect future risk taking. In an experiment, people who were led to believe they were 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 fewer opportunities 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 tension, they pay close attention to potential threats in the environment and are highly vigilant so as to preserve themselves and their resources (Eysenck, 1997; Pressman, 1997, Auti, Gallois, & Lupintz, 2010). This attention to threat and vigilance leads people to avoid risk (Coxwellen et al., 201)

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 space 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 cars 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 fulfillment of corporate objectives. Corporate objectives are usually not fully stated or well-defined by most corporations. Where the objectives have been established, they tend to be stated as internal, annual, and change objectives. This particular true of the operational 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 1 for illustrative risks that Corporates are exposed to while navigating the business environment.

TABLE 1 Illustrative Corporate Risks

<table>
<thead>
<tr>
<th>Corporate Functions</th>
<th>Risk Areas</th>
<th>Sales &amp; Marketing</th>
<th>Human Resources</th>
<th>IT &amp; Technology</th>
<th>Finance &amp; Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor employee morale</td>
<td>Poor customer loyalty &amp; retention</td>
<td>Poor morale &amp; talent retention</td>
<td>Poor employee morale</td>
<td>Poor customer loyalty &amp; retention</td>
<td>Poor morale &amp; talent retention</td>
</tr>
</tbody>
</table>

1.6 ICAI’s Standard of Internal Audit

1.6.1 Strategic Risks

- 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 utilized to manage the finances of the enterprise, as well as the 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 based on the impact to the business (contingency plan). For example, if the risk of a recession would severely affect the company, it is important to classify the risk as High or Critical.

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 significantly. Internal factors giving rise to such risks include:

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

External factors giving rise to such risks include:

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

1.1 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 ‘low’ understanding 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.) indicates 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.
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 I risk my money on the outcome of the contest, then I 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. The terms risk, risk appetite, and tolerance are often used similarly to describe an organization’s or individual’s ability toward 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 investors’ tolerance for 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 deviate from risky asset holdings in response to a decline in health, controlling for variables such as income, age, and out-of-pocket medical expenses.

Risk appetite: Occasional, Seldom, Remote, Unlikely, Possible, Likely, Almost certain, Certain.

Risk consequence: Insignificant, Minor, Moderate, Major, Catastrophic.

Risk consequence is the worst possible outcome and the risk score is derived by multiplying the risk occurrence with risk consequence.

Risk due to risk appetite is the lowest possible outcome and the risk score is derived by multiplying the risk occurrence with risk appetite.

Risk appetite is the lowest possible outcome and the risk score is derived by multiplying the risk occurrence with risk appetite.

Risk appetite is the lowest possible outcome and the risk score is derived by multiplying the risk occurrence with risk appetite.

Risk ceases to be an immeasurable one that it is not in effect an uncertainty at all. We accordingly restrict the appearance that a measurable uncertainty, or “risk” proper, as we shall use the term, is so far different from an organization’s ability toward 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 investors’ tolerance for 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 deviate from risky asset holdings in response to a decline in health, controlling for variables such as income, age, and out-of-pocket medical expenses.

Complexity, Volatility, Ambiguity and Uncertainty (CVUA)

VUCA is an acronym used to describe or reflect on the volatility, uncertainty, complexity and ambiguity of general conditions and situations for greater clarity when the matrix is used.

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

Example: Private investment after a natural disaster takes a supply off-line.

Approach: Build in stock and devote resources to preparedness for instance, storepile inventory or overstock tunnel. These steps are typically expensive, your investment should match the risk.

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 deviate from risky asset holdings in response to a decline in health, controlling for variables such as income, age, and out-of-pocket medical expenses.

Complexity, Volatility, Ambiguity and Uncertainty (CVUA)

VUCA is an acronym used to describe or reflect on the volatility, uncertainty, complexity and ambiguity of general conditions and situations for greater clarity when the matrix is used.

Example: Private investment after a natural disaster takes a supply off-line.

Approach: Build in stock and devote resources to preparedness for instance, storepile inventory or overstock tunnel. These steps are typically expensive, your investment should match the risk.

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 deviate from risky asset holdings in response to a decline in health, controlling for variables such as income, age, and out-of-pocket medical expenses.

Complexity, Volatility, Ambiguity and Uncertainty (CVUA)

VUCA is an acronym used to describe or reflect on the volatility, uncertainty, complexity and ambiguity of general conditions and situations for greater clarity when the matrix is used.

Example: Private investment after a natural disaster takes a supply off-line.

Approach: Build in stock and devote resources to preparedness for instance, storepile inventory or overstock tunnel. These steps are typically expensive, your investment should match the risk.
INTRODUCTION TO RISK

1.17

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 of gain. These uncertainties may be due to perils such as fire, flood, etc. or may arise from human actions such as theft, accident, etc. There are certain risk events that can result only in negative outcomes such as incidents of pollution 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 death, sickness, accident, and disability, unemployment, etc.
- Property risks - it includes value in assets due to physical damage, fire, flood, etc.
- Liability risks - the risk of legal liability for damages accruing to customer, supplier, vendor, etc. Such risks are also connected with compensation payable to employees for injuries and other harm caused to them.

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

Fundamental Risks are imposed 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 is normal, 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 individual, 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 preferences, distribution of income, product development, shifts in technology, etc. These are called Dynamic Risks. As they are less predictable, generally, they are not insurable.

There are certain types of risks that give rise to uncertainty about the outcome of a situation. These can be described as operational risks and are frequently associated with project risks. Uncertainties can be associated with the benefits that the project produces, as well as uncertainty about the delivery of the project on time, which is budgeted to be completed in the timeframe.

As per studies conducted by International Federation of Accountants (IFAC) - Proper risk management and internal control help organizations understand the risks they are exposed to, put controls in place to counter threats, and effectively pursue their objectives. They are therefore an integral, organization-wide approach to risk management and internal control—which ultimately helps create, enhance, and protect stakeholders' value.

The application of risk management tools and techniques in the management of hazard risks is the

© The Institute of Chartered Accountants of India

1.19

The introduction of new machines is an opportunity risk, where the intention is to achieve a better result of the machine. The new machine may 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 machines may substantially undermine the manufacturing operations of the organization.

4. Types of Risks

Events can have negative impact, positive impact, or both. Events with a negative impact represent negative risks. Events that have a positive impact represent positive risks. Risk and opportunity management are closely interrelated. Organizations with superior competencies and knowledge databases attempt to convert negative risk events into positive change by forming a focused group of experts who brainstorm on breakthrough ideas that could help the organization move in a positive direction. This is a contemporary phenomenon and is commonly referred to as “catching the ball” or “looking forward.” 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 wikipedia - Risk is part of GRC (Governance, Risk and Compliance). Management is the ability to effectively and cost-effectively mitigate risks that can hinder an organization's operations. GRC is used as a business-oriented, comprehensive, and forward-looking approach that allows one to anticipate and prepare for any potential problems. Businesses face different types and extent of risks, how may cause serious loss of profits or even bankruptcy. Large companies have extensive “risk management” departments. Smaller businesses tend to not look at the issue in such a systematic way but may have more hands-on approach to risk management. A successful business meets its competitors' comprehensive, well-thought-out business plan. However, business is dynamic thing, because the trend and sales can sometimes appear out of place. When the company’s strategy becomes less effective in the marketplace and it struggles to reach its goal as a result, the company is facing strategic risks or market risks. It could be due to technological changes, a powerful new competitor entering the market, shift in consumer demand, etc.

Businesses can be affected by the influence of two major risks - internal risks arising from the events taking place within the organization, and external risks arising from the events taking place outside the organization.

Risk events are caused on account of cause 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:

<table>
<thead>
<tr>
<th>Internal Factors</th>
<th>External Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controllable</td>
<td>Controllable</td>
</tr>
<tr>
<td>Stability and financial position of the entity</td>
<td>Compliance with regulatory changes</td>
</tr>
<tr>
<td>Labour strikes</td>
<td>Economic conditions</td>
</tr>
<tr>
<td>Machine failure</td>
<td>Financials</td>
</tr>
<tr>
<td>Staff morale</td>
<td>Earthquakes</td>
</tr>
<tr>
<td>Uncontrollable</td>
<td>Market scenario</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In addition to the business risks, organizations can face major risks external which will be applicable to any organization:

- 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 credit default due to the inability or unwillingness of the customer or counterparty to meet their commitments.
- Liquidity risk - the potential inability to meet commitments as they fall due. It arises whenever the bank is unable to generate cash to meet its liquidity payment obligations or increase in assets or its failure to manage the unplanned decreases or changes in the funding sources.
- Market risk - the potential inability to meet commitments as the underlying market variables change. It stems from changes in the market prices or interest rates.

The market risk can arise due to changes in marketable conditions such as, volatility of rate of interest on the Foreign Exchange rate, Government stability, etc. It is the risk that arises from the changes in the market prices of assets or liabilities, or the change in the market interest rates.
INTRODUCTION TO RISK

1.21

Risk management is a process that involves identifying, assessing, and prioritizing risks, and then developing, implementing, and maintaining a plan for dealing with the risks found. The main objective of risk management is to ensure that organizations are able to identify and manage risks effectively. This involves understanding the potential risks that an organization may face and developing strategies to mitigate those risks.

Risk management is a continuous process that involves identifying, analyzing, and responding to risk. It is a systematic approach to assessing and managing the risk of a particular event or situation occurring. The process involves defining the risks associated with a particular event or situation, assessing the potential impact of those risks, and developing strategies to mitigate those risks.

RISK MANAGEMENT

1.22

Risk management is a process that involves identifying, assessing, and prioritizing risks, and then developing, implementing, and maintaining a plan for dealing with the risks found. The main objective of risk management is to ensure that organizations are able to identify and manage risks effectively. This involves understanding the potential risks that an organization may face and developing strategies to mitigate those risks.

Risk management is a continuous process that involves identifying, analyzing, and responding to risk. It is a systematic approach to assessing and managing the risk of a particular event or situation occurring. The process involves defining the risks associated with a particular event or situation, assessing the potential impact of those risks, and developing strategies to mitigate those risks.

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
- Identify 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

Risk Identification is the action or process of recognizing various potential internal or external events, or threats or vulnerabilities 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 assessment matrix or risk register and communicating the risks to the executive management.

Risk Identification is the initial step in the process of risk 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-if questioning 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

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 reasonably 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 the future. The SWOT analysis exercise will facilitate development of sound business knowledge and communication of key business weaknesses, threats and opportunities to those in the risk management exercise.

© The Institute of Chartered Accountants of India

2. QUANTIFICATION OF RISK AND VARIOUS METHODOLOGIES

2.1 IDENTIFICATION AND SOURCES OF RISKS

The entity becomes aware of various risks through the Risk Identification thereafter deals with the risks at large. It must set objectives, integrated with the sale, production, marketing, financial and other activities so that the organization is operating in concert. It also must establish mechanisms to identify 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 believing that the key business processes and thereafter undertaking a "what can go wrong exercise".

5.2.15 of ICAS states that financial reporting is also subject to risks arising from a number of internal and external transactions, events or circumstances. These 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-organizations
- Expanded foreign operations
- New accounting pronouncements

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

- Strategic – Those include business model risk factors in terms of product element factors, availability of supply chain inputs at competitive rates, innovation, competition, financial stability and capital access, etc. These relate to the achievement of long-term strategic

© The Institute of Chartered Accountants of India

2.2 SOURCE AND EVALUATION OF RISKS

SOURCE AND EVALUATION OF RISKS

2.3 SOURCE AND EVALUATION OF RISKS

SOURCE AND EVALUATION OF RISKS

2.4 SOURCE AND EVALUATION OF RISKS

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 provides which risks need to be managed.
- Simple way of assessing risk is by assigning a probability and impact to the happening of an event. It is the risk that can occur. It is given by a probability of 0.0, if it is certain that it will occur. It is given by a probability of 1.0. 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 0.5. Uncertain risks are assigned between 0.5 and 1.0. Maximum risk impact may be a consequence of uncertainty.

© The Institute of Chartered Accountants of India

2.5 Quantitative Risk Assessment

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

© The Institute of Chartered Accountants of India

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 believing that the key business processes and thereafter undertaking a "what can go wrong exercise".

5.2.15 of ICAS states that financial reporting is also subject to risks arising from a number of internal and external transactions, events or circumstances. These 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-organizations
- Expanded foreign operations
- New accounting pronouncements

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

- Strategic – Those include business model risk factors in terms of product element factors, availability of supply chain inputs at competitive rates, innovation, competition, financial stability and capital access, etc. These relate to the achievement of long-term strategic

© The Institute of Chartered Accountants of India

2.2 SOURCE AND EVALUATION OF RISKS

SOURCE AND EVALUATION OF RISKS

2.3 SOURCE AND EVALUATION OF RISKS

SOURCE AND EVALUATION OF RISKS

2.4 SOURCE AND EVALUATION OF RISKS

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 provides which risks need to be managed.
- Simple way of assessing risk is by assigning a probability and impact to the happening of an event. It is the risk that can occur. It is given by a probability of 0.0, if it is certain that it will occur. It is given by a probability of 1.0. 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 0.5. Uncertain risks are assigned between 0.5 and 1.0. Maximum risk impact may be a consequence of uncertainty.

© The Institute of Chartered Accountants of India

2.5 Quantitative Risk Assessment

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.
probability and impact matrix is prepared where the levels of risk severity are depicted through a color scheme of red, green, yellow and blue, with red being the most severe or critical risk condition. This is also called as the traffic signal risk card.

Risk analysis is a method of analyzing 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 placed along the vertical bar of the area. 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 8, where the probability and impact rate the highest, requires immediate attention – Grid I. Those with a low rating of 1 or 2 require the least attention and may even be ignored, if insignificant – Grid VI.

### 2.2 Quantitative Risk Assessment

Quantitative risk analysis is the process of estimating the cost of risk to the business with 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.

![Quantitative Risk Assessment Diagram](https://via.placeholder.com/150)

#### 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, it is required a systematic educator and ongoing professional updating.

(b) **The Delphi Technique**: 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 'rate' the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposure 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 exposure depending on the severity, impact on occurrence, and costs involved. The product of the risk weight with the exposure weight of each characteristic gives us the weighted score. The sum of these weighted scores gives us the risk and exposure scores of the system. System risk and exposure is then ranked according to the scores obtained.

(d) **Quantitative techniques**: These 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 various events. Keeping in mind what often such an event may occur.

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

### 2.4 Risk Management

Component causes cost overruns for the manufacturing facility and delays schedule to customers and results in penalties from the customer.

### 2.5 Source and Evaluation of Risks

The objective of qualification 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 next 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 0.65. As per information generated via weather conditions, the following data is assembled.

- Chance of good weather: 46%
- Chance of bad weather: 65%

**Conclusion**

- 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)]
- [0.46 + 0.65]
- [1.11]
- [0.82 ± 0.30]
- [± 0.28 ± 0.18]
- [= 0.10]

This can also be translated as a 90% probability for a public event. While the cut-off criteria for the public event are 85%, 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 very early in the project and 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 are in unstructured ways (e.g., schedule delays may force consideration of a new strategy that reduces overall project duration);
- One risk event can cause multiple impacts, any 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.

---

**© The Institute of Chartered Accountants of India**
RISK MANAGEMENT

4. Checklists are information aids to reduce the likelihood of failures from potential hazards. They are specific tasks that have been developed usually from past experiences, either as a result of a previous risk assessment or as a result of good failures or incidents or history or industry learning. Auditors often prepare checklists of key controls to add to their assessment of control effectiveness and the internal control environment. Checklists are good guiding tools; however, care should be taken to be flexible and risk managers can make use out of such 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 “hypotheses” to stimulate participants to identify risks. It is commonly used for decision making purposes.

Scenario Analysis is a process to analyse future events by considering alternative outcomes or alternative worlds. Scenario planning 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 such scenario, the management analysts and analysts the potential consequences and potential causes when analysing risk. Scenario analysis can be used effectively to identify topics for fraud forecasting, managing financial risks, etc. Reserve Bank of India prescribes scenario analysis based testing of Liquidity position of banks in India.

7. Fault Tree Analysis (FTA) This method is similar to a form of creative thinking called creative brainstorming. This technique is used for identifying and analysing factors that can contribute to a specific undesired event (called the “top event”). Causal factors are first identified and organized in a logical manner and represented pictorially in a tree diagram. For example, if you want to improve customer service, define the objective in reverse i.e. “How can we not 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, listing and analyzing the pathways of a risk from cause to effect/sequence. 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 consequence for a brainstorming session. Bow tie analysis is a good way to clean up the ideas generated and consolidate the results into more appropriate risk statements.

9. Direct Observation This relatively simple technique is used daily in the workplace by staff who may observe situations and hazards regularly. It is also used in 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.

Incident Analysis - Incidents Analysis related to risks that have recently occurred. Recording incidents in a regular, conducting root cause analysis and periodically running some trend analysis helps to analyse incidents, i.e. it can potentially enable new risks to be identified. In addition, a high frequency of risk incidents can be a key risk indicator to a potentially larger problem.

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 organization’s risk culture. Internal auditors use surveys to assess the internal control environment. Some organizations use annual staff surveys to gauge staff understanding of key risk and governance policies and procedures.

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

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 risks or competitors.

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 objectives and its associated uncertainties.

Working groups - Compact working groups can be formed that could be cross functional.

Corporate knowledge - History of risk 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.
2.14 RISK MANAGEMENT

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 there, 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 final 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 those 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 measures will be allocated to functions with higher risks. The risk evaluation will directly affect the nature, timing and extent of audit measures 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?

2.15 SOURCE AND EVALUATION OF RISKS

- 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 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.
- What is the cost if what can go wrong does go wrong? (Exposure)

Risk evaluation is 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.

2.16 RISK MANAGEMENT

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 organization.

Internal risks arise from factors (that can be controlled) such as people or human factors, such as management, strikes, technological factors (emerging technologies), physical factors (failure of machinery, 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 risk, pricing pressures), 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 weak areas or threats exist in each case. A brief list is set out below:

- Pressure by competitors
- The employees
- The customers
- The new technologies
- Changes in the environment
- Laws and regulations
- Globalization and global events
- The operations
- The suppliers
- Natural disasters
- 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

Weaknesses:
- Commercial fragmentation
- Limited access to financing
- Lacks 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
Mumbai is one of the few vulnerable cities 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 storms and surge, 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 41% of India’s tax revenues, 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 concentrated with the presence of at least 1,000 hazardous old industrial units in the city. The worst event recorded in the Victoria dye explosion in 1944 which killed up to 4,000 and devastated 1.2 sq. Km. The most recent one was the Tardeo fire that occurred at the State Secretariat Building in 2012.

2. Floods. Mumbai civic authorities identify 10 sectors 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 perhaps the worst that the city has faced in long time, an exceptional series of random 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, Births, storms, terrorism, riots and tidal surge are additional hazards that need to be analyzed 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 read in, a poor 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 sewage system.

3.3 Global Risk Outlook

One of the most important sources 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 survey 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 prevalent, long-term trends such as inequality and deepening social and political polarization to exacerbate risks associated with, for example, the weaknesses of the economic recovery and the speed of technological change.

These trends came into sharper focus during 2016, with rising political discontent and dissatisfaction 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 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:

- Examining the potential of prevalent, long-term trends such as inequality and deepening social and political polarization to exacerbate risks associated with, for example, the weaknesses of the economic recovery and the speed of technological change.
- Examining the potential of prevalent, long-term trends such as inequality and deepening social and political polarization to exacerbate risks associated with, for example, the weaknesses of the economic recovery and the speed of technological change.
- Examining the potential of prevalent, long-term trends such as inequality and deepening social and political polarization to exacerbate risks associated with, for example, the weaknesses of the economic recovery and the speed of technological change.
- Examining the potential of prevalent, long-term trends such as inequality and deepening social and political polarization to exacerbate risks associated with, for example, the weaknesses of the economic recovery and the speed of technological change.

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 practitioners 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 analysis can be vital in determining the impact and effect of a risk event.

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...
2.23

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 very greatly, depending on industry, locale, and other business variables. The impact a risk could have on an organisation is multidimensional in nature. The levels of risk impact can be assessed across following areas:

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Impact Area</th>
<th>Nature of Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Strategy and business objectives</td>
<td>Delays, change management, failure to achieve objectives</td>
</tr>
<tr>
<td>2</td>
<td>Financial</td>
<td>Direct or indirect financial loss</td>
</tr>
<tr>
<td>3</td>
<td>Customer</td>
<td>Loyalty, relationship, payment terms, attrition</td>
</tr>
<tr>
<td>4</td>
<td>Employee</td>
<td>Morale, engagement, attrition</td>
</tr>
<tr>
<td>5</td>
<td>Vendor/supplier</td>
<td>Loyalty, relationship, payment terms, attrition</td>
</tr>
<tr>
<td>6</td>
<td>Compliance</td>
<td>Delays, penalties, fines, defaults, impairment</td>
</tr>
</tbody>
</table>

As seen from above table the impact of risk is all pervasive and organisations are wise to 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.

Examples:
- 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 consisting 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 sometimes impact a company's earnings, in a single day.

© The Institute of Chartered Accountants of India
### Source and Evaluation of Risks

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 prioritisation and thorough analysis of the risk factors based on probability models which can be closely related to the actual impact of the risk. Likewise, prioritising stakeholders by authority and degree of involvement and levels of risk threats is mandatory. 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, seeks 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 protecting the value of investment and generating more value to provide returns on investments to the shareholders. A modern view on this subject is that a business creates value 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 profit 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 expected 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, and 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, suppliers). The government wants the business to pay taxes, employ more people, follow laws, and truthfully report its financial condition. 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 Drynmans 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 statuses are:

- Government: taxation, legislation, job-unemployment and truthful reporting.
- Employees: 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, standards 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 exercises 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 risk each of them faces and successfully manage the risk factors. A stakeholder risk analysis is essential so that each stakeholder – be it an individual or an 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 Management**

- (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 losses, better performance, and profitability, and increased shareholder value.

It is necessary to evaluate all types of risks interacting with categories of stakeholders and find solutions to overcome the threats before the risk occurs. The mere awareness 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 a Risk Committee and casts onerous responsibilities on the Board and Audit Committees to discharge their related responsibilities in terms of materiality, probabilities, 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 organization. Risk Management Committee should comprise of people who have authority and influence over the organization’s 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. Source and Evaluation of Risks
   - 3.1 Manage the process for developing risk policies and procedures, risk limits and approval authorities.
   - 3.2 Monitor major, critical and minor risks.
   - 3.3 Manage the process for escalating critical risks to a higher level.
   - 3.4 Implement the risk management program and risk strategy. Ensure the risk management program and risk strategy are effectively integrated into product development and delivery methodology.
   - 3.5 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**

<table>
<thead>
<tr>
<th>Role</th>
<th>Function Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. To assess the company’s risk profile, risk appetite and key areas of risk in particular</td>
<td></td>
</tr>
<tr>
<td>2. To recommend the Board and adoption of risk assessment and rating procedures.</td>
<td></td>
</tr>
<tr>
<td>3. To articulate the company’s policy for the oversight and management of business risks.</td>
<td></td>
</tr>
<tr>
<td>4. To examine and determine the sufficiency of the company’s internal processes for reporting and managing key risk areas.</td>
<td></td>
</tr>
<tr>
<td>5. To assess and recommend board acceptable levels of risk.</td>
<td></td>
</tr>
<tr>
<td>6. To facilitate development and implementation of a risk management framework and internal control system.</td>
<td></td>
</tr>
<tr>
<td>7. To review the nature and level of insurance coverage.</td>
<td></td>
</tr>
</tbody>
</table>
RISK MANAGEMENT

8. To have special investigation into the areas of corporate risk and break downs in internal control.
9. To review management performance to the company auditor’s recommendations.
10. To report the trends of the company’s risk profile, reports on specific risk and the status of risk management process.
11. Responsibility
   1. To define the risk appetite of the organization.
   2. To exercise oversight of management responsibilities, and review the risk profile of the organization to ensure that it 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 ongoing 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 ongoing process to identify, to measure its potential impact against a broad set of assumptions and then to set pro-actively to manage those risks, and to decide the company’s appetite or tolerance for risk.
   8. To ensure that a systematic, documented assessment of the processes and the outcomes 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.

© The Institute of Chartered Accountants of India

6.4 Principles for Effective Implementation of Risk Management

Recommended By OECD

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 situations.
14. To fulfill its statutory, advisory 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 achieve 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.

© The Institute of Chartered Accountants of India

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.

IBM’s risk team spends more time on the strategic side, engaging with risk leaders and ensuring that business units pursue risk mitigation with their risk appetite.

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 list of people in a new risk department. IBM philosophy is that risk management should be integrated 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 limited resources, education, and training.

IBM has about 33 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 business units how to account for them, how to mitigate and control them. People that 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 most fast 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.
1.1 Determining Risk Appetite

The board of directors has the primary oversight responsibility for developing and implementing the organization's mission, values, strategy, and objectives and to define the contours and definition of the risk capacity, appetite, and tolerance levels. Specific responsibility regarding these issues is assigned to the risk management group. The board also originates risk philosophy, risk appetite, and risk tolerance. Risk management is a critical function of the organization's strategic management. It is the process whereby organizations methodically address the risks that they are exposed to with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.

1.2 Risks Appetite – Principles and Approach

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 Latin word “riso” which means danger or “riuscare,” which means to draw or French word “risquer.” Risk is known or unknown but is always inherent in individual or business actions therefore it is more of a “choice” rather than a lack. Risk and reward are two sides of the same coin. Good Risk leaders select their actions well and 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, Definitions, and Critical,” the modern terms for managing risk rose after World War II, but the discipline massively began as a study of using insurance to manage risk. Later, from the 1960s 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. Regulations started recognizing 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 risks and additional, rather it implies making informed and coherent choices. The ratio that this organization wants to take in pursuit of its objectives and in particular choices it makes to manage and mitigate those risks. Let us study below important views on the subject of Risk Management.

<table>
<thead>
<tr>
<th>Source</th>
<th>Thoughts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warren Buffet</td>
<td>Risk comes from not knowing what you are doing</td>
</tr>
<tr>
<td>Theodore Roosevelt</td>
<td>Risk management is about people and processes and not about models and technology</td>
</tr>
<tr>
<td>The Risk Management Standard, The Institute of Risk Management</td>
<td>Risk management is a central part of any organization’s strategic management. It is the process whereby organizations methodically address the risks that they are exposed to with the goal of achieving sustained benefit within each activity and across the portfolio of all activities</td>
</tr>
</tbody>
</table>

3.4 RISK MANAGEMENT

3.4.1 Concept of Risk Management

Risk management should be a continuous and developing process which runs throughout the organization’s strategy and the implementation of that strategy. It should address methodically all the risks surrounding the organization’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, then promoting operational efficiency at all levels.

Thomas S. Colelon, Practical Guide Risk Management, CPA Institute

Risk management is the art of using business from the past to mitigate marketplace 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 sales risk and market risk is simply part of managing returns and profits. Managing risk must be a core competency 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 those that are not successful. All successful firms, managing risk always has been and continues to be the responsibility of line managers—from the board through the CDO and down to individual trading units or portfolio managers. Managers have always known that it is their responsibility, 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 is that has been that the technical skills and knowledge required of line managers has grown up.

3.5 Objectives and Process of Risk Management

The following key principles have underpinned risk appetite:

1. Risk appetite can be complex. Excessive simplicity, while superficially attractive, leads to dangerous errors. 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 appetite may vary over time. Like in sourcing decisions, the Board may set vendor business share limits as they would make the entity dependent on few vendors companies that could eventually expect 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 (or 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 its risks and the regulatory environment within which it operates.

2. Objectives 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.
3.6 RISK MANAGEMENT

While a vision statement is often aspirational, the goals and objectives should ordinarily describe simple terms what is to be accomplished. They should be achievable 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 Analysis
(iii) Risk Mitigation.

A rubric, 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 process, the risk management process 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.

© The Institute of Chartered Accountants of India

3.7 RISK MANAGEMENT

1. Treat the Risk.
2. Evaluate or Rank the Risk.
3. Risk control – What should we do? (to prevent the loss from occurring or to recover if the loss does occur)
4. Sources of risk assurance for the Board have been identified and validated
5. Risk appetite, tolerance and constraints
6. Significant risks and key risk indicators
7. Risk appetite, tolerance and constraints
8. Risk control – What should we do? (to prevent the loss from occurring or to recover if the loss does occur)
9. Risk control – What should we do? (to prevent the loss from occurring or to recover if the loss does occur)
10. Risk control – What should we do? (to prevent the loss from occurring or to recover if the loss does occur)

© The Institute of Chartered Accountants of India
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 day-to-day operations. The management of an organization, enabled by its governance structures, 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 continue and grow their businesses. Risk management is recognized 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, analyzing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organizations to minimize losses and maximize opportunities.

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

Risk can be faced by 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 early, entities are able to actively protect value from any potential catastrophic and avoid 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, provide the impact, and put procedures in place to mitigate the risk, or even eliminate it if the risk is possible.

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.

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, tolerance, 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 the future.

(ii) Transfer

For some risks, the least 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 risk 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 tolerable, or acceptable to tolerable 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 project viable. For example, land acquisition for a project whose feasibility is based on that projected cost-benefit relationship is in jeopardy as the cost of treating the risk does not make the project viable.

(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 or an acceptable level.

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

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Questionnaires</td>
<td>Designed to identify the relevant risks and create risk history.</td>
</tr>
<tr>
<td>Flow Charts with Risk Flags</td>
<td>Designed to identify operational risks embedded in the processes.</td>
</tr>
<tr>
<td>Identified Controls to manage risks</td>
<td>Recognize controls and test their adequacy and operational effectiveness.</td>
</tr>
<tr>
<td>Risk Event Maps</td>
<td>Identify potential events that can have a significant impact on business to avoid negative surprises.</td>
</tr>
<tr>
<td>Risk Scenarios</td>
<td>A matching tool to track progress of risk management.</td>
</tr>
<tr>
<td>Capital Budgeting</td>
<td>A financial analysis tool to evaluate the future cash flows.</td>
</tr>
<tr>
<td>Risk Management Information System</td>
<td>A financial analysis tool to evaluate the future cash flows.</td>
</tr>
</tbody>
</table>

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 allocation and business strategy.

• Develop a common language in the organization 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 to reviewing the risk profile & loss statement along with the financial profit & loss statement to determine the health of their entities.

Identifying top threats to entity and asset protection measures.

• Linking risks to more efficient capital allocations and business strategy.

• Developing a common language in the organization for problem solving.

• Effectively respond to an evolving business environment.

• Identifying top threats to entity and asset protection measures.

• Linking risks to more efficient capital allocations and business strategy.

• Developing a common language in the organization for problem solving.

• Effectively respond to an evolving business environment.

Profit or loss is a result of the existence of risk. This is a fact that is often ignored. It is important to view profit or loss as a result of risk, and also to realize that profit or loss is a result of risk.

Risk management is an integral part of any business. It is important to view profit or loss as a result of risk, and also to realize that profit or loss is a result of risk.

Risk management is an integral part of any business. It is important to view profit or loss as a result of risk, and also to realize that profit or loss is a result of risk.
As in any cultural journey, a catalyst for change is essential. In this case, the catalyst was the CT1’s Executive Steering Committee formed a Risk Management Working Group (RMWG) and tasked the them to (1) identify examples of frequent risk categories, (2) determine what extent those need to change. It will also test how well current decision-making processes work, and what improvements are needed. The initial direction and expectation set by CT1 provided the "push" to make changes, but the real tests were the "pull" from project teams. The "pull" was driven by project teams who were frustrated with the current processes and wanted to make improvements. 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.

Case Study 1

An inappropriate risk culture isn’t always about taking too much risk. Externally, Kossak was trusted leading brand for over a hundred years. But its strategic failures to reinvent itself and exploit digital technology led it to a decent into Chapter 11 bankruptcy.

As its culture meant that Kossak avoided risky decisions, and instead developed procedures and policies to maintain the status quo rather than adapting to the changing external environment. (Vandewall, 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 challenges of the traders’ judgments by risk control functions; weak risk governance and inadequate scrutiny (Diamond, 2012).

According to the New York Times, inadequate management of trading positions was not effectively challenged, there were regular shifting practices and difficult personally issues.

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 essentially filed too low figures. This tactic sought to hide the level to which Barclays crisis, Barclays filed artificially low figures. This tactic sought to hide the level to which Barclays.

Diamond, along with Barclays chairman Marcus Agius. Barclays was fined 290m by UK and US regulators for rigging Libor and investigations are ongoing. Barclays have set up an independent review to assess the bank’s current values, principles and standard of operation and determine what extent these 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.

© The Institute of Chartered Accountants of India

© The Institute of Chartered Accountants of India

© The Institute of Chartered Accountants of India
4.2 RISK MANAGEMENT

1. POPULATION AND SAMPLE ANALYSIS

1.1 Population

It refers to the collection of all elements that comprise the entire universe possessing common characteristics. For example, we are studying grade point average of students in college, population is the set of all students. Also, if you own returns of all the stocks traded in NSE is an example of population.

Typically it is difficult, to sum up the entire population because not all the members are observable. If it is possible to enumerate the entire population it is often too costly to do and would take a lot of time.

Instead, we would take a subset of the population called a sample and use this sample to draw inferences about the population under study given some conditions.

1.2 Sample

Sample is a subgroup of the members of the population. It is a smaller, manageable version of a larger group. It is an unbiased sample of observations that is taken from a population. If the sample is unbiased, the sample data should be able to make inferences about the population. In order for a sample to be unbiased and random, it must be

- Representative of the population
- Randomly Selected
- Sufficiently large

For example, a sample of 50 stocks may be selected from all the stocks listed in NSE to represent the population of all the stocks traded in NSE.

There are many ways to select a sample and the study of this is called sampling theory. A commonly used method is called Simple Random Sampling. In Simple Random Sampling each member of the population has an equal probability of being included in the sample. It is a many other sampling methods e.g. Stratified sampling, Cluster sampling, etc.

1.3 Averages

Average is a measure of Central Tendency. Mean is the first moment of distribution. In statistics, there are actually three different types of averages: means, modes, and medians. By far the most commonly used average in risk management is the mean.

\[
\text{Mean} = \frac{\sum X}{n}
\]

The mode is the value that occurs most frequently.

The median and mode are also types of averages. The median represents the centre of a group of data within the group. Half the data points will be less than the median, and half will be greater.

It is used in finance for the calculation of average interest rates or returns. The geometric mean for recent years of equity returns. A mean of such a dataset, which is much more likely in practice, is

\[
\text{Geometric Mean} = \left(\prod_{i=1}^{n} X_i\right)^{\frac{1}{n}}
\]

However, in practice, we typically do not have the population. More often we have only a subset of the population or a dataset that cannot realistically be considered comprehensive; e.g., the most recent year of supply returns. A mean of such a dataset, which is much more likely in practice, is called the sample mean.

Sample Mean is the sum of all the values in a sample of the population \(\sum X\) divided by the no. of observations \(\bar{X} = \frac{\sum X}{n}\). But the difference between a population parameter (e.g., population mean) and a sample estimate (e.g., sample mean) is an essential to statistics, each sample will produce a different sample mean, which is likely to be near the true population mean but different depending on the sample. We use the sample estimate to infer something about the unobserved population parameter.

The population mean and sample mean are both part of Arithmetic means. The median and mode are also types of averages. The median represents the centre of a group of data within the group. Half the data points will be less than the median, and half will be greater.

The mode in the value that occurs most frequently.

1.4 Geometric Mean

It is used in finance for the calculation of average interest rates or returns. The geometric mean for a series of numbers is calculated by taking the product of these numbers and raising it to the inverse of the length of the series. It is often used to calculate investment returns over multiple time periods.

\[
G = \left(\prod_{i=1}^{n} X_i\right)^{\frac{1}{n}} = \left(\frac{1}{n} \sum X_i\right)^{\frac{1}{n}}
\]
When calculating the geometric mean for a return data set, it is necessary to add 1 to each value and then subtract 1 from the result. The geometric mean return (RG) can be computed using the following equation:

\[ RG = \left( \prod_{i=1}^{n} (1+R_i) \right)^{1/n} - 1 \]

**Example**

For the last three years, the returns for ABC common stock have been 10.3%, 21.3%, and 7.4%. Compute the compound annual return of ABC over the 3-year period.

Answer

\[ RG = \left( 1.103 \times 1.213 \times 1.074 \right)^{1/3} - 1 \]

1.5 Expected Value

Expected value exists when we have a parametric distribution (e.g., normal, binomial) which will be explained later in the chapter or probabilities. Expected value is the weighted average of possible values. In the case of a discrete random variable, expected value is given by:

\[ EV = \sum_{i=1}^{n} p_i y_i \]

Where \( p_i \) and \( y_i \) are the respective probabilities that the outcomes will occur.

\[ EV = \sum_{i=1}^{n} p_i y_i \]

1.6 Variance and Standard Deviation

Variance (and Standard Deviation) is the second moment of the distribution, most common measures of dispersion. It is basically the deviation from the mean.

\[ Var(x) = \sum_{i=1}^{n} (y_i - \mu)^2 p_i \]

The square root of Variance is the Standard Deviation. It is denoted by \( \sigma \) (sigma).

\[ \sigma = \sqrt{\sum_{i=1}^{n} (y_i - \mu)^2 p_i} \]

When calculating the geometric mean for a returns data set, it is necessary to add 1 to each value and then subtract 1 from the result. The geometric mean return (RG) can be computed using the following equation:

\[ RG = \left( \prod_{i=1}^{n} (1+R_i) \right)^{1/n} - 1 \]

**Example**

For the last three years, the returns for ABC common stock have been 10.3%, 21.3%, and 7.4%. Compute the compound annual return of ABC over the 3-year period.

Answer

\[ RG = \left( 1.103 \times 1.213 \times 1.074 \right)^{1/3} - 1 \]

1.5 Expected Value

Expected value exists when we have a parametric distribution (e.g., normal, binomial) which will be explained later in the chapter or probabilities. Expected value is the weighted average of possible values. In the case of a discrete random variable, expected value is given by:

\[ EV = \sum_{i=1}^{n} p_i y_i \]

Where \( p_i \) and \( y_i \) are the respective probabilities that the outcomes will occur.

\[ EV = \sum_{i=1}^{n} p_i y_i \]

1.6 Variance and Standard Deviation

Variance (and Standard Deviation) is the second moment of the distribution, most common measures of dispersion. It is basically the deviation from the mean.

\[ Var(x) = \sum_{i=1}^{n} (y_i - \mu)^2 p_i \]

The square root of Variance is the Standard Deviation. It is denoted by \( \sigma \) (sigma).

\[ \sigma = \sqrt{\sum_{i=1}^{n} (y_i - \mu)^2 p_i} \]

1.7 Covariance and Correlation

We have already covered variance which is the deviation from the mean for one variable. Covariance is the relationship between deviations of two variables.

Covariance is measured by:

\[ Cov(X,Y) = \frac{\sum_{i=1}^{n} (x_i - \mu_x)(y_i - \mu_y)}{n} \]

where \( X \) and \( Y \) are two random variables with means \( \mu_x \) and \( \mu_y \) respectively.

If the true means are unknown, the means are the sample means and the covariance is the sample covariance:

\[ Cov_{xy} = \frac{\sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{n-1} \]

Interpretation of Covariance is difficult as it can take very large values which can range from positive infinity to negative infinity and are usually expressed in squared units.

Correlation

Correlation is measured by dividing covariance with the standard deviation of two random variables. It is denoted by \( \rho \) (rho).

\[ \rho = \frac{Cov(X,Y)}{\sigma_x \sigma_y} \]

where \( Cov(X,Y) \) = Covariance between X and Y

\( \sigma_x = \) Standard Deviation of X Variable

\( \sigma_y = \) Standard Deviation of Y Variable

**Properties of Correlation Coefficient**

- It measures the strength of linear relationship between two random variables.
- It does not have any units.
- Correlation Coefficient value ranges from -1 to +1.

If \( Cov(X,Y) = +1 \), then the variables seems to have perfect positive correlation. The movement in one variable results in proportional movement in the other variable.

If \( Cov(X,Y) = -1 \), then the variables seems to have perfect negative correlation. The movement in one variable results in exact opposite movement in the other variable.

If \( Cov(X,Y) = 0 \), then there is no linear relationship between the variables.
RISK MANAGEMENT

2.4 Bayes Theorem

Bayes Theorem shows how a conditional probability of the form P(B|A) may be combined with the initial probability P(A) to obtain the final probability P(AB).

\[
P(AB) = P(A|B) \times P(B)
\]

\[
P(B|A) = \frac{P(AB)}{P(A)}
\]

EXAMPLE

Rohan is forecasting a stock's performance in 2012 conditional on the state of the economy of the country in which the firm is based. He divides the economy's performance into three categories of good, neutral and poor and the stock's performance into three categories of increase, constant and decrease. The estimates are:

- The probability that the state of the economy is good is 25%. If the state of the economy is good, the probability that the stock price increases is 80% and the probability that the stock price decreases is 25%.
- The probability that the state of the economy is neutral is 30%. If the state of the economy is neutral, the probability that the stock price increases is 50% and the probability that the stock price decreases is 25%.
- If the state of the economy is poor, the probability that the stock price increases is 15% and the probability that the stock price decreases is 75%.

Arjun, the supervisor, asks him to estimate the probability that the state of the economy is neutral given that the stock performance is constant. Rohan's best assessment of that probability is closest to what?

Answer

Using Bayes Theorem:

\[
P(\text{Neutral} | \text{Constant}) = \frac{P(\text{Constant} | \text{Neutral}) \times P(\text{Neutral})}{P(\text{Constant})}
\]

= \frac{0.25 \times 0.3}{0.25 \times 0.3 + 0.5 \times 0.15 + 0.15 \times 0.75}

= 0.267
### 4.12 Risk Management

Reinforcement learning are good examples 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 or better understanding of the relationship between the independent and dependent variables. Each 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 derive 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 clustering 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 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 person's diagnosis (Acute Myelogenous Leukemia, Acute Lymphoblastic Leukemia, or No Leukemia).

#### 4.3 Analytics - Risk Management Applications

Risk management faces new demands and challenges. In response to the crisis, regulations 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. A number of key domains – particularly operational and compliance risk – Big Data technologies will allow the development of models that will support every day.

<table>
<thead>
<tr>
<th>Risk Model</th>
<th>Learning Outcomes</th>
<th>Chapters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantitative Analysis</td>
<td>After going through the chapter student shall be able to understand:</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>✓ VAR</td>
<td>✓ Stress Testing</td>
</tr>
</tbody>
</table>
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 (µ = 0) and standard deviation (σ = 1). It can be used to measure broader measures of the distribution of potential losses.

\[ \text{VaR} = \mu + z\sigma \]

where

- \( \mu \) is mean return
- \( \sigma \) is standard deviation
- \( z \) is the critical value from the standard normal distribution corresponding to the chosen confidence level

1.1.1 VaR Computation

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 also can 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:

\[ \text{VaR}(99\%) = \text{VaR}(95\%) \times \sqrt{2} \]

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 options in options, the linear exposure will be delta. 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. This method is best used in portfolios which has a linear position.

\[ \text{Portfolio VaR} = \sum \left( \text{Delta} \times \sigma_i \right) \]

where

- \( \text{Delta} \) is the sensitivity of the portfolio value with respect to change in risk factor
- \( \sigma_i \) is the standard deviation of the underlying asset

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

\[ \text{ΔP} = \Delta * \text{P} \delta \]

where

- \( \Delta \) is the sensitivity of the portfolio value
- \( \delta \) is change in risk factor

Limits of the delta-normal method

It is only accurate for linear exposures, not 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 – In the full re-valuation 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 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
be enough historical data. Also, the variation of risk in the past may not represent the variation of risk in the future. This is the case in case of linking to correlations and volatilities.

(b) Bootstrap Simulation – Bootstrap simulation is an extension of historical simulation. It draws a sample from the dataset and resamples it. 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 this data will be the average of all sample VaR.

(c) Monte Carlo Simulation – This method is similar to bootstrap simulation except that 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 results which are supplied 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 return. 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 an 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 not fails, that is it is highly subjective and that generated scenarios may not be relevant going forward. The computational time is quite high and this method is expensive due to the requirement of advanced technological skills.

1.3 Coherent Risk Measures

We need 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 risks, a risk measure (thetis) 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 will impact the risk of the portfolio.

\[ \rho(kX) = k \rho(X) \]

- Monotonicity – Portfolios with greater total returns will likely have less risk.

\[ \rho(X) \geq \rho(Y) \implies \rho(kX) \geq \rho(kY) \]

- Risk free condition – The risk of a portfolio is dependent on the assets within the portfolio for all constant n.

\[ \rho(kX + \sigma^2 n) = \rho(X) \]

The second, third & fourth properties imply well behaved distributions. Homogeneity says risk of a portfolio 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, but 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 adds 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 99th percentile is the probability weighted average of all losses greater than the VaR of the 99% 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 cutoff variable 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.
5.10 RISK MANAGEMENT

planning process, which gives a degree of consistency with the inputs and approaches already adopted 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 that 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 tolerances for outcome in a stress to set risk appetite and cascade it down to risk appetite/ tolerance to individual product/businesses.
- Limits – Stress testing exposures 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 origination strategy.

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 bank’s 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 subsequent 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 subject to governance oversight at every level, beginning with scenario and model validation, to internal controls over data, and finally ending with close communication and review by senior executives and the 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 analyze 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 sequences or development of events which start from one set of assumptions in order to evaluate or may 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 scenarios. These episodes represent severe stress scenarios for many institutions. It is important to select scenarios that appropriately reflect the bank’s business profile of a particular financial institution.

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 a longer period. This type of scenario should be manageable within the normal situation of risks and responsibilities for daily decision. In this scenario, the credit portfolio can be more vigilance 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 scenario for many institutions. It is normally included in regular stress testing exercises and it will significantly 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 the environment.
- Near-Default Stress Scenarios – The global financial crisis that began in late 2008 falls into
5.14 RISK MANAGEMENT

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. Those 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 Scenario (Reverse Stress Test Scenarios) – Some institutions failed during global financial crises, this period represented stress to default scenarios. It involves extremely unlikely events which force the companies to think about their firm’s most serious vulnerabilities and design stress to default scenarios accordingly. Broad organizational involvement is essential when defining appropriate events like failures 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 stress tests as well as event specific tail risk. For example, markets with low historical volatility may experience large dislocation movements; the scenarios 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-year versus multi-period framework. Forward looking stress and stress 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 subject to detecting 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. Improbable issues might be considered and plausible losses might not be discovered.

© The Institute of Chartered Accountants of India

3.4 Basel Committee on Banking Supervision (BCBS) Principles for Sound Stress Testing Practices and 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 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. It is a complementary risk perspective to other risk management tools. It improves capital and liquidity management; enhances internal and external communication.

3. Stress testing programmes should take into account 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 sufficiently robust infrastructure in place. This 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 programmes, 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 the firm-wide level.

8. Stress testing programmes should cover a range of scenarios, including forward-looking scenarios, and be able to take into account systemic risks and feedback effects.

9. Stress tests should feature a range of scenarios, 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 stability 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 or exposure valuation.

© The Institute of Chartered Accountants of India

4. COUNTRY RISK

Country Risk is a broader concept which covers the adverse impact of host country’s economic, financial, and political environment. This risk is most important in cases of Multinationals National Corporations (MNCs) which establish 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 creditors who invest their money through PPP, 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 decision 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 a 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 foreign currency to local currency.

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

(iv) Tasse, Tax and Regulation Risk: This risk arises out of a sudden or stochastic change in Taxation and Regulations governing the host country. These sudden changes can be in any of the following forms:

- Unpredicted increase in tax rates applicable for MNCs operating in the host country.

- Compulsion to use local workforce.

- Compliance of stricter environmental standards.

- Insufficient 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.

- Reputation of Country: This type of risk arises on account recession of earlier awarded tarnish 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 hampers the reputation of the country severely from investment point of view but it saves a lot of foreign exchange of the Government.

5.18 RISK MANAGEMENT

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

- Ratio of country's Import to its Export
- 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 analysis 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 step comes of selecting most suitable techniques 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.

5.20 RISK MANAGEMENT

4.3.1 Qualitative Tools

This is one of the simplest techniques for country risk assessment because it is easy to use and requires very less technical expertise.

(i) - Numerical 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) - Color Coding: Different colors can be used to indicate the level of country risk. White color indicates higher risk. Green color indicates a risk free zone.
(iii) - Combination of Numerical and Color: 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 grades can be assigned such as A, AA, AA+, AAA by these agencies.
(b) - Gini Coefficient: This is one of the most popular index to gauge the rich-n-poor income countries. It measures inequality in income distribution.
(c) - Freedom in the world: It is one of the most popular index to measure freedom in the world.
(d) - Corruption Index: This index is published by Transparency International.
(e) - Human Development Index: This index is published by United Nations.
(f) - Global Peace Index: This index is published by Vision of Humanity.
(g) - Political Culture: This survey is conducted by Freedom House.
(h) - Life Expectancy and Standard of Living: These are some indices that can be used for Country Risk Analysis.

5.19 RISK MODEL

# 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

6. Credit Risk Measurement and Management

LEARNING OUTCOMES

- 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 partly 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 in part or 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. The 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 withdrawal 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 is also known as counterparty risk.

Hence, credit risk can be defined as refusal or inability of credit customer to pay the owed sum partly or in full or in time.

CREDIT RISK MEASUREMENT AND MANAGEMENT

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 an intermediary between provider of funds and seeker of funds.

Bank accepts deposits from one group and provides funds to another 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.

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 refusal for refund of advance before due date. In some cases, say for amortized credit such risks does not exist as period of receipt of credit is known with greater certainty. Due to uncertainty generally of balance sheet items create such risks. However, in such cases, the exposure is not associated with credit’s behavior rather their position in 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 mitigated through Collateral and Third Party Guarantee. However, evidence of these two risk management tools also carries risk.

(c) Collateral Risk: Although collateral reduces the credit risk but it happens only if collateral is sold at a significant value.

(b) Third Party Guarantee Risk: If there is no collateral in such cases then third party guarantee is used.

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

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

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

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:

\[ \text{D X A X (1 – r)} \]

\[ D = \text{Default %} \]
\[ A = \text{Amount of Exposure} \]
\[ R = \text{Recovery Rate %} \]

This formula 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:

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

(i) Concentration of credit in particular geographical locations or business segments.
(ii) Excessive lending to particular industry in order to fulfill its requirements.
(iii) Ignoring the purpose for which loan was sought by the customer.
(iv) Poor Quality or Liberal Credit Approval while granting the loan.
(v) Absence of efficient recovery mechanism.

(b) External Factors: These factors are external to the bank and beyond its control. These factors not only impact the profitability of bank but also affects its repayment capability. Some of such external factors are as follows:

(a) Fluctuation in exchange rates.
(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 to loan to an individual or company / corporate depending on the purpose of taking the loan / use. The tenure 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, credit cards, credit cards, small equipment loans like term loans, commercial vehicle loan etc. This is usually called as the BCL 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:

1.4 Fund Based Facilities

Fund based facilities are those where the borrower gets the money 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
RISK MANAGEMENT

6.6 RISK MANAGEMENT

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 corporations are discouraged
from accumulating too much of debt to be repaid from the sales 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
• Method 2 – MPBF = 75% of (Current Assets – Current Liabilities other than bank borrowings)
• Method 3 – MPBF = 70% of (Current Assets – Core Current Assets) – Current Liabilities other
than bank borrowings. The borrower should contribute 100% core current assets and 25% of
total current assets from long term sources. A minimum current ratio under this method
works out to be 1.5:1.

Various types of working capital loans include Bank Overdraft, Cash Credit, Factoring etc.
(i) Overdraft – 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 has a time 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 lending 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

CREDIT RISK MEASUREMENT AND MANAGEMENT

6.7 CREDIT RISK MEASUREMENT AND MANAGEMENT

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.

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 consideration on behalf of their clients. The fund position of the lending bank
remains intact. Types of non fund facilities are as follows:
(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 the case, the
importer applies to the bank (issuing bank) in his country to open a letter of credit in favour of
exporter whereby the importer’s bank undertakes to pay the exporter on fulfilling the terms
and conditions specified in the letter of credit.

6.8 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, classifies 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

© The Institute of Chartered Accountants of India

© The Institute of Chartered Accountants of India

© The Institute of Chartered Accountants of India

© The Institute of Chartered Accountants of India

© The Institute of Chartered Accountants of India
When a lender is convinced to provide a line of credit to the customer, it is his 6.13)
6.12 RISK MANAGEMENT

- Debt securities issued by banks, local authorities and certain other entities which meet the requirements as prescribed by Basel II.
- Bonds of various types, including those issued by governments, agencies and other entities.

© The Institute of Chartered Accountants of India

As Basel II norms, following are the different types of funded credit risk mitigation methods:
- Guarantee: A third party guarantees the performance of the borrower.
- Surety: A third party agrees to pay the principal and interest if the borrower defaults.
- Endorsement: The bank endorses a note or document, guaranteeing its collectability.
- Insurance: The bank obtains insurance to cover the risk of default.

7. How Credit risk is Mitigated

Apart from this major risk other minor risks such as foreign exchange risk, inter-bank transactions, letter of credit, derivative transactions like futures, options, swaps and forwards. Financial institutions also need to address the following issues: Magnitude of risk arising from long-term complex structures, Geographical spread of the operations of above organizations, and borrowing pattern of large organizations. The historical method of risk identification involves the identification of types of risk, 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 known situations. This helps the institutions to test, develop their own methodology to stress them.

7.2 Identification of Credit Risks

Identifying the credit risk at the first step in credit 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, broadly, may help 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, and other facilities. Herein, it is necessary to study the borrower's profile to understand the nature and capacity.

As per Basel II norms, following are the different types of funded credit risk mitigation methods:
- On Balance Sheet Noting: On balance sheet noting of mutual claims on the balance sheet, the counterparty creates effective security and collaterals. This norm accordingly be recognized 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 process.
- Collateral: Collateral such as accounts that are secured or depend on bank’s agreement of any loan advances, debt or credit lines. The types of collateral are:
  - Cash or cash equivalents – Cash or credit lines
  - Stock Pledging
  - Gold Pledging

CREDIT RISK MEASUREMENT AND MANAGEMENT

Apart from this major risk other minor risks such as foreign exchange risk, inter-bank transactions, letter of credit, derivative transactions like futures, options, swaps and forwards. Financial institutions also need to address the following issues: Magnitude of risk arising from long-term complex structures, Geographical spread of the operations of above organizations, and borrowing pattern of large organizations. The historical method of risk identification involves the identification of types of risk, 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 known situations. This helps the institutions to test, develop their own methodology to stress them.

7.2 Identification of Credit Risks

Identifying the credit risk at 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, broadly, may help 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, and other facilities. Herein, it is necessary to study the borrower's profile to understand the nature and capacity.

As per Basel II norms, following are the different types of funded credit risk mitigation methods:
- On Balance Sheet Noting: On balance sheet noting of mutual claims on the balance sheet, the counterparty creates effective security and collaterals. This norm accordingly be recognized 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 process.
- Collateral: Collateral such as accounts that are secured or depend on bank’s agreement of any loan advances, debt or credit lines. The types of collateral are:
  - Cash or cash equivalents – Cash or credit lines
  - Stock Pledging
  - Gold Pledging

CREDIT RISK MEASUREMENT AND MANAGEMENT

Apart from this major risk other minor risks such as foreign exchange risk, inter-bank transactions, letter of credit, derivative transactions like futures, options, swaps and forwards. Financial institutions also need to address the following issues: Magnitude of risk arising from long-term complex structures, Geographical spread of the operations of above organizations, and borrowing pattern of large organizations. The historical method of risk identification involves the identification of types of risk, 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 known situations. This helps the institutions to test, develop their own methodology to stress them.

7.2 Identification of Credit Risks

Identifying the credit risk at 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, broadly, may help 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, and other facilities. Herein, it is necessary to study the borrower's profile to understand the nature and capacity.

As per Basel II norms, following are the different types of funded credit risk mitigation methods:
- On Balance Sheet Noting: On balance sheet noting of mutual claims on the balance sheet, the counterparty creates effective security and collaterals. This norm accordingly be recognized 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 process.
- Collateral: Collateral such as accounts that are secured or depend on bank’s agreement of any loan advances, debt or credit lines. The types of collateral are:
  - Cash or cash equivalents – Cash or credit lines
  - Stock Pledging
  - Gold Pledging
6.14 RISK MANAGEMENT

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 bank / FIs.

(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 promissory / borrower money invested in the business and an indication 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 – It is the obligation that the borrower feels to repay the loan. Emphasis is given on the past 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 financial, ratio and cash flows.

For wholesale loans, the detailed appraisal would also take into consideration 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 capacity;
- Credit reference from the existing lenders/banks;
- Credit reference checks from credit bureaus;
- Cash flows from the project and its adequacy;
- Nature of Security and its enforceability;
- Credit rating ratemaking of rated by any external agency;
- Whether name of any of the directors of the borrower appear in the list of defaulters by use of reference to DIPRA. In case of any dubiety 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 this 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 visit;

Risk identification, risk allocation and risk mitigation;

Security requirements including adequacy and enforceability;

6.16 RISK MANAGEMENT

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 / appraisal formulae are specified for different customer segments like small & mid corporate, large corporate, project finance etc.

For wholesale credits, the detailed appraisal would also take into 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/banks;
- Credit reference checks from credit bureaus;
- Cash flows from the project and its adequacy;
- Nature of Security and its enforceability;
- Credit rating ratemaking of rated by any external agency;
- Whether name of any of the directors of the borrower appear in the list of defaulters by use of reference to DIPRA. In case of any dubiety 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 this 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 visit;

Risk identification, risk allocation and risk mitigation;

Security requirements including adequacy and enforceability;

6.17 CREDIT RISK MEASUREMENT AND MANAGEMENT

8. 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)
- Brickwork Rating India Private Limited (Brickwork)
- CARE Credit Analysis and Research Ltd (CARE)
- Brickwork Rating India Private Limited (Brickwork)

Rating Scale for Long term instruments is as follows:

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
<th>Instruments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA (Highest)</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>AA (High)</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>A (Average)</td>
<td>Instruments with this rating are considered to have adequate degree of safety regarding timely servicing of financial obligations. Such instruments carry medium credit risk.</td>
<td></td>
</tr>
<tr>
<td>BBB (Moderate)</td>
<td>Instruments with this rating are considered to have moderate degree of safety regarding timely servicing of financial obligations. Such instruments carry moderate credit risk.</td>
<td></td>
</tr>
</tbody>
</table>
RISK MANAGEMENT

6.18

BB (Moderate Risk)
- Instruments with the rating are considered to have moderate risk of defaulting relative to historical performance of financial obligations.

B (High Risk)
- Instruments with the rating are considered to have high risk of defaulting relative to historical performance of financial obligations.

C (Very High Risk)
- Instruments with the rating are considered to have very high risk of defaulting relative to historical performance of financial obligations.

D (Default)
- Instruments with the rating are in default or are expected to be in default soon.

A1
- Instruments with the rating are considered to have very high degree of safety regarding timely payment of financial obligations. Such instruments carry very low default risk.

A2
- Instruments with the rating are considered to have high degree of safety regarding timely payment of financial obligations. Such instruments carry low default risk.

A3
- Instruments with the rating are considered to have moderate degree of safety regarding timely payment of financial obligations. Such instruments carry medium default risk.

A4
- Instruments with the rating are considered to have high degree of safety regarding timely payment of financial obligations. Such instruments carry very low default risk.

6.20

RISK MANAGEMENT

Before the loan turns non-performing, banks/FIs will be required to identify incipient stress in the account creating a sub - asset category viz. Special Mention Account with three sub-categories as given below:

SMA sub-categories

Basis of classification

SMA – 0
- Principal or interest payment overdue for more than 30 days but account showing signs of incipient stress as illustrated in the annex to the framework as of Jan 30, 2014.

SMA-1
- Principal or interest payment overdue between 31-60 days.

SMA-2
- Principal or interest payment overdue between 61-180 days.

Portfolio risk management emanates from a clearly specified risk appetite of the organization to meet its strategic objectives. Portfolio Risk Management is predominantly driven through “Concentration Risk Management”. Concentration risk in banking terms denotes 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 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 industry on industry / sector / geography.

8.4 Credit Risk Rating Process

Credit Risk Rating or Credit Rating is an important tool to manage large dollar 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 organization 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) DSS/Audit credit enhancements for the particular facility provided by the Borrower, after applying buffer 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.

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 modeling 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 organization expects over an exposure over a certain time period, usually a year
- Unexpected Loss: The loss that the organization incurs over and above the average loss expected from an exposure over a certain time period, usually a year

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 obligation, 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 recovery 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 judgment techniques are used to estimate risk components (PD, LGD, EAD) for both funded and unfunded exposures.
3.22 RISK MANAGEMENT

3.22 Estimation of Loss Given Default

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 default occurs. It provides the loss that a bank is bound to incur when a default occurs. The component of the loss that will be incurred, given the default occurs, is called LGD. Larger values of LGD are Loss of principal. Cyclicing events and Workout expenses

LGD = EAD * LGD

where EAD is the exposure at default and LGD is the percentage loss at default.

CREDIT RISK MEASUREMENT AND MANAGEMENT

6.23 CREDIT RISK MEASUREMENT AND MANAGEMENT

6.23 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 reference loan) in the event of a loan default. The buyer of the CDS makes a payment (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.

Key features of RBI guidelines on CDS

© The Institute of Chartered Accountants of India

© The Institute of Chartered Accountants of India

© The Institute of Chartered Accountants of India

© The Institute of Chartered Accountants of India

CREDIT RISK MEASUREMENT AND MANAGEMENT

6.25 CREDIT RISK MEASUREMENT AND MANAGEMENT

6.25 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 or bankruptcy of Risky Corp in order 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 default 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 annualized protection price per $100,000 bonds and, in exchange, receives a payoff if the loan defaults. It was invented by Blythe Masters from JP Morgan in 1994.

The credit events specified in the CDS contract may cover: Bankruptcy, Failure to pay, Repudiation/moratorium, Obligation acceleration, Obligation default, Restructuring approved (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 contract individually. In order to facilitate documentation, and to avoid disputes as to whether a credit event had actually occurred and how a contract should be settled, CDS counterparties (in the international and US market) generally refer to the International Swaps and Derivatives Association (ISDA) Master Agreement. In India, the RBI guidelines specifically state 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 Guidelines state 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, if further details 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 manipulation.
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, authorising the counterparty to transact.

- 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 report their trades 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 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 prohibited default, insolvency or bankruptcy. The insurance protection 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 the buyer to non-governmental export credit agencies to business entities wishing to protect their accounts receivable from loss due to currency issues, political unrest, expropriation etc.

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. It is represented in terms of financial ratios such as maximum debt-equity ratio, debt to EBIDTA, minimum debt service coverage ratio etc. Banks / FIs periodically review the covenants to ensure the borrower default. RBI has not stipulated any minimum cover for security except for listed political risk insurance which is offered by the same insurers to insure the risk of non-payment by the buyer to non-governmental export credit agencies to business entities wishing to protect their accounts receivable from loss due to currency issues, political unrest, expropriation etc.

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 on the time of sanction and are legally binding. The covenants stipulated could be an indication of 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 the mselves should the borrower default. RBI has not stipulated any minimum cover for security except for listed shares where the cover should be minimum 2. Various types of securities depending upon the nature of facilities are:

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. It is represented in terms of financial ratios such as maximum debt-equity ratio, debt to EBIDTA, minimum debt service coverage ratio etc. Banks / FIs periodically review the covenants to ensure the borrower default. RBI has not stipulated any minimum cover for security except for listed shares where the cover should be minimum 2. Various types of securities depending upon the nature of facilities are:

8.9.1 Stipulation of Covenants

The other differences include:

- The seller is not 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, as it had insufficient reserves to meet the "cost" of unexpected payouts caused by the collapse of the housing bubble);
- Insurance requires the buyer to declare 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 variability 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 unwind.

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: direct control over escrows / cashflows; ring-fencing of cashflows; identified / cash flows carved out for banks loan repayment hence going visibility to the repayment; board representation / voting rights to the lender; priority of repayments over other lenders / creditors; exclusive charge or Put-purchase on the security with other lenders.

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 stream of money should an adverse event occur. However, there are also many differences, the most important being that an insurance contract provides an indemnity against the losses actually suffered by the policyholder 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 or equity.

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 on the time of sanction and are legally binding. The covenants stipulated could be an indication of 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 2. Various types of securities depending upon the nature of facilities are:

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: direct control over escrows / cashflows; ring-fencing of cashflows; identified / cash flows carved out for banks loan repayment hence going visibility to the repayment; board representation / voting rights to the lender; priority of repayments over other lenders / creditors; exclusive charge or Put-purchase on the security with other lenders.

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 stream of money should an adverse event occur. However, there are also many differences, the most important being that an insurance contract provides an indemnity against the losses actually suffered by the policyholder 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 or equity.

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 on the time of sanction and are legally binding. The covenants stipulated could be an indication of 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 2. Various types of securities depending upon the nature of facilities are:
found to be approximately 85%-90% accurate in predicting bankrupcy one year before the event, with a Type II error (false positives) of 15%-20% (Altman, 2000).

From about 1985, the Z-scores gained wide acceptance by auditors, management accountants, banks, and database systems used for loan evaluation (Biddleman). 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’-Scores) and non-publicly trading companies, respectively.

Neither the Altman models nor other balance sheet-based models are recommended for use with financial companies. This is because of the sparsity 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 Market Model), but these have limited predictive value because they rely on market data (fluctuations of shares 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 returns refer to the returns 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 reliable 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 movement of the market 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 termed as the “Jensen index”. Because of the intricacies of large funds and portfolios, as well as the forms of investing in general, comparing alpha values is only partial, 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 a 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, a financial company’s stock has a beta of 1.5, which means that its price is expected to decline 5% in a market downturn, and increase 15% in a market upturn. Beta is an important measure of risk, as it indicates how sensitive an asset’s returns are to movements in the market as a whole.

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 (ranging from 0 to 100%). An R-squared of 100% means that 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 pattern have been in line with the index. A fund with a low R-squared, at 70% or less, indicates the security does not act very 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 likely offering higher risk-adjusted returns.

9.2.1 Return on Risk Adjusted Capital (ROARAC)

The return on risk-adjusted capital (ROARAC) is a rate of return statistic commonly used in financial analysis, where varying projects, investments and opportunities are evaluated based on capital at risk. Projects with different risk profiles are easier to compare to each other once their individual ROARAC values have been calculated.

ROARAC = net income / allocated risk capital

Allocated risk capital is the firm’s capital, adjusted for a maximum potential loss based on estimated future earnings or the volatility of earnings. Companies use ROARAC to place greater emphasis on firm-wide risk management. For example, different corporate divisions with unique managers can use ROARAC to quantify and maintain acceptable risk-exposure levels. With ROARAC, however, the capital is adjusted for risk, not the risk of return. ROARAC is used when the risk varies depending on the capital asset being analyzed.

For example, assume a firm is evaluating two projects (P A & P B) that have engaged in over the previous year and needs to decide which one to eliminate. Project A had total revenues of $150,000 and total expenses of $150,000. The total risk-weighted assets involved in Project A were $400,000. Project B had total revenues of $200,000 and total expenses of $150,000. The total risk-weighted assets involved in Project B were $800,000. The ROARACs are calculated as below:

\[
\text{Project A ROARAC} = \frac{4,00,000}{4,00,000} = 12.5\%
\]

\[
\text{Project B ROARAC} = \frac{2,00,000}{1,000,000} = 2.0\%
\]

Even though Project B had twice as much revenue as Project A, once the risk-weighted capital of the project is taken into account, it is clear that Project A has a better ROARAC.

9.2.2 Economic Capital

Economic capital is the amount of capital that a firm, usually in financial services, needs to ensure 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 risk that it has.

Calculations of economic capital and their use in risk/return ratio reveal which business lines a bank should pursue that maximizes the risk/reward tradeoff. Performance measures that utilize economic capital include return on risk-adjusted capital (ROARAC), risk adjusted return on capital (RAROC) and economic value added (EVA). Business units that perform better in these measures or can reduce the own risk capital in order to optimize. Value-weighted (VW) 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)

The VaR is in statistical techniques 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 investment 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 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 basis yields the probability of a 2% loss at any time per month.
consistent and hence sustainable over the projected period or it's a spurt in one of the business activities. A high gearing ratio is indicative of high debt, which in turn raises the risk of default. To determine the credit score, various credit scoring models are available through the agencies or credit bureaus. Credit score ranges between 300 – 850 points, 850 being the highest credit rating possible. The methods which are used in credit scoring models are based on historical data and include factors such as credit history, payment history, and other financial information. Credit scoring models are vital for the organizations as it is a base to determine the credit management policy.

10. CREDIT SCORING MODELS

10.1 What is a Credit Scoring Model?

As per “Investopedia,” a credit score is a statistical analysis performed by lenders and financial institutions to access a person's creditworthiness. 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 the credit risk of an individual are as follows:

- 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.

- 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 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 based on the market's historical experience and industry norms. Return on equity measures a corporation's profitability by revealing how much profit a company generates with the money shareholders have invested.

9.3.3 Working capital analysis

(a) Account receivable days - Accounts receivable days is the number of days that a customer's invoice is outstanding before it is collected. The point of the measure 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: 
\[
\text{Accounts Receivable Days} = \left( \frac{\text{Accounts Receivable}}{\text{Sales}} \right) \times 365
\]

(b) Inventory days - The inventory turnover ratio is a ratio that measures how effectively inventory is managed by comparing cost of goods sold with average inventory for a period. This measure is used for various times average inventory is “turned” or sold during a period.

Formula: 
\[
\text{Inventory Days} = \left( \frac{\text{Average Inventory}}{\text{Cost of Goods Sold}} \right) \times 365
\]

(c) 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. Ratio = (Operating Income + Interest) / (Interest + Principal).

10.2 Types of Credit Scoring Model

Credit scoring models are mainly used by the credit rating agency to determine the creditworthiness of an individual. The degree of creditworthiness is dictated by the credit scores for each individual. Now a days, many financial institutions are using credit scores to evaluate the potential risk exposure by lending the money to consumers and to mitigate the losses organizations may suffer by the default risk. To determine the credit score versus credit scoring models are available through the agencies or credit bureaus.

In this section, we understand the different models predominantly used across the world. The score is an index of open or closed-ended behavior. The FICO Score is a popular measure of the creditworthiness of a lender's target to. FICO Scores are used in 90% of credit decisions, so they're a very good barometer of how your credit card looks 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 such as age, allowing them to make more informed lending decisions quickly and fairly.
### Evaluation of Risk Associated with Governance

Goverance risks mean significant deficiencies that can impact the reputation, existence and continuity of the organization. These arise on account of failure on 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 are 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 risk, developing corporate responses to risks that manage to address all key dimensions (strategy, people, detail, tasks, and drivers), effectively considering stakeholders’ and gatekeepers’ concerns, and addressing all these issues from an enterprise perspective. These challenges are faced by both financial and non-financial companies.

---

#### Vantage Score

Vantage score are based on the credit rating agencies. Vantage calculates the credit scores based on the three credit rating agencies that are Experian, Equifax and Transunion. As per the latest Vantage Score model the credit scores are being rated between 300 – 850.

This level of credit scores follows similar brackets as that of FICO. However, the rating is based on an A to F alphabet. A being the best and F being the poor.

The credit score range was realigned with new version of Vantage score model due to the credit behaviour as well as change in economy. Accurate results will lead to an 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 consumers 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 mentioned 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 – 850 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

---

#### Experian National Equivalency Score

Experian National Equivalency Score (ENES) is also called as FAKO credit score. This scoring model aims at estimating the credit worthiness of an individual customer. The score range is 380-640. It has been claimed by the Experian, institution who owns the ENES system, that it is quite similar to the FICO scoring model. The basic way of the mathematical calculation is not published by the model owners. But considering the facts that if it’s a replica of FICO model, one cannot expect drastic dissimilarity between these two models.

This 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.

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.

---

### Risk Associated with Corporate Governance

#### Learning Outcomes

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

---

### Risk Management

- The payment history, debt used and nature of credit history.
- An extended line. The PLUS Score range varies from 330 to 850. 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 this segment. This will ensure that the credit score will be ranked based on the percentile.
- For instance, your score may be rated as in the “65th percentile”, the “85th percentile” or the “100th percentile”. This simply means that your score is better than 65%, 85% or 100% of the public, respectively.
- The PLUS Score is an extension of the FICO score. For example, the PLUS Score is not as detailed as the FICO score, but it is still a reliable measure of creditworthiness.
- The FICO score is often used for credit card applications and mortgage applications, while the PLUS Score is typically used for auto loans and personal loans.
RISK MANAGEMENT

7.4

a) conducts periodic reviews of performance of the board and its sub-committees (by the board, management, or any other committee);
b) has a chair who is independent 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 on a by-risk basis;
f) is responsible for overseeing management's effective implementation of a firm-wide risk management framework and policies within the firm;
g) approves the risk appetite framework and ensures it is directly linked to the business strategy, capital plan, financial plan and compensation;
h) has access to any information requested and receives information from its committees at least quarterly;
i) 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 on a by-risk basis;
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;

7.3

2. THE RISK MANAGEMENT FUNCTION

a) It is independent of business lines (i.e., is not involved in revenue generation) and reports to the CRD;

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 continuously improving risk management capability. Undertaking a periodic review to assess the effectiveness of an entity’s risk management framework is essential to ensure that the board’s risk appetite and risk capacity are not exceeded. A sound RMF includes a clear, documented and approved risk appetite statement, criteria for measuring adherence to risk appetite and processes for managing breaches. The risk management framework should be aligned with the risk governance framework and include specific sub-frameworks for each type of risk (e.g., operational, credit, market, liquidity and reputational risk). The board should have a clear understanding of how the RMF is implemented and monitored, and should review the RMF at least annually to ensure its effectiveness in supporting the firm’s strategic and business plans.
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 five 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: (i) 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 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 or 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.

© The Institute of Chartered Accountants of India

3.2 Role of Risk Assessment with respect to Financial Reporting

Risk assessment underlies 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 would 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 controls over financial reporting will fail to prevent or detect a material misstatement caused by fraud usually is higher than the risk of failure to prevent or detect error. This auditor should focus more on or higher emphasis on the areas of highest risk. On the other hand, it is not necessary to test controls that, even if inefficient, 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 (RBA)

The definition of internal audit, as described in the Precepts to the Standards on Internal Audit, issued by the Institute of Chartered Accountants of India, expressly reflects the current thinking as to what is an internal audit: Internal audit is an independent management function, which investigates a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements therein and add value to and strengthen the internal 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 birth to Risk Based Audit Methodologies that are pursued by Auditors.

The business environment is increasingly throwing up newer challenges and opportunities with globalisation; disciplines technologies and risks being continually 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.

© The Institute of Chartered Accountants of India

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 conclusion may be different from the conclusion he would reach if the tests were applied in the same way to all items in the accounting or other population 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 related 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 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 contact of a firm’s audit practice.

© The Institute of Chartered Accountants of India
RISK MANAGEMENT

4. RISK MANAGEMENT DISCLOSURES IN INDIA

4.1 Indian Scenario

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 the charter 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.

4.2 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:

a) Under the heading 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.

b) The board of directors shall ensure that, while tightly encouraging positive thinking, they do not result in over-optimism that either leads to significant risks not being recognised or exposes the listed entity to excessive risk.

c) The board of directors shall have the ability to “step back” to assist executive management by challenging the assumptions underlying strategy, strategic initiatives (such as acquisitions), and critical systems in the key areas of the listed entity’s focus.

d) The listed entity shall lay down procedures to inform members of board of directors about risk assessment and monitoring procedures.

e) The board of directors shall be responsible for framing, implementing and monitoring the risk management plan for the listed entity.

© The Institute of Chartered Accountants of India

General information to shareholders:

Commodity price risk or foreign exchange risk and hedging

Integrated Reporting Framework

Let us study the annual report of Global major operating in the retail sector in 2016; Principal Risk

© The Institute of Chartered Accountants of India

4.3 Risk Management Disclosures – Global Scenario

In the 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 stated 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 roles 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 favorable or unfavorable 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 country 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 2013 concluded, however, “none of the existing guidelines on risk management is adequate for the purpose. Most of the guidelines are extremely high-level, are process-oriented and give scant guidance on how to create an effective risk management and assurance framework.” More recently, COSO published guidelines on risk assessments and on risk appetite (2012), which provides specific guidance on certain issues. In 2015, the International Organization for Standardization (ISO) 31000, has been released.

Enhancing Organisational Reporting: Integrating 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 development to wider goals of financial stability and sustainable development through the cycle of integrated reporting and thinking.

© The Institute of Chartered Accountants of India

4.4 Risk Management Disclosures – Germany

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 interconnectiveness between different reports. IFAC also strongly supports the International Integrated Reporting Council and the implementation of its Framework.

IFAC’s position paper No. 9 addresses reporting that provides decision-useful information to organizational stakeholders beyond 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 (COR) is a key component in the IRF. The details of the IRF as part of the IRP are as under:

a) Key risks impacting ability to create value in short term, medium term and long-term; these could be:
   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) Organization assessment of likelihood that the risk or opportunity will fulfill and probability and certainty of same.

d) Steps taken to mitigate or manage risk or create value from key opportunities including identification of associated strategic objectives, policies, targets and KPIs.

4.5 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

© The Institute of Chartered Accountants of India
### RISK ASSOCIATED WITH CORPORATE GOVERNANCE

#### RISK MANAGEMENT

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**

- Procedural 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

### 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.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Associated principal risks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competitive pressure</td>
<td>Brand, regulation and trust; Competition and markets; Customer</td>
<td>Failure to respond to fierce competition and changes in the retail market; increasing significance of M&amp;A: volume decline in core food categories with no offsetting price inflation, pulling pressure on margins.</td>
</tr>
<tr>
<td>Data security or regulatory breach</td>
<td>Brand, regulation and trust; Data security and data privacy; Political, regulatory, and compliance</td>
<td>A certain data security or regulatory breach results in a significant monetary penalty and a loss of reputation among customers.</td>
</tr>
<tr>
<td>Brexit impact</td>
<td>Competition and markets; Political, regulatory, and compliance</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 highlight the ability to address the viability of the Group. In the case of these scenarios arising, various options are available to the Group to maintain liquidity as to continue in operation such as acquiring new external funding early, more radical short-term cost reduction actions, and reducing capital expenditures. 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 Group will continue in operation and meet its liabilities as they fall due over the three-year period considered.

### 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 ensure 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,
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 external threats are sometimes seen as understandable, what about particular relationships with key customers that are especially at risk? When addressing questions read the road ahead. A small accident 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 specific 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 external risks can lead to overlap and may drag down a system. How well positioned is a company in respect of different 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 necessary. An excessively risk averse culture could prevent progress, but a step change in risk might be unsuitable 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 areas are addressed new ones may emerge. Are risk registers and management reports relating to risk over generalised? 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 overall 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 tools, tasks, technology and other support they need to effectively operate?
- Are the techniques used adequate in the situation and circumstances? How should looking and inclusive does risk management need to be?
- Are the risks of major and critical customers and business partners understood?
- Are business opportunities being identified for helping 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?

© The Institute of Chartered Accountants of India

5.3 Striking the Right Balance in Action and Reaction

Further, whether adequate security, measures to a company's supply chain, corporate data that is held externally and corporate systems that are operated by that party are, how they are working from home, equipment, customer support facilities and portable device? What advice and assistance is given to staff and business partners in these areas?

The management board should also consider and review the effectiveness of International frameworks and standards such as ISO/IEC 27001, ISO 31000, in enterprise risk management, in effective internal control and fraud prevention and mitigation and management of risk.

© The Institute of Chartered Accountants of India

6. OECD GUIDELINES (PRINCIPLES) FOR CORPORATE GOVERNANCE

The Organization for Economic Cooperation and Development (OECD) emphasized the importance of corporate governance and has developed set of principles for better corporate governance. The
RISK ASSOCIATED WITH CORPORATE GOVERNANCE

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 this 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 aligned 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, appointment 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 remedies.

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.

© The Institute of Chartered Accountants of India

RISK MANAGEMENT

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 membership, including their qualifications, the selection process, other company directorships and whether they are regarded as independent by the board.
- Related party transactions.
- Forecastable 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 its shareholders.
- The Board should adopt high ethical standards.
- The Board should review and guide corporate strategy, action plans, management policies and procedures etc.
- The Board should also monitor the company’s performance 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.

© The Institute of Chartered Accountants of India

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 scenarios, uncertainty arising from global events, discipline, competition, and professional agents of cultural mores and volatility of commodity and currency prices creates stress and complexity in managing businesses. Gradually, these events start planning on the means of stakeholders. The occurrence of rare events coupled with their pondering impacts organizational performance. Enterprise Risk Management (ERM) Business Risk Management (BRM) in a structured form assists organizations in preparing for the worst-case scenarios, 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 organizations, also a simplified approach to problem solving and making the organization nimble foiled; iconic entities that feature in the top global rankings currently 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 enunciated as below:

ERM 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 purpose, 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.

Website’s New World Law Dictionary
The process of assessing risk and acting in such a manner, or composing policies and procedures, as to avoid or minimize loss associated with such risk.

With a company-wide scan, 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 strategy to business by identifying events that could have an adverse effect on their organizations and then developing an active plan to mitigate them.

2. IMPLEMENTING ERM

COSO framework states that Enterprise Risk Management (ERM) is a defined as a process, affected by an entity’s board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage 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 risk 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 above risk appetite is considered to be an acceptable risk 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 free for operational purposes in the short term for uncommitted funds meant to pay off the quarterly installment of loans. This could result in delayed payment in due dates 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

ENTERPRISE RISK MANAGEMENT

By implementing ERM in conjunction with other operational elements in the current business environment, companies can also accelerate 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 linkages between the ERM initiative and adherence to capital market reporting disciplines and other corporate laws and regulations.
5. Align annual performance goals with risk identification and management.
6. Encourage and reward upward reporting of business risk opportunities and challenges.
7. Align other risk monitoring initiatives such as self-assessments, internal auditing activities, control assessments, continuous control monitoring, to organizational objectives.
8. Imaging 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 will balance the financial stability of the company.

Among the more widely known frameworks and/or, and the related ERM definitions that they provide 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 financial – that may shake hands with an organization’s operations and objectives. Religiously now 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.

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 devise 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 corporate’s board to address some of the recognized barriers and resistance points to ERM adoption.
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 rating, 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.

5.5.4. 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 natural 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 distracted by unnecessary paper work or issues other than their operations. In this mindset, coordinating activities and problem solving is considered an operational risk 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

5.5.5. RISK Maturity of an Organization

Key Characteristics at Different Levels of Risk Maturity

<table>
<thead>
<tr>
<th>Risk Maturity</th>
<th>Key Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Aware</td>
<td>Strategic risk based approach to risk management.</td>
</tr>
<tr>
<td>Risk Defined</td>
<td>Strategic policy in place and communicated.</td>
</tr>
<tr>
<td>Risk Maturity</td>
<td>Strategic plan approach to risk management development and communicated.</td>
</tr>
<tr>
<td>Risk Manager</td>
<td>Strategic plan approach to risk management development and communicated.</td>
</tr>
<tr>
<td>Risk Aware</td>
<td>Risk identified within functions and not across processes. Also risks not communicated across enterprises.</td>
</tr>
<tr>
<td>Risk Defined</td>
<td>Strategic policy in place and communicated. Risk appetite defined.</td>
</tr>
<tr>
<td>Risk Maturity</td>
<td>Strategic plan approach to risk management development and communicated.</td>
</tr>
</tbody>
</table>

The table given below shows the levels of risk maturity. Key Characteristics at Different Levels of Risk Maturity:

- Risk Maturity
  - Risk Aware: New formal approach developed for risk management.
  - Risk Defined: Strategic approach based risk management. Risks identified within functions and not across processes. Also risks not communicated across enterprises.
  - Risk Maturity: Strategic plan approach to risk management development and communicating.

5.5.5. RISK Maturity of an Organization

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.

RISK MANAGEMENT

Key 2: Building ERM using small but solid steps

Organization 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 single 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.

Focus initially on a smaller, manageable number of key risks that would not 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: Leveraging Existing Resources

Organizations often discover that they can rely on their existing staff, 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 ERM initiatives. In other instances, organizations have appointed a management committee, sometimes headed by their Chief Financial 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.
1. INTRODUCTION

1.2 Why does operational risk originate?

(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.

(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 policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to applicable laws and regulations, the safeguarding of its assets, the prevention and detection of fraud 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.

(c) 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 operational risk management are robust and defensible.
3. OPERATIONAL RISK MANAGEMENT

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 organization depending on the priorities and nature of the environment, it is strongly advisable to have a comprehensive policy documenting the governance mechanism of operational risk.

3.1.1 Operational Risk Management Policy

- Setting up an Operational Risk Management Committee comprising of senior management with an outline of the membership, purpose, 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;
- Reviews of Cyber risk (Information security);
- Reviews of Business Continuity and Disaster Recovery framework;
- Reviews of any development or external events that may impact the operational risk profile of the organization;
- 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 Institute of Chartered Accountants of India
The Operational Risk department, which while being part of the Internal Audit; it is independent of management control and reports to the highest levels of management and set the tone at the top. Examples are Code of Conduct, Risk, Control, Risk grading, Control Owner•

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 formalized in any governance process established by the ORMC Committee.

The Second line of defence is the Operational Risk department, which while being part of the management framework, sets up, oversaw the operational risk management of the first line of defence. The typical roles played by the second line 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 as 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 processes 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 scope.

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 measures.

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 such 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 “default” tier, 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 objectives.

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/individual 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 executed. 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 manipulation 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 facility specifications, technology used in the process or the sub-process, the assembly line, the specific department, 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
Broadly, risk types that often overlap or are caused by operational failures, used commonly are:

- Operational 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. Even with all stipulated laws, there may often be some overlapping areas that may often refer to the same group of potential risk; hence, most organisations use the word statutory risk to refer to violation of laws, 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. 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, to a terminal risk of financial reporting. This may be linked to financial risk in some specific risks, but not always.

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 an inter-related to legal risks, given the chance of disputes between parties, or the unpredictability or enforceability of the agreement due to a poorly defined contract.

- (e) Regulation risk: Risk of the organisation's reputation in public views is a key concern in current age of 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/customer/service provider refusing to do business due to reputational risks are all real risks that a business faces. Quite often, a failed operational transaction leading to a customer displacement 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 perpetrator 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 failure, such as those that allow an employee to deliberately tamper data (on systems or manually) leading to financial misstatement or a typical fraud risk, linked to operational risk (poorly designed process of reporting of data).

- (g) External risk: External risk is 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 does fall under operational issues.

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 based on qualitative and quantitative parameters and keep improving upon it with ongoing learnings with reference to the risk appetite.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial losses</td>
<td>Over 10 lacs (due to any event falling under any loss category)</td>
<td>5 to 10 lacs (due to any event falling under any loss category)</td>
<td>Below 5 lacs (due to any event falling under any loss category)</td>
</tr>
<tr>
<td>Regulatory violation</td>
<td>Design level error, over 1% violation in key regulatory compliance; may lead to regulatory action</td>
<td>Transaction level errors, above 2% and below 5% of transactions</td>
<td>Below 0.5% of transactions; any event falling under a regulatory category</td>
</tr>
<tr>
<td>Significant violation</td>
<td>Major violation in terms of non-compliance of applicable laws, may lead to regulatory violation</td>
<td>Transaction level errors, not leading to serious penalty / withdrawal of licence</td>
<td>Minor errors not leading to statutory penalty etc.</td>
</tr>
<tr>
<td>Operational risk</td>
<td>Failure of firewall may lead to regulatory violation; impact on investor / lender relationships</td>
<td>Loss of data of more than 1% / failure to ensure data confidentiality, leading to regulatory violation</td>
<td>Loss of data of up to 0.2% / minor loss of data</td>
</tr>
<tr>
<td>Cyber risk</td>
<td>Significant event involving regulatory and media attention; Significant violation and loss of data due to regulatory loss</td>
<td>Leader event involving moderate media attention, but no significant impact on financials / non-regulatory</td>
<td>Event with short term impact only</td>
</tr>
</tbody>
</table>

© The Institute of Chartered Accountants of India
RISK MANAGEMENT

9.16 RISK MANAGEMENT

• Low Impact – Low Probability
While the first and third categories tend to get sufficient attention by management, the high impact low probability often escapes the management decision process 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 a risk mitigation plan for them is very difficult. However, whatever possible the management must consider them on an evolving basis.
While it is easier for an operational risk practitioner to work for the buck, it is often enhanced by introducing an additional layer of Medium Probability and Medium Impact, depending on the organisation’s view on risk pacing.

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 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, lower the residual risk. Lower the control effectiveness, the residual risk would be same or similar to level of inherent risk. We shall discuss 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 type 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 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 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, verify that all documents are correct, 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) Reconciliation: 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 suppliers / 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 be 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 wherein an individual holding a key has to operate it first, and additionally the manager would use a different key in his presence 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 accept or reject it. Sometimes this is also classified as Authorisation if the authorisation is given by an authority superior to the one originating the transaction. Often, when the primary control is MIS (Management Information System) each 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 accepted upon by designated individuals. This control type is effective only when the process has already been audited, and hence only deviations are reviewed by authorities. For example, reporting of error rates in an operational process is an exception trigger. On reporting of a high balance in a suspense account beyond the usual acceptable levels can be an exceptional report from.

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 information

OPERATIONAL RISK MANAGEMENT

9.17 OPERATIONAL RISK MANAGEMENT

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) Reconciliation: 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 suppliers / 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 be 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 wherein an individual holding a key has to operate it first, and additionally the manager would use a different key in his presence 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 accept or reject it. Sometimes this is also classified as Authorisation if the authorisation is given by an authority superior to the one originating the transaction. Often, when the primary control is MIS (Management Information System) each 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 accepted upon by designated individuals. This control type is effective only when the process has already been audited, and hence only deviations are reviewed by authorities. For example, reporting of error rates in an operational process is an exception trigger. On reporting of a high balance in a suspense account beyond the usual acceptable levels can be an exceptional report from.

7. TECHNOLOGY RISK

As we see 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 intertwined 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) Unintended system deviation 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 new material. For example, a system failure in a financial lending organisation may lead to critical customer commitment 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 minimised in such
The operational risk manager is expected to have an overview of the specific facilities available in the technology department, to design the organization’s critical needs at times of failure.

(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 key risk in driving controls in an automated controlled environment. For example, in a lending institution, a credit officer or authorized to process operational activities beyond his job role may result in compromise of the segregation of duties that the process is designed for. If, as an outcome, this may have a higher level of access to changing customer data by one modification, while the process may require an authorization which was bypassed due to inadequate access control mechanism. 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 based on their job role. Organizations are required to delay or modify user Coke once employees move out from their roles or the organization itself.

(e) Accounting systems: From an audit and accounting perspective, the most intensive area is the technology platform that is used for accounting. There are obvious operational risks of manipulation in financial reporting if the accounting software is not configured properly. In complex organizations with several types of transactions that have a financial impact are performed in various systems, the lead in front other production systems is very important to check for accuracy across areas they are used in financial reporting. The feeds, if manual have their own risk of incorrect manual processing; in automated feeds, if incorrect data inflows that could lead to financial misstatements. In lending institutions, the loan management systems are different from the main accounting system; huge amount of data, at various frequencies, flows into the accounting system. The linkage of the source system to the correct GLS in the 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 analyzed to find out the source of the technological reason, and any incorrect programming. Exceptions are the data of customers as interest due, principal outstanding, overdrawn 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.
encompassed alone, 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 other technology providers and/or the business process itself to escalate, 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 power cuts or natural disasters;

(c) Human 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 then the area 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:

- Risk material in process being lost or spoil 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 fines;
- Liability to disbursement of losses that causes customer dissatisfaction;
- An in 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 place elsewhere, is in high in case of large scale business process failures.

Hence a Business Continuity Plan (“BCP”) is required to be adopted.

9.2 Functional Recovery Plan (“FRP”)

Here, once the BIA is approved at management level, is detailed plan as to alternate functioning of the selected processes/ sub-processes has to be made. This is by far the most challenging phase since it involves alternate resources, staffing, infrastructure and maybe technology systems as well. Depending on the complexity and nature of services provided by an organisation, each organisation has to decide the steps to be taken.

For example:

- In operations intensive company may decide to use an alternative, smaller hub to processes all key transactions; a customer service center, a company may have an alternative service center if the main one is down due to disruption.
- Roles identified as key in running an FRP in execution, are required to have formal back-ups 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-storages 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 roles who would take it up, the backup is the roles if the primary one is unable to perform in disruptive circumstances; the minimum resources such as telephones, internet, printers or access to internet, internal systems etc. an are indicative list;
- This needs to be documented and circulated, and retained by each employee and/or service provider who is involved in the FRP. Operational risk managers are required to oversee whether the framework is concrete 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, is a domain other than the primary office domain so that the role of others can be taken over in successful execution of FRP.

© The Institute of Chartered Accountants of India

9.24 Risk Management

9.25 OPERATIONAL RISK MANAGEMENT

9.26

9.27

© The Institute of Chartered Accountants of India

9.25

© The Institute of Chartered Accountants of India

9.27

© The Institute of Chartered Accountants of India

9.27

© The Institute of Chartered Accountants of India
### 11. CYBER RISK AND INFORMATION SECURITY CONTROLS

Cyber risk is a vast and complex subject by itself; hence we shall outline some of the key points that are relevant from an operational risk perspective. Information Security and Cyber risk by themselves are studied under specialized courses as CISA by those aspiring for professional certification in information security management domain.

Cyber risk term broadly refers to the risks an organisation is exposed to, due to a situation where its network systems, or its transactions are disrupted, compromised or damaged/broken 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 unauthorized access to the system of the organisation; this can cause customer disputes, class-action, 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 new employer.
- Malicious attack on an organisation that can lead to a complete or partial data loss of customers, accounts and or 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 originating communities demand money, often through illegal channels for release of such data.
- 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; the hapless is 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 after clicking it, the intruder gets access to the victim’s computer system; and, in cases, if accessed 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 perpetrator 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:

- 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 matching 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 decrypt 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 liabilities, losses 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 sectors to be adversely impacted.

It is highly advisable to maintain adequate documentation on technical standards followed and applied 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 required 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 or custodians of data or are part of governance of the system need different kinds 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 accepted 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 and when they happen, quantify them (both in financial and non-financial terms), and work on them short and long term. This is normally followed by an assessment of the controls of the specific process / sub-process in which the event occurred.

<table>
<thead>
<tr>
<th>Event type</th>
<th>Description</th>
<th>Categories (Level 2)</th>
<th>Activity example (Level 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal fraud</td>
<td>Losses due to intentional breach, misappropriation of property, violation of company rules, by an internal employee with an internal party</td>
<td>Unclassified activity</td>
<td>Unauthorised transaction with monetary loss; Transaction not reported/intentionally obfuscating of position intentionally.</td>
</tr>
<tr>
<td>Theft and Fraud</td>
<td>Fraud/Credit fraud, Identity theft, embezzlement, misappropriation of assets, malicious destruction of assets, forgery, smuggling, account impersonation, etc.</td>
<td>Unauthorised access to external party</td>
<td>Theft and Fraud.</td>
</tr>
<tr>
<td>External fraud</td>
<td>Losses due to an intentional breach, misappropriation, violation of law or contractual agreement by an external party</td>
<td>Unauthorised activity</td>
<td>Unauthorised transaction with monetary loss; Transaction not reported/intentionally obfuscating of position intentionally.</td>
</tr>
<tr>
<td>Theft and Fraud</td>
<td>Theft/Credit fraud, forgery, identity theft, embezzlement, etc.</td>
<td>Unauthorised access to external party</td>
<td>Theft and Fraud.</td>
</tr>
</tbody>
</table>
management

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 having an indirect financial impact (like the instance of an KYC due diligence failure, or a process failure not leading to compensation to customers etc.)

From a reporting perspective, it is necessary to examine all Operational risk events, since these are the failure in which the organisation needs to take some remedial action. Only in those cases where indirect financial loss is involved, an operational loss is booked.

© The Institute of Chartered Accountants of India

OPERATIONAL RISK MANAGEMENT

9.33

SYSTEMS SECURITY

Employees

- Identification
  - Compensations, benefits, termination issues
- Organized labor activity

Employee relations

- Compensations, benefits, termination issues
- Organized labor activity

© The Institute of Chartered Accountants of India

OPERATIONAL RISK MANAGEMENT

9.35

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 computations, other industries do not have such guidelines currently.

It is advisable to have on 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 incidentally 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.

© The Institute of Chartered Accountants of India
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. 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.