YES ACADEMY
Say Yes to CS

CS PROFESSIONAL

For June 23/Dec 23 Attempt

PART-1

GOVERNANCE RISK MANAGEMENT COMPLIANCES AND ETHICS

Adv. Chirag Chotrani

HIGHLIGHTS

- Sample Answer Writing Formats
- Summarised Case Laws

CS Vikas Vohra *(Founder)*

CSEET : Current Affairs
EXECUTIVE : Company Law
: Securities Laws & Capital Markets
PROFESSIONAL : Drafting, Pleadings and Appearances

CA CS Harish A. Mathariya *(Founder)*

CSEET : Business Environment
EXECUTIVE : Corporate & Management Accounting
: Financial and Strategic Management

CMA Vipul Shah

EXECUTIVE : Tax Laws
PROFESSIONAL : Advanced Tax Laws

Video lectures available *for all subjects of* **CS Course** *at all levels.*

Adv Chirag Chotrani

CSEET : Legal Aptitude
EXECUTIVE : Jurisprudence, Interpretation & General Laws
: Setting up of Business Entities and Closure
: Economic, Business and Commercial Laws
PROFESSIONAL : Governance, Risk Management, Compliances and Ethics
: Corporate Funding & Listings in Stock Exchanges

CS Vaibhav Chitlangia

CSEET : Logical Reasoning
: Economics
PROFESSIONAL : Multidisciplinary Case Studies
: Insolvency – Law and Practice
: Corporate Restructuring, Insolvency, Liquidation & Winding - Up

CS Muskan Gupta

CSEET : Business Communication
PROFESSIONAL : Secretarial Audit, Compliance Management and Due Diligence
: Resolution of Corporate Disputes,Non-Compliances & Remedies
: Labour Laws & Practice

For demo lectures *visit our Youtube Channel*

#yesacademyforcs

For purchasing our notes, **Call 8888 235 235 / 8888 545 545**
or
Visit our website **www.yesacademy.co.in**

SANDESH

CS Vikas Vohra **CA CS Harish A. Mathariya**

Welcome to YES Family!!

To begin with, we endorse our heartfelt thank you for showing your trust and confidence in YES Academy. We take pride to welcome you to this prestigious Academy, foundations of which are based on commitment, quality education and integrity. It has been our constant endeavour to deliver better and better. In our attempt to achieve mark of excellence and beyond, we would be even more grateful to have received your continued faith and love. We assure you, your trust will not go in vain and as reflected by our Vision Statement, we would continue to produce Best Company Secretaries as we have been doing for almost a decade now.

Combined experience of Team YES is 40 years+ and adding value each day. We have delivered outstanding results in the past with a bouquet of All India Rankers at all the levels of CS Course and with your efforts, we are confident, we will grow together.

Student convenience has always occupied a centre place at YES Academy and we strive to improve ourselves each day as we sincerely believe that improvement always has its own space, no matter what. Any suggestions from you are always welcome. Though Team shares a very good rapport with all of its students and the students feel very comfortable talking to any of their Teachers, still, if you wish to send us a suggestion, please feel free to write to us yesacademypune@gmail.com or get in touch with us at 8888 235 235/ 8888 545 545.

We assure you the best of success and pride. And yes, its not just a bond of 3 years of your term, but a relationship for life now. We welcome you in advance to this prestigious course of Company Secretaries.

On behalf of **TEAM YES**

CS Vikas Vohra CA CS Harish A. Mathariya
Founders

CHAPTER 12- RISK MANAGEMENT

RISK

- In the business world, the word risk has come to mean an impediment to the achievement of an organization's objectives.
- As per the Oxford Dictionary – "Risk is Exposure to the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility'.
- The other definitions of risks from various perspectives are as under:

1. Generic: 'A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action.'

2. Finance Perspective: 'The probability that an actual return on an investment will be lower than the expected return. Financial risk is divided into the following categories: Basic risk, Capital risk, Country risk, Default risk, Delivery risk, Economic risk, Exchange rate risk, Interest rate risk, Liquidity risk, Operations risk, Payment system risk, Political risk, Refinancing risk, Reinvestment risk, Settlement risk, Sovereign risk, and Underwriting risk.'

3. Food industry: 'The possibility that due to a certain hazard in food there will be an negative effect to a certain magnitude.'

4. Insurance: A situation where the probability of a variable (such as burning down of a building) is known but when a mode of occurrence or the actual value of the occurrence (whether the fire will occur at a particular property) is not.

5. Securities trading: The probability of a loss or drop in value. Trading risk is divided into two general categories: (1) Systemic risk affects all securities in the same class and is linked to the overall capital- market system and therefore cannot be eliminated by diversification. Also called market risk. (2) Non- systematic risk is any risk that isn't market-related or is not systemic. Also called non-market risk, extra- market risk, or un-systemic risk.

CLASSIFICATION OF RISKS

Systemic Risk

- It is not fully uncontrollable by an organization.
- It is not entirely predictable.
- It is usually of a macro nature.
- It usually affects a large number of organisations operating under a similar stream.
- It cannot be fully assessed and anticipated in advance in terms of timing and gravity.
- The example of such type of risks is Interest Rate Risk, Market Risk, Purchasing Power Risk.

Unsystemic Risk

- It is usually controllable by an organisation.
- It is reasonably predictable.
- It is normally micro in nature.
- If not managed it directly affects the individual organisation first.
- It can be usually assessed well in advance with reasonable efforts and risk mitigation can be planned with proper understanding and risk assessment techniques.
- The examples of such risk are Compliance risk, Credit Risk, Operational Risk.

TYPES OF RISKS ON THE BASIS OF IMPACT ON FINANCE

Financial Risk

- The risk which has some direct financial impact on the entity is treated as financial risk.
- This risk may be Market risk, Credit risk, Liquidity risk, Operational Risk, Legal Risk and Country Risk. The following chart depicts some of the various types of financial risks. Non-Financial Risk
- This type of risks do not usually have direct and immediate financial impact on the business, but the consequences are very serious and later do have significant financial impact if these risks are not controlled at the initial stage.
- This type of risk may include, Business/Industry & Service Risk, Strategic Risk, Compliance Risk, Industry Fraud Risk, Reputation Risk, Transaction risk, Disaster Risk.

Types of Financial Risks

(i) Market Risk

- This type of risk is associated with market ups and down.
- It refers to the risk of loss arising from the change/volatility in the market prices or economic values which are the deciding factors for the pricing of the product/financial assets.
- The market risks may be Absolute Risk (when it can be measured in rupee/currency term) and Relative Risk (relative to bench mark index).
- Hence the market risk may be defined as the risk to a firm due to the adverse changes in interest rates, currency rates, equity prices and commodity prices.

a) Interest Rate Risk

- The financial assets which are connected with interest factors such as bonds/ debentures, faces the interest rate risk.
- For example Interest rate risk adversely affects value of fixed income securities.
- Any increase in the interest reduces the price of bonds and debts instruments in debt market and vice - versa. So it can be said that the changes in the interest rates have an inverse relationship with the price of bonds.

b) Currency Risk

- The volatility in the currency rates is called the currency risk.
- These risks affect the firms which have international operations of business and the quantum of the risk depends on the nature and extent of transactions with the external market.

c) Equity Risk

- It means the depreciation in one's investment due to the change in market index.
- For example in the context of securities, Beta of a stock tells us the market risk of that stock and it is associated with the day-to-day fluctuations in the market.

d) Commodity Risk

- This type of risk is associated with the absolute changes in the price of the commodity.

- Since commodities are physical assets, hence the prices change on account of the demand and supply factor.

(ii) Credit Risk

- When a counter party is unable or unwilling to fulfil their contractual obligation, the credit risk arises.
- This type of risk is related to the probability of default and recovery date.
- Its effect is measured by cost of replacing cash flow if the other party defaults.
- For example, in case of loan given by a bank to the borrower and the borrower defaults in making payments of the installments or due interest on the due date, is termed as credit risk.

(iii) Liquidity Risk

- The liquidity risk arises due to mis-matches in the cash flow i.e. absence of adequate funds.
- Liquidity is altogether different from the word solvency.
- A firm may be in sound position as per the balance sheet, but if the current assets are not in the form of cash or near cash assets, the firm may not make payment to the creditors which adversely affect the reputation of the firm.
- The liquidity risk may be of two types, trading risk and funding risk.

(a) Trading Risk

- It may mean the absence of the liquidity or enough products or securities etc to actually undertake buy and sell activities.

  e.g. in the context of securities trading inability to enter into derivative transactions with counter parties or make sales or purchase of securities.

(b) Funding Risk

- It refers to the inability to meet the obligations e.g. inability to manage funds by either borrowing or the sale of assets/securities.
- It arises where the balance sheet of a firm contains illiquid financial assets which cannot be turned in to cash within a very short time.

(iv) **Operational / System/ Management Risk**

- It arises due to inadequate systems, system capacities, system failure, and obsolescence risk, management failure on account co-ordination, faulty control or human error.
- Some best practice against the operational risk includes clear separation of responsibilities with strong internal control and regular contingency planning.

(v) **Obsolescence Risk**

- In the rapid changing world Obsolescence risk is fast emerging and unless the companies are able to cope up with this timely, the impact will be quite heavy and may lead to closure of the units also. Nokia is the latest example on this.

(vi) **Legal Risk**

- This risk arises when a counter party does not have the legal or regulatory authority to engage in the transactions. It also includes the compliance and regulatory risk like insider trading, market manipulations, defaults and mismanagement of legal affairs etc.

(vii) **Political/ Country Risk**

- Political risk may be on account of declaration of elections in the territory, area specific risk and political uncertainity.
- The Country risk arises where the firm have its business operations abroad. This risk may arise due to out-break of war between countries, imposition of the ban on the business transaction of particular commodity/product.
- These can also be existing risks due a country's legal or political structure which drives other institutions like judiciary, legislative and general environment for business.

Types of Non-Financial Risks

(i) **Business/ Industry & Services Risk**

- Business risks implies uncertainty in profits or danger of loss and the events that could pose a risk due to some unforeseen events in future, which causes business to fail.

- Business risk refers to the possibility of inadequate profits or even losses due to uncertainties e.g., changes in tastes, preferences of consumers, strikes, increased competition, change in government policy, obsolescence etc.
- Every business organization contains various risk elements while doing the business.
- Such type of risk may also arise due to business dynamics, competition risks affecting tariff prices, customer relation risk etc.

(ii) Strategic Risk

- Business plans which have not been developed properly and comprehensively since inception may lead to strategic risk.
- For example, strategic risk might arise from making poor business decisions, from the substandard execution of decisions, from inadequate resource allocation, or from a failure to respond well to changes in the business environment.

(iii) Compliance Risk

- This risk arises on account of non-compliance or breaches of laws/ regulations which the entity is supposed to adhere. It may result in deterioration of reputation in public eye, penalty and penal provisions.

(iv) Fraud Risk

- Fraud is perpetrated through the abuse of systems, controls, procedures and working practices.
- It may be perpetrated by an outsider or insider.
- Fraud may not be usually detected immediately and thus the detection should be planned for on a proactive basis rather than on a reactive basis.

(v) Reputation Risk

- This type of risk arises from the negative public opinion.
- Such type of risk may arise from e.g. from the failure to assess and control compliance risk and can result in harm to existing or potential business relationships.

(vi) Transaction Risk

- Transaction risk arises due to the failure or inadequacy of internal system, information channels, employee's integrity or operating processes.

(vii) Disaster Risk

- On account of natural calamities like floods, fire, earthquake, man-made risks due to extensive exploitation of land for mines activity, land escalation, risk of failure of disaster management plans formulated by the company etc.

(viii) Regulatory Risk

- On account of change in Government policies and perceptions. Especially this type of risks is associated with Food and beverages and Pharmaceuticals industries.

(ix) Technology Risk

- Failure of system caused due to tampering of data access to critical information, non-availability of data and lack of controls.

AUDIT RISK

- Audit risk is the risk that financial statements are materially incorrect, even though the audit opinion states that the financial reports are free of any material misstatements.
- Over the course of an audit, an auditor makes inquiries and performs tests on the general ledger and supporting documentation.
- If any errors are caught during the testing, the auditor requests that management propose correcting journal entries. At the conclusion of an audit, after any corrections are posted, an auditor provides a written opinion as to whether the financial statements are free of material misstatement.
- Auditing firms carry malpractice insurance to manage audit risk and the potential legal liability.

Types of Audit Risks

- The two components of audit risk are the risk of material misstatement and detection risk.

1. Risk of Material Mis-statement

- The risk of material misstatement is the risk that the financial reports are materially incorrect before the audit is performed.
- In this case, the word "material" refers to a dollar amount that is large enough to change the opinion of a financial statement reader, and the percentage or dollar amount is subjective.
- The risk of material misstatement is even higher if there is believed to be insufficient internal controls, which is also a fraud risk.

2. Detection Risk

- Detection risk is the risk that the auditor's procedures do not detect a material misstatement.
- For example, an auditor needs to perform a physical count of inventory and compare the results to the accounting records.
- This work is performed to prove the existence of inventory.
- If the auditor's test sample for the inventory count is insufficient to extrapolate out to the entire inventory, the detection risk is higher.

RISK MANAGEMENT

- "Risk Management" is a term used to describe the processes which aim to assist organisations identify, understand, evaluate and take action on their risks with a view to increasing the probability of their success and reducing the impact and likelihood of failure.
- Effective risk management gives comfort to shareholders, customers, employees, other stakeholders and society at large that a business is being effectively managed and also helps the company or organisation confirm its compliance with corporate governance requirements.
- Risk management requires a detailed knowledge and understanding of the organization (both internal and external) and the processes involved in the business.

- Better risk management techniques provide early warning signals so that the same may addressed in time.
- Risk management requires commitment from the top management.
- Risk Management Process provides a framework to:
  - Ensure that all the foreseeable risks involved are actually understood and accepted before important decisions are taken.
  - Monitor new projects and ongoing operations to ensure that they continue to develop and no problems or new risks emerge.
- Risk Management is part of the corporate strategy.
- It is a key management tool to safeguard the business assets for its use for the productive purposes.

Advantages of risk management

Some of the key advantages of having risk management are as under:

- Risk Management in the long run always results in cost savings and prevents wastage of time and effort in firefighting.
- It can help plan and prepare for the opportunities that unravel during the course of a project or business.
- Risk Management improves strategic and business planning. It reduces costs by limiting legal action or preventing breakages.
- It establishes improved reliability among the stake holders leading to an enhanced reputation.
- Sound Risk Management practices reassure key stakeholders throughout the organization.

Steps in risk management process

The process of risk management consists of the following logical and sequential steps:

1. **RISK IDENTIFICATION**

- Risk identification is the first stage of the risk management strategy.
- The origin/source of the risk is identified. For example a risk may be due to transport of hazardous raw material to the factory. So the source of the risk origin is utmost important and from this point the journey start to manage the risks.

- By risk identification the organization can study the activities and places where its resources are placed to risk.
- Correct risk identification ensures effective risk management.
- If risk managers fails in identifying all possible losses or gains that challenge the organization, then these non-identified risks will become non manageable.
- The results of risk identification are normally documented in a risk register, which includes a list of identified risks along with their sources, potential risk responses and risk categories.
- This information is used for risk analysis, which in turn will support creating risk responses.

Objective:

- The objective of the risk identification process is to ensure that all potential project risks are identified.
- The ultimate purpose of risk identification is to minimize the negative impact of project hiccups and threats, and to maximize the positive impact of project opportunities.
- The purpose of risk identification is to provide information for the next step of the risk management process.

Process of Risk Identification:

1. Creating a systematic process - The risk identification process should begin with project objectives and success factors.
2. Gathering information from various sources - Reliable and high quality information is essential for effective risk management.
3. Applying risk identification tools and techniques - The choice of the best suitable techniques will depend on the types of risks and activities, as well as organizational maturity.
4. Documenting the risks - Identified risks should be documented in a risk register and a risk breakdown structure, along with its causes and consequences.
5. Documenting the risk identification process - To improve and ease the risk identification process for future projects, the approach, participants, and scope of the process should be recorded.
6. Assessing the process' effectiveness - To improve it for future use, the effectiveness of the chosen process should be critically assessed after the project is completed.

Seven Identification Essentials

Identification is a process of brainstorming. It isn't an exact science and should involve continuous implementation as new phases, experiences, and viewpoints are introduced.

1. Team Participation: Face-to-face interactions between project managers and the team promise better and more comprehensive communication. The team must feel comfortable to share and find hidden risks.
2. Repetition: Information changes appear as the risk management process proceeds. Keeping identified risks current and updated means the system is focused on mitigating the most prevalent issues.
3. Approach: Certain objectives require distinct approaches to best combat identification failure. One method is to identify all root causes, undesirable events and map their potential impacts. Another is to identify essential performance functions the project must enact, then find possible issues with each function or goal.
4. Documentation: Consistent and exhaustive documentation leads to comprehensive and reliable solutions for a specific project or future risk management team's analysis. Most communication is recorded by a project manager and data is copied, stored, and updated for continued risk prevention.
5. Roots and Symptoms: It is essential in the risk identification phase to find the root causes of a risk instead of mistaking them with the symptoms. A symptom can be confused with the root cause, making it critical to discover the origin of risks and denote what are their symptoms. Other essentials of risk identification involve the analysis phase.
6. Project Definition Rating Index (PDRI): PDRI is a risk assessment tool that helps develop mitigation programs for high-risk areas. It facilitates the team's risk assessment within the defined project scope, budget and deadlines. It also provides further detail of individual risks and their magnitude, represented by a score. The summation of scores is statistically compared to the project performance as a certainty level for the entire project
7. Event Trees: Commonly used in reliability studies and probabilistic risk assessments, event trees represent an event followed by all factors and faults related to it. The top of the tree is the event and it is supported by any condition that may lead to that event, helping with likelihood visibility.

II. RISK ANALYSIS

- After identification of the risk parameters, the second stage is of analyzing the risk which helps to identify and manage potential problems that could undermine key business initiatives or projects.
- To carry out a Risk Analysis, first identify the possible threats and then estimate the likelihood that these threats will materialize.
- The analysis should be objective and should be industry specific.
- Within the industry, the scenario based analysis may be adopted taking into consideration of possible events that may occur and its alternative ways to achieve the given target.
- Risk analysis is useful in many situations like:

➢ While planning projects, to help in anticipating possible problems.
➢ While deciding whether to move forward with a project.
➢ While improving safety and managing potential risks in the workplace.
➢ While preparing for events such as equipment or technology failure, theft, staff sickness, or natural disasters.
➢ While planning for changes in environment, such as new competitors coming into the market, or changes to government policy.
➢ When all the permutations-combinations of possible events/ threats are listed while analyzing the risk parameters and the steps taken to manage such risks, the risk matrix is designed before the decision making and implementing authority.

Process of Risk Analysis

a) **Identify Threats:** The first step in Risk Analysis is to identify the existing and possible threats that one might face. These can come from many different sources. For instance, they could be:

➢ **Human** – Illness, death, injury, or other loss of a key individual.
➢ **Operational** – Disruption to supplies and operations, loss of access to essential assets, or failures in distribution.
➢ **Reputational** – Loss of customer or employee confidence, or damage to market reputation.
➢ **Procedural** – Failures of accountability, internal systems, or controls, or from fraud.

- **Project** – Going over budget, taking too long on key tasks, or experiencing issues with product or service quality.
- **Financial** – Business failure, stock market fluctuations, interest rate changes, or non-availability of funding.
- **Technical** – Advances in technology, or from technical failure.
- **Natural** – Weather, natural disasters, or disease.
- **Political** – Changes in tax, public opinion, government policy, or foreign influence.
- **Structural** – Dangerous chemicals, poor lighting, falling boxes, or any situation where staff, products, or technology can be harmed.

A number of different approaches can be used to carry out a thorough analysis:

- Run through a list such as the one above to see if any of these threats are relevant.
- Think about the systems, processes, or structures used and analyze risks to any part of these.
- Ask others who might have different perspectives. Ask for input from team members and consult others in the organization, or those who run similar projects.
- Tools such as SWOT Analysis and Failure Mode and Effects Analysis can also help to uncover threats, while Scenario Analysis helps to explore possible future threats.

b) Estimate Risk:

- Once the threats are identified, it is required to calculate both the likelihood of these threats being realized, and their possible impact.
- One way of doing this is to make best estimate of the probability of the event occurring, and then to multiply this by the amount it will cost to set things on the right track.
- This gives a value for the risk:
  Risk Value = Probability of Event × Cost of Event
- As a simple example, imagine that a risk has been identified that your rent may increase substantially.
- You think that there's 80 percent chance of this happening within the next year, because your landlord has recently increased rents for other businesses. If this happens, it will cost your business an extra Rs. 500,000 over the next year. So the risk value of the rent increase is: 0.80 (Probability of Event) x Rs.500, 000 (Cost of Event) = Rs. 400,000 (Risk Value)

III. **RISK ASSESSMENT**

- Risk assessment is the way in which enterprises get a handle on how significant each risk is to the achievement of their overall goals.
- To accomplish this, enterprises require a risk assessment process that is practical, sustainable, and easy to understand.
- When assessing risks, it's important to determine whether the risk is - inherent risk, residual risk, or both.
- Inherent risk as the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.
- Residual risk is the risk remaining after management's response to the risk. Some entities interpret:

➢ inherent risk to be level of risk assuming responses currently in place fail,and

➢ residual risk to be the level of risk assuming existing responses operate according to design.

Process of Risk Analysis

1. Develop assessment criteria:

- The first activity within the risk assessment process is to develop a common set of assessment criteria to be deployed across business units, corporate functions, and large capital projects.
- Risks and opportunities are typically assessed in terms of impact and likelihood. Many enterprises recognize the utility of evaluating risk along additional dimensions such as vulnerability and speed of onset.

2. Assess risks:

- Assessing risks consists of assigning values to each risk and opportunity using the defined criteria.
- An initial screening of the risks and opportunities is performed using qualitative techniques followed by a more quantitative treatment of the most important risks and opportunities lending themselves to quantification (not all risks are meaningfully quantifiable).
- Qualitative assessment consists of assessing each risk and opportunity according to descriptive scales.

- The quality of the analysis depends on the accuracy and completeness of the numerical values and the validity of the models used.
- Model assumptions and uncertainty should be clearly communicated and evaluated using techniques such as sensitivity analysis.
- For qualitative assessments, the most commonly used assessment techniques are interviews, cross-functional workshops, surveys, benchmarking, and scenario analysis.
- Quantitative techniques range from benchmarking and scenario analysis to generating forward looking point estimates (deterministic models) and then to generating forward looking distributions (probabilistic models).

3. Assess risk interactions:

- Risks do not exist in isolation.
- Enterprises have come to recognize the importance of managing risk interactions.
- Even insignificant risks have the potential to cause great damage or create significant opportunity.
- Therefore, enterprises are gravitating toward an integrated or holistic view of risks using techniques such as risk interaction matrices, bow-tie diagrams, and aggregated probability distributions.

4. Prioritize risks:

- Risk prioritization is the process of determining risk management priorities by comparing the level of risk against predetermined target risk levels and tolerance thresholds.
- While each risk captured may be important to management at the function and business unit level, the prioritization helps provide focus to senior management and board in addressing and giving attention to key risks.
- Ranking and prioritizing is often done in a two-step process.
  - First, the risks are ranked according to one, two, or more criteria such as impact rating multiplied by likelihood rating or impact multiplied by vulnerability.
  - Second, the ranked risk order is reviewed in light of additional considerations such as impact alone, speed of onset, or the size of the gap between current and desired risk level (risk tolerance threshold).

- If the initial ranking is done by multiplying financial loss by likelihood, then the final prioritization should take qualitative factors into consideration.

5. Response to Risks:

- The results of the risk assessment process then serve as the primary input to risk responses whereby response options are examined (accept, reduce, share, or avoid), cost-benefit analyses performed, a response strategy formulated, and risk response plans developed.

6. Effective and sustainable risk assessment process:

- To be effective and sustainable, the risk assessment process needs to be simple, practical, and easy to understand. People aren't enough. To be efficient, they must be supported by the right technology.

IV. HANDLING OF RISK

- The ownership of risk should be allocated.
- Responsibilities and accountabilities of the persons handling risks need to be identified and assigned.
- Risk may be handled in the following ways:

1. Risk Avoidance: Risk Avoidance means to avoid taking or choosing of less risky business/project. For example one may avoid investing in stock market due to price volatility in stock prices and may prefer to invest in debt instruments.

2. Risk Retention/absorption: It is the handling the unavoidable risk internally and the firm bears/ absorbs it. Usually, retained risks occur with greater frequency, but have a lower severity. An insurance deductible is a common example of risk retention to save money, since a deductible is a limited risk that can save money on insurance premiums for larger. There are two types of retention methods for containing losses as under:

- Active Risk Retention: Where the risk is retained as part of deliberate management strategy after conscious evaluation of possible losses and causes.
- Passive Risk Retention: Where risk retention occurred through negligence. Such type of retaining risk is unknown or because the risk taker either does not know the risk or considers it a lesser risk than it actually is.

3. Risk Reduction: In many ways physical risk reduction (or loss prevention, as it is often called) is the best way of dealing with any risk situation and usually it is possible to take steps to reduce the probability of loss. The ideal time to think of risk reduction measures is at the planning stage of any new project when considerable improvement can be achieved at little or no extra cost. The cautionary note regarding risk reduction is that, as far as possible expenditure should be related to potential future savings in losses and other risk costs; in other words, risk prevention generally should be evaluated in the same way as other investment projects.

4. Risk Transfer: This refers to legal assignment of cost of certain potential losses to another. The insurance of 'risks' is to occupy an important place, as it deals with those risks that could be transferred to an organization that specialises in accepting them, at a price. Usually, there are 3 major means of loss transfer viz.,

- By Tort,
- By contract other than insurance,
- By contract of insurance.

The main method of risk transfer is insurance. The value of the insurance lies in the financial security that a firm can obtain by transferring to an insurer, in return for a premium for the risk of losses arising from the occurrence of a specified peril. Thus, insurance substitutes certainty for uncertainty. Insurance does not protect a firm against all perils but it offers restoration.

RISK MITIGATION STRATEGY

- Risk mitigation is defined as taking steps to reduce adverse effects.
- Risk mitigation is the process by which an organization introduces specific measures to minimize or eliminate unacceptable risks associated with its operations.
- Risk mitigation measures can be directed towards reducing the severity of risk consequences, reducing the probability of the risk materializing, or reducing the organizations exposure to the risk.

- The risk mitigation step involves development of mitigation plans designed to manage, eliminate, or reduce risk to an acceptable level.
- Once risks have been identified and assessed, the strategies to manage the risk fall into one or more of the following categories:

(i) Transfer Risk:

- Different agencies work together and these agencies take care to transfer risk in their areas to another agency which is better equipped to take care of a risk for a consideration.
- Here the concept of core competence curves in and whenever a particular agency, individual or a firm finds that it is dealing in an area where it does not have the core competence to deal with it seeks the help of another agency which has the specific core competence to transfer its own risk.
- The risk may be in the form of loss of reputation or sub quality performance and this risk is taken care of through transfer.

(ii) Tolerate Risk or Risk Retention:

- It is retention of the risk.
- It is accepting the loss when it occurs.
- True self insurance falls in this category.
- Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained.
- All risks that are not avoided, reduced or transferred are retained by default.
- War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured.

(iii) Reduce Risk:

- By far the greater number of risks will belong to this category.
- The purpose of treatment is not necessarily to obviate the risk, but more likely to contain the risk to an acceptable level.
- Outsourcing could be an example of risk reduction if the outsourcer can demonstrate higher capability at managing or reducing risks.

- In this case companies outsource only some of their departmental needs.
- This way, the company can concentrate more on business development without having to worry as much about the manufacturing process.
- Modern software development methodologies reduce risk by developing and delivering software incrementally.

(iv) Avoid Risk:

- This method results in complete elimination of exposure to loss due to a specific risk.
- It can be established by either avoiding to undertake the risky project or discontinuance of an activity to avoid risk.
- This means that no risky projects are undertaken.
- Alternatively, a project may be abandoned midway to mitigate the risk while handling a project.
- It is not performing an activity which could carry risk.
- An example would be not buying a property or business in order to not take on the liability that comes with it.
- Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed.
- Not entering a business to avoid the risk of loss also avoids the possibility of earning profits.

(v) Combine Risk:

- When the business faces two or three risks the overall risk is reduced by combination.
- This strategy is suitable mainly in the areas of financial risk. Different financial instruments say, shares and debentures are taken in a single portfolio to reduce the risk.

(vi) Sharing Risk:

- Insurance is a method of sharing risk for a consideration.
- For example, by paying insurance premium the company shares the risk with companies and the insurance companies themselves share their risk by doing re-insurance.

(vii) Hedging Risk:

- Exposure of funds to fluctuations in foreign exchange rates, prices etc., bring about financial risks resulting in losses or gain.
- The downside risk is often taken care.

MAINTAINING THE RISK STRATAGY

- It has already been noted that the risk environment of any organization is constantly changing and developing.
- The risk management process is therefore a dynamic and ongoing one.
- The process must allow for periodic review of risks and for consequent adjustment of the control response.
- Whatever option is adopted, it is important that those charged with control of the risk management process should regularly review it.
- One useful technique for doing this is to actively review the risks associated with each of the organizational objectives.
- A key tool is the use of ongoing Control and Risk Self Assessment (CRSA) procedures.

FRAUD RISK MANAGEMENT

- Fraud is a deliberate action to deceive another person with the intention of gaining some things.
- Fraud can loosely be defined as "any behavior by which one person intends to gain a dishonest advantage over another".
- Section 25 of the Indian Penal Code, 1860 defines the word, "Fraudulently", which means, a person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.
- Further according to section 17 of the Indian Contract Act, 1872, 'fraud' means and includes any of the following acts committed by a party to a contract, or with his connivance (intentional active or passive acquiescence), or by his agent with intent to deceive or to induce a person to enter into a contract.

1. The suggestion that a fact is true when it is not true and the persons making the suggestion does not believe it to be true;
2. The active concealment of a fact by a person having knowledge or belief of the fact;
3. A promise made without any intention of performing it;
4. Any other act fitted to deceive;
5. Any such act or omission as the law specially declares to be fraudulent.

- The Companies Act 2013 has also explained fraud. Explantion to Section 447 defines "fraud", which reads as under: "fraud" in relation to affairs of a company or anybody corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss.
- For prevention of the fraud, there should be in existence a robust internal check and control systems.
- For example in banking there is a concept of 'maker' and 'checker'. The day today transactions are entered by the maker and another person validates the transactions. So it is a self-balancing system.
- Further the internal/ concurrent audit also helps in early detection of the frauds.
- The management should be pro-active in fraud related matter. A fraud is usually not detected until and unless it is unearthed.
- Fraud Risk Management Policy should be incorporated, aligned to its internal control and risk management.
- Such policy/plan protects the company from any kind of uncertain happening which leads the company to a huge loss or damage (brand reputation, financial loss, assets).
- The Fraud Risk Management Policy will help to strengthen the existing anti-fraud controls by raising the awareness across the Company and

(i) Promote an open and transparent communication culture
(ii) Promote zero tolerance to fraud/misconduct
(iii) Encourage employees to report suspicious cases of fraud/misconduct.
(iv) Spread awareness amongst employees and educate them on risks faced by the company.

- Such a policy may include the following:

- Defining fraud: This shall cover activities which the company would consider as fraudulent.
- Defining Role & responsibilities: The policy may define the responsibilities of the officers who shall be involved in effective prevention, detection, monitoring & investigation of fraud.
- Communication channel: Encourage employees to report suspicious cases of fraud/misconduct.
- Disciplinary action: After due investigations disciplinary action against the fraudster may be considered as per the company's policy.
- Reviewing the policy: The employees should educate their team members on the importance of complying with Company's policies & procedures and identifying/ reporting of suspicious activity, where a situation arises.

Reporting of Fraud Under Companies Act, 2013

- The Companies Act, 2013 has introduced many new reporting requirements for the statutory auditors of companies.
- One of these requirements is given under the Section 143(12) of the Companies Act, 2013 which requires the auditors to report to the Central Government about the fraud/suspected fraud committed against the company by the officers or employees of the company.
- Consequence of non-compliance: if any auditor, cost accountant or company secretary in practice do not comply with the provisions, he shall be punishable with fine which shall not be less than one lakh rupees but which may extend to twenty-five lakh rupees.
- Section 143(12) includes only fraud by officers or employees of the company and does not include fraud by third parties such as vendors and customers.

Reputation risk management

- The Reserve Bank of India has defined the Reputation Risk as the risk arising from negative perception on the part of customers, counterparties, shareholders, investors, debt-holders, market analysts, other relevant parties or regulators that can adversely affect a bank's ability to maintain existing, or establish new, business relationships and continued access to sources of funding (eg through the interbank or securitization markets).
- Reputational risk is multidimensional and reflects the perception of other market participants.

Loss of Reputation has long lasting damages like:

- It destroys the Brand Value
- Steep downtrend in share value.
- Ruined of Strategic Relationship
- Regulatory relationship is damaged which leads to stringent norms.
- Recruitment to fetch qualified staff as well the retention of the old employees becomes difficult.

For managing the reputation risk, the following principles are worth noting:

- Integration of risk while formulating business strategy.
- Effective board oversight.
- Image building through effective communication.
- Promoting compliance culture to have good governance.
- Persistently following up the Corporate Values.
- Due care, interaction and feedback from the stakeholders.
- Strong internal checks and controls
- Peer review and evaluating the company's performance.
- Quality report/ newsletter publications
- Cultural alignments

Responsibility of Risk Management

- Section 134(3) (n) of the Companies Act, 2013 provides that a statement indicating development and implementation of a risk management policy for the company including identification of elements of risk, which in the opinion of the Board may threaten the existence of the company.
- SEBI (LODR) Regulations, 2015 also provides that company shall lay down procedures to inform Board members about the risk assessment and minimization procedures. The Board shall be responsible for framing, implementing and monitoring the risk management plan for the company.
- The Risk Management Plan must include all elements of risks.

- Risk management policies should reflect the company's risk profile and should clearly describe all elements of the risk management and internal control system and any internal audit function.
- A company should have Chief Risk Officer with the vision and the diplomatic skills to forge a new approach. He may be supported by "risk groups" to oversee the initial assessment work and to continue the work till it is completed.
- Regulation 21 of SEBI (LODR) Regulations, 2015, requires that every listed company should have a Risk Management Committee.

Role Of Company Secretary In Risk Management

- The company secretaries are governance professionals whose role is to enforce a compliance framework to safeguard the integrity of the organization and to promote high standards of ethical behavior.
- He has a significant role in assisting the board of the organization to achieve its vision and strategy.
- However the functions of a Governance Professional include:
- Advising on best practice in governance, risk management and compliance.
- Championing the compliance framework to safeguard organizational integrity.
- Promoting and acting as a 'sounding board' on standards of ethical and corporate behavior.
- Balancing the interests of the Board or governing body, management and other stakeholders.
- The listing agreement also provides for the establishment of the Risk Management Committee as per Regulations. Since it is the part of the Corporate Governance norms and non-compliance of the same is to be reported by the Company Secretary.
- In terms of Section 203(1)(ii), a Company Secretary is a Key Managerial Person. Hence being a top level officer and board confidante, a Company Secretary can pay a role in ensuring that a sound Enterprise wide Risk Management [ERM] which is effective throughout the company is in place.
- The board of directors may have a risk management sub-committee assisted by a Risk Management Officer.
- As an advisor to the board in ensuring good governance, a Company Secretary shall ensure that there is an Integrated Framework on which a strong system of internal control is built.

- Such a Framework will become a model for discussing and evaluating risk management efforts in the organization.
- Risk and control consciousness should spread throughout the organization.
- It will also create awareness about inter- relationships of risks across business units and at every level of the organization.

RISK GOVERNANCE

- Risk governance includes the skills, infrastructure (i.e., organization structure, controls and information systems), and culture deployed as directors exercise their oversight.
- Good risk governance provides clearly defined accountability, authority, and communication/reporting mechanisms.
- The board shall have to identify the extent and type of risks it faces and the planning necessary to manage and mitigate the same for ensuring growth for the benefit of all the stakeholders.
- Therefore, the Board has to define a risk philosophy and the extent to which it is willing to accept any consequence of taking of risks by the organisation and its functionaries in its day to day functioning.
- A strengthened management information system (MIS) supported by robust information technology platform is a necessary pre-requisite for enhancing Board efficiency in oversight and decision making.
- Strong MIS facilitates risk reporting to the boards in an effective and comprehensive manner, which in turn enhances transparency and causes informed decision taking.
- Robust information technology systems are a necessary condition for supporting the MIS framework.
- In addition to prescribing the risk appetite for the company, the board also needs to lay down appropriate risk strategy and ensure that this is institutionalized throughout the organization.
- The Boards must get much more intimately involved in risk matters and have a firmer understanding of the key risks faced by the business.
- Effective risk governance also demands that each director is aware of the breadth of risks faced by the company.

- The risk management committees have an important role to play in the overall risk governance framework. Apart from monitoring the company's strategic-risk profile on an on-going basis, such committees would also be responsible for defining the company's overall risk appetite; approving major transactions above a company's risk threshold, and; establishing limit structures and risk policies for use within individual businesses.
- Boards may lean on the expertise of outside consultants to help them review company risk management systems and analyze business specific risks.
- The annual risk management review should include communication from management about lessons learned from past mistakes.
- Risk oversight is the responsibility of the entire Board and the same can be achieved through a review mechanism which inter-alia could include:

1. Developing policies and procedures around risk that are consistent with the organization's strategy and risk appetite.
2. Taking steps to foster risk awareness.
3. Encourage an organizational culture of risk adjusting awareness
4. Maintenance of a Risk Register
5. A compliance certificate on the identification of risks and establishment of mitigation measures.

RISK MANAGEMENT FRAMEWORK AND STANDARDS

- Risk management is a fast-moving discipline and standards are regularly supplemented and updated.
- The different standards reflect the different motivations and technical focus of their developers, and are appropriate for different organisations and situations.
- Standards are normally voluntary, although adherence to a standard may be required by regulators or by contract.

1) Enterprise Risk Management – Integrated Framework

- In response to a need for principles-based guidance to help entities design and implement effective enterprise- wide approaches to risk management, Committee of Sponsoring

Organizations of the Treadway Commission (COSO) issued the Enterprise Risk Management – Integrated Framework in 2004.

- This framework defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management.
- The guidance introduces an enterprise-wide approach to risk management as well as concepts such as: risk appetite, risk tolerance, portfolio view.
- The Enterprise Risk Management – Integrated Framework which is one of the most widely recognized and applied enterprise risk management frameworks in the world.
- It provides a principles-based approach to help organizations design and implement enterprise-wide approaches to risk management.

Enterprise risk management encompasses:

- Aligning risk appetite and strategy – Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- Enhancing risk response decisions – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.
- Reducing operational surprises and losses – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- Identifying and managing multiple and cross-enterprise risks – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.
- Seizing opportunities – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
- Improving deployment of capital – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

Components of Enterprise Risk Management

- Internal Environment – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk

management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

- Objective Setting – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
- Event Identification – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities.
- Opportunities are channeled back to management's strategy or objective-setting processes.
- Risk Assessment – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- Risk Response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- Control Activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- Information and Communication – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- Monitoring – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

- Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

CASE STUDY

INFOSYS: MITIGATING WATER RISK AT INDIA-BASED HUBS

- For over 15 years, Infosys - provider of business consulting, IT and outsourcing services - has maintained a plan to mitigate its operational risks related to water supply.
- Collaboration between the enterprise risk management (ERM) and sustainability functions enables Infosys to address risks at the facility-level while conducting overall monitoring activities at the enterprise level.
- Implementing measures to save and monitor water availability makes Infosys a steward of its environment while also delivering value to its business and its stakeholders.

Risk of water scarcity

- Infosys employs more than 200,000 people at 116 global development centers, with 40 of its largest in India.
- The rapidly growing Indian population and increased demand for water resources has created a growing concern over water availability in the country.
- Because of its large campuses in major Indian cities, Infosys considers water stress and scarcity a significant near-term risk to its business operations India.
- Water supports the company's human capital (i.e., cooking, cleaning, bathrooms and drinking) at their campuses and is also necessary for landscaping and cooling towers.
- Water shortages during dry periods have the potential to halt operations at affected campuses, which would negatively impact the company's ability to fulfill contractual obligations with customers and achieve performance goals.

Response to water risks

- To address water risks, Infosys encourages collaboration between ERM and sustainability functions.
- The Infosys sustainability team conducts detailed risk assessments at individual facility locations while ERM conducts assessments at the corporate level.
- The company undertakes an iterative process: first assessing inherent risk and subsequently applying control measures and assessing residual risk.
- Infosys chooses among five risk response types in line with COSO's ERM framework: accept, avoid, pursue, reduce, escalate and share.

- In locations where water scarcity risk is high, avoiding or accepting the risk is not an option. In these cases, the company chooses to "reduce" the risk.
  - Infosys uses site-based water risk assessments and root cause analyses to develop action plans for reducing risks to "low" or "moderate" levels.
  - If actions taken do not fully mitigate the risks, Infosys may decide to reduce the impact by temporarily moving business operations or by reducing their footprint in the affected development center.
  - Infosys emphasizes the use of root cause analysis so that action plans focus on the underlying problem rather than symptoms.
  - In the case of water scarcity, this approach has helped them determine what is influencing the water shortages: water access, lack of water storage or other issues.
  - Following this analysis, the company implements mitigation measures to address the root cause and reduce risks to acceptable levels.

These measures have included:

- Water conservation through reduce, recycle and reuse measures (e.g., water efficient fixtures, wastewater treatment)
- Aquifer recharge through injection wells
- Rainwater harvesting and reuse
- Construction of underground reservoirs that hold water to last for at least five days across locations
- Efficiency programs led by smart water metering program that monitors water consumption and encourages water use reduction

- These measures are designed so that Indian campuses can sustain themselves for seven days using stored rainwater and potable water in the case of extreme water shortages.

Monitoring water scarcity

Sustainability and ERM work together to monitor water scarcity across the enterprise.

Sustainability teams collect and use the following types of data to monitor and assess water risk at its campuses:

- Rainfall data over a 10-year period for each geographic area;

- Water table data for each geographic area;
- Storage capacity of rainwater on each campus;
- Availability and cost of water via water tankers for delivery;
- Freshwater usage from municipalities, private providers, ground water and rainwater

- Corporate ERM monitors water scarcity as an emerging risk. It tracks an enterprise-wide metric of "per capita water consumption" using information provided by sustainability teams.
- Per capita water consumption is calculated by dividing the average monthly water consumption at Infosys locations by the average employee count per month, which is the sum of the swipe counts for employees and support staff in the Infosys offices.
- Corporate ERM actively tracks this metric to determine if water risk will become a higher corporate level priority in future years.

Business outcomes of managing water risk

The company's water risk management strategy in India enables the company to:

- Open new campuses in locations where competitors may not be able to operate due to water shortages.
- Maintain continuity in operations using stored water in times of scarcity, which helps maintain customer confidence and profitability.

- The outcomes stem from Infosys' organizational structure, which encourages sustainability to assess and mitigate risk at the local level while ERM maintains an enterprise wide view.
- Further, root cause analysis of local water issues empowered Infosys to develop effective responses and mitigation approaches at individual campuses.

Limitations

- Human judgment in decision making can be faulty,
- Decisions on responding to risk and establishing controls need to consider the relative costs and benefits,
- Breakdowns can occur because of human failures such as simple errors or mistakes,
- Controls can be circumvented by collusion of two or more people, and
- Management has the ability to override enterprise risk management decisions.

These limitations preclude a board and management from having absolute assurance as to achievement of the entity's objectives.

Roles and Responsibilities

- Everyone in an entity has some responsibility for enterprise risk management.
- The chief executive officer is ultimately responsible and should assume ownership.
- Other managers support the entity's risk management philosophy, promote compliance with its risk appetite, and manage risks within their spheres of responsibility consistent with risk tolerances.
- A risk officer, financial officer, internal auditor, and others usually have key Support responsibility.
- Other entity personnel are responsible for executing enterprise risk management in accordance with established directives and protocols.
- The board of directors provides important oversight to enterprise risk management, and is aware of and concurs with the entity's risk appetite.
- A number of external parties, such as customers, vendors, business partners, external auditors, regulators, and financial analysts often provide information useful in effecting enterprise risk management, but they are not responsible for the effectiveness of, nor are they a part of, the entity's enterprise risk management.

ISO 31000: INTERNATIONAL STANDARD FOR RISK MANAGEMENT

- ISO 31000 is the international standard for risk management. This standard is published on the 13th of November 2009.
- By providing comprehensive principles and guidelines, this standard helps organizations with their risk analysis and risk assessments.
- ISO 31000 applies to most business activities including planning, management operations and communication processes.
- By implementing the principles and guidelines of ISO 31000 in organization, the organisation can improve operational efficiency, governance and stakeholder confidence, while minimising losses.
- This international standard also helps to boost health and safety performance, establish a strong foundation for decision making and encourage proactive management in all areas.

Scope

- ISO 31000:2009 provides generic guidelines for the design, implementation and maintenance of risk management processes throughout an organization.
- This approach to formalizing risk management practices will facilitate broader adoption by companies who require an enterprise risk management standard that accommodates multiple 'silo-centric' management systems.
- ISO 31000 is not developed for a particular industry group, management system or subject matter field in mind, rather it provides best practice structure and guidance to all operations concerned with risk management.
- The scope of this approach to risk management is to enable all strategic, management and operational tasks of an organization throughout projects, functions, and processes be aligned to a common set of risk management objectives.

Accordingly, ISO 31000:2009 is intended for a broad stakeholder group including:

- executive level stakeholders
- appointment holders in the enterprise risk management group
- risk analysts and management officers
- line managers and project managers
- compliance and internal auditors
- independent practitioners.

Benefits of ISO 31000

ISO 31000 is designed to help organizations:

- Increase the likelihood of achieving objectives
- Encourage proactive management
- Be aware of the need to identify and treat risk throughout the organization
- Improve the identification of opportunities and threats
- Comply with relevant legal and regulatory requirements and international norms
- Improve financial reporting
- Improve governance
- Improve stakeholder confidence and trust

- Establish a reliable basis for decision making and planning
- Improve controls
- Effectively allocate and use resources for risk treatment
- Improve operational effectiveness and efficiency
- Enhance health and safety performance, as well as environmental protection
- Improve loss prevention and incident management
- Minimize losses
- Improve organizational learning
- Improve organizational resilience.
- Proactively improve operational efficiency and governance

Managing risk

ISO 31000:2009 gives a list on how to deal with risk:

1. Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
2. Accepting or increasing the risk in order to pursue an opportunity
3. Removing the risk source
4. Changing the likelihood
5. Changing the consequences
6. Sharing the risk with another party or parties (including contracts and risk financing)
7. Retaining the risk by informed decision

STRATEGIC RISK MANAGEMENT

- Strategic risk management is a crucial but often overlooked aspect of enterprise risk management (ERM).
- Studies of the largest public companies indicate that strategic risks account for approximately 60 percent of major declines in market capitalization. Operational risks have just half that impact (about 30 percent), and financial risks generate about 10 percent.

Meaning of Strategic Risk

- Strategic risk management is the process of identifying, quantifying, and mitigating any risk that affects or is inherent in a company's business strategy, strategic objectives, and strategy execution.
- These risks may include:
  - Shifts in consumer demand and preferences
  - Legal and regulatory change
  - Competitive pressure
  - Merger integration
  - Technological changes
  - Senior management turnover
  - Stakeholder pressure

Strategic risk is a bell curve

- Like any risk, strategic risk falls along a classic bell curve, with results along the x-axis and likelihood along the y-axis.
- The expected result of a given strategy would represent the peak of this curve. Most strategic planning considers only this peak while ignoring the slopes to either side.
- But imagine two strategic initiatives, each with a similar expected result. One falls along a narrow, steep curve, indicating a low risk of failure and little upside opportunity. The other is represented by a wider bell, with greater chances of both under- and over-performance.
- Which to choose? The answer depends on an individual company's appetite for risk.

Strategic risk management: shifting the curve

- Now imagine a third curve with that same expected result.
- This one rises steeply from the left but slopes more gently downward on the right.
- Here, downside risk has been minimized, and upside opportunity increased. That is the goal of strategic risk management: to shape the curve in a way that favors success.

Measuring and managing strategic risk

- A key tenet of ERM is measuring risk with the same yardsticks used to measure results. In this way, companies can calculate how much inherent risk their initiatives contain.

Strategic risk can be measured with two key metrics:

1. Economic capital is the amount of equity required to cover unexpected losses based on a predetermined solvency standard. Typically, this standard is derived from the company's target debt rating. Economic capital is a common currency with which any risk can be quantified. Importantly, it applies the same methodology and assumptions used in determining enterprise value, making it ideal for strategic risk.
2. Risk-adjusted return on capital (RAROC) is the anticipated after-tax return on an initiative divided by its economic capital. If RAROC exceeds the company's cost of capital, the initiative is viable and will add value. If RAROC is less than the cost of capital, it will destroy value.

Managing strategic risk involves five steps which must be integrated within the strategic planning and execution process in order to be effective:

1. Define business strategy and objectives. There are several frameworks that companies commonly use to plan out strategy, from simple SWOT analysis to the more nuanced and holistic Balanced Scorecard. The one thing that these frameworks have in common, is their failure to address risk. It is crucial, then, that companies take additional steps to integrate risk at the planning stage.
2. Establish key performance indicators (KPIs) to measure results. The best KPIs offer hints as to the levers the company can pull to improve them. Thus, overall sales makes a poor KPI, while sales per customer lets the company drill down for answers.
3. Identify risks that can drive variability in performance. These are the unknowns, such as future customer demand, that will determine results.
4. Establish key risk indicators (KRIs) and tolerance levels for critical risks. Whereas KPIs measure historical performance, KRIs are forward-looking leading indicators intended to anticipate potential roadblocks. Tolerance levels serve as triggers for action.
5. Provide integrated reporting and monitoring.

RISK MANAGEMENT AND INTERNAL CONTROLS

- Risk management focuses on identifying threats and opportunities, while internal control helps counter threats and take advantage of opportunities.
- Proper risk management and internal control assist organizations in making informed decisions about the level of risk that they want to take and implementing the necessary controls to effectively pursue their objectives.
- Successful organizations integrate effective governance structures and processes with performance-focused risk management and internal control at every level of an organization and across all operations.
- The risk profile of a company may be represented through a Risk Register, a suggestive template of which is illustrated below:

Sl.No	Risk Area	Key risks	Root cause	Mitigation measures
1	Business Risk	Decreasing market share	Lack of innovation, market survey etc.,	Keeping a vigil on latest developments and continuous monitoring
2	Financial risk	Leveraging capital structure and the cash flows	Inability to assess the appropriate funding requirements	Adoptiong a Resource planning policy
3	Regulatory and Compliance Risk	Noncompliance of applicable laws	Not keeping abreast of the latest changes in the Regulatory environment	Knowledge updation & maintenance of a robust compliance check list

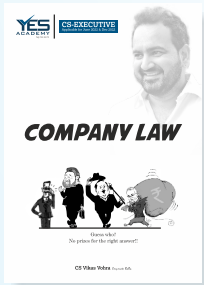
RISK MATRIX

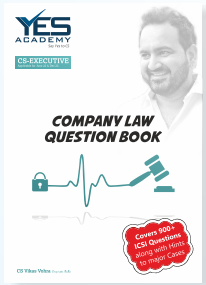
- Risk Matrix is a matrix that is used during Risk & Control Self Assessment (RCSA) activity to define the various levels of risk at each stage, activity, process and sub-process.
- Risk Matrix comprises of :

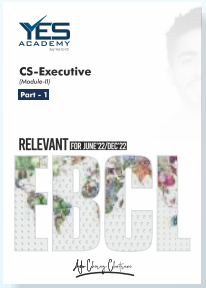
1. Impact analysis
2. Likelihood

Our Publications

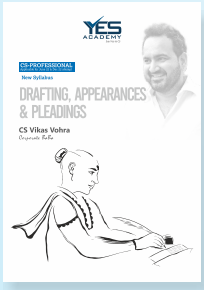
CS Executive

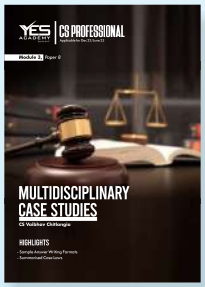


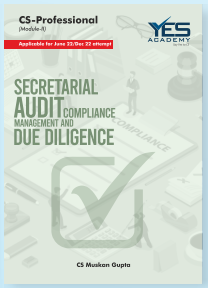




CS Professional







For demo lectures *visit our Youtube Channel*

#yesacademyforcs

Video lectures available *for all subjects of* **CS Course** *at all levels.*

Website: www.yesacademy.co.in

Adv. Chirag Chotrani

Adv Chirag Chotrani is a young yet experienced faculty in the field of Law. From being the topper of his batch, to creating many All India Rankers in the Field of Company Secretary, Chirag has proved his academic capabilities time and again.

Chirag is a Commerce and Law Graduate and holds a Masters Degree in Corporate Law, earned specialisation in Corporate Laws and in Arbitration Law and is currently completing his PHd in Corporate Laws.

The ease with which this faculty introduces the concepts is commendable and every student who has studied under him has passed in his subjects with flying colours. From the start of his career till now he has always been into teaching and has served in many Prestigious Institutions and is presently the Top Educator for CS Category at UNACADEMY Platform which currently caters to 10 Million students across the country.

YES ACADEMY
Say Yes to CS

Office 30A, 1st Floor, Gate No. 1, Kumar Prestige Point,
Behind BSNL Office, Bajirao Road, Shukrawar Peth, Pune - 411 002

8888 235 235, 8888 545 545, 8888 569 569, 8888 280 280
yesacademypune@gmail.com

yesacademy.co.in
/yesacademyforcs
/yesacademyforcs
/yesacademyforcs