

Risk Management

Lesson 18

KEY CONCEPTS

■ Risk Analysis ■ Cyber Risk ■ Social Risk ■ Financial Risk ■ Market Risk ■ Internal Audit

Learning Objectives

To understand:

- Risk Management
- Risk Identification
- Risk Analysis
- Risk Measurement
- Risk Mitigation
- Risk Elimination
- Importance of Risk Management Committee
- Role of Internal Audit
- Internal control, Material Risk and Opportunity Assessment
- Reputation Risk, Climate Risk, Fraud Risk Management
- Business Continuity Plan with Case Study
- Risk Related Disclosures
- Crisis Management, Disaster Risk Management
- Relationship between Business Continuity Plan, Crisis Management and Disaster Recovery Plan
- ESG Risk assessment
- Cyber Risk Management
- Fundamentals of cyber security threats and countermeasures
- Identifying most critical assets and threats
- Assessing Cyber Security Risks and
- Implementing a Cyber Risk Management Programme
- Role of CS in Risk Management
- Case studies in Risk Management

- Introduction
- Risk Management
- Advantages of Risk Management
- Steps in Risk Management Process
- Risk Mitigation
- Need for a CRM Framework in India
- Fraud Risk Management
- Fraud risk management processes
- Role of Company Secretary in Risk Management
- Internal Control
- Crisis Management
- ESG Risk Assessment
- Cyber Risk Management
- Case Studies
- Lesson Round-Up
- Glossary
- Test Yourself
- List of Further Readings
- Other References

INTRODUCTION

Key Concepts

“Today’s fast-paced business environment encounters a complex and ever-changing risk landscape that may negatively impact the organizational value. The only way to respond to it is by having a dynamic and holistic perspective of risk management approach to ensure business continuity.”

– Jack Zahran, President, Pinkerton

Most businesses now consider risk management to be essential. However, even within the same industry, organisations can have diverse structures for risk management. What then is risk? The term “risk” has come to be used in the business world to refer to anything that prevents an organization from achieving its goals.

According to 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”.

While there is some risk in every business, organisations and entrepreneurs must be willing to take risks because there can be no significant return without them. Risk cannot be avoided, like stress, and one must learn to deal with it. Risk can, at most, be controlled or reduced. This does not suggest taking a risk only for the purpose of taking a risk, but to reap the final benefits, risk management must be understood at every stage. However, both internally and externally, the cost of poor risk management is still frequently underestimated. This cost also includes the time required to manage a situation where risks were poorly assessed and managed. It might be accurate to state that no sustainable advantage is achievable without “risk management.”

The risk can be defined from various perspectives the below is the definition of risk from Finance Perspective: ‘The probability that an actual return on an investment will be lower than the expected return’.

RISK MANAGEMENT

The phrase “risk management” is used to refer to the procedures that help organizations identify, understanding, assessing, and managing their risks will increase the likelihood of their success while minimising the consequences and chances of failure. Effective risk management helps a company or organisation validate its compliance with corporate governance principles and reassures shareholders, customers, employees, other stakeholders, and society at large that a business is being managed properly governing principles.

All organisations, no matter how big or little, should practise risk management. Effective risk management procedures promote accountability, performance evaluation, and compensation, and they can boost productivity throughout the entire organisation at all levels. A thorough knowledge and comprehension of the organisation (internally and externally) and the business processes are necessary for risk management.

Better risk management strategies offer early warning signs so that the problem can be solved quickly. Traditional concepts solely viewed natural disasters like fires, earthquakes, and floods as risks, and they presumptively reduced those risks by maintaining safeguard equipment and other measures. However, new and different kinds of hazards have evolved as a result of the fast-paced developments in technology, business dimensions and complexity, regulatory changes, and environmental concerns. Therefore, managing different forms of risks has become crucial in the age of the rapidly evolving global economy, numerous regulatory compliances, cross-border commercial activities, and the need to maintain the survival, viability, and sustainability of businesses.

The company strategy incorporates risk management. It is an essential management tool for protecting company assets so they can be used productively. The goal of risk management is to enable an organisation to minimise losses and maximise possibilities by establishing the context, detecting, analysing, assessing, treating, monitoring, and communicating risks connected with any action, function, or process.

ADVANTAGES OF RISK MANAGEMENT

Strategic planning involves risk management heavily. It is crucial to effective project management. The main objectives of a successful risk management strategy are to detect and evaluate potential hazards. Following are some of the main benefits of risk management:

- In the long run, risk management always saves a large amount of money and reduces the need for firefighting. It creates solid contingency plans.
- It can aid in making plans and getting ready for chances that present themselves throughout a project or business.
- Strategic and corporate planning is enhanced by risk management. By reducing legal action or avoiding breakages, it lowers costs.
- It establishes greater dependability among the interested parties, resulting in increased reputation.
- Reliable Risk Management procedures comfort significant stakeholders across the entire firm.

STEPS IN RISK MANAGEMENT PROCESS

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

- Risk Identification
- Risk Analysis
- Risk Assessment
- Handling of Risk

Risk Identification

Effective risk management depends on accurate risk identification, hence this is the first stage of the risk management strategy. Risk managers will not be able to control these unidentified risks if they are unsuccessful in recognising all potential losses or gains that pose a threat to the firm. Classifying organisational risks based on their various categories is the first responsibility of risk management. Establishing the essential surveillance areas both inside and outside of the organisation is the first stage in planning the implementation of the risk management function. Then, specific risk identification tasks must be delegated to the departments and employees.

Ensuring that all potential project risks are detected is the goal of the risk identification process. The ultimate goal of risk identification is to maximise the benefits of project possibilities while minimising the negative effects of project setbacks and threats. The team is better able to accomplish the project's time, schedule, and quality goals when they are aware of potential project risks, which lowers the amount of surprises during project delivery. Finally, the goal of risk identification is to supply data for the following stage of the risk management process.

Process of Risk Identification

Taking an inventory of the potential project risks that can have an impact on project delivery is the first step in the risk identification process. For effective risk management throughout the project, this stage is essential. Project managers' uncertainty is decreased by the outputs of the risk identification process, which are used as an input for risk analysis. Throughout the course of a project, this iterative process must be continuously repeated. To ensure that all potential dangers are found, the procedure must be rigorous. The following actions should be taken as part of an efficient risk detection process:

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.

Risk Analysis

The analysis of the risk, which comes after the identification of the risk factors, aids in the detection and management of prospective issues that could jeopardise important business efforts or projects.

To do a risk analysis, first list the potential dangers and then calculate the likelihood that they'll come to pass. The analysis ought to be impartial and sector-specific. The scenario-based analysis may be used inside the industry, taking into account potential outcomes and alternative strategies for achieving the specified goal.

Risk analysis can be difficult since it calls for the use of specific data, including project plans, financial data, security measures, marketing projections, and other pertinent data. However, it's a crucial tool for planning and one that could save time, money, and reputations.

Risk analysis is useful in many situations like:

- While planning projects, to help in anticipating and neutralizing possible problems.
- While deciding whether or not 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 / popped-up before the decision making and implementing authority.

Process of Risk Analysis

The risk analysis includes the following two process:

1. Identify Threats
2. Estimate Risk

Identify Threats: Identification of current and potential hazards is the first stage in risk analysis. These might originate from a wide range of sources. For example, they might 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.

Estimate Risk: After threats have been identified, it is necessary to determine their likelihood of materialising as well as their potential impact. Making the best assessment of the likelihood that the event will occur and multiplying it by how much it will cost to get things back on track are two methods of doing this. “Risk Value is the product of Event Probability and Event Cost”.

Risk Assessment

Businesses determine the importance of each risk to achieving their overall objectives through risk assessment. Enterprises need a practical, long-lasting, and simple risk assessment procedure in order to achieve this. It's important to keep the process organised and disciplined. It must be properly scaled for the size, complexity, and geographic reach of the company.

It's critical to identify if a risk is inherent, residual, or both when evaluating it. The risk to an entity that exists even in the absence of any management activities that might change the likelihood or severity of the risk. The risk that remains after management has addressed the problem is known as residual risk.

Process of Risk Assessment



1. Develop Assessment Criteria

The first step in the risk assessment process is to create a standard set of evaluation standards that will be used by all business units, corporate departments, and major capital projects. The impact and possibility of risks and opportunities are often considered while evaluating them. Many businesses understand the value of considering risk along other dimensions like vulnerability and onset speed.

2. Assess risks

Using the established criteria, values are assigned to each risk and opportunity as part of the risk assessment process. Prior to treating the most significant risks and opportunities that lend themselves to quantification, the risks and opportunities are first initially screened using qualitative methodologies (not all risks are meaningfully quantifiable). Each danger and opportunity is evaluated using the descriptive scales established in the preceding section as part of a qualitative assessment. Using information from various sources, quantitative analysis involves numerical numbers for both impact and likelihood.

The most popular qualitative assessment methods are benchmarking, questionnaires, cross-functional workshops, interviews, and scenario analysis. Benchmarking, scenario analysis, creating forward-looking point estimates (using deterministic models), and finally creating forward-looking distributions are all examples of quantitative approaches (probabilistic models). Causal at-risk models used to project gross profit margins, cash flows, or earnings over a certain time horizon at specified confidence levels are among the most effective probabilistic models from an enterprise-wide perspective.

3. Assess risk interactions

Risks don't exist by themselves. Businesses now understand how crucial it is to manage risk interactions. Even risks that seem modest on their own have the capacity to provide big opportunities or great harm when they interact with other circumstances and events. Because of this, businesses are inclining toward a holistic or integrated view of risks utilising tools like risk interaction matrices, bow-tie diagrams, and aggregated probability distributions.

4. Prioritize risks

The next stage, prioritising for risk response and reporting to various stakeholders, can be accomplished by viewing the risks as a whole portfolio once they have been assessed and their interconnections have been documented. By comparing the degree of risk to predetermined target risk levels and tolerance limits, risk prioritisation establishes the priorities for risk management. The prioritising aids in giving senior management and the board focus when addressing and paying attention to key risks, even though each risk captured may be significant to management at the function and business unit level.

5. Response to Risks

The outcomes of the risk assessment process are then used as the main input for risk responses, where accept, minimise, share, or avoid response choices are considered, cost-benefit evaluations are carried out, a response strategy is defined, and risk response plans are created.

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.

Handling of Risk

Risk ownership needs to be distributed. The people handling risks need to have their responsibilities and accountability allocated. When a danger materialises, the affected parties should note it and inform the

appropriate authorities so that prompt action can be taken to reduce it. Risk management options include the following:

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

Because insurance cannot be acquired for this sort of risk or because it may be too expensive to cover the risk, the company handles the inevitable risk internally instead, which is far more cost-effective. Retained dangers typically occur more frequently but are less serious. Since a deductible is a small risk that can reduce insurance premiums for greater risks, it is a typical example of risk retention to save money. There are two different retention techniques for limiting losses, as follows:

- Active Risk Retention: When a risk is kept in mind when developing a management strategy after carefully considering potential losses and their sources.
- Passive Risk Retention: where risk retention happened because of carelessness. Such a risk is unknown, or the risk taker either doesn't understand the risk or thinks it's less of a risk than it is.

3) Risk Reduction

Physical risk reduction, also known as loss prevention, is frequently the most effective way to handle any risk situation, and in most cases, it is possible to take precautions to lower the likelihood of loss. The planning stage of any project is the optimal time to consider risk reduction methods because new project when a significant improvement may be made with little or no additional expense. The cautious remark regarding risk reduction is that expenditures should, to the extent possible, be tied to potential savings in losses and other risk costs in the future; in other words, risk prevention generally should be evaluated in the same way as other investment projects.

4) Risk Transfer

The cost of certain possible losses are being legally assigned to another party. As it deals with risks that may be transferred to a company that specialises in absorbing them for a fee, "risks insurance" is to occupy a significant position. Typically, there are three main ways to transfer losses:

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

The main method of risk transfer is insurance.

RISK MITIGATION

Taking action to lessen negative impacts is referred to as risk mitigation. The practise of reducing or eliminating unacceptable risks associated with an organization's activities is known as risk mitigation. Risk mitigation strategies can be used to lessen the seriousness of the effects of the risk, lessen the likelihood that the risk will materialise, or lessen the exposure of the organisation to the risk. The risk mitigation stage entails creating plans for managing, removing, or reducing risk to a manageable level.

Once risks have been identified and assessed, the strategies to manage the risk fall into one or more of the following categories:

1) Transfer Risk

Execution is typically fought with hazards in project assignments or diverse exercises. When working together, various agencies make sure to transfer risks in their respective fields to another agency that is more suited to handle them for a fee. This is where the idea of core competence comes into play, and anytime a certain agency, person, or corporation discovers that it is dealing in a field that it lacks the core competence to handle, it seeks the assistance of another agency that has the particular core competence to transfer its own risk. The risk, which might take the shape of reputational damage or poor performance, is managed through transfer.

2) Risk Retention or Tolerate Risk

Retaining the risk is what it is. Accepting a loss as it happens is doing so. This type of insurance includes true self-insurance. For tiny risks where the cost of insurance would outweigh the overall losses incurred over time, risk retention is a practical strategy. By default, all risks that are not eliminated, diminished, or transferred are preserved. This covers hazards that are so significant or catastrophic that they cannot be covered by insurance or whose premiums are unaffordable.

3) Reduce Risk

There will be a much higher number of risk in this category. The goal of treatment is more likely to control the risk to a tolerable level than to completely eliminate it. Internal controls are initiatives taken within the organisation that are intended to limit risk to acceptable levels, even though their consequences may be felt outside the organisation.

If the outsourcer can show greater capacity at managing or lowering risks, outsourcing could serve as an example of risk reduction. In this situation, businesses only outsource a portion of their departmental needs. For instance, a business might manage its own operations while contracting out solely its software development, hard good manufacturing, or customer service requirements to another organisation. With less concern for the manufacturing process, the corporation can focus more on commercial development.

4) Avoid Risk

The exposure to loss due to a certain risk is entirely eliminated as a result of this strategy. It can be proven by refraining from taking on the dangerous endeavour or ceasing an activity to prevent risk. This indicates that no projects involving risk are carried on. As an alternative, a project might be abandoned in the middle to lessen risk.

It is not engaging in a potentially dangerous activity. An illustration would be to refrain from purchasing a property or company in order to avoid the associated liability. Another option would be to avoid flying altogether to avoid the chance of an aircraft hijacking. 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.

5) Combine Risk

When a company is exposed to two or three dangers, they work together to lower the overall risk. This tactic works best when dealing with financial risk. To lower risk, various financial instruments, such as shares and debentures, are combined into one portfolio.

6) 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.

7) 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.

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”. In other words, fraud is an act or omission which is intended to cause wrongful gain to one person and wrongful loss to the other, either by way of concealment of facts or otherwise.

A structured approach to lowering fraud in an institution is called fraud risk management. For scams to be discovered at an early stage, a business should have a fraud risk management procedure. Fraud rates can be significantly decreased with the aid of a well-executed fraud risk management procedure. When fraudulent conduct is discovered, the appropriate and essential steps must be taken to address it. It's referred to as fraud risk management. In other words, identifying internal and external fraud risks in a firm and then creating an anti-fraud programme in order to stop fraudulent actions before they happen constitute fraud risk management.

Need of Fraud Risk Management

Modern advancements in technology provide fraudsters a variety of chances nowadays. Even though technological advancements might facilitate fraud risk management for businesses, it is a fact that these advancements also provide opportunities for con artists. PWC's 2022 Global Economic Crime and Fraud Survey found that 46% of questioned organisations had experienced fraud incidents in the previous two years. Over 1200 CEOs from 53 countries and regions participated in the survey.

Organizations' reputations could be damaged by fraud cases within their organisations. Additionally, it might damage the public's perception of their brand. All of these result in a decline in patron loyalty and trust. Customers that lose faith in the company can eventually quit doing business with it. Companies and organisations run the risk of losing prospective new customers in addition to their current clients. Fraud charges may cause businesses to lose clients due to reputational damage.

Fraud risk management processes:



Identifying Risks

For a corporation to effectively manage its fraud risk, it is absolutely essential to identify risks. It is important to determine which workers and departments are most likely to perpetrate fraud and what strategies they might take. Risk identification calls for employee brainstorming. Prioritizing the risks comes next after risk identification. Prioritizing risks is crucial when there isn't enough time or money to mitigate the effects of current risks. As a result, businesses tackle hazards that require prompt attention and stop losses.

Assessing Risks

Based on several examples, organisations should recognise problems and develop appropriate solutions in order to resolve them. Although this is a good and legitimate technique to handle problems, businesses need to go above and above. They should start by attempting to identify the causes of the hazards. The root causes of the risk should be addressed. They should also consider how those risks might impact the company.

Responding to Risks

After recognising and evaluating the risks, companies should take the best action they can. They must develop risk-mitigation plans and choose who will be in charge of carrying them out. Additionally, they should take the appropriate steps to stop the risks from happening again. Additionally, businesses should consider what to do in the event that same risks recur in the future.

Monitoring and reviewing risks

The process of managing fraud risk is ongoing. Risk assessment is therefore never carried out. To be able to adjust simply and swiftly to changing situations and environments, businesses need to continuously monitor and analyse their fraud risk management. Additionally, new dangers could materialise at any time, so businesses should be ready for them as soon as possible.

Reporting risks

Companies can reduce the risk of losing important information and receiving questionable findings by adopting an effective fraud risk management strategy. When reporting concerns, one should act objectively, take concrete steps, and offer advice on how to reduce the likelihood of fraud.

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 therein of elements of risk, if any, 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. The traditional elements of potential likelihood and potential consequences of an event must be combined with other factors like the timing of the risks, the correlation of the possibility of an event occurring with others, and the confidence in risk estimates.
- 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's risk management policies should clearly describe the roles and accountabilities of the board, audit committee, or other appropriate board committee, management and any internal audit function.
- A company should have identified Chief Risk Officer manned by an individual 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 (details are provided under the chapter of Board Committees).

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 behaviour. He has a significant role in assisting the board of the organization to achieve its vision and strategy. The activities of the governance professional encompass legal and regulatory duties and obligations and additional responsibilities assigned by the employer. However, in essence, 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 behaviour.
- 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 play 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. A Company Secretary can ensure that this happens so that the risk factor will come into consideration at the every stage of formulation of a strategy. It will also create awareness about inter-relationships of risks across business units and at every level of the organization.

A Company Secretary can ensure that the following questions [an illustrative list] are effectively addressed at the board level:

- What is the organization's risk management philosophy?
- Is that philosophy clearly understood by all personnel?
- What are the relationships among ERM, performance, and value?
- How is ERM integrated within organizational initiatives?
- What is the desired risk culture of the organization and at what point has its risk appetite been set?
- What strategic objectives have been set for the organization and what strategies have been or will be implemented to achieve those objectives?
- What related operational objectives have been set to add and preserve value?
- What internal and external factors and events might positively or negatively impact the organization's ability to implement its strategies and achieve its objectives?
- What is the organization's level of risk tolerance?
- Is the chosen risk response appropriate for and in line with the risk tolerance level?
- Are appropriate control activities (i.e., approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, segregation of duties) in place at every level throughout the organization?

- Is communication effective — from the top down, across, and from the bottom up the organization?
- How effective is the process currently in place for exchanging information with external parties?
- What is the process for assessing the presence and performance quality of all eight ERM components over time?

Reputation Risk

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 (e.g. through the interbank or securitisation markets).

This risk 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 the risks is not controlled at the initial stage.

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.

Reputation Risk Management

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.

INTERNAL CONTROL

Internal control is essential to the smooth operation and daily operations of a firm and it helps the organisation accomplish its corporate goals. The range of internal control is extensive. It includes all controls included into the strategy, governance, and management processes, including the full spectrum of activities and operations carried out by the organisation and not simply those directly associated with financial operations and reporting. Its scope encompasses all facets of a business, including those that could be broadly categorised as compliance matters as well as aspects related to performance.

Control must not be viewed as a burden on business but rather as a tool for maximising business prospects

and minimising possible losses brought on by unfavourable circumstances. Successful businesses should also avoid being complacent or oblivious to their own success. There are many instances of businesses whose success has been at risk due to a lack of or flaws in internal controls.

Scope of risk management and internal control

It is the responsibility of each business to put in place risk management and internal control systems that are suitable for the circumstances.

In a group, the parent company must make sure that each of its subsidiaries has internal control and risk management procedures in place. These systems must be modified to account for the unique traits of the subsidiaries and their interactions with the parent company.

A parent company should take care to consider the possibility of familiarising itself with and reviewing its affiliate's measures regarding risk management and internal control when it has a sizable equity interest and significant influence over an affiliate.

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.

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:

S. 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	Adopting Resource planning policy
3.	Regulatory and Compliance Risk	Non-compliance of applicable laws	Not keeping abreast of the latest changes in the Regulatory environment	Knowledge updation and maintenance of a robust compliance check list

INTERNAL AUDIT

As defined in scope of the Standards on Internal Audit, Internal Audit means “An independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest

improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity's strategic risk management and internal control system".

Applicability of Provisions of Internal Audit

As per section 138 of the Companies Act, 2013 the following class of companies (prescribed in rule 13 of Companies (Accounts) Rules, 2014) shall be required to appoint an internal auditor or a firm of internal auditors, namely-

- (a) every listed company;
- (b) every unlisted public company having-
 - (i) paid up share capital of fifty crore rupees or more during the preceding financial year; or
 - (ii) turnover of two hundred crore rupees or more during the preceding financial year; or
 - (iii) outstanding loans or borrowings from banks or public financial institutions exceeding one hundred crore rupees or more at any point of time during the preceding financial year; or
 - (iv) outstanding deposits of twenty five crore rupees or more at any point of time during the preceding financial year; and
- (c) every private company having-
 - (i) turnover of two hundred crore rupees or more during the preceding financial year; or
 - (ii) outstanding loans or borrowings from banks or public financial institutions exceeding one hundred crore rupees or more at any point of time during the preceding financial year.

It is provided that an existing company covered under any of the above criteria shall comply with the requirements within six months of commencement of such section.

Importance of Internal Audit

An internal audit is essential to maintain operational efficiency and financial reliability and to safeguard the assets. It provides independent assurance that an organization risk management, governance, and internal control process are operating effectively. The following are the importance of Internal Audit:

1. **Increase productivity:** Internal audit is an objective assurance and consulting activity designed for add value and improve business operation. Internal audit can help an organization accomplish its strategic objectives by bringing a systematic, discipline approach to evaluating and improving the effectiveness of risk management, control and governance process. By continuously monitoring and reviewing the organization processes, internal auditor can identify the control recommendation to improve the efficiency and effectiveness of these processes and they also help to an organization to dependent on processes rather than on people.
2. **Evaluate Risk and protect the assets:** A regular internal audit assess a company control and help to uncover evidence of frauds, help to identify any gaps in the environment and allow for a remediation plan to take place. Internal audit program will help to an organization to track and document any changes that have been made to environment and ensure the mitigation of any found risks.
3. **Quality Control:** Internal auditor help the organization how well system and process are designed and keep the company goals on track and also provide the consulting on how to improve those system and processes if and when necessary.
4. **Independent and unbiased insight:** Internal audit provides unbiased view into how effective internal

controls of your business. If an organization has limited resources and they are unable to setup an independent audit team, they could cross-train employees to audit each other's departments.

5. **Good Corporate Governance:** Internal audits evaluate a company's internal controls, including its corporate governance and accounting processes. They ensure compliance with laws and regulations, accurate and timely financial reporting and data collection. They also help maintain operational efficiency by identifying problems and correcting lapses before they are discovered in an external audit.

ROLE OF INTERNAL AUDITOR IN STRENGTHENING INTERNAL AUDIT

The internal audit department is responsible, within the scope of its duties, for assessing the operation of the internal control system and for making recommendations to improve it.

It helps raise awareness and train management personnel in internal control, but is not directly involved in the design or the day-to-day running of the system.

As part of its work plan approved by executive management, it examines compliance with laws and regulations, ensures that executive management's instructions are properly carried out and verifies the proper functioning of the company's internal processes relating to the reliability of reporting channels and information systems.

The internal audit manager draws up a work programme in light of the main risks incurred by the company and reports the significant findings of work carried out to executive management and, in accordance with the procedures defined by each company, to the board.

Ensuring the success of an organization and bridging the gap between the board of directors and the corporate management team is a key performance indicator. Below are some of their specific responsibilities and duties:

- i. Evaluating risk management activities within the organization.
- ii. Determining the organization's compliance with relevant laws and regulations.
- iii. Evaluating and making recommendations that can assist in improving internal control.
- iv. Investigating fraud via a fraud risk assessment that uses fraud deterrence principles.
- v. Offering an objective source of independent advice to help reach the goal and achieve legality and validity.
- vi. Performing audit assignments assigned to them
- vii. Learning and studying the organization's policy and guidelines.
- viii. Identifying audit scope and developing annual plans within the organization.
- ix. Gathering, analyzing, evaluating, and presenting accounting documentation, reports, data, and flowcharts.
- x. Following up the audits to monitor the managements' intervention.
- xi. Promoting ethics and identifying improper conduct within the company.

CRISIS MANAGEMENT

Crisis Management is an organization's process- and strategy-based approach for identifying and responding to a threat, an unanticipated event, or any negative disruption with the potential to harm people, property, or business processes.

Dealing with crises in a way that limits harm and helps the impacted business to recover swiftly is the goal of

crisis management. Public relations for a corporation may benefit greatly from handling a crisis effectively. There are many different types of crises, hence it is advised that a corporation develop a crisis management plan in advance.

Types of Crisis

There are several different types of crises that can be faced by a firm. Analyzing the different scenarios has led to some of the companies' most frequently occurring mishaps. Few of them have been listed below:

Natural Disasters

These kinds of mishaps fall under the category of "acts of God" and take place spontaneously without any human interference. A broad geographic area can be impacted by floods, earthquakes, tsunamis, storms, droughts, or any other circumstance, endangering the enterprise based there.

These are the most difficult from a managerial standpoint to foresee and counteract. When one of these natural disasters puts the company's resources in danger, the crisis management teams need to know what to do.

Technological Crisis

Every human's life includes technology in some way. However, if technology is used improperly, the negative effects it can have can sometimes outweigh the positive ones. Data breaches, malware, spyware, and other problems can hinder a company's growth. Managers must be well informed of what transpires in these circumstances and take strong action to limit damage.

Organizational Misdeeds

Sometimes, a crisis can be caused by the wrong steps taken by a firm. The manager devising the crisis management strategy should know about all the decisions taken by the firm. They must ensure every company's action is legally and ethically correct to avoid any mishap in the future.

Confrontational Crisis

Different departments might be found within a single corporation. They might even have various governments in the case of any kind of multinational enterprise. These groups could clash due to differences in beliefs, ideologies, and requirements. So that no party is favoured and the situation does not worsen, the company must have preparations for how to address the problem. These crises can include blockades, sit-ins, union boycotts, etc.

Rumours

When the competition between rival businesses heats up, some competitors may try to win by making false accusations against the opposition. This starts to damage the company's reputation and causes losses for it. The crisis management plan must quickly compile the appropriate certificates and other supporting evidence to demonstrate to the public how untrue the rumours are.

Crisis Management Plan

The following guidelines are recommended for establishing good crisis management plans:

- Identify an individual from your workforce to take over the crisis management role as a manager. Or a firm can employ a professional crisis manager who can help you in planning crisis management processes.
- Initiate frequent training and refresher courses on handling crises. Drills and practice operations must frequently take place to keep refreshing stakeholders on emergency responses to crises.
- Form a crisis team to work under the leadership of a crisis manager. When a crisis occurs, this is the team that should be able to respond quickly. A veteran of several training sessions and drills for such

occurrences, it is expected to be on the frontline in directing other stakeholders on what to do and where to assemble to avoid further damage.

- Planning responses and crisis management processes for various potential crises is highly recommended. It takes several approaches and processes to address different crises.
- Initiate systems that can effectively monitor or detect foreseeable crises signals early enough in order to tackle the situation before it gets out of hand. Examples of such systems are smoke detectors that can detect potential fire long before it gets out of hand.
- Provide a list of key persons in case of a crisis and their contact information. The contact information must be displayed where anyone can see it and easily access them.
- Identify the ground person to be notified immediately when a crisis occurs. Apart from a crisis manager, there must be a coordinating person among employees who possesses first-hand news on a looming crisis. This should be a person who can be trusted by his colleagues with vital information during any suspected crisis.
- Identify a central point where employees can assemble and the exit points to use in case of a crisis. Emergency exit doors with ease of opening them must be labeled well and an emergency central gathering place identified and properly labeled as well.
- Regular testing of the crisis management process and emergency equipment and updating them frequently or as needed.

ESG RISK ASSESSMENT

ESG is an acronym for environmental, social, and governance. Investors are increasingly using these non-financial factors as part of their analytical process to identify significant risks and growth opportunities. ESG metrics are not typically included in mandatory financial reporting, despite the fact that businesses are increasingly revealing information in their annual report or a separate sustainability report. To make it simpler to incorporate these factors into the investment process, many organizations—including the Sustainability Accounting Standards Board (SASB), the Global Reporting Initiative (GRI), and the Task Force on Climate-related Financial Disclosures – are working to develop standards and define materiality (TCFD).

1. Environmental Risks

These risks include environment-related issues such as Greenhouse gas emissions (GHG), deforestation, pollution, water usage, biodiversity, waste, etc.

2. Social Risks

These include factors such as customer relations, human rights, labor rights, employee relations, occupational safety and health, supply chains, diversity, inclusion, etc.

3. Governance Risks

These risks include issues such as succession planning, board management practices, executive compensation diversity among board and management, corruption, fraud, data hygiene, security, equity, etc.

Significance of ESG Risk Assessment

1. Enhanced Sustainability

With a better understanding of ESG risks, companies can effectively utilize their resources, tackle rising operation costs, make safe investments, improve employee retention and adhere to regulations easily.

Recognizing these potential risks and effectively managing them not only makes the organization resilient to future challenges but also provides a competitive advantage.

2. **Improved Regulatory Compliance**

With the growing stakeholder demands for accountability, there is also an increase in the regulatory obligations for ESG.

Integrating ESG factors as a part of the risk management structure makes communicating effectively with governing authorities easier thereby, minimizing the resource burden and requirement for legal intervention.

3. **Increased Investment Potential**

Socially aware investors are now seeking the integration of ESG values into their portfolios to ensure sustainable investments. Those organizations that have well-established ESG risk management systems fare better in attracting investors.

4. **Better Employee Productivity**

Organizations with the highest employee satisfaction had ESG scores 14% higher than the global average, likely due to their strong environmental performance [Marsh & McLennan].

An ESG-conscious organization can enhance employee productivity, motivation, and retention by inculcating a sense of purpose among the workforce.

Additionally, organized ESG risk management promotes employee well-being through considerations such as health & safety, work schedules, diversity, and inclusion. This not only enhances employee experience but also stimulates better performance.

5. **Greater Profitability**

Mitigating ESG risks not only makes a company favorable for investments but also enhances its profitability.

According to McKinsey research, ESG strategies can affect operating profits by as much as 60%. ESG responsive organizations are more likely to attract customers and top talent thereby, promoting their top-line growth.

ESG RISK MANAGEMENT

Like other risk forms, ESG risk management also involves the same three steps – Identify the risk, quantify the risk, and manage it for better organizational sustainability.

With this new focus on ESG factors in risk analysis, decision-makers need to quantify the ESG risks for effective risk management.

ESG risks are quantified and reported in the form of a company's ESG risk score or rating. A low-risk rating indicates effective risk management and a high-risk score signifies inconsistencies in ESG risk management.

Every company is vulnerable to ESG risks and requires ESG risk management to avoid financial or reputational damage. Irrespective of the size of the company or organization, incorporating ESG risk factors in the decision-making process amounts to effective risk management.

ENVIRONMENTAL RISKS

The risks with which this report is concerned are all in some way 'environmental'. They arise in, or are transmitted through, the air, water, soil or biological food chains, to man. Their causes and characteristics are, however, very

diverse. Some are created by man through the introduction of a new technology, product or chemical, while others, such as natural hazards, result from natural processes which happen to interact with human activities and settlements. Some can be reasonably well anticipated, such as flooding in a valley or pollution from an industrial smelter. Others are wholly unsuspected effects at the time the technology or activity was developed, such as the possible effects on the earth's ozone layer of fluorocarbon sprays or nitrogen fertilizers

While being diverse in themselves, environmental risks, as defined here, share a second common feature in addition to being transmitted through environmental media. They cause harm to people who have not voluntarily or specifically chosen to suffer their consequences, and thus they require regulation on the part of some authority above that of an individual citizen - that is, they require managing. These consequences can fall on other groups in the future as well as today, as for example in the mismanagement of natural resources. In this report, environmental risks exclude personal choices such as smoking, rock-climbing or tampering with electrical circuits. The immediate consequences of this latter group fall upon the individual who is voluntarily accepting such risks and the government role is usually to educate the public rather than to regulate or control the risks. Even in these cases, the transmission of risk to others through environmental media can be of concern. The risks of smoking to non-smokers present, for example, is probably small but it is the subject of current risk assessment and changes in public policy.

Environmental risks are receiving more attention from investors and consumers as people become more conscious of climate change, greenhouse gas emissions, resource usage, and biodiversity protection. The potential for an organisation to have a detrimental impact on the environment is known as environmental risk. The followings are the few of the example of the environmental risks:

- Impact of climate change on GHG emissions
- Security and use of water
- Reducing waste and recycling
- Pollution control and prevention
- Deforestation
- Safeguarding thriving ecosystems
- The effect on biodiversity
- Safeguarding maritime resources
- Making the switch to a circular economy
- Techniques for environmental management

Please elaborate this point, as it appears to be incomplete and lacks synchronization). Apart from energy oriented enterprises, also cover other forms of enterprise/s that give birth to environmental risk.

SOCIAL RISK

The following are some instances of social risks: product recalls, labour violations, boycotts, and treatment of employees. All parties involved in the firm, from suppliers and local communities to employees and customers, may be affected at once by these difficulties since they are numerous, complicated, and pervasive. Maintaining positive relationships with these stakeholders is essential to a company's long-term success, especially if that business depends on the confidence of the general public.

Examples of societal risks are:

- Inclusion, equity, and diversity

- Workplace and safety circumstances
- Observing human rights
- Development of the workforce and training
- Data security
- Community participation
- Fair labour standards for vendors and suppliers

All parties involved in a firm are typically impacted by social issues. For a business to maintain long-term competitive advantages, it can be crucial to be able to prevent tarnishing its reputation and relationships.

GOVERNANCE RISK

“Governance is the culture, values, mission, structure, layers of policies, processes and measures by which organizations are directed and controlled”.

Governance defines how the organization should perform, describing through policies what is acceptable and unacceptable and compliance is the area responsible for inspecting and proving that they are adequately, being implemented and followed.

Governance is also responsible for risk and compliance oversight, as well as evaluating performance against enterprise objectives. The board acts as an active monitor for shareholders’ and stakeholders’ benefit, with the goal of Board oversight to make management accountable, and thus more effective.

Properly implemented compliance oversight is proactive and regularly monitors and evaluates the organization’s Content Management System with the emerging regulatory landscape. Accordingly, governance should be able to understand and foresee the organization’s vulnerabilities and, hence make decisions to reduce them. Also, governance should distribute power to provide insight and intelligence, at the right time, so that the right people in the management can make risk-aware

decisions in accordance with key business objectives. Risk-awareness is possible through the close proximity that governance should have with risk management, which may provide very useful information in strategy setting and decision making.

Governance needs to touch every part of the organization. It needs to be at the heart of corporate culture when in today’s complex global ecosystems, risks are becoming more interconnected.

Although most investors are aware of strong governance principles, no one solution works for all. Finding out where and how best practices might impact corporate performance can be challenging. Risks associated with governance include:

- Corporate morals and ethics
- Conduct and practices that are anti-competitive
- ESG regulation compliance (including emerging regulations)
- ESG transparency
- Open communications
- Grievance policies and processes
- Preventing fraud and corruption
- Compensation for executives

- Diversity of the Board of Directors
- Corruption and extortion
- Standards and regulations
- Paying taxes

PNB Scam- Case Study

On 14 February 2018, PNB revealed that fraudulent transactions by billionaire jeweler Nirav Modi and related entities amounted to 110 billion rupees (US\$1.77 billion). The key accused in the case were jeweler and designer Nirav Modi, his maternal uncle Mehul Choksi, and other relatives and some PNB employees. Nirav Modi and his relatives escaped India in early 2018, days before the news of the scam became public.

Nirav Modi and the companies linked to him colluded with bank officials to get guarantees or letters of undertaking to help fund buyer's credit from other overseas banks. Multiple fake LoUs were opened in favour of branches of Indian banks for import of pearls for a period of one year, for which Reserve Bank of India guidelines lay out a total time period of 90 days from the date of shipment but the guidelines were ignored by overseas branches of Indian banks. They failed to share any document/information with PNB, which were made available to them by the firms at the time of availing credit from them.

The Enforcement Directorate (ED) recovered bank token devices of the foreign dummy companies used by the fugitive diamond trader to transfer the fraudulent funds. The probe agency found that Nehal Modi, brother of Nirav Modi had destroyed the devices and had even secured a server located in the United Arab Emirates (UAE) soon after the scam broke out. These dummy firms had been receiving the fraudulent PNB LoUs and were based out in British Virgin Island and other tax havens.

This case was a result of the mismanagement from the internal regulatory bodies within the PNB itself and also from the side of the Reserve Bank of India (RBI). This is not the only instance in itself where the public sector banks have failed to perform their duties and therefore major changes need to be incorporated into the regulatory mechanisms to prevent such frauds.

In the aftermath of this case, RBI has directed banks to integrate SWIFT and core banking systems. It has also constituted a committee to look into the reasons for high divergence observed in asset classification, various incidents of fraud and necessary interventions (also in terms of information technology) to prevent such frauds.

The government passed the Fugitive Economic Offenders Act (2018) which came into force on 21st April 2018. The Act was enacted to prevent economic offenders in the ilk of Nirav Modi from escaping the country.

ESG Risk Management

ESG is a specialised aspect of risk management, although having a broad range of potential applications. ESG assurance is less intimidating than you may think if you take a sound strategy and use the right tools, just as in every other area of risk management. ESG risk management is essential for identifying, managing, and reducing all associated risks. Be on the lookout for ESG software that can automate some of the steps necessary to evaluate your business or your clients' degree of ESG practise.

When evaluating ESG risks, there is no one universal strategy. Global regulators have not yet established a single standard that would apply to all countries or harmonise all ESG components. A corporation should be able to define ESG and the specific risks to which they may be exposed through data gathering and analysis. To review the business processes and determine whether they are in line with ESG objectives, a thorough risk assessment must be completed, just like for any other form of risk.

Climate Risk

Globally, weather and climate-related risks, which potentially cause loss and damage, have increased dramatically over the past few decades. The most recent climate projections indicate a significant increase in the frequency, duration and intensity of extreme weather events as well as severe slow-onset climate related changes. These pose a growing risk to sustainable development of communities and countries. Internationally there is an increasing recognition that adaptation and mitigation may not be enough to manage the impacts of climate change and both climate science and the international climate negotiations stress the urgent need to develop and implement effective climate risk assessment and management approaches in order to avert, minimize and address losses and damages.

So far there has been no accepted official definition of loss and damage. The working definition of Loss and Damage (L&D) as defined by UNFCCC is as follows:

“Loss and damage refers to negative effects of climate variability and climate change that people have not been able to cope with or adapt to.”

Climate Risk Management Process

The six step climate risk management (CRM) process operationalises climate risk management at scale (see Figure 1).

1. Assess and match information needs with risk management objectives.
2. Define System of Interest.
3. Develop context-specific methodology.
4. Risk identification to identify low and high-levels of climate-related risk.
5. Risk evaluation to identify acceptable, tolerable and intolerable risks.
6. Assessment of risk management options.

Need for a CRM Framework in India

According to India's 2nd National Communication to the UNFCCC, a majority of its population is vulnerable to climate change and its impacts. The economy is closely tied to climate sensitive sectors such as agriculture, forestry and water among others, as well as to its natural resource base, thereby increasing its exposure and sensitivity to changes in existing climatic conditions. Exposure and sensitivity to climate change is exasperated by the fact that nearly 18% of the world's population is occupying only 2.3% of the world's land area. Thus, there is an immense stress to harness indigenous resources efficiently while ensuring a sustainable development pathway. The country's distinct topography and geographic features results in a wide range of climatic conditions across different regions. These climatic aspects continue to influence the biological, cultural and economic conditions. However, the climatic variability and geographic features also result in various forms of disaster occurrences such as cyclones, earthquakes, landslides and flooding among others. Thus, given the confluence of climatic vulnerabilities and disaster risks, there is a clear and present need for India to develop a robust CRM framework which can be utilized to help make decisions in tackling both these issues.

Business Continuity Plan (BCP):

A business continuity plan (BCP) is a document that outlines how a business will continue operating during an unplanned disruption in service. It is a system of prevention and recovery from potential threats to a company.

A business continuity plan (BCP) can be tailored to specific departments such as finance, HR, and marketing operations.

With respect to finance operations, a BCP would focus on maintaining financial systems and processes,

ensuring that the company has access to sufficient financial resources, and maintaining financial reporting and regulatory compliance. The plan would outline procedures for securing financial data, restoring critical financial systems, and ensuring that key financial personnel are available to respond to the crisis.

For HR operations, a BCP would focus on maintaining personnel resources and ensuring that the company is able to continue to pay its employees and provide benefits. The plan would outline procedures for securing personnel data, maintaining payroll and benefits systems, and ensuring that key HR personnel are available to respond to the crisis.

For marketing operations, a BCP would focus on maintaining marketing systems and processes, ensuring that the company is able to continue to promote its products and services, and maintaining the company's image and reputation. The plan would outline procedures for securing marketing data, restoring critical marketing systems, and ensuring that key marketing personnel are available to respond to the crisis.

In each case, the BCP provides a framework for the department to follow in the event of a crisis, and it helps to ensure that the department can respond effectively and maintain its operations during the crisis.

features of an effective business continuity plan (BCP)

The components of business continuity are:

- **Strategy:** Objects that are related to the strategies used by the business to complete day-to day activities while ensuring continuous operations
- **Organization:** Objects that are related to the structure, skills, communications and responsibilities of its employees
- **Applications and data:** Objects that are related to the software necessary to enable business operations, as well as the method to provide high availability that is used to implement that software
- **Processes:** Objects that are related to the critical business process necessary to run the business, as well as the IT processes used to ensure smooth operations
- **Technology:** Objects that are related to the systems, network and industry-specific technology necessary to enable continuous operations and backups for applications and data
- **Facilities:** Objects that are related to providing a disaster recovery site if the primary site is destroyed

Steps to Creating a Business Continuity Plan

Step 1: Assemble a Business Continuity Management Team

The makeup of your team depends on your continuity objectives and the size of your company.

A good BCP should detail what your staff needs to do in the event of a disaster, what communication methods are required, and the timeframe in which critical IT services need to be available.

- Create a contact list of key people involved in your company's BCP, including names, titles, and communication info (both work and personal) such as phone numbers, email addresses.
- Provide a detailed overview of their roles and responsibilities so that everyone knows what is expected of them in an outage event.
- Have a process in place for how your BCP will be updated and how these updates will be communicated to the team.

This team will prepare standards for the project and train additional team members. They will also identify clear processes to improve project flow.

Step 2: Ensure the Safety and Wellbeing of Your Employees

- When planning, you must prepare to **prioritize the safety of your employees** amid a crisis. They will look to you, their community, and the government for guidance. Be proactive and transparently address their concerns. Right now, many companies have to decide to initiate or expand remote work arrangements and other policies that allow employees to work flexibly.
- Depending on your industry, you'll want to reallocate resources and reorganize teams, as well as establish employee wellbeing programs and procedures that **support a safe working environment**.
- Make sure you have proper communication channels in place to get in touch with all of your employees at the same time. Sending an email may not be sufficient if the wifi is down. Consider implementing a BC Planning software with an integrated emergency messaging tool to ensure all business processes are continuous, and everyone is safe. Communicate with your teams early and regularly. You want to engage your employees as you navigate through the current crisis.

Step 3: Understand the Risks to Your Company

Once your business continuity management team is assembled, you must conduct a business impact analysis (BIA).

This type of analysis will help you identify specific threats to financial performance, operations, supply chains, reputation, employees. It can serve as a starting point when identifying risks.

You and your team should brainstorm a list of threats and potential risks to your business. Then discuss how the risks mentioned above could affect business operations.

Step 4: Implement Recovery Strategies

Once a disaster occurs, and financial losses begin to grow, it can be challenging to get back on track without a BCP in place. Consider the following questions as you discuss options with your team:

- Do you have a way to get sales, HR, manufacturing, and support personnel back to work after a disaster to continue operating your business?
- How will you continue to meet the demand for products or services if your equipment or facility is damaged?
- If your facilities are impacted, will your employees work remotely at home or from an alternate location?

Step 5: Test, Test Again and Make Improvements

No matter how long you spend perfecting it, a business continuity plan is never truly finished—just as the risks and requirements of your industry are never set in stone.

Testing your business continuity plan allows you to validate it as you manage risks. While 88% of companies test their strategies to identify gaps, 63% of them do so to validate their plans.

Crisis Management Plan (CMP)

The process of handling and reacting to a sudden, unexpected occurrence that poses a serious threat to an organization is known as crisis management. A **crisis management plan (CMP)** is a specific type of BCP that focuses on the procedures and protocols for dealing with a crisis, such as a public relations crisis or a safety emergency.

Crisis management can involve different roles and responsibilities for finance, marketing, and HR managers, depending on the specific crisis and the company's operations.

For a finance manager, crisis management may involve overseeing the company's financial response to the

crisis, ensuring that the company has access to sufficient financial resources, and maintaining financial reporting and regulatory compliance. The finance manager may also work with the company's legal and regulatory teams to ensure that the company follows all relevant laws and regulations as it responds to the crisis.

For a marketing manager, crisis management may involve overseeing the company's marketing response to the crisis, ensuring that the company is able to continue to promote its products and services, and maintaining the company's image and reputation. The marketing manager may also work with the company's public relations team to manage the company's image and reputation during the crisis.

For an HR manager, crisis management may involve overseeing the company's personnel response to the crisis, ensuring that the company is able to continue to pay its employees and provide benefits, and maintaining personnel resources. The HR manager may also work with the company's legal and regulatory teams to ensure that the company is in compliance with all relevant laws and regulations as it responds to the crisis.

In each case, the manager plays a crucial role in the company's response to the crisis, and their actions and decisions can have a significant impact on the company's ability to maintain its operations and recover from the crisis.

Here cover features of Crisis Management Plan

Need for Crisis Management

- Crisis Management prepares the individuals to face unexpected developments and adverse conditions in the organization with courage and determination.
- Employees adjust well to the sudden changes in the organization.
- Employees can understand and analyze the causes of crisis and cope with it in the best possible way.
- Crisis Management helps the managers to devise strategies to come out of uncertain conditions and also decide on the future course of action.
- Crisis Management helps the managers to feel the early signs of crisis, warn the employees against the aftermaths and take necessary precautions for the same.

Essential Features of Crisis Management

- Crisis Management includes activities and processes which help the managers as well as employees to analyze and understand events which might lead to crisis and uncertainty in the organization.
- Crisis Management enables the managers and employees to respond effectively to changes in the organization culture.
- It consists of effective coordination amongst the departments to overcome emergency situations.
- Employees at the time of crisis must communicate effectively with each other and try their level best to overcome tough times.

YES Bank Crisis- Case study

YES Bank was once the country's fifth-largest private lender by market capitalization. YES Bank had been founded by Rana Kapoor and Ashok Kapoor in 2004. The bank was ranked number 1 bank in the Business Today-KPMG Best Banks Annual Survey 2008. YES Bank was the first institution globally to receive funding through IFC's Managed Co-Lending Portfolio Programme and the first Indian bank to raise loan under IFC's A/B loan facility.

What has led to a crisis at YES Bank?

The bank's loan book on March 31, 2014, was Rs 55,633 crore, and its deposits were Rs 74,192 crore. Since then, the loan book has grown to nearly four times as much, at Rs 2.25 trillion as on September 30, 2019. While deposit growth failed to keep pace and increased at less than three times to Rs 2.10 trillion. The bank's asset quality also worsened and it came under regulator RBI's scanner. Yes bank was lending aggressively disregarding the risk limits and also under-reporting the bad loans. They were lending to corporates that were already in very risk businesses and facing some challenges in their business like the Anil Ambani-led Reliance group, DHFL and IL&FS. All this happened in Rana Kapoor's (Founder of Yes Bank) tenure. The exposure of loans to such bad performing companies was huge in Yes Bank's case, and to add up they were hiding the NPAs (Non-performing assets) or misreporting the same. After the above fiasco, Ravneet Gill took charge of Yes Bank but struggled to revive as deposits kept depleting and he wasn't able to raise enough capital given the loss of confidence in the market. The tipping point came when one of the bank's independent directors Uttam Prakash Agarwal, resigned from the board in January 2020 citing governance issues.

Several reasons behind the crisis of YES bank were:

1. NPAs: YES Bank ran into trouble following the central bank's asset quality reviews in 2017 and 2018, which led to a sharp increase in its impaired loans ratio and uncovered significant governance lapses that led to a complete change of management. The bank subsequently struggled to address its capitalisation issues. YES Bank suffered a dramatic doubling in its gross NPAs between April and September 2019 to Rs 17,134 crore.
2. NBFC crisis: The crisis in India's shadow-banking space started with the unravelling of Infrastructure Leasing & Financial Services (IL&FS) and then extended to Dewan Housing Finance Limited (DHFL). YES Bank's total exposure to IL&FS and DHFL was 11.5 per cent as of September 2019. In April 2019, the bank had classified about Rs 10,000 crore of its exposures, representing 4.1 per cent of its total loans under watch list, as potential non-performing loans over the next 12 months.
3. Governance issue: YES Bank faced several governance issues that led to its decline. On January 10, independent director Uttam Prakash Agarwal quit citing deteriorating corporate governance standards and compliance failure at the lender. In 2018-19, the bank under-reported NPAs to the tune of Rs 3,277 crore, prompting RBI to dispatch R Gandhi, one of its former deputy governors, to the board of the bank.

Rana Kapoor, who was instrumental in building YES Bank from scratch, was asked to step down as chief executive in January 2019.

4. Excessive withdrawals: YES Bank's financial condition dissuaded many depositors from keeping funds in the bank over a longer term. The bank showed a steady withdrawal of deposits, which burdened its balance sheet and added to its woes. The bank had a deposit book of Rs 2.09 trillion at the end of September 2019.

Steps taken by RBI against YES Bank

1. RBI has taken over the YES Bank management
2. The central has imposed a moratorium on the lender
3. RBI announced a draft 'Scheme of Reconstruction' that entails SBI investing capital to acquire a 49% stake in the restructured private lender.

How can such conflicts between Management and Board be avoided?

The global best practice recommends that at least three-quarters of board members should be independent, the board should have an independent chairman and not an individual who serve the role of both CEO & Chairman of the board, annual board elections should be conducted as this forces directors to make more careful decisions and be more attentive to shareholders because they can cast the vote to keep or eliminate a director each year.

Also, every year board self-assessment practices should be conducted, independent directors should annually/quarterly meet and openly discuss various policies, management, and compensation without concerns about management influence.

Also cover a case study of any listed company in BSE /NSE.

Disaster Recovery Plan (DRP)

A disaster recovery plan (DRP) is a comprehensive plan that outlines the procedures and strategies that a corporation will use to restore its critical operations and services in the event of a disaster. The goal of a DRP is to ensure that the corporation can quickly and effectively recover from a disaster and return to normal operations.

In the corporate world, disaster recovery planning is a critical component of risk management and business continuity planning. Companies invest in DRPs to minimize the impact of disasters on their operations, protect their assets and data, and ensure that they can continue to serve their customers and stakeholders.

A DRP typically includes a detailed analysis of the potential risks and consequences of a disaster, as well as a plan for responding to and recovering from the disaster. This may include strategies for backing up data and systems, providing alternative means of communication, and establishing contingency operations to continue business activities.

In addition to developing the DRP, companies in the corporate world also regularly test and update their plans to ensure that they are prepared for any type of disaster that may occur. This helps to minimize the impact of the disaster on the company and ensures that the company can quickly return to normal operations.

Here cover the features of Disaster Recovery Plan**Elements of Disaster Recovery Plan**

One way your organization can prepare and protect itself from disasters is to create and implement a disaster recovery plan (DRP). Organizations should create a disaster recovery plan that can address any type of disaster. The plan should be easy to follow and understand, and be customized to meet the unique needs of the organization. Typical elements in a disaster recovery plan include the following:

1. Create a disaster recovery team. The team will be responsible for developing, implementing, and maintaining the DRP. A DRP should identify the team members, define each member's responsibilities, and provide their contact information. The DRP should also identify who should be contacted in the event of a disaster or emergency. All employees should be informed of and understand the DRP and their responsibility if a disaster occurs.
2. Identify and assess disaster risks. Your disaster recovery team should identify and assess the risks to your organization. This step should include items related to natural disasters, man-made emergencies, and technology related incidents. This will assist the team in identifying the recovery strategies and resources required to recover from disasters within a predetermined and acceptable timeframe.
3. Determine critical applications, documents, and resources. The organization must evaluate its business processes to determine which are critical to the operations of the organization. The plan should focus

on short-term survivability, such as generating cash flows and revenues, rather than on a long term solution of restoring the organization's full functioning capacity. However, the organization must recognize that there are some processes that should not be delayed if possible. One example of a critical process is the processing of payroll.

4. Specify backup and off-site storage procedures. These procedures should identify what to back up, by whom, how to perform the backup, location of backup and how frequently backups should occur. All critical applications, equipment, and documents should be backed up. Documents that you should consider backing up are the latest financial statements, tax returns, a current list of employees and their contact information, inventory records, customer and vendor listings. Critical supplies required for daily operations, such as checks and purchase orders, as well as a copy of the DRP, should be stored at an off-site location.
5. Test and maintain the DRP. Disaster recovery planning is a continual process as risks of disasters and emergencies are always changing. It is recommended that the organization routinely test the DRP to evaluate the procedures documented in the plan for effectiveness and appropriateness. The recovery team should regularly update the DRP to accommodate for changes in business processes, technology, and evolving disaster risks.

In summary, an organization must develop a recovery team to create a disaster recovery plan that includes identifying and assessing disaster risks, determining critical applications, and specifying backup procedures. Other procedures may be included in the plan based on the organization. The recovery team and organization must then implement the DRP and follow through on the plan procedures. The DRP should be continually tested and maintained to consistently prepare the organization for evolving disasters and emergencies.

Also cover a case on disaster recovery plan of any company listed in BSE / NSE.

Relationship between Business Continuity Plan, Crisis management and Disaster recovery plan in corporate world

In the field of risk management and organizational resilience, business continuity planning and crisis management are two ideas that are closely related. A business' key operations will be maintained during and after a disruptive event, such as a natural disaster, cyberattack, or pandemic, according to a thorough document called a business continuity plan (BCP). BCP's goal is to guarantee that crucial operations and services can continue with the least amount of disruption possible and that the business can quickly recover from the incident.

The relationship between business continuity planning and crisis management is that a BCP provides the overarching framework for maintaining business operations during and after a disruptive event, while a CMP provides specific guidance for managing a crisis. Both BCP and CMP are essential components of a comprehensive risk management program, and they work together to ensure that an organization can continue to operate and recover from a disruptive event.

After the above para, please provide a table here to elaborate the relationship between Business Continuity Plan, Crisis Management and Disaster Recovery plan for ease of learning for the students. This table may be inserted after the example given below to understand the relation

Let's understand this relation with an example: -

Imagine that a multinational corporation is facing a financial crisis, caused by a sudden drop in demand for its products or a significant financial loss. The senior finance manager of the company is responsible for overseeing the company's financial response to the crisis and ensuring that the company's operations are maintained.

The senior finance manager immediately activates the company's business continuity plan (BCP), which outlines

the procedures and strategies that the company will use to maintain its critical operations and services during the crisis. The BCP provides a roadmap for the senior finance manager and the crisis management team to follow, and it helps to ensure that the company's financial response is organized and effective.

The senior finance manager also assembles the company's crisis management team, which includes representatives from various departments, to respond to the crisis. The crisis management team uses the BCP to assess the situation and determine the best course of action. They quickly identify the critical financial systems and services that are most likely to be impacted by the crisis and prioritize their efforts to protect those systems and services.

The senior finance manager also works closely with the company's legal and regulatory teams to ensure that the company follows all relevant laws and regulations as it responds to the crisis. They also work with the company's public relations team to manage the company's image and reputation during the crisis.

In this scenario, the senior finance manager plays a crucial role in ensuring that the company's financial operations are maintained during the crisis, and that the company's response is organized and effective. The BCP and crisis management plan provide a framework for the senior finance manager and the crisis management team to follow, and they help to ensure that the company's response is as effective as possible.

We can conclude that in a crisis, the BCP provides a roadmap for the crisis management team to follow, and the DRP provides a roadmap for the recovery process. The BCP and DRP work together to ensure that the company can maintain its critical operations and services during the crisis and quickly recover from the disaster. The crisis management process helps to ensure that the company's response to the crisis is organized and effective, and that the BCP and DRP are implemented as effectively as possible.

CYBER RISK MANAGEMENT

We have a responsibility to better understand the vulnerability and threat landscape given the rise in infections and attack scenarios. An active risk assessment method should be designed to help in the determination of how to best deploy security measures, according to risk management protocols to safeguard financial assets, information databases, and intellectual property resources. A number of methods are also available for setting up risk reduction procedures. In order to develop an effective and tenable plan for the short- and long-term protection of assets, it is necessary to consult with legal and insurance carriers.

In the modern landscape of cybersecurity risk management, one uncomfortable truth is clear—managing cyber risk across the enterprise is harder than ever.

History of cyber security risk management

According to Jeff Yost, in his article, *A History of Computer Security Standards*, the field of cybersecurity got its start alongside the development of the first computers, developed by the US Department of Defense in the late 1960s. Beginning with the Advanced Research Projects Agency Network (ARPANET), a pre-internet network of interconnected computers widely regarded as the first real network as we know it, governmental agencies relying on this network naturally relied on it to be secure.

As computer technology moved from private, governmental usage to public usage, this need for security continued, but it also became more complicated. Like other attacks against communication systems, such as the manipulation of tones used by the telephone system in order to gain access to the network, make free calls, or otherwise exploit telecom networks, the initial attacks waged against the early computer networks were also primarily based on seeking out and exploiting technical weaknesses.

Cybersecurity in the 1980s

The 1980s saw the emergence of the first commercially available antivirus software. Companies such as

Symantec, McAfee, and Trend Micro led the way in providing reliable protection against malicious programs. This period also saw an increase in computer viruses, as hackers began to target personal computers and business networks. In addition, this decade marked the rise of Internet security and the emergence of the international Computer Emergency Response Team (CERT).

Cybersecurity in the 1990s

The 1990s saw further development in cybersecurity, with the launch of firewalls, which act as a barrier to keep unwanted threats out. Companies such as Check Point Software Technologies created firewall systems that help protect against intrusions and malicious attacks. This decade also saw a huge increase in the number of cybercrimes, with hackers increasingly targeting critical infrastructure and corporate systems. As a result, governments around the world began to focus on improving their cybersecurity capabilities by introducing laws and regulations to protect citizens from online threats.

Cybersecurity in the 2000s

The start of the 21st century saw the emergence of sophisticated cyber threats. As technology continues to evolve, so too does the sophistication of malware and other malicious software. The 2000s saw a rise in phishing scams, ransomware, and zero-day attacks, prompting governments and companies to increase their investments in cybersecurity solutions. This decade also marked the beginnings of large-scale data breaches as hackers began targeting sensitive data.

Cybersecurity in the 2010s

The 2010s saw the emergence of cloud computing, which enabled companies to store data remotely on shared networks. However, this also created new risks, as malicious actors were now able to target multiple systems at once. To protect against these threats, businesses began investing heavily in security measures such as multi-factor authentication, encryption, and cyber insurance. This decade also saw an increase in the use of artificial intelligence (AI) and machine learning algorithms to detect potential threats before they can cause any damage.

Cybersecurity in the 2020s

The 2020s have brought even more challenges to the world of cybersecurity, including state-sponsored attacks, quantum computing, and the rise of 5G networks. In response, governments and companies are investing heavily in innovative technologies such as blockchain and artificial intelligence to help protect their systems from malicious actors. As cybersecurity continues to evolve, we expect to see further advances in the technology used to protect our data and networks. Cybersecurity is an ever-changing field, but with the right information and resources, we can all stay safe online.

By understanding the history of cybersecurity, businesses, organizations, and individuals can create an informed approach to security. Whether it's protecting against malicious threats or building a secure infrastructure for data storage, having a knowledge of the past can help us shape the future of cybersecurity.

Cyber Security Risk Management Process

Provide genesis of Cyber Risk Management and then cover the points mentioned below

1. Identify the risks that might compromise your cyber security. This usually involves identifying cyber security vulnerabilities in your system and the threats that might exploit them.
2. Analyse the severity of each risk by assessing how likely it is to occur and how significant the impact might be if it does.
3. Evaluate how each risk fits within your risk appetite (your predetermined level of acceptable risk).

4. Prioritise the risks.
5. Decide how to respond to each risk. There are generally four options:
 - *Treat* – modify the risk's likelihood and/or impact typically by implementing security controls.
 - *Tolerate* – make an active decision to retain the risk (e.g., it falls within the established risk acceptance criteria).
 - *Terminate* – avoid the risk entirely by ending or completely changing the activity causing the risk.
 - *Transfer* – share the risk with another party, usually by outsourcing or taking out insurance.
6. Since cyber risk management is a continual process, monitor your risks to ensure they are still acceptable, review your controls to ensure they are still fit for purpose, and make changes as required. Remember that your risks continually change as the cyber threat landscape evolves, and your systems and activities change.

Cyber security measures

As defined by the International Telecommunication Union Cyber security measures are classified as: legal, technical, organizational, capacity building, and cooperation aspects.

- Legal measures aim to provide legislations and an implementable regulatory framework to protect the cyber space.
- Technical measures consider the technological tools (software and hardware) to prevent, detect, mitigate, and respond to cyber-attacks.
- Organizational measures are important for the proper implementation of any type of national initiative or policy.
- Capacity building measures aim to enhance knowledge and know-how in order to promote cyber security.
- Cooperation measures aim to establish partnership between different stakeholders to increase cyber resilience of the organizations against cyber threats.

CASE STUDY-1

Risk Governance and Management at TATA STEEL

Tata Steel operates in an interconnected world with stringent regulatory and environmental requirements, increased geopolitical risks and fast-paced technological disruptions that could have a material impact across the value chain of the organisation. Tata Steel has implemented an Enterprise Risk Management (ERM) process to provide a holistic view of aggregated risk exposures as well as to facilitate more informed decision-making.

The following are the Risks faced by the Steel companies:

1. Macroeconomic Risks
2. Financial Risks
3. Regulatory Risks
4. Operational Risks
5. Market Related Risks

6. Climate Change Risks
7. People Risks
8. Strategic Risks

The followings are detailed analysis of various risks and their mitigation strategies

1. Macroeconomic Risks

Overcapacity and oversupply in the global steel industry as well as increased levels of imports may adversely affect steel prices, impacting profitability.

- Newer developments in the competitive global business environment and potential consolidation among competitors may adversely impact the Company's financial condition and prospects.
- Slower than expected pace of growth in India, coupled with expansion in domestic steel capacity, may result in lower than expected realisations.

Key Mitigation Strategies

- Diversification of product portfolio
- Development of alternate markets
- Participation in industry consolidation.

2. Financial Risks

- Fluctuation in foreign exchange rates due to volatility in financial markets may impact the Company's debt servicing and create uncertainties in accessing the financial markets.
- Substantial amount of debt on the balance sheet may have an adverse impact on the Company's ability to raise finance at competitive rates.
- Changes in assumptions underlying the carrying value of certain assets may result in the impairment of such assets.

Key Mitigation Strategies

- Maximising operational cashflow
- Terming out debt and refinancing debt with favourable covenants
- Appropriate foreign exchange hedging policies
- Integration of business planning and cashflow projections with liquidity management.

3. Regulatory Risks

- Non-compliance to increasing stringent regulatory environmental norms may result in liabilities and damage to reputation.
- The Company operates leased mines. Non-renewal of mining leases may result in the Company having to purchase minerals at higher prices from the open market, impacting its profitability.
- Removal of favourable trade measures such as anti-dumping laws, countervailing duties, etc. may impact the Company's business and prospects.

Key Mitigation Strategies

- Focus on compliance
- Dialogue with regulatory authorities for greater clarity and availing legal consultations for timely clearances
- Working with industry associations towards simplification of rules, a predictive policy regime and transition time for regulatory changes.

4. Operational Risks

- The steel industry is prone to high proportion of fixed costs and volatility in the prices of raw materials and energy. Limitations or disruptions in the supply of raw materials could adversely affect the Company's profitability.
- Failure of critical information systems/ servers that control the Company's manufacturing plants may adversely impact business operations.
- Violation of safety standards, unsafe acts and conditions may lead to Lost Time Injuries (LTIs) or fatalities, resulting in stoppage of operations, loss of personnel, and damage to assets and reputation.

Key Mitigation Strategies

- Enhancing in-house capability and leveraging from past learnings and expertise
- Establishing sources of supplies from alternate geographies
- Enhancing in-house capability in rail logistics and developing Deep Sea Port capacity
- "Committed to Zero" - Safety drives across the Company.

5. Market Related Risks

- Steel is a cyclical industry and excess volatility in the steel and raw material markets may adversely impact the Company's financial condition.
- Competition from substitute materials, or changes in manufacturing processes, may lead to a decline in product demand, resulting in loss of market share.
- Product liability claims could have an adverse impact on the Company's finances.

Key Mitigation Strategies

- Development of value-added products and enhanced services and solutions
- Strengthening contractual agreements.

6. Climate Change Risks

As of May 2018, 195 United Nations Framework Convention on Climate Change (UNFCCC) members have signed the Paris Agreement and 176 countries, including India, have become party to it. The Agreement aims to keep a check on the rising global temperatures and intensify actions required for a sustainable low-carbon future. Going forward, the steel industry will face stringent international and domestic regulations relating to Greenhouse Gas (GHG) emissions. Increasingly stringent climate control regulations may impact the Company's operations and prospects.

Key Mitigation Strategies

- Continued investment in environment related projects
- Collaboration with academic/research institutes for projects on climate change issues.

7. People Risks

- Any labour dispute or social unrest in regions where the Company operates may adversely affect its operations and financial condition.
- Loss of one or more members of the Senior Management, or inability to attract and retain employees, may affect the Company's business and prospects.

Key Mitigation Strategies

- Build relations with key stakeholders including local/regional influential people, interest groups and bureaucracy across levels of administrative machinery (taluka to state level) to address labour or social unrest
- Succession planning for Senior Management to ensure continuity in business
- People related policies for attracting and retaining talent.

8. Strategic Risks

- The Company is growing its Indian operations through organic and inorganic routes. The Company may be unable to realise the anticipated benefits of these growth plans which could have a material adverse impact on its financial condition and reputation.
- The Company may be subject to business risk relating to proposed joint venture with thyssenkrupp AG, including potential delays in completing the proposed transaction and/or the proposed transaction not consummating successfully.

Key Mitigation Strategies

- Strong engineering and project team to commission the expansion project within budgeted time and cost
- Ensuring that learnings from previous projects are applied for improved execution and faster ramp-up of production
- Deputation of experienced team from Tata Steel along with strong review and governance to accelerate the performance of the acquired assets
- Integrate the management of the acquired company to drive synergies. Bring Tata Steel expertise to the acquired assets in operations, maintenance and marketing to ensure high capacity utilisation, cost competitiveness and better product mix
- Experienced team driving focussed consultations with the relevant stakeholders in Europe.

CASE STUDY-2**Risk Management at MARICO**

Marico is one of India's leading consumer products companies in the global beauty and wellness space. The following are the risks associated and their mitigation methods:

Risk management framework At Marico**Identify**

Identify top risk for each function/ business unit level

**Quantify**

Rate the risks on 'impact' and 'vulnerability' factors

Prioritise Top 10 risks at company level

**Plan**

Develop mitigation plan for each risk with relevant efforts and result metrics

Recommend plan to the Board for approval

**Implement**

Implement the risk mitigation plan

**Monitor**

Examine whether the mitigation plans are on track.

Periodically review the existing risks and related metrics

Strategic risk

Strategic risk refers to the internal and external events that may make it difficult, or even impossible, for an organisation to achieve their objectives and strategic goals. These risks can have severe consequences that impact organisations in the long term.

Strategic risk may arise from decisions taken by enterprise leadership or from the organization's position in its environment.

Some examples of strategic risk are:

- The introduction of new products or services by a competitor;
- Unsuccessful mergers or acquisitions;
- Evolving customer demands;
- Changes in senior leadership;
- Damage to the company's reputation;
- Poor cash flows and other financial challenges;
- Changes to the competitive or industry landscape (such as a merger of two rivals into a single, larger one);
- Supply chain issues, such as problems with suppliers or vendors;
- Technology risk.

In addition, some organizations also consider the following as sources and examples of strategic risk:

- Human resource issues, such as staffing shortages;
- Cybersecurity or IT disasters;
- Economic instability;
- Political risk;
- Exchange rate risk.

Any of these risks can affect the firm's future performance and innovation capability. They can also make it harder to respond to change and deal with supply chain and other disruptions.

<i>Risk type</i>	<i>Description</i>	<i>Mitigation strategy</i>	<i>Stakeholders impacted</i>	<i>Capitals impacted</i>
Changing consumer preference	Demand could be adversely affected by shift in consumer preferences. Given the explosion of social media, the speed of such a shift could be unparalleled.	- Investment in consumer insighting to adapt to changing consumer preferences - Actively monitor social media trends to spot early consumer trends; quickly respond to these trends with innovative offerings	- Consumers - Shareholders	- Financial - Social and Relationship - Intellectual
Competitive market conditions	Increase in the number of competing brands in the marketplace, counter campaigning and aggressive pricing by competitors could create a disruption.	- Diversification in product offerings (entered into categories such as healthy foods, male grooming, skincare, premium haircare) - Protect volumes in preference to short-term profitability - Invest in brand building - Agile response mechanism to counter competitive moves	- Consumers - Shareholders	- Financial - Social and Relationship
Under performance of new product launches	The success rate for new product launches in the FMCG sector is typically low. New products may not be accepted by the consumer or may fail to achieve the sales target. This risk is even more pronounced in cases where industry leaders invest in creating new categories.	- Invest in a new product development process with a funnel approach to ensure continuous flow of new ideas, coupled with rigorous governance around scalable innovations - Prototyping approach to new product introductions for accelerated learning and adjustment - Identify and invest in big-ticket new ideas in the chosen categories for driving growth - Resilient presence in marketplace with adequate investments in brand building	- Consumers - Shareholders	- Financial - Social and Relationship - Intellectual

Private labels	Expansion of modern trade and e-commerce could lead to the emergence of private labels.	Invest in brand building to improve the saliency of our brands in the consumers' mind and partner with modern trade and e-commerce in category management	Consumers Shareholders	Financial Social and Relationship
-----------------------	---	---	------------------------	-----------------------------------

Financial risk

Financial risk is the possibility of losing money on an investment or business venture. Some more common and distinct financial risks include credit risk, liquidity risk, and operational risk. Financial risk is a type of danger that can result in the loss of capital to interested parties.

Key Takeaways

- Financial risk generally relates to the odds of losing money.
- The financial risk most commonly referred to is the possibility that a company's cash flow will prove inadequate to meet its obligations.
- Financial risk can also apply to a government that defaults on its bonds.
- Credit risk, liquidity risk, asset-backed risk, foreign investment risk, equity risk, and currency risk are all common forms of financial risk.
- Investors can use a number of financial risk ratios to assess a company's prospects.

Pros and Cons of Financial Risk

S.No.	Pros	Cons
1	Encourages more informed decisions.	Can arise from uncontrollable or unpredictable outside forces.
2	Helps assess value (risk-reward ratio).	Risks can be difficult to overcome.
3	Can be identified using analysis tools.	Ability to spread and affect entire sectors or markets

The four types of financial risks are- income risk, expenditure risk, asset or investment risk, and credit risk.

Risk type	Description	Mitigation strategy	Stakeholders impacted	Capitals impacted
Volatility in interest rates	Though the FMCG sector is not capital intensive, fund requirements arise on account of inventory position building, capital expenditure undertaken or funding inorganic growth.	• Well-defined framework for capital gearing • Maintain a liquidity chest for immediate working capital requirements • In case offoreign currency borrowings, implement hedging as per policy	• Shareholders	• Financial

	Changes in the interest regime and in the terms of borrowing could impact the financial performance of the Company. Further, this risk may also impact income on Company's investment and mark-to-market hit on its investment portfolio.	• Manage interest rate risk to investments by implementing board-approved investment policy, which focuses on safety and liquidity, thereby mitigating short-term interest risks.		
Foreign currency exposure	Marico has significant local presence in Bangladesh, South East Asia, Middle East, Egypt and South Africa. The Company is thus exposed to a wide variety of currencies. Fluctuations in these currencies could impact the Company's financial performance.	• While the 'translation risk' will continue to be unhedged, Marico has a well-defined hedging framework for managing any foreign exchange risk in India and Bangladesh. The Board-approved policy in this regard is periodically reviewed for its effectiveness.	• Shareholders	• Financial
Macro-economic factors	Factors such as low GDP growth and high food inflation could result in down trading from branded to non-branded or premium to mass market products.	• Focus on value-added products available to masses at affordable prices by driving aggressive cost management • Focus on franchise growth in preference to short-term profitability • Portfolio diversification, which is one of the pivots of the future	• Consumers • Shareholders	• Financial • Social and Relationship
Cyber and data security	Disruption in business operation due to non-availability of critical information systems through cyber-attack and loss of sensitive information due to unauthorised access.	• Identification of business critical IT systems and putting in place disaster recovery plan. The plans are tested periodically and kept relevant. • Implementation of IT security practices in line with ISO 27001 standards	• Shareholders • Value-chain partners • Consumers	• Financial • Intellectual • Social and Relationship

		• Implementation of the latest cyber security technologies with preventive, detective and reactive controls		
--	--	---	--	--

Operational risk

Operational risk is the risk of losses caused by flawed or failed processes, policies, systems or events that disrupt business operations. Employee errors, criminal activity such as fraud, and physical events are among the factors that can trigger operational risk.

Most organizations accept that their people and processes will inherently incur errors and contribute to ineffective operations. In evaluating operational risk, practical remedial steps should be emphasized to eliminate exposures and ensure successful responses.

If left unaddressed, the incurrence of operational risk can cause monetary loss, competitive disadvantage, employee- or customer-related problems, and business failure.

The challenges witnessed in mitigating operational risks are as under:

1. The data required is not readily available.
2. Operational complexity is growing in enterprises.
3. The universe of operational risk types expands.
4. Operational risk oversteps with other risk functions.
5. Other risk functions feel threatened by what seems like duplicative risk function and don't cooperate.
6. Operations staff complain that monitoring and reporting take time away from their other responsibilities.

<i>Risk type</i>	<i>Description</i>	<i>Mitigation strategy</i>	<i>Stakeholders impacted</i>	<i>Capitals impacted</i>
Commodity risk	Unexpected changes in commodity prices and supply could impact business margins and ability to service demand. The past few years have witnessed wide fluctuations in input prices. As a result, the overall uncertainty in the environment continues to be high.	• Commodity procurement is driven by a comprehensive process manual for each category that governs norms related to price discovery, inventory policy, supplier management, governance mechanism • Company policy defines purchase of commodity in line with business requirement and in accordance with the inventory policy and does not encourage speculative buying or trading of said commodity either in physical form or in exchange	• Shareholders • Value-chain partners	• Financial • Manufactured

Political instability in operating geographies	Unrest and instability in countries of operation could significantly impact business results.	• A comprehensive insurance programme to hedge all insurable risks • At a macro level, our country selection template emphasises geopolitical stability and robust growth prospects	• Shareholders • Members	• Financial • Manufactured
Underperformance of acquisition deliverables	Acquisitions may impose a financial burden on the parent entity. Integration of operations and cultural harmonisation may also take time, thereby deferring benefits of synergies.	A well-defined playbook for selection of targets, due diligence, value finalisation and • Well-defined performance tracking systems to monitor progress periodically • Cross-application of governance practices of the parent organisation soon after the takeover to ensure controls	• Shareholders • Members	• Financial • Human

Compliance and Governance risks

Compliance risk is an organization's potential exposure to legal penalties, financial forfeiture and material loss, resulting from its failure to act in accordance with industry laws and regulations, internal policies or prescribed best practices. Compliance risk is also known as integrity risk.

Governance risk includes the risks related to an organization's ethical and legal management, the transparency and accuracy of company performance, and involvement in other ESG initiatives important to stakeholders.

<i>Risk type</i>	<i>Description</i>	<i>Mitigation strategy</i>	<i>Stakeholders impacted</i>	<i>Capitals impacted</i>
Non-compliance with regulatory requirements	Inadequate compliance systems and processes can pose reputation risk for the Company. This could expose the Company to legal consequences, resulting in financial losses and penalties.	• Invest in IT-enabled compliance systems and processes • Ensure all functions and units are aware of the laws and regulations to comply with • Ensure adequate monitoring mechanism towards compliance • Communicate periodically to reiterate the importance of compliance	• Government body • Members	• Financial • Social and Relationship

Violation of ethics and business integrity	Failure to act with integrity or behave in a manner inconsistent with the Marico purpose statement and values defined, can damage corporate reputation and business results.	• Code of Conduct (CoC) and Marico Code of Business Ethics (MCoBE) outlines the Company's commitment to ethics and integrity • Robust vigil mechanism, which enables the stakeholders to report concerns about unethical behaviour, fraud or violation of code • Detailed personal orientation and mandatory certification on CoC for all employees • Effective oversight by the Board of Directors	• Members • Value-chain partners	• Financial • Human • Social and Relationship
--	--	--	---	---

Environmental risk

Environmental risk is the probability and consequence of an unwanted accident. Because of deficiencies in waste management, waste transport, and waste treatment and disposal, several pollutants are released into the environment, which cause serious threats to human health along their way.

Examples of environmental hazards include:

- Air contaminants.
- Toxic waste.
- Radiation.
- Disease-causing microorganisms and plants.
- Pesticides.
- Heavy metals.
- Chemicals in consumer products.
- Extreme temperatures and weather events.

<i>Risk type</i>	<i>Description</i>	<i>Mitigation strategy</i>	<i>Stakeholders impacted</i>	<i>Capitals impacted</i>
Disruption due to climate change events	Climate change related events that have the potential to disrupt Marico's operations, include changes in weather patterns	• Embrace climate change adaption and mitigation measures • Promote scientific farming practices that are	• Shareholders • Community • Value-chain partners	• Financial • Natural • Manufactured • Social and Relationship

	such as increased temperatures and altered rainfall patterns. This will affect the planning and day-to-day operation as the risk arises from availability of agriculture input materials, climate-related policy changes, evolving regulations and increased consumer concerns.	resilient to climate-related adverse impacts • Continuous monitoring of environmental policies and regulations • Investment in low-carbon technologies and equipment, and renewable and clean energy sources • Adoption of CDP climate change disclosures and science based target (SBT) framework approach to minimise operational environmental footprint	• Consumers • Government Body	
Adverse impact of energy and water scarcity	Energy and water are crucial for our business and day-to-day operations, Non-availability of these resources will lead to operational disruptions and impact production plans and product delivery.	Continuous focus on energy conservation measures Investment in energy-efficient systems Operationalising reduce-reuse-recycle model of water management across plants Comprehensive watershed management programmes leading to harvesting and ground water recharge augmenting supply and water availability for community	• Shareholders • Community	• Financial • Natural • Manufactured • Social and Relationship
Handling of plastic packaging and waste	The regulatory, consumers and community response to the environmental impact of plastic wastes and emerging regulation by different state governments on ban of use of certain plastics, require us to find sustainable packaging solutions.	Adopt circular approach based on 4Rs - reduce, recycle, replace and recover Investment in R&D measures to enable design innovations and reduce weight of plastic used undervalue enhancement approach by Marico	• Community • Government body • Value-chain partners	• Natural • Social and Relationship • Intellectual

		Strategic partnerships and collaborations to drive penetration of recyclable plastics and enhance use of recycled plastics Honour obligations under the Extended Producer Responsibility (EPR) commitments Continuous monitoring and tracking of plastic waste policies and regulations		
--	--	--	--	--

Social risks

Social risk comes from activities that affect the communities around the business. Things like labor issues, human rights issues, public health issues, and political uncertainty qualify as social risk.

<i>Risk type</i>	<i>Description</i>	<i>Mitigation strategy</i>	<i>Stakeholders impacted</i>	<i>Capitals impacted</i>
Talent acquisition and retention	Mismatch in hiring and attrition of skilled talent the Company's ability to pursue its growth	• Marico's culture of openness, transparency and meritocracy coupled with its growth orientation helps attract top talent • Marico's talent value proposition of building challenging, enriching and retaining top talent • Invest in 'hiring right' and 'talent development and engagement' best practices	• Employees	• Human • Manufactured
Community distress in operating locations	Social licence to operate refers to the level of acceptance by local communities in proximity to our operations. The absence of understanding and inability to maintain a harmonious relationship with communities could	• Commitment to sustainable and inclusive growth in all social outreach programmes and initiatives with an aim to augment social infrastructure • Constant engagement channels with the local community stakeholders to understand their needs	• Community	• Manufactured • Social and Relationship

	result in damage to our brand, reputation and pose risk to our operations.			
Failure to meet product quality and safety requirements	The quality and safety of our products are of paramount importance for our brands and our reputation. Any failure to meet the product quality and safety requirements reputational risk, loss of consumer trust and potential exposure to regulatory actions.	• Robust system to ensure compliance to regulatory requirements • Assessment of quality and safety aspects of products at each stage in the value chain • Stringent quality and safety compliance check for suppliers before inducting in the system • Ingredients assessment in line with the requirements set for its usage according to the law of the land • Facilitate consumer feedback on product safety and quality through dedicated Consumer Service Cell (CSC) • Robust crisis management framework	• Government • Consumers • Value-chain partners	• Financial • Manufactured • Intellectual • Social and Relationship

CASE STUDY-3

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.² 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. The sustainability team monitors water resources at all campuses and develops tailored responses at each campus.

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

Infosys’ risk management approach to water scarcity at the site and regional levels has been critical for realizing value for its customers, employees and communities. 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.

CASE STUDY-4

Enterprise Risk Management in Banking

A risk management framework and a risk appetite statement serve as the two pillars around which Toronto-based TD Bank structures its risk management. The enterprise risk framework outlines risk management procedures for identifying, evaluating, and controlling risk as well as defining the risks the bank must manage. The bank’s readiness to accept risk in order to achieve its growth goals is described in the risk appetite statement. The risk committee of the company’s board of directors is in charge of both pillars.

The International Organization for Standardization’s (31000) standard, which has subsequently been modified, included risk management frameworks as a significant component. The standards offer general recommendations for risk management initiatives.

Also, the Committee of Sponsoring Organizations of the Treadway Commission’s efforts led to the creation of risk management frameworks (COSO). The organisation was formed to combat corporate fraud, and one of its focuses was risk management.

TD moves on to the risk appetite statement after finishing the ERM framework.

The bank, which established a sizable foothold in the United States through significant acquisitions, decided that it will only take on risks that satisfy the following three requirements:

- The risk is appropriate for the company’s plan, and TD can recognise and control it.
- The risk does not expose the bank to a high danger of suffering a sizable loss.
- The danger does not put the business at risk of damage to its reputation and brand.

Strategic risk, credit risk, market risk, liquidity risk, operational risk, insurance risk, capital adequacy risk, regulator risk, and reputation risk are a few of the significant hazards the bank faces. These categories are described by managers in a risk inventory.

Annual reviews are conducted of the risk framework and appetite statement, which are monitored on a dashboard against indicators including capital adequacy and credit risk.

To mitigate risk, TD employs a three lines of defence (3LOD) strategy, a technique that is well regarded by ERM professionals. These are the three lines:

- A business unit and corporate policies that implement controls, manage risk, and keep track of it.
- Rules and oversight that ensure risk monitoring, evaluation, and adherence to the risk appetite and framework.
- Internal reviews that independently confirm the effectiveness of risk-management practises.

CASE STUDY-5

Enterprise Risk Management in Pharmaceuticals

Risks to drug firms include those related to consumer trust, regulatory action, and challenges to product quality and safety. ERM experts stress the significance of ensuring that strategic aims do not contradict in order to prevent these risks.

Such a dispute resulted in a breakdown in risk management for Britain's GSK, among other problems. Early in the new millennium, the corporation worked to boost profits and sales while simultaneously making sure that its products were safe and effective. Failure to adhere to current good manufacturing standards (CGMP) at the company's plant in Cidra, Puerto Rico, was one danger the business faced.

CGMP involves overseeing and controlling the manufacturing process, managing risk, and assuring the safety of both raw materials and final pharmaceutical products. Escalating repercussions for CGMP non-compliance might include warnings, recalls, and even criminal charges.

In order to resolve U.S. allegations over medications produced at the Cidra plant, which the company eventually closed, GSK's unit entered a guilty plea and made a \$750 million payment in 2010. In 2004, a sacked GSK quality manager notified authorities and brought a whistleblower action. The U.S. Department of Justice stated in its announcement of the consent decree that the plant had a history of bacterial contamination and that several medications produced there in the early 2000s breached safety regulations.

The whistleblower claimed that GSK's ERM process was unable to respond to warning indicators of CGMP non-compliance in a number of ways. The U.S. Food and Drug Administration sent the corporation warning letters about the activities at the plant in 2001, but the company did not address the problems.

Also, the business disregarded the quality manager's compliance report, which recommended that GSK shut down the plant for two weeks in order to address the issues and alert the FDA. Court documents claim that plant employees simply skimmed off the top of rejected goods and sold them illegally. Also, they manually scraped the interior of an antibiotic tank to obtain more product, contaminating the product in the process.

CASE STUDY-6

Enterprise Risk Management in Insurance

The Zurich Insurance Group in Switzerland recognises that risk is a given for insurers and strives to take calculated risks within a given risk tolerance.

The enterprise risk management framework of the multinational insurer attempts to safeguard capital, liquidity, earnings, and reputation. Risk management is based on governance, and the framework specifies who is responsible for accepting, managing, overseeing, and disclosing risks.

The business monitors internal and external threats to its strategy and financial plan using an unique process called Total Risk Profiling (TRP). TRP evaluates risk based on probability and severity, and aids in developing and putting into action mitigating actions.

Zurich's tolerance for risk is constrained by its desire to maintain a sufficient level of capital to receive a rating of AA from rating agencies. The business employs its own Z-ECM, or Zurich Economic Capital Model, for this. With a statistic that compares risk profile to risk tolerance, the model estimates risk tolerance.

The corporation wants to hold capital between 100 and 120 percent of capital at risk in order to keep the AA rating. Under 90 percent is below risk tolerance, while beyond 140 percent is deemed overcapitalized (therefore at risk of limiting growth) (meaning the risk is too high). The insurer considers taking mitigating action on either side of 100 to 120 percent (90 to 100 percent and 120 to 140 percent).

Regulators' expectations for the amount of capital that Zurich must maintain are heavily influenced by Zurich's estimate of risk and the characteristics of those risks. The risk matrix is a well-liked tool for risk assessment, and "Free, Customized Risk Matrix Templates" contains a number of different templates.

Zurich discovered that its biggest exposures in 2020 were market risk, including declining asset valuations and interest rate risk, insurance risk, including significant payouts for covered customer losses, which it hedges through diversification and reinsurance, credit risk in assets it holds and receivables, and operational risks, including internal process failures and external fraud.

ADDITIONAL CASE STUDIES IN RISK MANAGEMENT

1. *Cyber Security Risk Management*

Case study 1: A Medical Practice is Hit with Ransomware

Medical practices are a prime target for ransomware attacks due to the amount of valuable data they hold. In addition to a potential ransom payment, personal data and credit card information can be sold by cyber criminals on dark web marketplace forums. Small individual and group practices may also lack comprehensive cybersecurity, making them an easy target for malicious attacks.

Ransomware frequently enters the system via a virus on an email attachment. It searches on the computer for data to encrypt and then spreads to other computers and files on the network. The virus encrypts the data, making it unreadable and unusable. The attacker then demands an untraceable digital payment in exchange for a decryption key. The data may or may not be released after payment.

The Cybersecurity Challenge

The billing department of a medical practice received a ransomware demand on their desktop screen. The practice manager contacted their IT support person. IT shut down the network and began investigating. The practice had no access to anything on their network and switched to handwritten paper records for scheduling, clinical notes and prescription writing.

The IT support provider was not able to solve the issue, and needed cybersecurity expertise to investigate and halt the attack. Cybersecurity experts determined that the virus had entered the system as an email attachment that resembled an invoice. Once it was on the computer, the virus searched for data to encrypt and then spread to the rest of the network.

Fortunately, the practice had offsite physical backup of most of the records and did not need to pay the

requested ransom. The backup data was requested from storage, shipped, cleared of any remnants of the virus and then reloaded back onto the network. Unfortunately, recovery took more than a week due to the method of backup and created unexpected additional charges for recovery services.

Recovery solutions and key takeaways

This practice averted devastating failure by having backup data available to reload. The cybersecurity team provided disaster response, mitigation and recovery services and then implemented updates and additional protections to lessen the risk of cyber-attacks and data breaches. Many of the security products in use at the practice were unpatched and outdated and had not been reviewed for years. The team conducted a full assessment and submitted a comprehensive plan. Here are some of the changes, updates and improvements put in place:

Technical Controls:

- Email filters
- Antivirus software update
- Local and cloud data backup
- Firewall updates
- Administrative access restrictions
- HIPAA policy and procedure controls addressed

Employee Awareness Training:

- Recognizing suspicious emails
- Downloading from unfamiliar websites
- Recognizing phishing attempts
- Using approved portable storage devices
- New employee HIPAA security and privacy training
- Physical safeguards for data
- Updated policies and procedures enacted

Disaster Response and Business Continuity Planning:

- Data backup plan
- Backup testing
- Disaster recovery plan

Monitor Staff Usage and Practices:

- Phishing assessments
- User activity monitoring
- Security assessments
- Compliance requirement adherence
- Verify cybersecurity capability and knowledge of IT employees

Insurance review:

- Update professional liability insurance for data breaches
- Review cyber insurance for coverage for data breaches and response

Case Study 2: Phishing Attack and Employee Password Compromise

Phishing attacks are a type of social engineering attack designed to steal data, login credentials and credit card numbers. Cybercriminals masquerade as a fellow employee or other trusted entity and trick users with a malicious link. The link may be used to spread ransomware in the system or get information such as passwords and logins or credit card numbers. These attacks can have devastating results, including financial loss and damage to credit and reputation, and can also be part of a scheme to gain access to a larger partner company's data.

The Cybersecurity Attack Challenge

An employee at a regional grocery retailer received an email from his co-worker, informing him that she was sharing a document with him. He had received documents from her before, but wasn't expecting one that day. The email was vague and had no project details, which was unusual. He clicked the link, and it opened to what looked like the usual file-sharing site the company typically uses. He was asked to enter his login and password, then got an error message. He tried again and got another error message.

The employee contacted his manager to request a password reset and report trouble downloading a shared document. He also mentioned that he called the co-worker, and she said she had not sent him anything. The manager was suspicious that this was likely a hacking incident.

Remediation, Recovery and Awareness Training

The cybersecurity team was contacted and immediately reset everyone's passwords. They verified that the email was a phishing attempt using a fake site. They also checked security settings for any suspicious rule changes, and informed everyone at the company about the incident. Two-factor authentication for signing into accounts was implemented to alert users to any new sign-ins from their account. The security team also scheduled security awareness training and testing for this company. Employees who receive comprehensive training are better able to spot phishing attempts by learning techniques such as checking the URLs of any suspicious emails and verifying with the sender directly about anything that appears unusual.

Thankfully, the employees alerted management right away, which helped prevent data theft and compromise. Management made the decision to engage the cybersecurity team to respond quickly, halt the attack and verify no other systems were compromised. The phishing attack alerted upper management to the need for additional security training to educate and reduce cyber risk in this area.

Case Study 3: Infrastructure Monitoring and Weak Passwords

An industrial thermostat manufacturer noticed unusual activity on the network. The cybersecurity team examined logs that indicated someone was logging in to networks and servers at unusual times using company credentials. No evidence of malware or Trojans was found. The cybercriminal logged in at will using a very weak, common password. After changing the password, the team investigated to determine whether anything was stolen and whether the attacker was still getting into the system.

The cybersecurity experts were able to remotely image the servers and preserve the forensic data of the incident and remediation for reporting and insurance purposes. The investigation revealed that the cybercriminals stole a large amount of data by converting it into an image and hiding it on the website. They could revisit at any time to retrieve the image without logging in.

Incident Response and Recovery Objectives

The data stolen was not considered confidential or protected by regulations, so no customers or regulators had to be notified. The incident did serve to highlight cyber defense weaknesses in the company's daily practices and infrastructure monitoring. A remediation plan was put in place by the cybersecurity consultants that included these items:

- Update security policy and regularly test for compliance
- Conduct regular employee security awareness training
- Regularly change strong passwords
- Monitor administrative accounts for unusual usage
- Monitor network traffic and data access
- Protect and monitor infrastructure security

2. Financial Risk**Case Study : USAA**

According to the banking and compliance press, the Financial Crimes Enforcement Network (FinCEN) and the Office of the Comptroller of the Currency (OCC) fined USAA Federal Savings Bank (FSB) \$140 million by for failing to implement and maintain a BSA/AML compliance program.

Deficiencies pointed out include inadequate internal controls; detection, evaluation, and reporting of suspicious activity; staffing; training, and third-party risk management, as well as significantly understaffed BSA/AML compliance departments.

This is a common practice in banking, especially when many workloads are coupled with tight deadlines. However, USAA failed to train or ensure contractors had the necessary qualifications, worsening the situation.

It has been reported that the new transaction monitoring system implemented by USAA FSB is "too sensitive and generates an unmanageable number of alerts and cases."

An important lesson from this case is that "Ignore regulatory findings at your own risk." Heavy regulatory fines do not occur by accident: They result from accumulating failures and procrastinating about implementing the necessary changes and improvements to meet regulatory requirements. Due to the difficulty and discomfort associated with transformations and change, most firms delay implementing changes in response to regulatory findings until the last minute. This may be too late, as in the case of USAA.

A weak control environment can attract fines by regulators anywhere in the world, as has happened in the US, UK, and Asia.

In Asia, for example, regulators charged banks fines totaling \$5.1 billion for failing to comply with AML laws. Banks are required to review, verify, and report suspicious activity in response to regulatory findings and sanctions.

An AML risk management framework should incorporate technology and automation for detection and alerts as well as proper recording of false positives and false negatives.

Moreover, the COVID-19 pandemic changed customer and business behavior, particularly with the rise of remote transactions, which makes it more difficult for financial institutions to detect anomalies.

Fraud risk management and AML are constantly changing as new opportunities present themselves for fraudsters in new economic and business environments.

3. Market Risk

Case Study 1: China Aviation Oil (Singapore) Corporation Limited's Jet Fuel Scandal (2005)

China Aviation Oil (Singapore) Corporation Ltd. (CAO) was involved in the biggest scandal of the city-state of Singapore since the Nick Leeson case (1995), in which Baring Bank collapsed and lost around \$1.3 billion in speculative trading. Following losses of around \$550 million, CAO filed for bankruptcy in November 2004. Improper application of accounting principles, and inadequate risk management systems for the speculative options deal, were the major contributing factors towards CAO's failure.

CAO's major portion of business came from deals in jet fuel procurement. By 2000 it obtained 92% market share of jet fuel imported to China's civil aviation industry. A marked increase in the profits of the company was due to the monopoly CAO had in the market. Enjoying monopoly in the market the following years showed a marked increase in the profits of the company. However, wrong bets on fuel prices in 2004, by taking a bearish stance in the jet fuel market, forced the company into a scandal which cost CAO dearly.

The CEO, Mr. Chen Juilin, was held responsible for the loss and arrested and charged with fraud and failure to report losses and subsequently was fined \$330,000/= and imprisoned for over 4 years.

Trajectory to Devastation

CAO started its option trading in 2002. Initially, CAO used to deal only in derivatives of futures and swaps to hedge its jet fuel market risk. However, in the mid-2003, in order to bolster its profile in the market, CAO started trading in speculative derivative options.

The objective behind the speculative options trading was to generate profits from the premium. However, the risk of such trades was not properly assessed by CAO; in fact CAO did not have the proper risk management framework to handle such complex options. The PwC reports:

The fact that the company commenced speculative options trading in the first quarter of 2003, without putting in place a proper risk management environment, raised questions on the strength of its corporate governance.

Originally, CAO took a bullish view of the jet fuel market. Predicting that the market price of jet fuel would continue its upward trend, CAO took a long position in the market, and sold puts and bought calls. CAO predicted correctly. Favourable market trends resulted in CAO exercising the call options at expiry. Written put options expired worthless. CAO gained from the exercise of call options and from the premium of put options; this strategy yielded enormous profit for CAO in the first three quarters of 2003.

By the end of 2003, CAO revised its strategy to a bearish stance; CAO predicted that the trend of jet fuel prices would reverse and the prices of jet fuel would go down. The CEO signed contracts with several banks, buying put options and selling call options. But that was a wager the company lost. The prices soared well above the strike price of the call of \$38 and CAO faced a large deficit.

Losses could have been floored if CAO had followed the risk management procedure, where a stop-loss limit would have affectively applied and further trading halted. However, despite mark to market losses of \$30 million by mid-2004, the CEO increased the bet; he bought back the short-dated option and sold longer dated option. That was done in the hope that the jet fuel prices would eventually decline and the premium could be used to cover the losses. The move instead resulted in increased exposure for CAO.

The jet fuel price continued its upward trend and by October 2004, the mark-to-market losses increased to \$180 million. By November 2004, when the losses had mounted to \$550 million, CAO was required to meet

the margin requirements but was not completely successful in doing so. CAO in their Scheme of Arrangement, dated the 30 November 2004, stated:

“the company was unable to meet some of the margin calls arising from its speculative trades, resulting in the company being forced to close the positions with some of its counter parties. From 26 October 2004 to date, the accumulated losses from these closed positions amounts to approximately US\$390 million. The Company is in the process of closing the remaining outstanding positions and estimates the losses from the closure of these positions to be approximately US\$160 million” (China Aviation Oil).

Reporting

CAO started trading options in 2002 and 2003 but the trading was not disclosed in the financial statements. Then from March 28, 2003, CAO started trading options on its own account. By not following the best accounting principles, CAO made a very crucial error in the valuation of options. CAO valued options at intrinsic value and ignored time value of money. Such erroneous valuation of the option was done throughout 2004 by CAO. That resulted in accounting errors being present in the all quarterly disclosures.

According to the assessment done PwC, CAO should have followed IAS 39 and FAS 133; two accounting standards that recognized derivatives at fair market value. Taking time value of money into consideration, losses and not profits as reported by CAO in its disclosures, were incurred for each of the quarters:

S\$ Million	1Q**	2Q	YTD*** June 04	3Q	YTD September 04
Reported PBT*	19.00	19.30	11.30	11.30	49.60
Adjusted PBT*	-6.40	--58.00	-64.40	-314.60	-379.00

* PBT = Profit before tax

** Q = Quarters

*** YTD = Yield to maturity

(Source: PricewaterhouseCoopers)

Following such heavy losses, on December 02, 2004, COA announced it would be seeking protection from creditors to avoid bankruptcy.

Penalties

In August 2005, China Aviation Oil Holding, the parent company, paid an S\$8 million penalty. China Aviation Oil Holding breached Singapore's insider trading laws by selling 15% shares of CAO to Deutsche Bank without informing the share holders.

In February 2006, CAO's former finance chief, Peter Lim, was sentenced two years in prison for his part in the derivatives trading scandal. He was found guilty of conspiring to cheat adviser Deutsche Bank and fined S\$150,000 (US\$92,000) for releasing false information.

On March 15, 2006, former CEO of CAO, Mr. Chen Juilin, pleaded guilty to six criminal charges; he was fined S\$330,000 and was sentenced to 51 months in jail.

Chronology of the Events

Dates	March 2003	Last term of 2003	Throughout 2004	November 30, 2004	December 02, 2004	February & March 2006
Events	Enters the speculative market with bullish strategy in jet fuel market	Took a bearish view of the jet fuel market	CAO facing significant mark-to-market losses because of jet fuel prices rising steeply	Discloses losses of \$550 million	Announced it would be seeking protection from creditors	Perpetrators punished

Cause of Collapse

CAO had a risk management system in place since 2002. But neither the board nor the internal audit committee had the time and the expertise to understand the system. Additionally, the system was not prepared with speculative options derivative trading in mind but was designed for swaps and futures trading. Even then when mark-to-market losses were increasing, the system provided a loss-stop limit which was blatantly ignored by CAO. CEO restructured the options more than once in the period of crises which further increased risk exposure of CAO.

The accounting methods used were not meant for complex options. The accounting methods used looked at the intrinsic value of the option and ignored the time value component; the values of options differed significantly from those of the counter parties. Additionally, losses were not reported and accounting errors were made to show favorable financial statements.

Key Takeaways

The scandal provides another example in which: regulatory compliance, profit reporting and bending laws took precedence over the risk management and proper accounting reporting. There was a lack of oversight and inadequate knowledge of the market. Considering this, the lessons to take away from this case study are:

1. Better control and enhancement of risk management is necessary in order to avoid sharp, unprecedented and unexpected losses.
2. An independent risk management department which provides on the ground vigilance and responsiveness to ensure risk management policies are adhered to.
3. A team which has the required expertise to manage risk.
4. Build early-warning systems, which encourage employees to find potential risks and report them to management.
5. The financial reporting must follow the best practice with frequent and detailed disclosures.
6. In order to know the loss in different scenarios stress testing must be done.
7. One should not indulge in a market one does not have good knowledge of.

Many of the factors contributing to the failure of CAO are similar and equally applicable to different business contexts so it is important to learn from it and not to repeat it

Case Study 2: JP Morgan Chase London Whale CIO synthetic credit portfolio (SCP) debacle*Introduction*

JPM's CIO was responsible for investing the excess cash of the bank. The main investment was in high quality

income bearing securities such as whole loans, mortgage backed securities, corporate securities, sovereign securities, asset backed securities, etc. The synthetic credit portfolio (SCP) was constructed in 2007 in order to protect the bank against adverse credit scenarios such as widening credit spreads during the financial crisis.

The synthetic credit portfolio positions were based on standardized credit default swap (CDS) indices. The positions were the purchase and sale of protection against credit events of the corporate issuers tied to the basket of CDS included in the indices. If the protection was bought (short risk positions) the cash flows were as follows:

Pay	Receive
Periodic Premiums	Payments if and when a company included in the CDS basket defaulted, filed for bankruptcy or restructured debt.

If the protection was sold (long risk positions) the opposite would be true – in exchange for receiving premiums, the CIO would have to pay protection if a credit event were to occur in the concerned index. Positions were in the different CDS indices & tranches (CDX, iTraxx; Investment grade and High Yield).

While the SCP performed well in 2009 netting the CIO \$1 billion, the notional size of its synthetic portfolio increased significantly from \$4 billion to \$51 billion during 2011, in light of the European default crisis. In December 2011, following a more positive outlook for the economy, CIO was asked to reduce the exposure of SCP and the risk weighted assets of the CIO.

Given the loss estimate of \$500 million for unwinding synthetic credit portfolio positions by selling them off due to current market conditions, loss of premium & execution costs, and following a chance win of \$400 million on a speculative trade, the CIO instead opted to reduce RWA by implementing a hedging strategy using a portfolio of options, in line with the Comprehensive Risk Measure (CRM) of Basel 2.5, and a new VAR model to calculate the risk & limits.

The new model significantly reduced risk numbers, allowing the traders to implement the options portfolio strategy. However, the strategy did not work as expected, given that the market environment and correlation between positions were not in line with traders' expectations, and instead resulted in trading losses that continued accumulating. CIO traders tried to defend their existing positions by further growing their portfolios with huge trades to support market prices. Given the illiquidity of the markets, however, the CIO became significant market movers in these securities, thus reducing their ability to exit the markets without being impacted negatively by it.

For the first quarter financial results, CIO traders had tried to downplay mark to market losses by setting marks that were at significant variance to the midpoints of dealer quotes in order to show a better than actual MTM picture on the books. This eventually led to a restatement of the first quarter earnings and refiling of financial results. Mark to market losses grew to \$5.8 billion as of 30th June 2012.

Chronology of Events

Years / Dates	Events
2007	Launch of SCP
2011 Last Quarter	SCP asked to evaluate reducing RWA
January 2012	Trading losses of \$15 million on unwinding positions. VaR & CSBPV limit breaches.
23 January 2012	Temporary approval of VaR limit increased

31 January 2012	Implementation of new VaR model
January - March 2012	Notional value increased to balance portfolio & defend positions
February & March 2012	Issues & RWA reduction strategy not discussed in review meetings
21 March 2012	Fears that the SCP's positions leaked to market
22 March 2012	CSW 10% limits exceeded
23 March 2012	CIO head calls for SCP to stop trading
29 March 2012	Stress limits breached
March – April 2012	Understatement of MTM losses
5 April 2012	CIO head informed JPM's senior management of some SCP issues
6 April 2012	London Whale article published by Bhoomingdale & WSJ
April 2012	Misleading loss estimates & market recovery shared with senior management
29 April 2012	Firm wide Market Risk handed over responsibility of CIO
30 April 2012	\$800 million losses over 6 trading days
10 May 2012	Discloses \$2 billion losses for SCP & a reversion to the former VaR model
13 July 2012	Restatement of first quarter results

Absence of regulatory and corporate oversight

The CIO was not a client facing unit of the bank. For this reason, it did not receive the same scrutiny as other portfolios would receive in terms of regulatory compliance and corporate oversight.

There were no separate portfolio limits based on market values or asset type limits set for the synthetic credit portfolio (SCP) and there was no daily reporting that was specific for the SCP to senior management. In addition, Risk committee meetings were held infrequently and did not seem to have any specific charter or mandate and were rarely attended by other than CIO personnel.

Due to the lack of oversight CIO traders were able to engage in speculative and risky derivative trades which were not in line with the CIO's traditional investment strategy of long term investments with credit derivatives for hedging purposes only.

Regulatory oversight too was lacking. The Office of the Comptroller of Currency did not follow up on previous concerns raised regarding the transparency of the CIO's investment decisions. They also did not raise the alarm when the update to a new VaR model resulted in risk numbers that were 50% lower than prior numbers, being unaware that a new model was being used.

London Whale – Inexperienced and unqualified personnel – CIO CRO

Risk management specifically for the credit derivatives portfolio of the CIO unit does not appear to have been a priority until after the size of the synthetic credit portfolio had already become unwieldy in January 2012. The task force assigned by JP Morgan Chase Bank to investigate CIO Losses reported that the risks of the trading strategies were neither adequately analyzed nor questioned prior to their implementation.

Prior to February 2012 the risk management function was overseen by Peter Weiland chief market risk officer who reported directly to the bank's CRO, Barry Zubrow. Mr. Zubrow, as the JPM task force report admits, did not take adequate steps to strengthen the risk and control framework for the CIO, while Mr. Weiland did not have the necessary clout to withstand the pressures from the traders and CIO management. Further, the CIO Risk team was unstaffed and did not have proper direction.

In February 2012, after the SCP had already gotten out of hand, Irv Goldman was appointed as the CIO's first CRO. For Mr. Goldman, this was his first risk management position in his career which mainly had a capital markets focus. He would not have had the necessary experience to adequately address the deteriorating risk position of SCP during the period February 2012 to May 2012 as he was still learning the ropes of his new position.

With respect to corporate governance, Mr. Goldman's appointment is itself a matter of controversy considering his lack of risk management experience, his appointed by his brother in law, Zubrow, his contentious past, having been fired from a previous position at Cantor Fitzgerald for insider trading in 2007.

Quantitative analyst – VaR model for the synthetic credit portfolio

The head of the European Equity and Credit unit of the International Investments Office, Javier Martin-Artajo and his Relative Value Strategic Trading head, Bruno Iksil (the London Whale) came up with a strategy to hedge the existing portfolio with a portfolio of options on the credit indices, so as to reduce the losses as well as the associated RWA of the synthetic credit portfolio.

However, at that time, the SCP was already in breach of the VaR limits set for the portfolio. The new strategy would further increase the size of the breach as the overall exposure of the portfolio would increase with its implementation.

A solution was to implement a new VaR model for setting VaR limits. The new model would also influence the amount of risk weighted assets that were being calculated for the CIO. The premise for implementing a new model was that the existing one was too conservative which lead to an overstatement of risk thus resulting in limit breaches. This new VaR model was researched and built by the CIO itself specifically by Patrick Hagan, a front office quant, who had never before built or implemented a VaR model.

While the model was built after a number of months of research, it had mathematical & operational flaws which were highlighted by the bank's Model Risk and Development Office. There were a number of additional issues that came to light much later. These included:

1. Manual updates required in EXCEL spreadsheets
2. Lowered volatility for illiquid securities based on the assumption that prices for days on which trades did not occur would be the same as the price when last traded
3. Coding errors in the calculation of hazard rates and correlation estimates
4. Use of a wrong Uniform Rate option in the built in analytics suite instead of the Gaussian Copula model option required under Basel 2.5.

The Model Risk and Development Office required that the model be automated and that illiquid positions receive increased monitoring.

However, instead of a truly independent review of the model by the model review group and the standard parallel run of the old and new model during a probationary review period, the new model was implemented under pressure & without resolving the issues highlighted in it. Further, the analytics suite that the model utilized remained untested as of the date of implementation. The new model produced results that were as much as 50% lower than the existing model which did not raise questions of its appropriateness or accuracy at that time.

Reporting line & disclosure deficiencies

Regular risk reporting of the CIO's risk, prior to February 2012 was made officially to the bank's CRO rather than to Ina Drew. The latter received reports being head of the CIO but was not the direct official reporting line.

Even after the appointment of the CRO, only aggregate CIO portfolio risk numbers were provided to Ina Drew. She still did not receive separate numbers for the synthetic credit portfolio positions.

There was no segregation or independent evaluation of the risk of the SCP by the bank wide risk management team. The bank's risk management team depended on the risk numbers reported by the CIO's risk team.

The CIO team was selective in communicating their strategy and portfolio position of the SCP to JP Morgan senior management in month end business reviewing meetings. In the meeting held in February 2012, for example, they mentioned that they were working on reducing RWA as tasked by the bank, but they failed to mention that their strategy required them to increase overall portfolio exposure and that the SCP was already making significant losses.

In addition to this in April 2012, senior management was misinformed about the potential losses and market recovery of the SCP positions. The analysis used to make the assessment was based on a Monte Carlo model that produced more favorable results showing losses between \$-150 million to \$250 million as compared to economic scenario analysis models that showed losses in the range of \$750 million to \$1.925 million. Further, the bank's senior management was informed that the losses were temporary and would resolve once the market behaved as per expectations.

Conflicts of interest

Ina Drew was the reporting line for both the investment and risk management teams. These teams would have conflicting interests, i.e. between optimizing returns from the investments for the trading team against reducing the risk for the risk management team.

The mandates given to the SCP team enhanced this conflict. CIO was tasked to reduce its RWA given the Basel 2.5 deadline. It focused on SCP because the nature of its investments made it RWA expensive and because of the bank's bullish view of the credit markets.

This came at the cost of trading losses given market conditions as well as from inadequate protection as expired protection was not replaced. While traders were asked to reduce RWA they were also asked to keep an eye on profit and loss impact of their trades by the head of the CIO.

There was no indication from the bank as to the level of tolerance for the trading losses including whether or not traders would be penalized for losing money when unwinding positions to meet the reduced RWA objective. Therefore there was nothing to benchmark the growing risk appetite of the traders in the light of more favorable risk limits following a revision to the VaR model nor their determination to continue to trade to defend existing positions so as to minimize the negative impact on PNL.

PNL was negatively impacted by mark to market losses of their existing portfolio position as the portfolio was not behaving as it was designed. Short and long positions in the portfolio were meant to neutralize the Credit Basis Point Value of the portfolio for credit moves. Instead, the long positions in investment grade credit indices were losing money while short positions in high yield indices were not generating as much return to cover these losses.

In addition, as the securities in the SCP were fairly illiquid and because the CIO was a significant part of the market any attempt to sell would cause prices to dip thus worsening the position.

The focus of the SCP seems to have blurred from the original motivation of setting up the SCP which was to hedge the credit risk of the long term income bearing portfolio of the CIO. Traders' focus had shifted from hedging to profit making, particularly following the implementation of the revised VaR model. In order to reduce

the negative impact on PNL, the SCP team started making speculative high risk trades as well as defending their positions against adverse price movements by buying and growing (instead of reducing) the portfolio.

An additional conflict was that the new VaR model was constructed by a quantitative analyst whose direct reporting head was the CIO head trader responsible for the trades. The timeline and the depth of research and resources expended for construction and implementation were dictated by the demands of the traders rather than the standard practice of a thorough review and testing of the model.

Inadequate controls

VaR works well for liquid markets because of the existence of a credible price history- it may not be appropriate for illiquid markets with numbered institutional investors where price history is more fragmented and less frequent. Credit Spread Basis Point value and Credit Spreading Widening inform of the sensitivity to the portfolio to changes in the credit spread. The former is appropriate for small moves in credit spread but does not account for the convexity present in more complex portfolios.

Limits were not granular enough, being reported only at the aggregate CIO portfolio level instead of also separately for the SCP. Further, there were no limits on portfolio composition or asset concentration or by risk factor as well as no limits on the actual market value of the SCP.

In addition, these limits were not hard limits, i.e. they did not automatically lead to action by the CIO to reduce risk, and from a post mortem of the debacle, do not appear to have been taken seriously most of the time. There were over 300 hundred breaches during the early months of 2012 and the SCP's losses steadily built up as these were ignored. Most of the risk metric breaches were not fast tracked to the CIO head and as mentioned earlier, separate risk numbers, exposure or daily trade data for the SCP were not communicated to Ina Drew. Further, in some instances instead of addressing the increased risk, limits were inflated so that the trades/positions would no longer be in breach.

While a new VaR model was implemented, limits related to the VAR metric were not reassessed until May 2012 and the same limits structure that was set based on the existing model (which produced higher VaR numbers and thus limits), was allowed to continue.

Pricing deficiencies

Due in part to the illiquid nature of the indices, traders had too much flexibility when setting prices to be used as marks for the mark to market process. Highly subjective judgment and inconsistent selection processes were used to determine the most favorable marks. Instead of averaging the midpoints of bid ask prices from several different dealers with significant trades in the instruments, only those that were favorable were chosen by the traders to set the prices. As long as these were within its allowable pricing thresholds, the Valuation Control Group (VCG) of the CIO deemed that they were okay to use.

However, no one questioned the validity of the VCG's assessment given that:

1. JP Morgan Chase Bank's internal audit had already identified that the VCG was using untested and poorly documented models and setting weak allowable pricing thresholds
2. The marks set by the CIO often were at significant variance to the mid-point quotes from the dealer, thus not representing good faith estimates of the prices.

JP Morgan Chase & Co. (an Investment Banking firm)'s Chief Investment Office in London tried to sidestep capital regulation laws of risk management by fulfilling the bare minimums of regulatory requirements. Traders were given the incentive to score big, so instead of focusing on simplicity, traders focused on the complexities of derivative markets. Chief Investment Office did everything including misguiding the authorities by placing trust upon untested models which showed less risk (which in turn provided freehand for traders to try to exploit riskier options) and ignoring all the danger signals provided by the stress testing.

The simplest and fastest way to cut risk was to sell positions but it would have had cost them \$516 million. Under Drew's direction, the London traders embarked, instead, on a strategy to reduce the appearance of risk for regulatory purposes. They also hedged investments with securities that moved in the opposite direction. The London-based traders amassed a large, complex financial portfolio (consisting significantly of Credit Default Swaps) in the hope that doing so would help the bank avoid the loss.

London Whale – Timeline of Events

The traders started to substantially increase their investment-grade long positions. By the end of January, the firm booked year-to-date, mark-to-market losses of about \$100 million. Additionally, the bank began using a new formula for value at risk that cut Mr. Iksil's estimated losses by about half. The bank eventually conceded that the new VaR standard was seriously flawed (JP Morgan), but not before the change emboldened traders to increase the size of the London Whale bet, which resulted in doubling down after a loss with bigger and bigger bets; eventually leading to even greater losses. Mark-to-market losses grew to \$169 million by the end of February 2012.

By March 23, 2012, the traders had added significant long positions to the Synthetic Credit Portfolio; after assessing the situation, the Chief Investment Office ordered the suspension of trading in the portfolio. Even after that, the estimated mark-to-market losses continued to grow throughout the end of March and the year-to-date losses reported by the traders totaled at about \$400 million through March 29, 2012.

However, on March 30, 2012, the reported estimation of mark-to-market loss was at \$138 million only. That was later confirmed as deception by Mr. Martin-Artajo, who directed Mr. Iksil to use the "best" possible prices. A separate spreadsheet was still kept by Mr. Iksil which showed the estimate losses at over \$400 million.

The Chief Investment Office on April 5, 2012, sent an e-mail to the JP Morgan Operating Committee making them aware of an article that would be published in the Wall Street Journal and Bloomberg. The Office also assured them that the situation was under control and that the Synthetic Credit Portfolio was generally "balanced," that the market was currently dislocated, and that the mark-to-market losses were temporary and manageable. That prompted Mr. Dimon, the company's CEO to declare the Synthetic Credit Portfolio a "tempest in a teapot" and Mr. Braunstein (Chief Financial Officer) to further state that the Firm was "very comfortable" with its positions as mark-to-market prices in the Synthetic Credit Portfolio would "mean revert" (Kopecki).

It was further revealed that on the evening of April 7, 2012, Mr. Grout formulated a loss estimate by constructing numerous loss scenarios. He evaluated how those scenarios would impact the Synthetic Credit Portfolio's positions. In that way, he generated a number of probability-weighted profit-and-loss estimates for the second quarter; the estimates ranged from losses of \$750 million to gains of \$1.925 billion. However, the Mr. Martin-Artajo felt these scenarios were very unrealistic and thus directed that trader to simply run a "Monte Carlo" simulation to determine the potential losses for the second quarter, against Mr. Grout's recommendation. Nevertheless, he performed the requested analysis and came to a loss estimate of -\$150 million to +\$250 million which was provided to senior management.

It was not until after the Earnings Meeting – on April 13, 2012 – that the company realized the predictions were all wrong and "mean revert" was not going to happen. Messrs. Dimon, Braunstein, Hogan and Ms. Drew commissioned a thorough review of the Synthetic Credit Portfolio, conducted by personnel outside of the Chief Investment Office, in order to better understand the losses it was experiencing and to know whether the Synthetic Credit Portfolio was properly managed.

On April 26, 2012, Mr. Hogan directed senior members of firm-wide Market Risk to commence a position-by-position review of the Synthetic Credit Portfolio and eventually to take over the responsibility of the Synthetic Credit Portfolio. (JP Morgan) The firm's own review showed that the Synthetic Credit Portfolio was not protected against various market scenarios. In addition, they found that the market's knowledge of the positions resulted in investors at other banks and hedge funds that were trading with JPMorgan to take advantage of the situation so that a liquidity risk reduction was not possible.

Following the firm's audit report, on May 10, 2012, the firm disclosed that there were significant problems with the trading strategy for the Synthetic Credit Portfolio and the strategy was "flawed, complex, poorly reviewed, poorly executed, and poorly monitored." (JP Morgan) The firm disclosed that the Synthetic Credit Portfolio had incurred slightly more than \$2 billion in mark-to-market losses up to that point in the second quarter, with the possibility of additional future losses and volatility.

Accordingly, on July 13, 2012, the firm restated its first-quarter net income after lowering it by \$459 million. At the same time, the firm that the cumulative year-to-date losses through June 30, 2012, had grown to approximately \$5.8 billion.

In this case, the bank was not alone at fault. The regulators overseeing the bank at the Treasury Department's Office of the Comptroller of the Currency didn't detect the risk accumulating in the Chief Investment Office's synthetic-credit portfolio when it increased to a hundred and fifty-seven billion dollars, in the first quarter of 2012. The regulators should also have taken note when the risk profile of the Synthetic Credit Portfolio suddenly improved by fifty percent.

London Whale- Summary of Events

Dec-11	51 billion in net notional positions of credit index and tranche position
Jan-12	mark-to-market losses of about \$100 million. Created the new VaR model
Feb-12	mark-to-market losses of about \$169 million
29-Mar-12	mark-to-market losses of about \$400 million
30-Mar-12	mark-to-market losses of about \$138 million.
5-Apr-12	Chief Financial Officer sends the e-mail
6-Apr-12	The London Whale Article
6-Apr-12	Grout forced to go back on his analysis
13-Apr-12	the Earnings Meeting
26-Apr-12	Firm-wide Market Risk commences
10-May-12	disclosed \$2 billion in mark-to-market losses
13-Jul-12	disclosed \$5.8 billion in mark-to-market losses
16-Jan-13	Report of JPMorgan Chase & Co.
Sep-13	\$920 million fine
16-Oct-13	\$100 million fine

The penalties

Following the incidents, the UK and U.S. Attorney's Office opened an official investigation into the matter. It was investigated whether the traders at JPMorgan's Chief Investment Office in London intentionally inflated the value of their portfolio to conceal losses. Federal officials charged the responsible persons on five counts, including securities fraud, conspiracy, filing false books and records, wire fraud and making false filings with the U.S. Securities and Exchange Commission. (Hurtado)

The bank agreed in September 2013 to pay \$920 million to resolve related U.S. and U.K. probes into its internal controls and handling of the trades, which inflicted at least \$6.2 billion in losses to the bank. The selling cited by the CFTC was a “manipulative device” that disregarded consequences to the broader market. And further, on October 16, 2013, the bank agreed to a \$100 million settlement with the Commodity Futures Trading Commission, which found that it had deployed a reckless trading strategy. Thus the total amount of fines exceeded \$1 billion (Brush).

Results of the Crises

In JP Morgan’s Chief Investment Office, new and more robust committee structures have been instituted. The new management has enhanced its key business processes and reporting and a revision of basic policies and procedures with respect to valuation and price verification was done. The firm has also mandated a self-assessment of the Risk function within each line of business which includes the firm conducting a spot check of significant drivers of the firm’s VaR (JP Morgan).

LESSON ROUND-UP

- Risk is inherent in the business. Different types of risk exist in the business according to the nature of the business and they are to be controlled and managed.
- In traditional concept the natural calamities like fire, earthquake, flood, etc. were only treated as risk and keeping the safeguard equipment’s etc. were assumed to have mitigated the risk. But due to rapid changes, the various types of risks have emerged viz. Compliance risk, legal risk, country risk, operational risk.
- Risk may be controllable or uncontrollable. In other words, the systematic risk which stands at macro level is not controllable, but the unsystematic risk which is at micro level is controllable with the risk mitigation techniques.
- The risk may broadly be segregate as Financial Risk and Non-financial Risk.
- Financial Risk includes market risk, credit risk Liquidity risk, Operational Risk, Legal Risk and Country Risk. Non-financial risk does not have immediate financial impact on the business, but its consequence is serious.
- Non-Financial Risk do not have immediate financial impact on the business, but its consequence are very serious and later may have the financial impact. This type of risk may include, Business/ Industry & Service Risk, Strategic Risk, Compliance Risk, Fraud Risk, Reputation Risk, Transaction risk, Disaster Risk.
- To mitigate the various types of risks, which a business entity faces, a proper risk management process should be in force. It is a continuous process and is applied across the organisation. It is basically the identification of risk areas, assessment thereof, evaluating the impact of such risk, develop the risk mitigation techniques, establishing the sound internal control process and continuous monitoring thereof, setting of standards for each process and abnormal variances to be vetted.
- Risk management plays vital role in strategic planning. It is an integral part of project management. An effective risk management focuses on identifying and assessing possible risks.
- The process of risk management consists of the following logical and sequential steps, Identification of risk, Assessment of risk, Analysing and evaluating the risk, Handling of risk (Risk may be handled through the Risk Avoidance, Risk Retention/ absorption, Risk Reduction, Risk Transfer) and Implementation of risk management decision.

- ISO 31000 published as a standard on the 13th of November 2009, provides a standard on the implementation of risk management. ISO 31000 contains 11 key principles that position risk management as a fundamental process in the success of the organization.
- Fraud has been defined as, 'A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank'.
- 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 (e.g. through the interbank or securitisation markets).
- SEBI (LODR) Regulations, 2015 requires that every listed company should have a Risk Management Committee.
- Secretarial Audit is a process to check compliance with the provisions of all applicable laws and rules/regulations/procedures; adherence to good governance practices with regard to the systems and processes of seeking and obtaining approvals of the Board and/or shareholders, as may be necessary, for the business and activities of the company, carrying out activities in a lawful manner and the maintenance of minutes and records relating to such approvals or decisions and implementation.
- Secretarial Audit helps the companies to build their corporate image. Secretarial Audit facilitates monitoring compliances with the requirements of law through a formal compliance management programme which can produce positive results to the stakeholders of a company.

GLOSSARY

Risk Management: Risk management is the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

Fraud Risk: A fraud risk assessment is a tool used by management to identify and understand risks to its business and weaknesses in controls that present a fraud risk to the organization.

Secretarial Audit: Secretarial Audit is an audit to check compliance of various legislations including the Companies Act and other corporate and economic laws applicable to the company. It provides necessary comfort to the management, regulators and the stakeholders, as to the statutory compliance, good governance and the existence of proper and adequate systems and processes.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. What do you mean by Risk Management?
2. Discuss about the Controllable and Un-controllable Risks.
3. Elaborate on different types of Financial and Non-financial Risk.
4. Describe the Risk Management Process and its advantages?

5. What do you understand by Fraud risk? What strategy can adopt to mitigate such a risk?
6. What do you mean by Business Continuity Plan, Crisis management and Disaster recovery plan and give the Relationship between Business Continuity Plan, Crisis management and Disaster recovery plan in corporate world.

LIST OF FURTHER READINGS

- Risk Management: Concepts and Guidance, Fifth Edition by Carl L. Pritchard
- The Essentials of Risk Management by Michel Crouhy, Dan Galai, Robert Mark
- A Practical Guide to Risk Management by Thomas S. Coleman
- Financial Risk Management- A Practitioner's Guide to Managing Market and Credit Risk by Steve L. Allen
- The Failure of Risk Management: Why It's Broken and How to Fix It (Second Edition) by Douglas W. Hubbard

OTHER REFERENCES

- <https://corporatefinanceinstitute.com/resources/management/crisis-management/>
- <https://grm.institute/blog/what-is-esg-and-why-its-important-for-risk-management/>
- <https://www.centraleyes.com/esg-risk-management/>
- https://nidm.gov.in/PDF/pubs/GIZ_NIDM_Climate%20RiskManagementFramework.pdf
- Mapping vulnerability to multiple stressors: climate change and globalisation in India, O'Brien et al, 2004, pp307, Accessed at: https://www.researchgate.net/profile/Robin_Leichenko/publication/222564691_Mapping_Vulnerability_to_Multiple_Stressors_Climate_Change_and_Globalization_in_India/links/0046352b455c18ae07000000.pdf
- <https://www.cfainstitute.org/-/media/documents/article/rf-brief/rfbr-managing-material-risk.pdf>
- <https://www.investopedia.com/terms/b/business-continuity-planning.asp>
- <https://brandfolder.com/resources/crisis-management/>
- <https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan>
- <https://www.smartsheet.com/content/crisis-management-examples>
<https://www.techtarget.com/searchdisasterrecovery/definition/Business-Continuity-and-Disaster-Recovery-BCDR>
- <https://www.itgovernance.co.uk/cyber-security-risk-management>
- <https://www.tatasteel.com/investors/integrated-report-2017-18/pdf/RiskGovernanceandmgmt.pdf>
- <https://marico.com/page/DigitalReport2019-2020/risk-management.html>
- <https://www.smartsheet.com/content/enterprise-risk-management-examples>
- <https://dpncglobal.com/importance-of-internal-audit-functions-in-a-company/>

- <https://www.researchoptimus.com/blog/esg-risk-management-key-aspects-you-need-to-know/>
- https://scope.dge.carnegiescience.edu/SCOPE_15/SCOPE_15_11_chapter1_1-14.pdf
- <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2021/dec/doc202112101.pdf>
- <https://www.kyndryl.com/in/en/learn/plan#:~:text=A%20key%20component%20of%20a,business%20needs%20can%20be%20met.>
- <https://www.agilityrecovery.com/article/5-essential-steps-business-continuity-planning>
- <https://mksh.com/5-elements-of-a-disaster-recovery-plan-is-your-business-prepared/>
- <https://www.livingsecurity.com/blog/cyber-risk-management>
- <https://reciprocity.com/resources/what-is-strategic-risk/>
- <https://www.techtarget.com/searchsecurity/definition/operational-risk#:~:text=Operational%20risk%20is%20the%20risk,that%20can%20trigger%20operational%20risk.>
- <https://www.digiguardsecurity.com/resources/case-studies.html>
- <https://analystprep.com/study-notes/frm/part-2/operational-and-integrated-risk-management/case-study-financial-crime-and-fraud/>
- <https://financetrainingcourse.com/education/2014/04/china-aviation-oil-singapore-corporation-limiteds-jet-fuel-scandal-2005-casestudy/>

[illegible]

[illegible]

PART III

**ENVIRONMENT &
SUSTAINABILITY
REPORTING**



