Referencer for Quick Revision

Final Course Paper-6A: Risk Management

A compendium of subject-wise capsules published in the monthly journal "The Chartered Accountant Student"

Board of Studies
(Academic)
ICAI

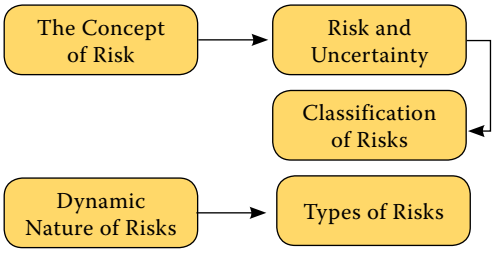
INDEX

RISK MANAGEMENT: A CAPSULE FOR QUICK REVISION

The subject "Risk Management" basically involves applying the knowledge and techniques of Risk Management to identify, measure, assess, quantify, monitor and mitigate risks in an organization. So, the Risk Management is basically a continuous process to keep identifying the risk inherent in an organization, monitoring it and taking steps to treat and mitigate it, wherever required. In this regard, an attempt has been made to convey the concepts of Risk Management to the students in a lucid and simple manner in the form of capsules.

CHAPTER 1: INTRODUCTION TO RISK

Chapter Overview



Introduction

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.

ICAI Guide on Risk Based Internal Auditing

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

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

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

ICAI's Standard of Internal Audit - Enterprise Risk Management defines Risk as 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.

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.

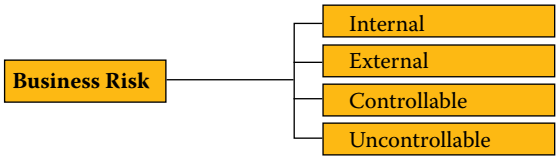
Occupational Health & Safety Advisory Services (OHSAS)

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.

Illustrative Corporate Risks

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

Classification of Business Risk



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 the management significantly.

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.

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.

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, and new technology.

ICAI's Standard of Internal Audit

Risk may be broadly classified into Strategic, Operational, Financial and Knowledge.

Strategic Risks	They are associated with the primary long-term purpose, objectives and direction of the business.
Operational Risks	They are associated with the on-going, day-to-day operations of the enterprise.
Financial Risks	They 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	They are associated with the management and protection of knowledge and information within the enterprise.

Open Group Standard

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

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

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

Frequency could be indicated as follows:

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

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.

The ICAI Guide on Risk Based Internal Audit

All risks have two attributes, viz.

- Likelihood of risk occurrence.
- Risk consequence.

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

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

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

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

Difference between Risk & Uncertainty

Uncertainty	Risk
The lack of complete certainty, that is, the existence of more than one possibility. The "true" outcome/state/result/value is not known.	A state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome.
Measurement of uncertainty: A set of probabilities assigned to a set of possibilities.	**Measurement of risk:** A set of possibilities each with quantified probabilities and quantified losses.
Example: "There is a 60% chance this market will double in five years".	**Example:** "There is a 40% chance the proposed oil well will be dry with a loss of $12 million in exploratory drilling costs".

Complexity, Volatility, Ambiguity and Uncertainty

Complexity

- **Characteristics:** The situation has many interconnected parts and variables. Some information is available or can be predicted, but the volume or nature of it can be overwhelming to process.
- **Example:** you are doing business in many countries, all with unique regulatory environments, tariffs, and cultural values.
- **Approach:** Restructure, bring on or develop specialists, and build up resources adequate to address the complexity.

Volatility

- **Characteristics:** The challenge is unexpected or unstable and may be of unknown duration, but it's not necessarily hard to understand; knowledge about it is often available.
- **Example:** Prices fluctuate after a natural disaster takes a supplier off-line.
- **Approach:** Build in slack and devote resources to preparedness-for instances, stockpile inventory or overbuy talent. These steps are typically expensive; your investment should match the risk.

Ambiguity

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

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

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

Uncertainty

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

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

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

Categorization of Risks

Pure Risks are associated with uncertainties which may cause loss. In a pure risk situation, a loss occurs or no loss occurs – there is no possibility for gain. These uncertainties may be due to perils such as fire, floods, etc. or may arise from human action such as theft, accident etc.

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.

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.

Internal and External factors of Risks

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

Type of Risks- Illustrative

- **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** - 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.
- **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.
- **Operational Risk**- The risk associated with the operations of an organization. It is the risk of loss resulting from failure of people employed in the organization, internal process, systems or external factors acting upon it to the detriment of the organization.
- **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 a 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.
- **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 Reputation Risk.
- **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.
- **Management risk** – It means the risks associated with ineffective, destructive or underperforming management, which hurts shareholders and the company or fund being managed.
- **Foreign exchange risk** – Risk of loss that the entity may suffer on account of adverse fluctuations in the exchange rate movements in currencies.
- **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.
- **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 out-dated 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.

- **Country risk** – Helps to address the issues of identifying, measuring, monitoring and controlling country exposure risks.
- **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. Also, security arrangements risk means risk which arises from vulnerability of security systems.
- **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 the other. They include unsafe conditions that can cause injury, illness and death.

CHAPTER 2: SOURCE AND EVALUATION OF RISKS

Chapter Overview

Identification and Sources of Risks → 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

Identification and Sources of Risk

Risk Identification

Meaning – It is the action or process of identifying some potential internal or external event, or threat or vulnerability or a fact that could cause damage to the entity or prevent it from achieving its objectives.

Inclusion - It includes documenting the potential risks in the form of a risk questionnaire or risk register and communicating the risks to the executive management.

Effectiveness - 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. Further, the risk management team should undertake a Strength, Weakness, Opportunity and Threat assessment exercise so as to document the factors that could give rise to potential risks in future.

Participants in the Risk Identification Process

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

Business Functions Assessment from Risk Perspective

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

Strategic – These include business model risk factors in terms of product demand factors, availability of supply chain inputs at competitive rates, innovation, competition, financial stability and capital access, etc.

↕

Operational – These include process execution and day-to-day issues that the entity is exposed to.

↕

Financial – These concern the effective management and control of the finances of the organization and the effects of external factors such as availability of credit, working capital, foreign exchange rates, interest rate movement and other market exposures.

↕

Knowledge management – Factors contributing to knowledge risks include the unauthorised use or abuse of intellectual property/competitive technology. Internal factors may include loss of key staff.

↕

Compliance management – To manage compliances effectively entities undertake a detailed compliance risk assessment exercise wherein each applicable law is mapped for specific compliance obligation and the mitigating compliance action plan against it is documented.

Quantification of Risk and Various Methodologies

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

Risk Measurement
Once risks have been identified, they are assessed and measured in order to determine their probability of occurrence, costs, opportunity, social and eventual impact on the entity's profitability and capital.

Risk quantification
The process of evaluating and defining the cost and benefits associated with the risk consequences.

Qualitative Risk Assessment

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

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

Risk Impact Matrix

Impact			
	Grid I High impact & low probability; may be reviewed every quater	**Grid II** High impact & medium probability; needs qurterty review with real time monitoring	**Grid III** High impact & high probability; needs quarterly review with online monitoring
	Grid IV Medium impact & low probability; may be reviewed every six months	**Grid V** Medium impact & medium probability; may be reviewed every six months	**Grid VI** Medium impact & high probability; may be reviewed every quater
	Grid VII Low impact & low probability; may be reviewed annually	**Grid VIII** Low impact & medium probability; may be reviewed annually	**Grid IX** Low impact & high probability; may be reviewed every six months

Likelihood (probability)

Tools and Techniques for Risk Quantification

Judgment and intuition
In many situations, the management and auditors have to use their judgment and intuition for risk assessment.

The Delphi approach
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.

Scoring
First the risks in the business, system and their respective exposures are listed, and weights assigned then product of the risk weight with the exposure weight of every characteristic is computed. The sum of these weighted score gives us the risk and exposure score of the system. System risk is then ranked according to the scores obtained.

Quantitative techniques
These techniques involve the calculation of an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs.

Qualitative techniques
These techniques are most widely used approaches to risk analysis. Probability data is not required and only estimated potential loss is used.

Expected monetary value
It is the product of two numbers Risk event probability--an estimate of the probability that a given risk event will occur and Risk event value--an estimate of the gain or loss that will be incurred if the risk event does occur.

Simulation
Simulation ties together sensitivities and probability distributions.

Decision Tree
It is a diagram that depicts key interactions among decisions and associated chance events as they are understood by the decision maker.

Expert Judgement
It can often be applied in lieu of or in addition to the mathematical techniques described above.

Frequency of Loss
It measures the number of times losses occur during a particular period of time.

Scenario Analysis
It is extension of Sensitivity Analysis where only one variable at a time is analyzed. Here, we could see the combined effects of changes in more than one variable.

Risk Identification and Assessment Approaches

Some of the important techniques of risk identification are detailed hereunder:

Analysis of processes

Under this technique, material or significant business processes are flow charted.

Brainstorming

Under brainstorming a group of employees put forward their ideas or sensation of risk.

Questionnaires & Interviews

Focused on detecting the concerns of staff with respect to the risks or threats that they perceive in their operating environment.

Checklists

These are information aids to reduce the likelihood of failures from potential hazards, risks or controls that have been developed usually from past experience, either as a result of a previous risk assessment or as a result of past failures or incidents or history or industry learning.

"What-if" Technique (WIFT)

This is a structured, team exercise, where the expert facilitator utilizes a set of "indicators" or "hints" to stimulate participants to identify risks.

Fault Tree Analysis (FTA)

This method is similar to a form of creative thinking called reverse brainstorming. This technique is used for identifying and analyzing factors that can contribute to a specified undesired event (called the "top event").

Bow Tie Analysis

Bow tie analysis is a diagrammatic way of describing, linking and analyzing the pathways of a risk from causes to effects/ consequences.

Direct Observations

This relatively simple technique and is used daily in the workplace by staff who may observe risky situations and hazards regularly.

Incident Analysis

Recording incidents (that has already happened) in a register, conducting root cause analysis and periodically running some trend analysis reports to analyze incidents, which can potentially enable identification of new risks.

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.

Workshops

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

Comparison with other organizations

The technique used for comparing one's own organization with the competitors.

Stakeholder analysis

It includes the process of identifying individuals or groups who have a vested interest in the objectives. It also involves engaging them to better understand the objective and its associated uncertainties.

Working groups

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

Corporate knowledge

History of risks provides insight into future threats or opportunities through: -

- Experiential knowledge
- Documented knowledge
- Lessons learned

Risk Treatment Options

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

Impact of Business Risk

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

Classification of Risks on the basis of impacts

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

Analyzing the Level of Risk

To analyze risks, we need to work out the likelihood of its happening (frequency or probability) and the consequences it would have (the impact) of the risks that are identified.

A risk analysis can be presented in the form of a matrix as follows:

Likelihood scale

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

Consequences scale

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

Once the level of risks are completed, we then need to create a risk rating table by multiplying Likelihood Scale with the Consequences Scale to evaluate the risk for making a decision about its severity and ways to manage it.

Risk rating table

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

Identify and Assess the Impact upon the Stakeholders Involved in Business Risk

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

Principles For Effective Implementation of Risk Management Recommended By OECD

Risk managers were often separated from management and not regarded as an essential part of implementing the company's strategy. Most important of all, boards were in a number of cases ignorant of the risk facing the company.

↓

The aim is to ensure that risks are understood, managed and, when appropriate, communicated.

↓

Effective implementation of risk management requires an enterprise-wide approach rather than treating each business unit individually.

↓

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

↓

To assist the board in its work, it should also be considered good practice that risk management and control functions be independent of profit centers and the "chief risk officer" or equivalent should report directly to the board of directors along the lines.

↓

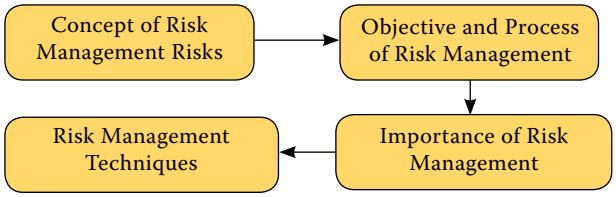
The process of risk management and the results of risk assessments should be appropriately disclosed.

↓

Corporate governance standard setters should be encouraged to include or improve references to risk management in order to raise awareness and improve implementation.

CHAPTER 3: RISK MANAGEMENT

Chapter Overview



Concept of Risk Management

Source	Views
Warren Buffet	Risk comes from not knowing what you are doing.
Theodore Roosevelt	Risk management is about people and processes and not about models and technology.
The Risk Management Standard, The Institute of Risk Management	Risk management is a central part of any organization's strategic management. It is the process whereby organizations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.
Thomas S. Coleman, Practical Guide Risk Management, CFA Institute	Risk management is the art of using lessons from the past to mitigate misfortune and exploit future opportunities—in other words, the art of avoiding the stupid mistakes of yesterday while recognizing that nature can always create new ways for things to go wrong.

Risk Attitude, Appetite, and Tolerance

Risk Attitude – It depends upon one's temperament such as whether a particular individual or an organization is risk-averse, risk-neutral, or risk-seeking.

Risk tolerance – Means how much risk an organization can tolerate or willing to withstand.

Risk appetite – The risk taking capacity and looks at how much risk one is willing to take.

Risks Appetite – Principles and Approach

Risk appetite can be complex

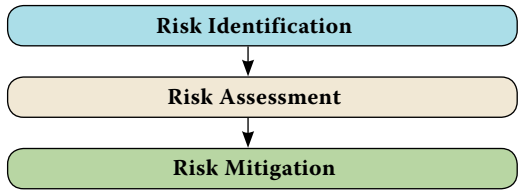
Risk appetite needs to be measurable

Risk appetite is not a single, fixed concept

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 appetite must be integrated with the control culture of the organization

Objectives of risk management



Step by Step Process of Risk Management

Steps	Action	Principles
Step 1: Identify the Risk	Uncovering, recognizing and describing risks that might affect your project or its outcomes.	Risk identification – What can go wrong?
Step 2: Analyze the risk.	Determining the likelihood and consequence of each risk.	Risk analysis – How will it affect us?
Step 3: Evaluate or Rank the Risk.	Evaluating or ranking the risk by determining the risk magnitude, which is the combination of likelihood and consequence.	Risk control – What should we do?
Step 4: Treat the Risk.	Minimizing the probability of the negative risks as well as enhancing the opportunities by creating risk mitigation strategies, preventive plans and contingency plans.	Risk treatment – If something does happen, how will you pay for it?
Step 5: Monitor and Review the risk.	Reviewing the Risk Register and use it to monitor, track and update risks.	Risk Monitoring – How can we continuously look at foresight and hindsight?

Risk Management Techniques

Tolerate: The exposure may be tolerable without any further action being taken.

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

Terminate: Some risks can only be treatable, or containable to acceptable levels, by terminating the activity itself.

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