CHAPTER 2

SOURCE AND EVALUATION OF RISKS

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

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

1. IDENTIFICATION AND SOURCES OF RISKS

Newly Added

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. QUANTIFICATION OF RISK AND VARIOUS METHODOLOGIES

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

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

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

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

Nov 18
May 18
MTP
MCQ

2.1 Qualitative Risk Assessment

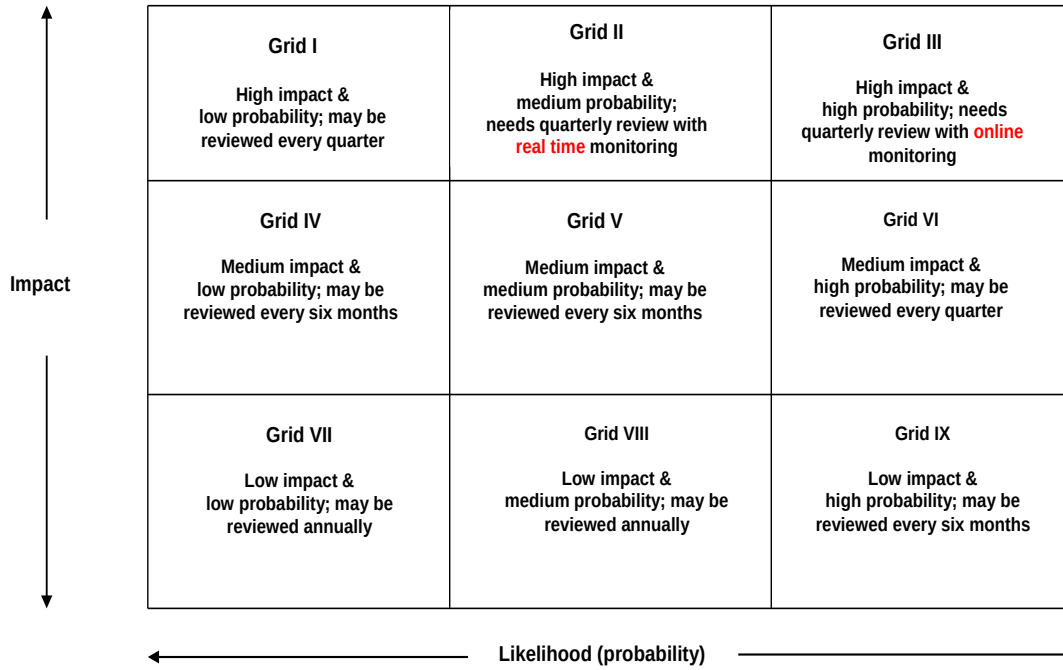
Nov 18 MTP MCQ

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

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

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

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



2.2 Quantitative Risk Assessment

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

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

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

Example Decision Tree

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

Chance of good weather: 40%

Chance of bad weather: 60%

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

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

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

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

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

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

= 0.28 + 0.18

=0.46

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

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

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

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

2.3 Tools and Techniques for Risk Quantification

Important

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

May 19 MTP MCQ

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

ICAI Case study 2 MCQ + May 18 Exam MCQ +Nov 18 MTP MCQ + Nov 19 MTP MCQ CS -5

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.4 Other Business Risk Measurements

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

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

2.5 Outputs from Risk Quantification

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

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

Nov 18 MTP MCQ

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

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

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

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

ICAI Case Study 2

3. RISK IDENTIFICATION AND ASSESSMENT APPROACHES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

See next page

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

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

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

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

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

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

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

May 20 MTP 1 MCQ

The purpose of a risk evaluation is to:

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

3.1 Sources for Identification of Risks

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

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

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

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

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

A brief list is set out below:-

Sources of Risk

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

Nov 2020 MTP Q.3.8

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

Example - SWOT

Strengths-

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

Weakness-

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

Opportunities-

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

Threats-

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

Exhibit

A GENERIC RISK SOURCES MATRIX

Governance	*Finance*	*Operational*	*Preparedness*	*Integrity*
Authority	Funding	Quality	Morale	Management fraud
Leadership	Financial instruments	Customer service	Workplace environment	Employee fraud
Performance	Financial reporting	Pricing	Confidentiality	Illegal acts
Corporate direction and strategy	Foreign exchange/currency	Obsolescence	Communication flow	Unauthorized use
Incentives	Cash flow	Sourcing	Communication infrastructure	
	Investment evaluation	Product development	Change acceptance	
	Treasury	Product failure	Change readiness	
	Payroll	Business interruption	Challenge	

	Debtor/creditor management	Contingency Planning	Ethics	
Compliance	Environment	Human Resources	Reputation	Technology
Health and safety	Seasonality	Competencies	Brand	Reliability
Environment	Globalization	Recruitment	Reputation	Management information systems
Copyright and trademarks	Competition	Retention	Intellectual property	Access /availability
Contractual liability	E-commerce	Performance measurement	Stakeholder perception	IT security
Taxation	Share price	Leadership development		
Data protection	Strategic uncertainty	Succession planning		

Example – Threat Assessment for Mumbai metropolitan city

Vulnerability Profile of Mumbai City:-

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

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

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

3.2 High Value Threats & Risks Analysed

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

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

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

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

3.3 Global Risk Outlook

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

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

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

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

The global risk indicators that are currently in trend include:- Nov 18 MCQ

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

Organisational Risks

Epstein and Rejc, 2005 depict organizational risks as:-

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

3.4 Risk Identification and Root Cause Analysis

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

often leads to ineffective mitigation activities.

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

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

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

3.5 Use of Specific Tools to Identify Risks

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

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

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

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

3.6 Risk Treatment Options Important

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

The primary objective of risk treatment is:-

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

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

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

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

ICAI Case Study 2

Outsourcing also part of

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

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

- **Insurance:** An organization may buy insurance to mitigate such risk. Under the scheme of the insurance, the loss is transferred from the insured entity to the insurance company in exchange of a premium. However while selecting such an insurance policy one has to look into the exclusion clause to assess the effective coverage of the policy. Under the Advanced Management Approach under Basel II norms (AMA), a bank will be allowed to recognize the risk mitigating impact of insurance in the measures of operational risk used for regulatory minimum capital requirements. The recognition of insurance mitigation is limited to 20% of the total operational risk capital charge calculated under the AMA.

Nov 19 Exam MCQ

- **Outsourcing:** The organization may transfer some of the functions to an outside agency and transfer some of the associated risks to the agency. One must make careful assessment of whether such outsourcing is transferring the risk or is merely transferring the management process. For example, outsourcing of telecommunication line viz. subscribing to a leased line does not transfer the risk. The organization remains liable for failure to provide service because of a failed telecommunication line. Consider the same example where the organization has outsourced supply and maintenance of a dedicated leased line communication channel with an agreement that states the minimum service level performance and a compensation clause in the event failure to provide the minimum service level results in to a loss. In this case, the organization has successfully mitigated the risk.

- **Service Level Agreements (SLAs):** Some of risks can be mitigated by designing the service level agreement. This may be entered into with the external suppliers as well as with the customers and users. The service agreement with the customers and users may clearly exclude or limit responsibility of the organization for any loss suffered by the customer and user consequent to the technological failure. Thus a bank may state that services at ATM are subject to availability of service there and customers need to recognize that such availability cannot be presumed before claiming the service. The delivery of service is conditional upon the system functionality. Whereas the service is guaranteed if the customer visits the bank premises within the banking hours.

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

4. IMPACT OF BUSINESS RISK

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

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

plan for the organisation.

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

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

Nov 18 MCQ + May 20 MTP MCQ

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

Example –

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

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

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

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

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

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

- Severe
- Major
- Moderate
- Minor
- Insignificant

Also see page no.9.22

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

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

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

- Loss of life
- Lost sales and income

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

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

Analysing the Level of Risk

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

Level of risk = consequence x likelihood

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

Example

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

Likelihood scale example Important Case Study 1

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

Consequences scale example Important

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

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

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

Evaluating risks

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

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

Risk rating table example Important Nov 2019 MTP MCQ + May 2018 Exam

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

Risk evaluation should consider:

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

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

See May 19 MTP CS-2

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

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

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

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

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

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

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

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

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

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

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

Risk Analysis

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

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

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

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

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

Stakeholder Value Creation by Enterprise Risk Management

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

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

Important
May 2020 MTP
Nov 2019 Exam

(a) enhanced working environment,

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

(c) Sustained or improved corporate reputation, and

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

Successful Stakeholder Risk Management

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

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

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

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

CRO See Page no. 7.4

6.1 The Role of the Risk Manager

15 Tasks

The role of the Risk Manager includes following tasks:-

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

6.2 Role and Responsibility of Risk Management Committee

Role

10 Roles

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

Risk Committee-See page 7.3

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

Responsibility 19 Responsibilities

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

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

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

6.3 IBM Case Study – Role of Risk Management Function

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

The role of the Enterprise Risk Management function at IBM

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

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

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

6.4 Principles for Effective Implementation of Risk Management Recommended By OECD

Nov 18 Theory Question Exam

OECD also page no. 7.20

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

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

6 Principles

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

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

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

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

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

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

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