CHAPTER 1

INTRODUCTION TO RISK

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

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

© The Institute of Chartered Accountants of India

1. INTRODUCTION & DEFINITIONS

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

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

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

1.1 ICAI Guide on Risk Based Internal Auditing

Meaning of Risk

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

In a larger sense, risks are those uncertainties of outcome, whether an opportunity or threat,

© The Institute of Chartered Accountants of India

arising out of actions and events. While looking at them narrowly, risks are those uncertainties which impede the achievement of the objective.

Business Risk

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

All entities exist to provide recognizable benefits for their stakeholders or, in other words to create value for them. Value is created if a stakeholder gets more of something he finds important. Value is created or destroyed by (management) decisions. Decisions entail the recognition of risk and opportunity and require that management considers information about the internal and external environment, deploys scarce resources and recalibrates activities to changing circumstances.

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

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

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

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

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

Take the example of traveling by an aeroplane. For most people, traveling by an aeroplane is an

© The Institute of Chartered Accountants of India

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

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

Examples

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

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

Examples (of more riskier propositions in comparison to above)

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

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

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

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

© The Institute of Chartered Accountants of India

ICAI's Standard of Internal Audit

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

Risk can cause financial disadvantage, for example, additional costs or loss of funds or assets. It can result in damage, loss of value and /or loss of an opportunity to enhance the enterprise operations or activities.

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

SA 315 of ICAI defines Business Risk as

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

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

Source	*Definition of risk*
ISO Guide 73 ISO 31000	Effect of uncertainty on objectives. Note that an effect may be positive, negative, or a deviation from the expected. Also, risk is often described by an event, a change in circumstances or a consequence.
Institute of Risk Management (IRM)	Risk is the combination of the probability of an event and its consequence. Consequences can range from positive to negative.
Institute of Internal Auditors	The uncertainty of an event occurring that could have an impact on the achievement of the objectives. Risk is measured in terms of consequences and likelihood. Risk is defined as the possibility that an event will occur, which will impact an organization's achievement of objectives (The Professional Practices Framework 2004)
Paul Hopkins	Event with the ability to impact (inhibit, enhance or cause doubt about) the mission, strategy, projects, routine operations, objectives, core processes, key dependencies and / or the delivery of stakeholder expectations.
Institute of Chartered Accountants of India, SA 315	Business risk – A risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies.

© The Institute of Chartered Accountants of India

Oxford English Dictionary	(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility.
International Federation of Accountants,1999 :	Uncertain future events which could influence the achievement of the organization's strategic, operational and financial objectives.
CIMA Official Terminology, 2005	Risk is a condition in which there exists a quantifiable dispersion in the possible outcomes from any activity. It can be classified in a number of ways.
Basel II	Operational risk is defined as the risk of loss resulting from inadequate or failed processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.
ICAI – SA 315	A risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies.
COBIT,ISACA	Risk is generally defined as the combination of the probability of an event and its consequence. COBIT 5 - defines IT risk as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.
ICAI Risk Based Internal Audit Guide	Audit risk relates mainly to the internal and external audit efforts to achieve its objectives, i.e., provide effective, timely and efficient assurance to the Board. Audit risk has traditionally been seen strictly as the risk of incorrect audit conclusions. Contemporary views however include big-picture audit risks; specifically, that the internal audit-function is not doing the right things or working in the best ways. Even from internal auditing perspective, an organization with well-established risk management processes decreases audit risk. Where the organization has a formal enterprise-wide risk management program (ERM) in place, the internal auditor would assess it for design adequacy and compliance to decide whether to rely on the risk register and where found reliable then focus on auditing the risk responses to significant risks. By relying on significant risks as determined by management, internal auditing becomes more efficient.

© The Institute of Chartered Accountants of India

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

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

Financial Risks

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

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

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

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

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

© The Institute of Chartered Accountants of India

1.2 Occupational Health & Safety Advisory Services (OHSAS)

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

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

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

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

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

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

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

© The Institute of Chartered Accountants of India

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

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

Studies and research papers on the subject of Emotional Intelligence have revealed that when people are anxious or in a state of emotion, they pay close attention to potential threats in the environment and are highly vigilant so as to preserve themselves and their resources (Eysenck, 1997; Pacheco Unguetti, Acosta, Callejas, & Lupiañez, 2010). This attention to threat and vigilance leads people to avoid risk (Loewenstein et al., 2001).

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

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

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

TABLE 2. Illustrative Corporate Risks

Corporate Functions	*Risk Areas*
Human Resources	Poor morale & talent retention
Sales & Marketing	Poor Customer loyalty & retention

© The Institute of Chartered Accountants of India

Operations	Inability to Digitize/ automate processes
Treasury	Low return on investments
Information Technology	Hacking and unauthorized access
New Product development	Product failure
Treasury	Mismatch in cash flows
Finance & Accounts	Unreliable financial statements

Business risks often vary by industry.

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

1.3 Classification of Business Risk

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

Business Risks: Internal and External

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

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

External risks arise due to events occurring outside the business organisation. Such events are generally beyond the control of the management. Hence, determining the likelihood of the resulting risks cannot be done with accuracy.

External factors giving rise to such risks include:

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

© The Institute of Chartered Accountants of India

Business Risks: Controllable and Non-controllable

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

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

- Recessionary economy.
- New competitor locating nearby.
- New technology.

Each business faces risks that are unique to that business. Businesses should consider these carefully and briefly describe what steps would be taken if an uncontrollable risk actually happens to the business (contingency plan). For example, if the risk of a recession would severely affect the company,

1.4 Risk Categories by COSO

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

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

1.5 Inherent Risk and Residual Risk

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

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

© The Institute of Chartered Accountants of India

1.6 ICAI's Standard of Internal Audit

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

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

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

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

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

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

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

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

Frequency could be indicated as follows:

- **Frequent**: Likely to occur very often and/or continuously.
- **Likely**: Occurs several times over the course of a transformation cycle.

© The Institute of Chartered Accountants of India

- **Occasional**: Occurs sporadically.
- **Seldom**: Remotely possible and would probably occur not more than once in the course of a transformation cycle.
- **Unlikely**: Will probably not occur during the course of a transformation cycle.

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

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

1.7 The ICAI Guide on Risk Based Internal Audit

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

All risks have two attributes, viz.

- Likelihood of risk occurrence.
- Risk consequence.

To facilitate understanding and usability in decision making of risk, comparison helps. To enable comparison a risk score is used. By measuring the two risk attributes a risk score can be derived for that risk. This risk score is meant for comparison between a cut-off point normally the 'risk appetite' or comparing to other risks thereby filtering for 'significant risks'.

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

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

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

- Insignificant (score 1).
- Minor (score 2).

© The Institute of Chartered Accountants of India

- Moderate (score 3).
- Major (score 4).
- Catastrophic (score 5).

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

Risk score for that risk is a numeric multiple of the likelihood of the risk and the risk consequences. As an example the Board may have a risk appetite of 12 and any risk with a score above 12 becomes significant risk and to be included in the audit plan.

2. RISK & UNCERTAINTY

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

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

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

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

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

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

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

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

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

© The Institute of Chartered Accountants of India

In this sense, **one may have uncertainty without risk but not risk without uncertainty**. We can be uncertain about the winner of a contest, but unless we have some personal stake in it, we have no risk. If we bet money on the outcome of the contest, then we have a risk. In both cases there is more than one outcome. The measure of uncertainty refers only to the probabilities assigned to outcomes, while the measure of risk requires both probabilities for outcomes and losses quantified for outcomes.

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

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

Complexity, Volatility, Ambiguity and Uncertainty (VUCA)

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

Complexity

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

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

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

Volatility

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

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

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

© The Institute of Chartered Accountants of India

Ambiguity

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

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

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

Uncertainty

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

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

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

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

3. CLASSIFICATION OF RISKS

3.1 Nature of Risks

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

3.2 Categorisation of Risks

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

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

© The Institute of Chartered Accountants of India

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

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

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

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

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

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

There are certain types of risks that give rise to uncertainty about the outcome of a situation. These can be described as ***control risks*** *and are frequently associated with project management. Uncertainties can be associated with the benefits that the project produces, as well as uncertainty about the delivery of the project on time, within budget and to specification.*

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 important aspect of an organization's governance, management, and operations. Professional accountants can and should play a leading role in helping their organizations achieve an integrated, organization-wide approach to risk management and internal control—which ultimately helps create, enhance, and protect stakeholder value.

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

© The Institute of Chartered Accountants of India

best and longest-established branch of risk management, and much of this text will concentrate on hazard risks. There is a hierarchy of controls that apply to hazard risks and this will be discussed in a later chapter. Hazard risks are associated with a source of potential harm or a situation with the potential to undermine objectives in a negative way. Hazard risks are the most common risks associated with organizational risk management, including occupational health and safety programmes.

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

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

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

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

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

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

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

Example

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

© The Institute of Chartered Accountants of India

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

4. TYPE OF RISKS

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

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

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

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

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

© The Institute of Chartered Accountants of India

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

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

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

  Liquidity risk may arise due to changes or variations in the market conditions such as, volatility of rate of interest or the Foreign exchange rate /Investment mismatch or risk or poor economic conditions like depression / inflation / loss of confidence in the business by its customers/ rumors about the business and its effects of run on the liquidity/ failure of some of the banks where its deposits got struck or blocked or war like situations with the enemies of state are some of the examples where the businesses will be facing liquidity crisis as it may cause heavy out flow of funds.
- **Market risk** - the risk of losses caused by adverse changes in the market variables such as interest rate, Foreign Exchange rate, equity price and commodity price. RBI has defined the Market Risk as the possibility of loss to a bank caused by the changes in market rates / prices. Market risk is the possibility for an investor to experience losses due to factors that affect the overall performance of the financial markets in which he has invested money. Market risk, also

© The Institute of Chartered Accountants of India

called "systematic risk," cannot be eliminated through diversification, though it can be hedged against. Sources of market risk include recessions, political turmoil, and changes in interest rates, natural disasters and terrorist attacks.

- **Operational Risk**- risk associated with the operations of an organization. It is the risk of loss resulting from failure of people employed in the organization, internal process, systems or external factors acting upon it to the detriment of the organization. It includes Legal Risk and excludes strategic and Reputational Risks as they are not quantifiable.
- **Strategic Risk** - the current and prospective impact on earnings, capital, reputation or good standing of an organization arising from its poor business decisions, improper implementation of decisions or lack of response to industry, economic or technological changes. Failure of strategies will adversely impact the business objectives and attainment of the goals.
- **Compliance Risk** – It includes material financial loss or loss of reputation which may occur as result of its failure to comply with the laws includes, regulations, rules, related self-regulatory organization, standards and code of conduct applicable to its business activities.
- **Regulatory Risk** - Regulatory Risk arises due to changes made in policies and procedures by the regulators viz, RBI, Central and State Governments, SEBI, IRDA, etc. Withdrawal of licenses, change in capital adequacy requirements, change in NPA norms etc. may be grouped under this category. Any changes in the rules and regulations which may have a negative impact on the business activities can be classified under this risk.
- **Reputation risk** – adverse publicity regarding an entity's practices will lead to a loss of revenue or litigation. Any event which affects the name or brand image of the entity is Reputational Risk. Any adverse publicity, news coverage, comments etc. has the ability to dent the trust created by the entity and becomes detrimental to the business of the entity.
- **Legal risk** - arises from the uncertainty due to legal actions or uncertainty in the application, interpretation of contracts, laws or regulations. Legal risk is the risk arising from failure to comply with statutory or legal requirements.
- **Interest rate risk** - risk where changes in the market interest rates might adversely affect the Net interest Income earnings. It is the threat that interest paid may be more than the interest collected resulting in financial loss.
- **Foreign exchange risk**- risk of loss that the entity may suffer on account of adverse fluctuations in the exchange rate movements in currencies.
- **Management risk** – risk of management interference in day to day operations and putting undue demands and restrictions on staff. Quality of senior management affects the decision making and contributes to management risk. It means the risks associated with ineffective, destructive or underperforming management, which hurts shareholders and the company or fund being managed. This term refers to the risk of the situation in which the company and shareholders would have been better off without the choices made by management.

© The Institute of Chartered Accountants of India

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

© The Institute of Chartered Accountants of India

- Electrical hazards like frayed cords, missing ground pins, improper wiring.
- Confined spaces.
- Machinery-related hazards (lockout/tag out, boiler safety, forklifts, etc.).

Significant Risk

Significant risk is a term used by auditors where in their assessment the risk is significant enough to include it in the audit plan. Usually these risks in their inherent state have a risk score higher than the risk appetite for that risk.

Entity Risk Assessment and Business Process Risk Assessment

Entity risk is the assessment of strategic risks. Organizational objectives and strategies are delivered through business processes; hence business process risk assessment is the preferred way to carry out the exercise.

Indirect Risks to Business

People and organisations often make the mistake of overlooking things that don't directly impact their business and are therefore unprepared to deal with change. For example, while your business might not be directly affected by a natural disaster, you may still suffer if it affects your suppliers, customers or general location.

Consider how these scenarios could affect business:

- If your suppliers are affected, you may run out of the products you sell, or the materials you need to make products.
- If your customers are personally affected their priorities may change and you could experience a reduced demand for your products or services.
- If your general location is affected, you and your customers may not be able to access your premises, or your utilities could be affected.
- For example, you could lose power, which could mean you:
  - will not be able to operate your business;
  - may need to throw out any perishable goods and replace them, which can be costly.

© The Institute of Chartered Accountants of India