YES ACADEMY
CA | CS | LAW

CS PROFESSIONAL

MODULE 1 | DEC 25/JUNE 26

ESG

summary notes

Adv. Chirag Chotrani

CHAPTER 18

DEC 2025/JUNE 2026

Ch 18 - Risk Management (Part 1) (20mks)

- Risk is an exposure to the possibility of any loss / injury / any unwelcoming circumstance.

- Risk management is the process through which an organisation identifies / analyse / assess and mitigate their risk and attempts to increase the likelihood of success of the organization.

- Better risk management strategies helps an organizations get early warning signs, so that an organization can be in a position to respond.

- Advantages:-
  a) saves large amount of money as org. is well prepared in advance.

  b) Avoids breakdowns and reduces litigations

  c) Increased reputation and greater dependibility

  d) Helps in making a plan for a successful project

- Steps of Risk management:-
  1) Identification
  2) Analysis
  3) Assesment
  4) mitigation.

* Risk Identification :-

a) This is the first stage of risk management process and is considered crucial, as if the risk remains unidentified the entire risk management process will fail.

b) Firstly, all the risks are identified & then classified and those specified risks are then transferred to their respective departments.

c) The objective is two fold wherein, to maximise the benefits of the project is the first objective and to supply data for the subsequent stages of risk management is the second objective.

* Process of Risk Identification :-

1) Creating a systematic process -
The first step is to set the project objectives and the success factors which helps in making a well customized risk identification process.

2) Gathering of information -
The next step is to gather data from reliable and dependable sources.

3) Apply risk identification tools and techniques -

Once the raw data is gathered the organization selects various tools and techniques to classify the raw data and to identify the risks which are to be passed on.

4) Document the risk identified -
All the identified risks are then documented in a risk register.

5) Document the risk identification process -
This helps in future referrence for like projects.

6) Assess the process effectiveness -
To improve process it should be regularly monitered

* Risk Analysis:-
a) This is the second step in the risk management process wherein the threats from the risk are identified as well as estimated

b) Risk analysis has the following advantages:-
i) While planning the project it helps in deciding whether to move forward or not.

ii) Helps in improving the safety at workplace

iii) Helps in anticipating as well as neutralizing possible problems.

* Process of Risk Analysis :-

1) Identifying threats :-

A risk can bring various threats which amongst many may include following :-

a) Human — illness / death of person
b) Operational — Disruption to supplies & operations.
c) Reputational — Loss of customer
d) Financial — Business fluctuations / stock market fluctuations
e) Natural — Natural disasters
f) Political — changes in tax, pub. opinion.

2) Estimate Risk :-

a) Once the threat is identified the next is to determine the probability of that threat materializing and the potential impact

b) So risk value can be calculated by finding out event probability & multiplying it with the cost of event

* Risk Assesment :-

a) Each risk comes with its own importance & it is at this stage that the business determines its importance

b) Every activity comes with an inherent risk which means if no treatment is done that is the risk which can materialize and the other risk is residual risk, which is the leftover risk after the management has addressed the problem.

* Process of Risk Assesment:-

1) Developing an assesment criteria -
In this the organization creates a set of evaluation standards which are used by the organization to evaluate the identified risks

2) Assess Risk -
The second step of risk assesment process is to assign values to each risk and thereafter treating the most significant risks on priority.
Before assigning values the risk first is screened through qualitative methodology and then through quantitative analysis

3) Assess Risk Interactions -
Risk never comes in isolation hence the businesses have to be more inclined towards the holistic view of the risk as a risk might look modest, but it may do great harms.

4) Prioritize Risks -
In this stage the identified risks are compared to the target risk level that is the risk appetite & to prioritize the risk which are beyond risk appetite.

5) Response to Risk -
Based upon risk assessment process a risk response is developed where either the risk maybe accepted, minimize, shared or avoid.

6) Effective and sustainable risk assessment process must be practical & easy to understand.

* Handling of Risk :-
There are various risk mitigation strategies amongst which few are as follows:-

A] Risk Avoidance - In this the business avoids the project and opts for a less riskier business project, for instance if the investor finds severe risk in equity investment, he may prefer to invest into debt.

B] Risk Retention - Is nothing but Risk acceptance which can further be of two types.

(a) Active Retention
When the risk is deliberately accepted as a part of risk management strategy.
(a) Passive Retention
Where the risk retention happens because of carelessness or where the risk taker dosen't understand the impact of the risk.

c] Risk Reduction - When the risk is higher than the risk appetite then another strategy is to reduce and minimize that risk and to bring it within the risk appetite.
The best ~~time~~ time to reduce the risk is in the planning stage, as same maybe acheived without any additional expenses.

(risk sharing)
D] Risk Transfer - In this org. identifies its core activities, where it excels & separate it from its non core activities which are then transfered to expert agencies which specializes in them. for a fees.
(ex - outsourcing)
Through this the company transfers its risk to a specialized agency.
Three ways of Risk Transfer -
a) Insurance
b) Contracts other than insurance (outsourcing)
c) Torts (compensation).

E] Combined Risk - In this the company tries to balance out the risk by combining both the risks in which one risk carries higher impact & the other carries lesser impact.
for instance investing in equity & debt at the same time.

* Fraud Risk Management

1) Fraud is an intentional statement / action done by one person with the intention to deceive another person and causing him wrongful loss

2) fraud risk mgmt is a structured approach to lower the fraud risk by creating an anti fraud program.

3) Steps:-
a) Identifying the risk :
The first step in FRM is to identify the dept/ areas which are most likely to do fraud.

b) Assesing risk :
An organisation doing FRM should not confuse by treating the symptoms but rather should aim to find out the root cause and attempt to treat the same.

c) Responding to Risk :
Based upon the assessed risk the organizations should prioritize those risks which are beyond the risk appetite and formulate the strategy to mitigate & respond.

d) monitoring :
The process of FRM is an ongoing process hence monitoring becomes one of the most crucial element to adjust with the changing situations, as risk never comes in isolation & keeps on changing.

e) Risk Reporting :

* Handling of Risk / Risk Mitigation
There are various risk mitigation strategies amongst which few are as follows:

1) Risk Avoidance :
In this the business avoids the project and opts for a less riskier business project for instance if the investor finds severe risk in equity investment he may prefer to invest into debt.

2) Risk Retention :
Risk retention is nothing but risk acceptance which can further be of 2 types
a) Active retention - when the risk is deliberately accepted as a part of risk management strategy
b) Passive retention - where the risk retention happens because of carelessness or where the risk taker doesn't understand impact of risk.

* Role of Company Secretary.

1) A company secretary being a governance professional is expected to perform various functions which aids in risk management. In order to safeguard the integrity of organization & to promote high ethical standards.

2) The functions include :-
a) Advising the best practices in governance & risk management functions.
b) Balancing the interest of all the stakeholders
c) making a robust compliance culture in order to safeguard the integrity of org.

3) A CS also plays a very important role in promoting an effective risk management framework which includes :-
a) Understanding the orgatisations risk management philosophy.
b) Taking steps to make all the personnel aware about the risk philosophy
c) Determining the risk appetite / tolerance level.
d) Monitoring that is the choosen risk response appropriate and reporting the deficiencies if any.

* Reputational Risk

1) Its the risk arising from negative perception on the part of the stakeholders (customers, sh·holders, debt holders) which may adversely affect the bank's ability to maintain or establish business relationship.

2) It is a type of non financial risk which do not have an immediate impact, but is not controlled it may have severe financial risk as well.

3) A reputational risk has long lasting damages like
- it destroys brand value.
- Steep downtrend in share value.
- Ruined strategic relationship.

4) Such risk calls for an effective reputational risk management function which should be based on following principles:-
a) A reputational risk like other risks must be integrated while forming the business strategy.

b) It can be achieved by effective board oversight

c) Some of the ways to manage reputational risk includes strong internal check / evaluating company's own performance and peer reviews.

d) A company which is regular with its compliances has a lesser reputational risk, hence promoting compliance culture should be the end.

e) Quality report & newsletter publications.

* Internal control

1) Internal control is a process established by the organisation to ensure -
   a) Reliability of financial reporting
   b) Improved operational efficiency
   c) Adherence to the applicable laws.

2) Further it includes systems and procedures designed to manage the risk identified through the risk management process which in turn supports the acheivement ~~of~~ of organizational objectives.

3) It is the responsibility of every business to integrate the risk management and the internal control system as these two are closely related but not same., they rather compliment each other in creating a robust framework for managing risk.

4) So, in a nutshell, risk management focuses on identifying and estimating the threats and opportunities on the other hand internal control helps in providing defences / counter to the threats.

* Forex :-

In a mfg company it has identified the risk of supply disruption which may affect the production capacity [this was the task of risk management function] & for this the company has put up a robust internal control

System which does a regular inventory check and ~~hence~~ has also finalised back up vendors.

In the above example, finding the risk as well as its possible impact was the ~~rist~~ task of risk management, while taking steps to reduce and monitor the risk was the task at internal control.

Risk Register

Srno	Types of Risk	Risk concern	Root cause	mitigation measures.

Internal Audit

It is an independent function of the management which involves a critical and continuous appraisal of the functioning of the entity done with the objective of suggesting improvements to the overall governance mechanism and to strengthen the internal control system

Applicability

(a) Every listed company
(b) Every unlisted public company
- outstanding deposits 25@ cr or
- paid up capital 50cr or
- turnover 200cr or
- o/s loan 100cr

(c) Private companies
- turnover 200 cr
- loans 100 cr.

Internal audit increases productivity by bringing a disciplined approach in evaluating and improving the effectiveness of risk management process as well as the overall governance.

Further, internal audit helps discover gaps and areas of frauds and helps in forming a plan to evaluate and protect assets of company.

It further helps in quality control as it provides valuable insights as to how to improve system and processes.

It provides an independent and unbiased insight.

Role of internal auditor in strengthening internal ~~audit~~ control:

1. It is an independent management function setup to assess internal control system and to reccommend measures to improve it.

2. It does not make the plan but rather helps in identifying the gaps in the ~~in~~ current internal control system which inturn helps in training personnel to reach the desired objective.

3. Apart from the above it examines the compliance with the applicable laws and ensures that there is reliable reporting.

4. Following are some of the duties of an internal auditor:
(a) Evaluating risk management process
(b) Evaluating internal control process.
(c) Recommending improvements in both the above procedures.
(d) Evaluating the compliances done by the entity.
(e) Investigating any fraud
(f) Promoting ethical culture in organisation.

* Crisis Management

1. A crisis is an unanticipated event or negative disruption which is or which may harm the people / property of the organisation.

2. A crisis management is a process set up by an organisation for identifying and responding to such crisis. with a aim to limit such harm and recover swiftly.

Types of crisis

@) Natural Disaster - These are those events which takes place spontaneously and it generally happens without human intervention and are typically classified as act of god.

(b) Technological crisis - Technology may be a boon or curse, because if used improperly the negative effects may outweigh positive ones.
ex - data breach / virus which may hinder an organisation's growth.

(c) Confrontational Crisis - This is a type of crisis arising because of a clash between the people forming organisation because of their belief or idealogy.

(d) Rumours - Sometimes other businesses may try to win by making false accusations which inturn becomes one of the biggest crisis a business may face.

* Organisational Misdeeds

1. This kinds of crisis may arise because of the wrong steps taken by a firm.

Crisis management plan (Prerequisites)

1. Form a crisis team out of which one shall be selected as a crisis manager to whom the leadership is entrusted.

2. Initiate training and refresher courses as to how to handle crisis.

3. Plan responses for all the potential crisis which can be reasonably forseen.

4. Identify a ground person who shall be notified in the event of any crisis.

5. monitor and detect dt the forseable crisis.

Effective Crisis Management Plan.

1. A CMP is a type of BCP which deals with setting up procedures for dealing with a crisis.

2. A crisis management plan may involve different people depending upon the type of crisis a company might be facing.

3. For instance, if it is a financial crisis, the finance manager may be involved in preparing a response for such crisis, whose primary task would be to ensure that the company has sufficient financial resources and adequate financial reporting, and to keep a check that the company complies with all the relevent laws.

4. For instance, if it is a marketing crisis, the marketing manager may be involved in preparing a response for such crisis, whose primary task would be to promote and sell company's goods / services and to maintain a brand image of the company.

* Features of Crisis Management / Need.

(a) It helps the management to analyse and understand all the events which might lead to crisis.

(b) It helps the managers and employees to respond effectively.

(c) Promotes effective coordination.

(d) It helps the managers to devise strategies to respond to uncertain events and to decide upon future course of action.

* ESG Risk Assesment / Management

1. It is not a mandatory type of risk assesment, but rather a voluntary activity being taken up by the company, which helps in assesing the various, environmental, social, governance risks.

2. Significance / importance of ESG risk assesment:

(a) Enhanced Sustainability
(b) Improved Regulatory Compliance
(c) Increased Investment Potential
(d) Better Employee Productivity

3. ESG risk management follows the same three steps: (a) Identify
(b) Assess (quantify)
(c) Mitigate (manage).

- Environmental Risk.

The risk with which this report deals are all environmental of which some are created by man while some are natural hazards.

Few types of environmental risk are:

a. Climate change because of GHG emissions
b. Deforestation

- Social Risk

1. These are the risks which are concerned with all the parties involved in the firm i.e. from the suppliers to the local community to the employees.

2. Since the stakeholders are numerous this is one of the most critical risk to deal with. and is of utmost priority to ensure the long term success of the company.

3. Examples of social risk are:
1) Workplace Safety
2) Data Security
3) Fair labour standards for vendors / suppliers.

Governance Risk

1. Governance means the values and the culture and the measures by which organizations are directed and controlled.

2. A governance risk includes the following:
   (a) Low corporate ~~model~~ morals and ethics
   (b) Conduct and practices that are anti competitive
   (c) Ineffective grievience mgmt policies.
   (d) Ineffeciency in preventing fraud & corruption
   (e) Ineffective compensation of executives
   (f) Diversity in the board.

ESG Risk Management.

1. In this an organisation prepares to identify / manage / reduce all the ESG related risks

2. It is not a universal process, hence, all corporations should define their ~~specific~~ ESG practices and the specific risk to which it is exposed to.

3. Lastly, a review of the same shall be done on a continuous basis.

Climate Risk

1. Globally, climate related risk has shown a significant increase which pose a growing risk to sustainable development of community as well as country.

2. Nationally, as well as internationally there has been recognition of new measures to mitigate climate risk but the same should be integrated by the companies in their risk mgmt process.

Climate risk mgmt process:

1. Gathering all information concerning risks relating to climate
2. Analyse risk → identify → high level / low level
3. Assess evaluate → risk → to decide mitigation strategy (accept / retain / avoid)
4. Assess entire process.

* Business Continuity Plan (BCP)

1. A BCP is a document which outlines how the business will continue in the event of an unplanned disruption.
2. It has two fold function where 1st being prevention and the 2nd being recovery in the event of any disruption.
3. A BCP is made tailored, specific to the departments ~~th~~ which are at risk.
4. For instance, if the finance operation is at risk the BCP would then focus on maintaining steady financial flow & ensure that they are doing adequate financial reporting & also it focuses on the procedure to restore critical fin. system, while ensuring that a key fin personnel is alway

available to respond.

5. In case of the HR operations being at risk the plan would focus on maintaining adequate personnel resources ensuring that the co. would be able to pay to its employees in the event of any disruption & it ensures that key HR personnel is available to respond in the event of any crisis.

6. In each case the BCP provides for framework for the respective departments to follow in the event of any crisis.

* Steps for creating BCP

Step 1: Assemble a BC mgmt team :-
(a) Create a contact list of important people involved in company's BCP & provide their basic details.
(b) Provide the details about roles & resp of each one of them.
(c) make a process to communicate the BCP as well as any updates to it with the people.

Step 2: Ensure safety of your employees :-
(a) While planning and forming a BCP the primary focus should be on the safety of the employees, for instance to provide them remote working facility in the event of any disruption without compromising their safety.

(b) Make sure to have a proper communication channel which allows easy, early & regular communication.

Step3: Analyse & Understand the Risk to your Co:-
(a) How the company moves on to conduct a business impact analysis to identify threats to the financial performance, operations etc.
(b) Once the risks are identified discuss the most critical risk which could affect the risks.

Step4: Implement Recovery Strategies :-
(a) While forming recovery strategies the following questions must be addressed :
- Does the business has a way to continue operations after a disaster has hit?
- How the demand will be met if your equipment is damaged?

Step5: Test, Test Again & make improvements :-
(a) No matter how long you spend perfecting it, a BCP is never truly finished, just as the risk evolves the BCP also evolves.

Components of BCP
a) Strategy - Because the object is to form Strategies to ensure continuous operations.

b) Processes - The object is to identify all those critical business processes necessary to run the business so as to ensure smooth operations.

c) Technology - The object is to ensure availibility of industry specific technology necessary to enable continuous operations.

d) Facilities - The object is to prepare for a disaster recovery site if the primary site is destroyed.

e) Application & Data - The object is to identify softwares necessary to enable continuous operations in event of any crisis.

* Disaster Recovery Plan (DRP)

- In a DRP a business makes a plan setting out procedures & strategies that a corporation will use to restore its critical operations in the event of any disaster.

- The goal is to ensure quick & effective recovery from any disaster & return to normal operations.

- It is a component of RM & BCP & is created to minimize the impact of any disaster on the operations of the corporation.

- Under this the companies analyse the risk & consequences of any disaster as well as the response plan & plan for recovering from the disaster.

* Elements of DRP

(a) Create Disaster recovery team -

A DR team shall be responsible for developing

& implementing a DRP.

(b) Identify and assess disaster risk-
The team formed above shall be responsible to identify & assess all the risk to the organization, it should include items related to natural disaster, manmade emergencies which helps team in identifying appropriate strategy.

(c) Determine those operations, applications of the organization which are the most imp & the plan should focus on short term survivability rather than restoring org's full capacity.

(d) Specify backup & offsite storage procedures-
The business should identify what is to be backed up, by whom it is to be done, how to perform the backup, location of backup & how frequently it should occur.
In regards to documents following can be backed up: latest FS, tax returns, contact info & current list of employees, etc.

(e) Test & maintain DRP-
All the organizations should test DRP to evaluate the procedures & how effective & appropriate it is.

* Relationship between BCP, crisis mgmt & DRP :-

1] BCP is an umbrella that includes within it DRP as well as CMP.

2] Herein, BCP is a comprehensive strategy ensuring

that the business continues / atleast critical business operation continues during / after a disruption.

3] So, a BCP is a proactive approach in which risk is identified, assessed & planned for.

4] Crisis mgmt focuses on immediate response to any unexpected event (like a cyber attack)

5] A DRP on the other hand focuses on restoring critical operations in the event of any disaster.

6] The relationship b/w BCP & Crisis mgmt is that a BCP provides framework for business operations, while CMP provides guidance for managing a crisis & on the other hand DRP focuses on recovery from a disaster.

* Cyber risk Management :-

1] The Cyber risk mgmt is a process to identify & mitigate all the cyber risk of an organization.

2] The process of cyber risk mgmt is as follows :-

→

(a) Identify the risk that may compromise your cyber security, which involves identifying the vulnerabilities in the system.

(b) Analyse all the risk and assess it to check as to the likelihood & significance of the risk.

(c) Evaluate the risk against your risk appetite

(d) Prioritize the risk

(e) Risk response -
- Treat
- Tolerate
- Terminate
- Transfer

3) It is a continuous process so the business should always monitor the risk to ensure that it is within the risk tolerance levels.

Cyber security measures :-

- The cyber security measures are classified in following :-

(a) legal measures to provide legislations & an implementation framework to protect cyber space.

(b) Technical measures to consider the technological tools to prevent, detect, mitigate & respond to cyber attacks.

(c) Organizational measures for the implementation of risk initiatives.

(d) Capacity building to enhance the knowledge in order to promote cyber security.

(e) Cooperation measures to establish partnership b/w stakeholders to increase cyber resilience against cyber threats.