QUESTION BOOK

ESG

CHAPTER 18:

RISK MANAGEMENT

QUESTION 1:

Himagiri Foods Ltd., a well-established food retail chain in Chennai having turnover more than ₹ 1000 crore, operates both online and offline through more than 200 outlets, including restaurants and sweet shops across India. The operations of the Company have been growing considerably over the last few years. The management is trying to corporatise its style of functioning and planning to implement processes and controls for better operations. One of the major issues which the Company faces is managing the quality of raw materials and storage of finished items, considering the short shelf life of its products. Recently, the Company faced a major crisis due to non-compliance with legal and quality standards. An inspection was conducted by government agencies in five locations across Chennai, wherein several lapses were noted. The government survey conducted by the state's food and labour departments uncovered several violations, including:

- **Adulteration and failed quality tests of sweets and milk products**
- **Employment of child labour**
- **Non-registration with authorities under Labour laws, Provident Fund and ESI**
- **Failure to maintain testing laboratory**
- **Failure to adhere housekeeping norms relating to display and maintenance of records etc. under FSSAI regulations.**

Print and electronic media have caught attention of the public. Many clips and reels of the inspection coverage were being circulated on social media and many food influencers have

called for boycotting the Company's products. The Company has paid huge fines and lost reputation in the market. Company's management has been forced to shut several outlets. These infractions have resulted in huge financial loss, significant media backlash, and reputational damage impacting its market position and customer trust. Company's management has called for a high-level management meeting to design a strategy to address the present crisis. One of the senior managers from Finance team indicated that the crisis arose due to lack of risk management. The Company should appoint a professional who would provide a robust list of potential risks that can have an impact on the business. Once such risks are identified, controls can be designed to address them. Renu, a Company Secretary and risk management professional has been appointed by the Company to provide a comprehensive risk management plan. In the background of above facts, answer the following:

(i) Outline the actions which the Company should take for effective risk detection.

(ii) Briefly explain risk analysis and steps involved.

(iii) Explain 'reputation risk' and outline the principles to manage reputation risk.

(iv) Enumerate the need and essential features of crisis management. (5 MARKS EACH) (JUNE 2025)

Ans:

(i)

- Risk management is the process through which an organization identifies, analyses, assess and mitigate their risk and attempts to increase the likelihood of the success of the organization.
- First and foremost step of the risk management process is risk identification or risk detection. If the risks remain unidentified, the whole risk management process will collapse. Hence, it is considered as the most crucial stage.
- In the instant case, the Company can take following actions for effective risk detection:
  - **(a) Formation of risk management committee:** The committee is generally responsible for formulating a risk management policy for identifying and mitigating internal as well as external risks to the company.
  - **(b) Developing risk management policy:** Risk management policy should be developed after capturing all the potential risks and all the risks should be categorized and prioritized on the basis of the probability of the impact that risk would create.

(c) **Conducting Internal audits:** Regular Internal audits would aid to identify operational lapses if any such as non-compliances.

(d) **Monitoring regulatory framework:** Continuous check and regular monitoring of the updated laws will enable the company to proactively identify compliance-related risks.

(e) **Conducting risk awareness programmes:** Training the staff on identifying, reporting and mitigating risks through workshops and regular communication will aid the company in effectively managing risks.

(f) **Creating risk register:** Risk register can serve as a centralized database for decision makers, aiding in effective risk identification, prioritization and response planning.

(ii)

- Risk analysis is the second step in the risk management process, following risk identification. The potential risks are identified as well as estimated in this stage.
- Risk analysis aids in deciding whether to move forward with the project or not, in anticipating as well as neutralizing the possible problems and in improving safety at workplace.
- Steps involved in risk analysis are as follows:

(a) **Identify threats:** Identification of current and potential hazards is the first stage in risk analysis, which amongst many include the following:

1. **Human:** Illness, death, injury or other loss of key individual.
2. **Operational:** Disruption to supplies and operations, loss of access to essential assets or failures in distribution.
3. **Reputational:** Loss of customer or employee confidence or damage to market reputation.
4. **Financial:** Business failure, stock market fluctuations, interest rate changes.
5. **Natural:** Weather, natural disasters, or disease.
6. **Political:** Changes in tax, public opinion, government policy or foreign influence.

(b) **Estimate risk:** Once the threat is identified, the next step is to determine the probability of that threat materializing and the potential impact it may cause. The risk value can be calculated by finding out the event probability and multiplying it with the cost of event. (Event probability × Cost of event)

(iii)

- Reputational risk is a risk arising from negative perception on the part of all the stakeholders such as customers, shareholders, investors, debtholders or any other relevant parties which may adversely affect the entity's ability to maintain existing or establishing new business relationships and continued access to source of funding.
- It is a type of non-financial risk which wouldn't have an immediate impact but if not controlled, it may have significant financial impact as well. Loss of reputation can cause long lasting damages such as destroyed brand value, steep drop downtrend in share value, ruined strategic relationships, difficulty in recruitment and retention of employees
- Such risks call for an effective reputational risk management which should be based on the following principles:
  (a) Integration of risk while formulating business strategy
  (b) Effective board oversight
  (c) Image building through effective communication
  (d) Promotion of compliance culture so as to have good governance
  (e) Strong internal checks and peer review evaluating company's performance

(iv)

- A crisis is an unanticipated event or negative disruption which may harm people or property of the organization. Crisis management is an organizational process for identifying and responding to threat or such crisis with an aim to limit such harm and recover swiftly.
- Types of crisis are as explained below:
  (a) Technological crisis: Technology may be a boon or a curse because if used improperly, the negative effects may outweigh the positive ones. E.g. Data breach & viruses.
  (b) Confrontational crisis: This is a type of crisis arising because of clash between the people forming the organization because of their belief or ideologies.
  (c) Rumours: In various scenarios, businesses may try to make false accusations which in turn become one of the biggest crises a business may face.
  (d) Organizational misdeed: The manager must ensure every action is legally and ethically correct to avoid any mishap in future. Organizational misdeeds are the kinds of crises caused because of wrong steps taken by a firm.

- Essential features of crisis management plan are as follows:
  (a) Form a crisis management team out of which one shall be selected as crisis manager to whom the leadership is entrusted.
  (b) Initiate training and refresher courses for the employees regularly as to how to handle crisis.
  (c) Plan responses for all the potential crises which can be reasonably foreseen.
  (d) Identify a ground person who shall be notified in the event of any crisis
  (e) Initiate systems that can effectively monitor or detect foreseeable crisis signals early enough to tackle the situation before it gets out of hand.

QUESTION 2:

Buland Investments Ltd, is a Jaipur-based Non-Banking Finance Company (NBFC) and has more than 300 branches/customer service points (CSP) across India. Company mainly offers housing loans, loans against property, and personal loans to all segments of society including salaried employees, professionals and businessmen. The Company has a paid-up capital of ₹ 100 crore, public deposits of ₹ 250 crore and borrowings of ₹ 80 crore (₹ 40 crore each from public and private sector banks). Most of its operations in online mode with customers applying online and uploading their KYC and other financial documents through a secured web portal.

Though the Company is on a growth trajectory, it still does not have robust policies and procedures which guide its operations. Recoverability from the customers, loan defaulters is a challenge on operational front. From a corporate perspective, adhering to Reserve Bank of India (RBI) Digital Lending norms and Cyber Security Frameworks are key challenges for the Company. It has hired few IT professionals to develop an inhouse IT security team. However, despite these efforts, the Company suffered a major cyber-attack recently, leading to theft of sensitive KYC data of large number of customers. RBI has imposed huge penalties and suspended the Company's operations. The media coverage of the incident has further damaged the Company's reputation, causing panic among customers, depositors and investors.

In this context, answer the following questions:

(i) Explain Cyber Security Measures.

(ii) Few investors commented, the Company should have a Disaster Recovery Plan (DRP). Indicate the elements of DRP.

(iii) Describe compliance risks and the mitigation strategy which the Company should adopt.

(iv) Discuss the relationship between Business Continuity Plan, Crisis Management and DRP, with an example. (5 MARKS EACH) (JUNE 2025)

Ans:

(i)

- Cyber security risk refers to the potential for harm or loss resulting from a failure or weakness in an organization's information systems or digital assets which can cause cyberattack or security failures.
- Cyber security risk management is a continuous process as the business must always monitor the risk to ensure that it is within the risk tolerance level.
- Cyber security measures are classified as legal, technical, organizational, capacity building and cooperation.
  (a) Legal measures to provide legislations and implementation framework to avoid and protect the cyber space.
  (b) Technical measures consider the technological tools to prevent, detect, mitigate and respond to cyber attacks.
  (c) Organizational measures are important for the proper implementation of any type of national policy.
  (d) Capacity building measures aim to enhance knowledge and know-how in order to promote cyber security.
  (e) Cooperation measures aim to establish partnerships between different stakeholders to increase cyber resilience of the organizations against cyber threats.

(ii)

- A disaster recovery plan is a plan setting out procedures and strategies that a corporation will use to restore its critical operations in event of any disaster.
- DRP aims to ensure quick and effective recovery from any disaster and return to normal operation.
- Under the DRP, the company analyses the risk and consequences of any disaster as well as the response plan and plan for recovery from the disaster. Elements of DRP:
  (a) Create a disaster recovery team: A disaster recovery team shall be responsible for developing and implementation of disaster recovery plan.

(b) Identify and assess disaster risk: The team formed shall be responsible for identifying and assessing all the risk to the organization. It should include items related to natural disaster, manmade emergencies which may arise from them in identifying appropriate strategy.

(c) Determine the operations, applications of the organization which are the most important and the plan should focus on short term survival rather than restoring organization's full capacity.

(d) Specify backup and offsite storage procedures: The business should identify what is to be backed up by whom it is to be done, how to perform the backup, location of backup and how frequently it should occur.

(e) Test and maintain DRP: all the organizations should test DRP to evaluate the procedures and how effective and appropriate it is.

(iii)

- compliance risk refers to potential for legal potential for legal penalties financial Setback and material loss that the company may Suffer we to failure with compliance to laws, regulations, Code of conduct, or standards good practice.
- In the instant case, the major compliance rinks Include.
  (a) Non-compliance with RBI digital lending norms.
  (b) Breach of cyber Security framework.
  (c) Violation of data protection obligations.
  (d) lack of internal control Systems.
  (e) Non-alignment with ESG regulatory reporting requirements.
- Mitigation strategies that the company should adopt are as follows:
  (a) Establish a compliance management framework: Appointing a compliance officer will ensure board oversight in line with SEBI (LODR) regulation and ESG governance codes.
  (b) Maintain a risk register: Maintaining a risk register to log, classify, and track Compliance risks will aid in early identification of threats.
  (c) compliance training: Conduct regular compliance training for employees and management, and the board. Promote awareness on cyber laws, data protection, environmental laws etc.
  (d) Technological advancement: Invest in secure IT infrastructure to avoid Cyber security risk and to detect breaches or Security risk lapses in compliance if any.

(e) Internal audit: Independent internal audits and reviews periodically should be conducted to assess adherance to laws and regulations.

(iv)

(a) Business continuity plan in an umbrella term that includes within it disaster recovery plan as well as crisis management plan.

(b) Herein BCP is a comprehensive strategy ensuring that the business continues at least all its critical operations during or after a disruption. BCP is a proactive approach in which risk is identified, assessed and planned for.

(c) Crisis management focuses more on immediate response to any unexpected event like cyber-attack that cannot be foreseen in advance.

(d) A disaster recovery plan on the other hand focuses on restoring critical operations in the event of any disaster.

(e) The relationship between BCP, DRP and CMP is that a BCP provides Framework for business operations while guidance for managing a crisis and on the other hand DRP focuses on Recovery from a disaster.

QUESTION 3:

Hardware Solutions Ltd (HSL) offers to its client's hardware solutions, including chip manufacturing, planning and integration for a variety of uses. In a recently concluded Board meeting, while reviewing risk management practices of the Company, one of the Board members indicated about increased threat of new and severe non-financial risks which are now challenging basic assumptions about control effectiveness. For example, HSL so far has relied on automation to speed up processes, lower costs, and reduce manual errors. At the same time, the risks of large-scale breaches and violations of data privacy have increased dramatically, heightening during the COVID-19 crisis as digitization accelerated substantially. With less risk of manual errors but greater risk of large-scale failures, HSL will require to adjust their risk appetites and associated controls to reflect evolving risk profiles The Chief Risk Officer (CRO) of HSL agrees with the view of the Board member. He informed the Board that risk management strategies require revision and it should also cover the event of a major control breakdown, so that HSL is able to switch quickly to crisis response mode, guided by an established Business Continuity Plan. He further agreed that HSL has done little to prepare for crisis, seemingly taking an attitude that it won't happen here and hence risk culture also need to be improved. There is a consensus that HSL will need to build crisis-preparedness capabilities systematically. As the COVID-19 crisis has

demonstrated, companies with well-rehearsed approaches to manage through a crisis have been more resilient to shocks. The CRO further briefed the Board that preparation in this respect would involve identifying the possible negative scenarios unique to HSL and the mitigating strategies to adopt before a crisis hits. That includes periodic simulation involving both senior management and the Board. There is a plan to maintain and periodically update a detailed crisis management register. Their strategies would typically include details on when and how to escalate issues, preselected crisis-leadership teams, resource plans and road maps for communications and broader stakeholder stabilization. The internal auditor has also pointed out several control weaknesses and not appropriately recognising risk appetite in the context of control culture of the Company. In the background of aforementioned facts, answer the following questions:

(i) From a perspective of Companies Act, 2013 and SEBI regulations, discuss in detail the responsibility of Board of Directors relating to risk management.

(ii) The Chief Risk Officer accepts that the Company has done little to prepare for the crisis. What type of crisis is HSL currently experiencing? And also narrate other crisis, which the Company may encounter in future.

(iii) Explain Business Continuity Plan and its key components.

(iv) To protect against malicious threats or building a secure infrastructure for data storage for HSL, outline the cyber security risk management process. (DEC 2024) (5 MARKS EACH)

Ans:

(i)

(a) Risk is an exposure to the possibility of any loss/injury or any unwelcoming circumstance. Risk management is the process through which an organization identifies, analyzes, assess and mitigate their risk and attempts to increase the likelihood of success of the organization.

(b) The Board of Directors hold a vital role in establishing a sound risk management framework within an organization. Under the Companies Act, 2013 and SEBI (LODR) Regulations, 2015, several provisions govern and outline the responsibilities of the Board in relation to risk identification, assessment and mitigation.

1. **As per Companies Act, 2013 – Section 134 the Board's Report must mention:** The development and implementation of a Risk Management Policy, The types of risks identified by the Board that could seriously harm the company's survival and ensure steps are taken to manage them.

2. **As per SEBI (LODR) Regulations, 2015:** The company must have systems in place to inform Board members about possible risks and how to reduce them. The Board must create, implement, and regularly monitor the Risk Management Plan. The plan should cover all types of risks, internal as well as external.
3. **Risk Management Policy:** The company's Risk Management Policy should match its risk profile. It should clearly explain how risk and internal controls are handled and the responsibilities of the Board, Audit Committee, Management, and Internal Audit Team.
4. **Appointment of Chief Risk Officer (CRO):** The company should have a Chief Risk Officer. The CRO may be supported by risk teams who help in identifying and managing risks.
5. **Risk Management Committee (RMC):** As per SEBI rules, every listed company must have a Risk Management Committee. This committee looks after the creation, implementation, and monitoring of the risk management process and reports to the Board.

(ii)

HSL is currently experiencing a technological crisis.

Technological crisis: Technology plays a role in every person's life today. However, when misused, its negative impact can sometimes be greater than its benefits. Issues like data breaches, malware, and spyware can slow down or harm a company's growth. Therefore, managers need to stay well-informed about such situations and take prompt and effective steps to minimize the damage.

There are several different types of crises that can be faced by HSL in the future. Few of them have been listed below:

(a) Natural disasters: these are those events which take place spontaneously and are generally without and human interference and are typically classified as 'act of god'. They include events such as flood, draught, tsunami, storms, earthquakes etc. These are the most difficult from a managerial standpoint to foresee and counteract.

(b) Organizational misdeeds: At times, a crisis may arise due to incorrect decisions made by a company. The manager responsible for creating the crisis management strategy should be fully aware of all actions taken by the firm. It is their duty to ensure that every decision complies with legal and ethical standards to prevent future issues.

(c) **Confrontational crisis:** It is a type of crisis arising because of clash between the people forming the organization because of their belief or ideology. These crises can include sit-ins, union boycotts, etc.

(d) **Rumors:** sometimes other businesses may try to win by making false accusations which in turn become one of the biggest crisis a business may face.

(iii)

(a) A business continuity plan(BCP) is a document which outlines how the business will continue in the event of an unplanned disruption. It has two-fold function where first being prevention and the second being recovery in the event of any disruption.

(b) A BCP is made tailored, specific to the departments which are at risk. For instance, if the finance operation is at risk the BCP would then focus on maintaining steady financial flow and ensure that they are doing adequate financial reporting and also it focuses on restoring critical financial systems while ensuring that a key financial personnel is always available to respond.

(c) The components of business continuity plan are:

- **Strategy:** The plans a business uses to do its daily work and keep things running smoothly.
- **Organization:** How the company is set up, including people's skills, roles, and how they communicate.
- **Applications and Data:** The software the company uses to work, and how it keeps that software running all the time.
- **Processes:** The important tasks the company needs to do every day, and the IT support that keeps everything working.
- **Technology:** The systems and tools (like networks) the company needs to keep working without interruption and to back up data.
- **Facilities:** Backup locations the company can use if the main office or site gets damaged.

(iv)

(a) The cyber risk management is a process to identify and mitigate all the cyber risks of an organization. An effective risk assessment approach should be developed to determine the most suitable way to apply security measures, following risk management guidelines, in order to protect financial assets, information databases, and intellectual property.

(b) The process of cyber risk management is as follows:

1. **Identify Potential Cyber Risks:** Start by finding the cyber security risks in your system. This includes spotting vulnerabilities and the threats that could have a severe impact on the organizational security.
2. **Assess the Severity of Each Risk:** Figure out how likely each risk is to materialize and how much damage it could cause if it does.
3. **Compare Risks to Your Risk Appetite:** Evaluate how each risk fits within your risk appetite.
4. Prioritize the Risks based on amount of harm they can cause, so you know which ones to deal with first.
5. **Risk response:** Decide on the best way to respond.
   Treat – Reduce the chance or impact of the risk by adding security measures.
   Tolerate – Accept the risk if it's within the risk appetite.
   Terminate – Eliminate the risk by avoiding the project and opting a less riskier one.
   Transfer – Shift the risk by separating core and the non-core activities, like through insurance.
6. Cyber risk management is a continuous process so the business should always monitor the risk to ensure that it is within the risk tolerance levels.

QUESTION 4:

Allgood Ltd, a listed company, announced the appointment of Sumer, as the Company's executive director. Despite opposition by few shareholders, the management offered justifications for the new structure to be more independent and investor friendly. It indicated that foreign investors were optimistic about the future of the Company and expected better financial results. The Company has been actually witnessing and struggling to address certain corporate governance challenges. A small shareholder filed a law suit against the Board of Directors' misuse of corporate funds. Rishi, the present Chairman and CEO, was working with the Company since last sixteen years and was a close family friend of Promoters. His leadership style being democratic, he was liked and praised by everyone. He was often found meeting people at all levels within the organisation and called for trying new things. His philosophy diminished conflicts and tensions in pursuit of goal setting and achieving. He believes that as long as dividend is paid to shareholders and earnings per share increases, the market values the stock. To address the changing business situations and the perception of the various stakeholders, Rishi had a detailed discussion with Sumer,

to identify the further course of action, as Sumer had experience in managing crisis. Both of them evaluated various aspects threadbare and concluded that they should appoint some professional firm, who would do a detailed review and suggest the way forward to address these issues. In consultation with other directors and senior management, they appointed Mangal & Co., a consulting firm, to evaluate the present situation and suggest the best practices to mitigate these issues. The consultants were provided with the following shareholding pattern as on March, 31, 2024:

Type of shareholder	Holding %
Promoters	51.60
Mutual fund	7.25
Domestic financial institutions and banks	24.75
Foreign institutional investors	10.40
Corporate bodies	4.60
individuals	1.40
Total	100.00

Mangal & Co., performed a detailed evaluation of the Company's process and procedures, including its corporate governance practices and suggested that the Company should strengthen the role and position of a Company Secretary, who would not only be a focal point for the governance aspects, but also assist in the risk management process. Develop a robust system of internal controls and internal audit, which would support the management and also have a crisis management plan, which would help the Company to prepare a strategy in identifying and responding to threats. In the background of the above facts, answer the following:

(i) Explain the risks associated with governance in case of such corporates

(ii) Outline the role of Company Secretary in risk management

(iii) Explain internal control and indicate the difference in scope of risk management and internal control.

(iv) List the guidelines which the Company shall follow to establish a good crisis management plan. **(5 MARKS EACH) (DEC 2024)**

Ans:

(i)

(a) Governance means the values, culture and the measures by which organizations are directed and controlled. Governance sets the rules for how an organization should

operate by creating policies that define what is acceptable and what is not. It also oversees both risk management and compliance.

(b) Compliance is a part of governance that checks whether these rules are being followed properly. A well-implemented compliance management system is proactive and continuously monitors and assesses the organization's Compliances to ensure that it stays aligned with changing regulatory requirements.

(c) Governance should ensure that the right information reaches the right people at the right time, so that management can make informed, risk-aware decisions. Being aware of risks is only possible when governance works closely with risk management, as this connection provides valuable insights for setting strategies and making decisions.

(d) Risks associated with governance include:

1. Low Corporate morals and ethics
2. Conduct and practices that are anti-competitive
3. ESG regulation compliance
4. Transparency
5. Grievance policies and processes
6. Preventing fraud and corruption
7. Compensation for executives
8. Diversity of the Board of Directors
9. Standards and regulations
10. Paying taxes

(ii)

- The company secretaries in the organization are governance professionals or compliance officers whose role in to enforce a compliance framework to safeguard the integrity of the organization and to promote high standards of ethical behaviour.
- Role of company secretaries includes:
  (a) Advising on best practice in governance, risk management and compliance
  (b) Promoting standards of ethical & corporate behaviour.
  (c) Balancing the interest body, of the board or governing body, management, and other stakeholders.
- A CS should ensure that the following questions are effectively addressed at the board level:
  (a) what in the organizations RM policy?

(b) How in ERM integrated within organizational initiatives
(c) what is the organization's level risk tolerance?
(d) In the chosen risk response appropriate for and In line with the risk tolerance level?

(iii)

- Internal Control in a process established by the organization to ensure:
  (a) Reliability of the financial reporting.
  (b) Improved operational efficiency.
  (c) Adherence to the applicable laws.
- Further, it includes Systems and procedures designed to manage the risk identified through the risk management process. which in turn of support the achievement of organization objectives.
- It is the responsibility of every business to integrate the risk management and internal control system as they are closely related but not same, they rather compliment each other in creating robust framework for managing the risk.
- So in a nutshell, risk management focuses on identifying and estimating the threats and opportunities on the other hand, internal control helps in providing defenses and counters to threats.
- Example - In a manufacturing company it has may identified the risk of supply disruption which may affect the production capacity and for this the company has put up a robust internal control system which does a regular inventory check and has also finalized backup vendors.
- In the above example, finding the risk as well as its possible impact was the task of risk management while taking steps to reduce and monitor the risk was the task of internal control.

(iv)

(a) A crisis is an unanticipated event or negative disruption which is or which may harm the people property of the organization. A crisis management is a process set up by the organization to identify and respond to such crisis. With an aim to limit such harm and recover swiftly.

(b) The following guidelines are recommended for establishing good crisis management plan:

1. Form a crisis management team out of which one shall be selected as a crisis manager to whom the leadership is entrusted or a firm can even employ a professional crisis manager who can help them in planning crisis management.
2. Initiate training and refresher courses as to how to handle crisis. Drills and practice operations must frequently take place to keep refreshing stakeholders on emergency responses to crises.
3. Plan responses for all the potential crisis which can be reasonably foreseen.
4. Initiate systems that can effectively monitor or detect foreseeable crises signals early enough in order to tackle the situation before its too late.
5. Identify a ground person who shall be notified in the event of any crisis. Apart from a crisis manager, there must be a coordinating person among employees who possesses first hand news on a looming crisis.
6. Monitor and detect all the foreseeable crisis. Regular testing of the crisis management process and emergency equipment and updating them frequently or as needed.

QUESTION 5:

Newgen Technologies Ltd. (NTL) is a multimillion-dollar public limited company with over two decades of time-tested experience for clients across the globe. As a leading offshore software development company, headquartered at Hyderabad in India, NTL employs over 525 plus professionals across the globe. In the last year, NTL earned a reputation and niche for its services. For example, a super critical boiler in a thermal power plant takes 10-12 days to be fine-tuned or synchronized. It means system is shut for power generation and lead to loss of millions of dollars. NTL came up with a solution that cuts the time taken to synchronize a boiler from 10-12 days to 3-4 days through the use of software and services of IT professionals. The main strength of NTL is the IT professional they employed with it. It captured data through sensors on the boilers, use the algorithm built in house to check nearly 240 parameters and over 10,000 combinations to tune the boiler. It also helped a global heating, ventilation and air conditioning firm to bring down the time taken to design an AC solution in a building or office from 9 days to just 2 hours now. However, traditional outsourcing business of NTL is dying a slow death as clients cutting their budgets on such services and shifting their focus on newer areas such as digital and cloud. Three-fourth of the revenue of NTL is from traditional services. However, half of its revenue still comes from fixed price projects which allow it the flexibility to determine the resources it deploys and

use software tools to deliver services. Now, the aim is to increase that goal by reducing the dependency on people and more on software led services which coincide with its goal of IT Modernization. NTL derives a major portion of its revenues from customers discretionary spending which is linked to their business outlook. Its major revenues are from UK, USA and other European countries. Some draft legislations in USA have been made to restrict the availability of work visas. Such protectionist policies threaten the prospect of global mobility of people which may also affect the work of NTL as distributed software development requires free movement of people. Appreciation of the rupee against any major currency results in the revenue denominated in that currency to appear lesser in reported terms. Then, there may be different exchange rate when sale took place and when invoice is collected. Internal Financial Control System: The internal Financial Control System of NTL has been laid down as below :

a. Recording and providing reliable financial and operation information.
b. Safeguarding Assets.
c. Ensuring compliance with corporate policies.
d. Well defined delegation of power.
e. Efficient ERP system.
f. Internal audit by one of the big audit firm.
g. Audit Committee found internal financial control adequate.

Based on the above inputs, answer the following questions:

(i) Discuss the SWOT analysis of Newgen Technologies Limited.
(ii) Elucidate the types of exposures risks to be encountered by the Company.
(iii) Discuss the efficacy of the Internal Financial Control System of Newgen Technologies Limited.
(iv) Briefly explain the political risk to be encountered by Newgen Technologies Limited. (8 MARKS) (JUNE 2024)

Ans:

(i) SWOT analysis of Newgen technologies limited is as follows:

(a) Strengths

1. Over 2 decades of time tested experience.
2. Global presence
3. Better time utilization
4. The IT professionals employed.

(b) Weakness:

1. Company is mainly dependent on traditional methods of outsourcing which are phasing out as clients are shifting their focus to new areas such as digital and cloud .
2. Three fourth of revenue of the company arises from traditional services.

(c) Opportunities

1. Reduction of time taken to design AC from 9 days to 2 hours.

(d) Threats

1. Appreciation of rupee against any major currency
2. Difference in exchange rate on date of sale versus date of invoice.
3. restrictions towards availability of work visas by the USA, which affect work mobility of people.

(ii) The types of risks that are to be encountered by the company are:

(a) Business risk: The company's traditional outsourcing business is gradually declining as clients are now focusing more on digital and cloud-based solutions.

(b) Political risk: change in visa regulations by USA government.

(c) Operational risk: manpower shortage may arise due to change in visa regulations.

(iii) The efficacy of internal control system of Newgen technologies is pretty effective due to following reasons:

- Recording and providing reliable financial and operation information.
- Safeguarding assets.
- Ensuring compliance with corporate policies.
- Well defined delegation of power.
- Efficient ERP system.
- Internal audit by an independent audit firm.
- Periodic audit by specialized third party consultants.

(iv) Political risk refers to the possibility that political decisions, events, or conditions in a country will negatively affect business operations or investments. In the instant case, The political risk arises from the toughening of visa policies by the current U.S. government. This change could restrict the free movement of IT professionals from India to the U.S., which may negatively impact NTL's operations.

QUESTION 6:

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. Fraud charges may cause businesses to loose clients due to reputational damage. In order to challenge the brunt of frauds, Explain the 'fraud risk management processes' that a company may adopt to effectively manage its fraud risks. (6 MARKS) (JUNE 2024)

Ans:

(i) Fraud is an intentional act or an omission done by a person with an intention to deceive other person irrespective to wrongful loss or wrongful gain.

(ii) Fraud risk management is a structured approach to lower the fraud risk by creating an anti-fraud program. Fraud Risk Management Processes is as follows:

(a) Identifying risks: To manage fraud risk effectively, a company must first focus on identifying potential risks. This includes understanding which employees or departments are more likely to commit fraud and the possible methods they might use. Once risks are identified, the next step is to prioritize them.

(b) Assessing risks: The organization should begin by identifying the underlying causes of the risks. Addressing these root causes is essential. Additionally, companies should evaluate how these risks could potentially affect their operations and overall performance.

(c) Responding to Risks: Once risks have been identified and assessed, companies need to create risk-mitigation plans and clearly assign responsibility for implementing them. It's also important to take measures that prevent these risks from occurring again.

(d) Monitoring and reviewing risks: Managing fraud risk is a dynamic process. To respond quickly and effectively to changing conditions, companies must regularly monitor and evaluate their fraud risk management strategies.

(e) Reporting risks: By implementing a strong fraud risk management strategy, companies can minimize the chances of severe long term impact. When the risks are reported, it's important to remain objective, take clear actions, and provide guidance on how to lower the risk of fraud.

QUESTION 7:

In the context of Risk Management, answer the following questions:

(i) Which of the following is not an Internal Risk ?

(a) Economic factors such as price fluctuations, changes in consumer preference, inflation.

(b) Technological factors, unforeseen changes in the techniques of production or distribution resulting into technological obsolescence etc.

(c) Physical factors such as fire in the factory, damages to goods in transit.

(d) Human factors such as strikes and lock-outs by trade unions; negligence and dishonesty of employees, accidents or deaths in the factory.

(ii) Which one of the following would LEAST likely be included as a source of market risk?

(a) Natural Disasters.

(b) Recessions

(c) Political Turmoil

(d) None of the above

(iii) Corporate Governance Risk is not intended to identify deficiencies that can damage the following important existential aspects of the company :

(a) Reputation

(b) Existence

(c) Sales Growth

(d) Continuity (JUNE 2024)

Ans:

(i) Economic factors such as price fluctuations, changes in consumer preference, inflation.

(ii) None of the above.

(iii) Sales Growth.

QUESTION 8:

Mr. P is an investor and he has got the proposal for investment in Company A & Company B. The particulars of Company A and Company B are herein given below :

(i) Company A is a highly diversified company. It has stable market share and investment in this company is thought to be safe.

(ii) Company B is a start-up company and investment in this company is thought to be highly risky with high reward.

In view of above, explain the concept of systematic risk and unsystematic risk and classify the risk involved for investment in company A and company B under the categories of systematic risk and unsystematic risk.

Ans:

Securities trading involves the probability of a loss or drop in value. Trading risk is divided into two general categories:

(i) Systemic risk which affects all securities in the same class and is linked to the overall capital- market system and therefore cannot be eliminated by diversification also called market risk.

(ii) Non-systematic risk which is any risk that isn't market-related or is not systemic also called non-market risk, extra- market risk, or un-systemic risk.

Sr no.	Basis	Systematic risk	Unsystematic risk
1.	Control	It is not fully controllable by organization.	It is usually controllable by an organization.
2.	Timing and gravity	It cannot be fully assessed and anticipated in advance in terms of timing and gravity.	It can be usually assessed well in advance with reasonable efforts and risk mitigation can be planned with proper understanding and risk assessment techniques
3.	illustration	Examples of such type of risks are interest rate risk market risk, purchasing power risk.	Examples of such risk are compliance risk, credit risk, operational risk.
4.	No. of organization	It usually affects a large number of organizations operating under a similar stream.	If not managed, it directly affects the individual organization first.
5.	Nature	It is usually of a macro nature	It is normally micro in nature.
6.	Predictable	It is not entirely predictable.	It is reasonably predictable.

Keeping above in view, investment in "Company A" would be covered under unsystematic risk and investment in "Company B" would be covered under systematic risk.

QUESTION 9:

A Chocolate Company since inception in 1990 has been largely responsible for satisfying the country's demand for Chocolates and Sugar Confectionery. The plant has various lines producing a wide range of confectionery like Éclairs. Toffees, Fudges. Caramels, Hard Boiled Candy and Enrobed Chocolates. These products are available in attractive packaging and premium Gift Boxes making them ideal for gifting as well as for own consumption. Most of the packaging in the Gift Pack segment has been carefully selected to ensure its enduring utility, thereby giving our valued customers an added benefit. The confectionery is produced by experienced personnel under stringent quality control and hygiene standards. State-of-the art manufacturing facilities ensure products of international quality. The company in its relentless pursuit of quality obtained relevant Certification in April, 2004. The Company, through its uncompromising stand on quality and competitive pricing, has successfully penetrated countries all over the Gulf, the African continent. Asia, Australia, New Zealand, Canada, South Africa, USA and the UK. The principal business processes involved are:

- **Procurement of raw materials and consumables, Production and Quality Control.**
- **Distribution and marketing, Inventory Management, Pricing and cost control.**
- **Feedback from consumers and redressal systems, Publicity and promotional activities, Investor relations.**
- **Recruitment and HR, Finance & Administration.**
- **Corporate communications and public relations, Legal and secretarial matters.**
- **Maintenance of equipment and other assets, Capital expenditure for equipment and other purposes.**
- **IT systems and telecommunications, Transportation and Logistics.**

Today, manufacturing sector companies like chocolate manufacturing operates in increasingly complex, competitive and global markets. The ability to manage risks across geographies, products, assets, customer segments and functional departments is of paramount importance. The inability to manage these risks can cause irreparable damages. Chocolate company will always face the likelihood of being impacted by uncertain or adverse future events. These uncertainties will have an impact on a company's ability to generate capital and shareholders returns. The company Board expects that management will not only look at where the company may be exposed to risk, but also how these risks can be managed to influence favourable business outcomes. Considering the above, answer the following questions :

(i) What are the fundamental principles to be considered by company to develop an appropriate Risk Policy Framework for the Company?

(ii) What are the various risks, the company is exposed to?

(iii) Discuss some approaches for risk impact assessment.

(iv) What do you understand by Liquidity Risk? What are the techniques to control liquidity risk? (5 MARKS EACH) (JUNE 2023)

Ans:

(i)

(a) Risk is an exposure to the possibility of any loss/injury or any unwelcoming circumstance. Risk management is the process through which an organization identifies, analyses, assesses and mitigate their risk and attempts to increase the likelihood of success of the organization while minimizing the consequences and chances of failure.

(b) Effective risk management helps a company or organization ensure compliance with corporate governance principles. It also reassures shareholders, customers, employees, other stakeholders, and society at large that the business is being managed responsibly and ethically.

(c) There are five crucial components that must be considered when creating a risk management framework. They include the following.

1. **Risk identification:** The first step in identifying the risks a company faces is to define all the possible risks. After listing all possible risks, the company can categorize them into core and non-core risks. Core risks are those that the company must take in order to drive performance and long-term growth. Non-core risks are often not essential and can be minimized or eliminated completely.
2. **Risk assessment:** Risk assessment helps a company understand the quantum of risk it is facing either from one specific risk or from all risks combined and how likely it is that these risks could lead to a loss.
3. **Risk mitigation:** Risk mitigation relates to the process by which an organization introduces specific measures to minimize or eliminate risks associated with the risk. mitigation step involves development of mitigation plans, designed to manage, eliminate or reduce risk to an acceptable level.
4. **Risk reporting and monitoring:** Reporting provides timely and accurate risk information to management and stakeholders, supporting informed decision-

making and enhancing transparency. Effective monitoring and reporting help ensure that risks do not escalate unexpectedly.

5. **Risk governance:** Risk governance is the process that ensures all employees carry out their responsibilities in line with the company's risk management framework. It includes clearly defining employee roles, separating duties and providing a holistic view of the organization's risk management policy.

(ii)

(a) Market Risks: Market risk is the possibility that fluctuations in currency exchange rates, interest rates, or commodity prices may adversely affect the company's value. The market risks identified for this chocolate company are as follows:

- Government Policy risks
- Product Risks
- Environmental risks
- Volatility of export orders
- Price Competition in the local & export market
- Currency fluctuation for export orders

(b) Operational Risks: Operational risk is the chance of loss from failures in people, processes, systems, or external events. The operational risks identified at chocolate company are as follows:

- Fire & Allied Risks
- Machinery breakdown/ obsolescence
- Volatility of Raw material & Packing material prices
- Quality/ Ageing risks of Raw material/ Packing material
- Delivery risk of Suppliers
- Loss of data & information- IT security
- Manpower Availability risks
- Accidents
- Inventory carrying risk

(c) Reputation risk: reputation risk is a risk arising from negative perception on the part of the stakeholders. which may adversely affect the entity's ability to maintain existing or establish any new relationships. The Reputation risks identified at this company are as follows:

- Contamination-hygiene
- Product expiry/Shelf life

- Corporate Governance

(d) Credit Risks: Non receipt of receivables or delay in receipts is the credit risks attributable to the company. These may be identified as:

- Payment risk
- Security from customers
- Advance to Suppliers

(e) Liquidity Risks: The possibility is that the company will be unable to fund present and future financial obligations. These may be identified as:

- Cash flow & working capital management
- FOREX decisions
- Cost overruns

(f) Strategic Risks: Risk those are arising from adverse business decisions or the improper implementation of such decisions. These may be identified as follows:

- Business Plan forecasts.
- Attrition of key people.

(iii)

Organizations can take several approaches to assess risks. Each risk assessment method helps check an organization's risks but involves balancing pros and cons.

(a) Quantitative: A quantitative risk approach is a method that uses numerical data to measure and analyze the potential impact and likelihood of risks in precise, measurable terms. However, quantitative methods can also be quite complex. Communicating the results beyond the boardroom can be difficult.

(b) Qualitative: A qualitative risk approach is a method that assesses risks based on subjective judgment, using descriptive categories like high, medium, or low to evaluate the likelihood and impact of risks without relying on numerical data. On the other hand, these approaches are opinion based. Without a solid financial foundation, risk options can be difficult to prioritize.

(c) Vulnerability based: A vulnerability-based risk approach focuses on identifying and assessing weaknesses or gaps within an organization, helping to understand how these vulnerabilities increase the likelihood and impact of risks. However, this approach might not identify all the different threats an organization could face.

(d) Threat based: A threat-based risk approach involves identifying potential threats that could harm an organization and evaluating the likelihood and impact of those threats, helping to prioritize risks based on the nature and source of the threats.

(iv)

(a) Liquidity risk is the risk that a company will not have enough cash to meet its financial obligations on time. The risk arises when a company cannot buy or sell an investment in exchange for cash fast enough to pay its debts.

(b) Effective liquidity risk management includes systems to identify, measure, monitor, and control liquidity exposures. Management must accurately and promptly identify and quantify both current and potential future sources of liquidity risk.

(c) A good risk management process needs a strong MIS (Management Information System) to track, control, and report liquidity risks. A good MIS gives clear, accurate, and timely data for daily use and during tough times. The information should be well-organized, complete but simple, and easy to access. Some commonly used liquidity measurement and monitoring techniques are:

1. **Contingency Funding Plans (CFP):** To manage liquidity risk well, the company should have backup plans for stressful situations. It ensures that the company can handle normal and unexpected changes in cash flow effectively.
2. **Cash Flow Projections:** These projections predict the company's cash coming in and going out, showing whether there will be a surplus or deficit over a certain period.
3. **Liquidity Ratios and Limits:** The company can use different ratios to measure liquidity and set limits for managing it.
4. **Internal Controls:** To effectively enforce policies and procedures, the company should establish review processes to ensure compliance with the rules and limits set by senior management.

QUESTION 10:

"Responsibilities and accountabilities of the person handling risks need to be identified and assigned." Explain the ways of handling the different types of risk existing in the business. (5 MARKS) (DEC 2022)

Ans:

Risk ownership should be clearly assigned, with defined responsibilities and accountability for those managing risks. When a risk occurs, the responsible person should document it and promptly report it to higher management to enable early actions to minimize the risk. Risks can be managed using the following methods:

(i) **Risk avoidance:** Risk avoidance means to avoid taking or choosing of less risky business or projects. For example one may avoid investing in stock market due to price volatility In stock prices and may prefer to invest in debt instruments.

(ii) **Risk retention/absorption:** Risk retention is nothing but risk acceptance. There are two main types of risk retention:

- **Active risk retention:** This occurs when the company consciously chooses to retain the risk as part of its risk management strategy.
- **Passive risk retention:** This happens unintentionally, often due to lack of awareness. The company may not recognize the risk or may underestimate its potential impact.

(iii) **Risk reduction:** When the risk is higher than the risk appetite then another strategy is reduce and minimize that risk and bring it within the risk appetite. The best time to reduce risk is the planning stage as the same may be achieved without any additional expenses.

(iv) **Risk transfer:** In this the organization identifies its core activities and separates it from its non-core activities which are then transferred to expert agencies which specializes in them for a fees. There are three main methods of transferring risk:

- Through Torts (compensation)
- Through Contracts other than insurance.
- Through Insurance.

QUESTION 11:

What are the different dimensions of identifying threats in Risk Analysis process? In a company there is a probability of increase of 40% cost of raw material from present level of Rs 10 crores. What shall be risk value of cost of production? (5 MARKS) (2019 JUNE)

Ans:

(i) **Risk analysis:** risk analysis is the second step in risk management process where the risks are identified as well as estimated. Risk analysis aids in deciding whether to move forward with the project or not; in anticipating as well as neutralizing the possible problems; and in improving safety at workplace. The first step in Risk Analysis is to identify risks or threats both existing and possible which may pertain to:

1. **Human –** Illness, death, injury, or other loss of a key individual.
2. **Operational –** Disruption to supplies and operations, loss of access to essential assets, or failures in distribution.

3. **Reputational –** Loss of customer or employee confidence, or damage to market reputation.
4. **Procedural –** Failures of accountability, internal systems, or controls, or from fraud.
5. **Project –** Going over budget, taking too long on key tasks, or experiencing issues with product or service quality.
6. **Financial –** Business failure, stock market fluctuations, interest rate changes, or non-availability of funding.
7. **Technical –** Advances in technology, or from technical failure.
8. **Natural –** Weather, natural disasters, or disease.
9. **Political –** Changes in tax, public opinion, government policy, or foreign influence.
10. **Structural –** Dangerous chemicals, poor lighting, falling boxes, or any situation where staff, products, or technology can be harmed.

(ii) Once the threat is identified the next step is to determine the probability of that threat materializing all the potential impacts it may cause.

(iii) In the instant case, the risk value of the cost of the production can be derived by the following formula:

Risk value = probability of event x cost of event

By putting the values,

Risk value = 0.40 (probability of the event) x 10 cr (cost of event)

= 4 crores