J.K. SHAH® TEST SERIES

SUGGESTED SOLUTION

CS PROFESSIONAL

Subject – Corporate Governance, Risk Management, Internal Control, Reporting and Compliances

Topic – Part B – Risk Management (Chapter 12)

Head Office : Shraddha, 3rd Floor, Near Chinai College, Andheri (E), Mumbai – 69.

Tel : (022) 26836666

Answer to Q1.A.

ISO 31000 is the international standard for risk management. This standard is published on the 13th of November 2009. By providing comprehensive principles and guidelines, this standard helps organizations with their risk analysis and risk assessments.

ISO 31000 applies to most business activities including planning, management operations and communication processes. Whilst all organizations manage risk to some extent, this international standard's best-practice recommendations were developed to improve management techniques and ensure safety and security in the workplace at all times.

By implementing the principles and guidelines of ISO 31000 in organization, the organisation is able to improve operational efficiency, governance and stakeholder confidence, while minimising losses. This international standard also helps to boost health and safety performance, establish a strong foundation for decision making and encourage proactive management in all areas.

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

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

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

<u>Benefits of ISO 31000</u>

ISO 31000 contains 11 key principles that position risk management as a fundamental process in the success of the organization. ISO 31000 is designed to help organizations:

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

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

(5 marks)

Answer to Q1.B.

The various non-financial risk faced in a business may be listed as follows:

1. Business/ Industry & Services Risk- Business risks implies uncertainty in profits or danger of loss and the events that could pose a risk due to some unforeseen events in future, which causes business to fail. Business risk refers to the possibility of inadequate profits or even losses due to uncertainties e.g., changes in tastes, preferences of consumers, strikes, increased competition, change in government policy, obsolescence etc. Every business organization contains various risk elements while doing the business. Such type of risk may also arise due to business dynamics, competition risks affecting tariff prices, customer relation risk etc.

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

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

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

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

6. Transaction Risk- Transaction risk arises due to the failure or inadequacy of internal system, information channels, employees integrity or operating processes.

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

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

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

(5 marks)

Answer to Q2.A.

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

Risk management plays vital role in strategic planning. It is an integral part of project management. An effective risk management plan focuses on identifying and assessing possible risks.

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

l Risk Management in the long run always results in significant cost savings and prevents wastage of time and effort in firefighting. It develops robust contingency planning.

l It can help plan and prepare for the opportunities that unravel during the course of a project or business.

l Risk Management improves strategic and business planning. It reduces costs by limiting legal action or preventing breakages.

l It establishes improved reliability among the stake holders leading to an enhanced reputation.

l Sound Risk Management practices reassure key stakeholders throughout the organization.

(5 marks)

Answer to Q2.B.

The formula for calculating the Risk Value is:

Risk Value = Probability of Event x Cost of Event

By putting the values, we get: 0.80 (Probability of Event) x Rs.500, 000 (Cost of Event) = Rs. 400,000 (Risk Value)

(5 marks)

Answer to Q.3.A.

Risk management and corporate governance principles are strongly interrelated. An organization implements strategies in order to reach their goals. Each strategy has related risks that must be managed in order to meet these goals. Risk is an important element of corporate functioning and governance. There should be a clearly established process of identifying, analyzing and treating risks, which could prevent the company from effectively achieving its objectives. It also involves establishing a link between risk-return and resourcing priorities. The Board has the ultimate responsibility for identifying major risks to the organization, setting acceptable levels of risk and ensuring that senior management takes steps to detect, monitor and control these risks. The Board must satisfy itself that appropriate risk management systems and procedure are in place to identify and manage risks.

Corporate governance concerns the relationships among the management, board of directors, controlling shareholders, minority shareholders, and other stakeholders. Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to foreign capital. Incorporating risk management in corporate governance of an organisation is very important. Risk governance includes the skills, infrastructure and culture deployed as directors exercise their oversight. Good risk governance provides clearly defined accountability, authority, and communication/reporting mechanisms.

A process for risk management cannot be initiated unless there is a perception and knowledge of risk surrounding the business. The board shall have to identify the extent and type of risks it faces and the planning necessary to manage and mitigate the same for ensuring growth for the benefit of all the stakeholders.

The updated G20/OECD Principles of Corporate Governance provides on considering the establishment of specialized board committees in areas such as remuneration, audit and risk management.

<u>The sixth principle of OECD Principles of Corporate Governance deals with the responsibilities of the board with respect to Risk Management provides-</u>

• The board should fulfill certain key functions, including - reviewing and guiding corporate strategy, major plans of action, risk management policies and procedures, annual budgets and business plans; setting performance objectives; monitoring implementation and corporate performance; and overseeing major capital expenditures, acquisitions and divestitures.

• Ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.

(5 marks)

Answer to Q3.B.

The management should be pro-active in fraud related matter. A fraud is usually not detected until and unless it is unearthed. A Fraud Risk Management Policy should be incorporated, aligned to its internal control and risk management.

The Fraud Risk Management Policy will help to strengthen the existing anti-fraud controls by raising the awareness across the company and promote an open and transparent communication culture. It would also promote zero tolerance to fraud/misconduct and encourage employees to report suspicious cases of fraud/misconduct. The policy would spread awareness amongst employees and educate them on risks faced by the company.

<u>The major aspects to be included in Fraud Risk Management Policy are –</u>

• Defining fraud : This shall cover activities which the company would consider as fraudulent.

• Defining Role & responsibilities : The policy may define the responsibilities of the officers who shall be involved in effective prevention, detection, monitoring & investigation of fraud. The company may also consider constituting a committee or operational structure that shall ensure an effective implementation of antifraud strategy of the company. This shall ensure effective investigation in fraud cases and prompt as well as accurate reporting of fraud cases to appropriate regulatory and law enforcement authorities.

• Communication channel : Encourage employees to report suspicious cases of fraud/misconduct. Any person with knowledge of suspected or confirmed incident of fraud/misconduct must report the case immediately through effective and efficient communication channel or mechanism.

• Disciplinary action : After due investigations disciplinary action against the fraudster may be considered as per the company's policy.

• Reviewing the policy : The employees should educate their team members on the importance of complying with Company's policies & procedures and identifying/ reporting of suspicious activity, where a situation arises. Based on the developments, the policy should be reviewed on periodical basis.

(5 marks)

Answer to Q4.A.

Section 143(12) of the Companies Act, 2013 read with rule 13 of the Companies (Audit and Auditors) Rules, 2014 provides that if an auditor of a company in the course of the performance of his duties as auditor, has reason to believe that an offence of fraud involving an amount of rupees one crore or above, is being or has been committed in the company by its officers or employees, the auditor shall report the matter to the Central Government.

Rule 13(2) of Companies (Audit and Auditors) Rules, 2014 provides that the auditor shall report the matter to the Central Government as under: • Reporting the matter to the Board/ Audit Committee immediately but not later than two days of his knowledge of the fraud, seeking their reply or observations within 45 days. • on receipt of such reply or observations, the auditor shall forward his report and the reply or observations of the Board / Audit Committee along with his comments to the Central Government within 15 days from the date

of receipt of such reply or observations. • in case the auditor fails to get any reply or observations from the Board / Audit Committee within the stipulated period of 45 days, he shall forward his report to the Central Government along with a note containing the details of his report. • the report shall be sent to the Secretary, Ministry of Corporate Affairs in a sealed cover by Registered Post with Acknowledgement Due or by Speed Post followed by an e-mail in confirmation of the same • the report shall be on the letter-head of the auditor containing postal address, email address and contact telephone number or mobile number and be signed by the auditor with his seal and shall indicate his Membership Number, and • the report shall be in the form of a statement as specified in Form ADT-4.

Rule 13(3) of Companies (Audit and Auditors) Rules, 2014 further states that in case of a fraud involving lesser than one crore rupees, the auditor shall report the matter to Audit Committee / Board immediately but not later than two days of his knowledge of the fraud and he shall report the matter specifying the nature of Fraud with description, approximate amount involved; and Parties involved and the same shall also be disclosed in the Board's Report.

The provisions of Rule 13 of the Companies (Audit and Auditors) Rules, 2014 shall mutatis mutandis apply to a cost auditor conducting cost audit under section 148 and a company secretary in practice conducting Secretarial Audit under section 204 of the Companies Act, 2013.

Penal Provisions : The person guilty of the offence shall be punishable with fine which shall be five lakh rupees in case of listed company and one lakh rupees in case of other company.

Answer to Q4.B.

The process for risk identification starts by taking inventory of the potential project risks that can affect the project delivery.

This step is crucial for efficient risk management throughout the project. The outputs of the risk identification are used as an input for risk analysis, and they reduce a project manager's uncertainty. It is an iterative process that needs to be continuously repeated throughout the duration of a project. The process needs to be rigorous to make sure that all possible risks are identified.

An effective risk identification process should include the following steps:

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.

(5 marks)

Answer to Q5.A.

Enterprise risk management is a process, put in place by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Enterprise risk management encompasses: i. Aligning risk appetite and strategy. ii. Enhancing risk response decisions. iii. Reducing operational surprises and losses. iv. Identifying and managing multiple and cross-enterprise. v. Seizing opportunities. vi. Improving deployment of capital.

Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process.

<u>These components are</u>: 1. Internal Environment 2. Objective Setting 3. Event Identification 4. Risk Assessment 5. Risk Response 6. Control Activities 7. Information and Communication 8. Monitoring Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

<u>Limitations</u>

While enterprise risk management provides important benefits, it also has certain limitations. In addition to factors discussed above, limitations result from the realities that human judgment in decision making can be faulty, decisions on responding to risk and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures such as simple errors or mistakes, controls can be circumvented by collusion of two or more people, and management has the ability to override enterprise risk management decisions. These limitations preclude a board and management from having absolute assurance as to achievement of the entity's objectives.

(5 marks)

Answer to Q5.B.

The Reserve Bank of India in its Master Circular number RBI/2015-16/85 DBR.No.BP.BC.4./21.06.001/2015- 16 July 1, 2015 has defined the Reputation Risk as the risk arising from negative perception on the part of customers, counterparties, shareholders, investors, debt-holders, market analysts, other relevant parties or regulators that can

adversely affect a bank's ability to maintain existing, or establish new, business relationships and continued access to sources of funding (eg through the interbank or securitization markets).

Reputational risk is multidimensional and reflects the perception of other market participants. Furthermore, it exists throughout the organisation and exposure to reputational risk is essentially a function of the adequacy of the bank's internal risk management processes, as well as the manner and efficiency with which management responds to external influences on bank-related transactions.

Loss of Reputation has long lasting damages like:

- It destroys the Brand Value
- Steep downtrend in share value.
- Ruined of Strategic Relationship
- Regulatory relationship is damaged which leads to stringent norms.
- Recruitment to fetch qualified staff as well the retention of the old employees becomes difficult.
- For managing the reputation risk, the following principles are worth noting:
- Integration of risk while formulating business strategy.
- Effective board oversight. l 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

(5 marks)