DISCLAIMER

This Suggested Answer hosted on the website do not constitute the basis for evaluation of the student's answers in the examination. The answers are prepared by the Faculty of the Board of Studies with a view to assist the students in their education. While due care is taken in preparation of the answers, if any error or omission is noticed, the same may be brought to the attention of the Director of Board of Studies. The Council of the Institute is not in anyway responsible for the correctness or otherwise of the answers published herein.

Further, in the Elective Papers which are Case Study based, the solutions have been worked out on the basis of certain assumptions/views derived from the facts given in the question or language used in the question. It may be possible to work out the solution to the case studies in a different manner based on the assumptions made or views taken.

PAPER-6A – RISK MANAGEMENT

The Question Paper comprises five case study questions. The candidates are required to answer any four case study questions out of five.

Answers to Multi Choice Questions are to be marked on the OMR answer sheet only.

Answer to other questions to be written on the descriptive type answer book

Answer to MCQs, if written in the descriptive type answer book will not be evaluated.

Candidates may use calculator.

CASE STUDY: 1

About the Company:

- *BCSPL, situated in TIDEL Park, Chennai, is providing computer system related services to offshore major Information Technology (IT) companies. It was established in the year 2015 and has good reputation in its provision of services. BCSPL has 300 staff consisting of software professional and accounting and administrative staff. At present Virtual Office Management System (VOMS) is enabled in the laptop computers of about 30% of its staff. BCSPL is thinking of adopting VOMS for the working of its entire staff members.*

VOMS:

- *VOMS is a service in which a range of functions relating to a company is provided that facilitates their staff to work remotely by accessing such functionalities through Internet. The main aim of VOMS is to enable the staff members to seamlessly connect to the computing services of BCSPL irrespective of the time and geographical distance. BCSPL proposes to approach a cloud services provider to hold the data on cloud and run cloud-based software services.*

New Proposal:

- *To accomplish, expanding VOMS to 100% of its staff, SPL proposes to buy good quality laptops and provide them to the remaining members of the staff.*

Security concerns of BCSPL:

- *With the increase in cyber-attacks and the important and confidential nature of the data being handled, BCSPL is very much concerned about the possible compromise of the data. Cyber-attack may happen in the form malicious software attacks, hacking, phishing, ransomware attacks etc. The staff may not be thoroughly aware in the security aspects of the system. Mr. Peter, BCSPL's IT manager suggested to implement robust security*

measures including installation of strong firewall mechanism, installation of Virtual Private Network (VPN) etc., to counter the increasing security risks.

Integrating Risk in the Strategic Planning Process:

- *As the proposed adoption of VOMS is a strategic move by BCSPL, the strategic risks associated with the same have to closely monitored as they would have an impact on BCSPL' s ability to deliver its goals which are generally articulated in the strategic plan or intent document of BCSPL. Given the velocity with which threats and risk events strike, BCSPL would find it useful to integrate significant risk factors in the strategic planning processes.*
- *The management knows that the strategy of BCSPL should make it clear as to how it intends to mitigate or manage risks and maximize opportunities and BCSPL should develop objectives and strategies accordingly by allocating the resources in a planned manner.*

Risk Management:

- *As the new proposal might bring-in many unknown risk factors, BCSPL wants to (i) embed risk management and internal controls into its various operations and (ii) make sure that enterprise-wide approach to risk management is developed and communicated across BCSPL. BCSPL requested Mr. Kishore, the Risk Manager, to suggest some techniques to the achieve the above.*
- *BCSPL is aware that the primary responsibilities for risk management and the associated controls are with the management and the management is required to adopt suitable policies, procedures and strategies as the philosophy of embracing the risk management increases day-by-day. BCSPL is required to show that effective risk evaluation has revealed the risks that BCSPL is exposed to and have appropriate controls are in place that would prevent materialisation of possible risks.*

Term Loan from Bank:

- *To meet the needs of purchase of laptops, BCSPL decided to approach its bankers for a term loan for ₹ 2 crores.*

You are required to answer the following questions:

Multiple Choice Questions

Choose the most appropriate answer from the given options:

(1.1) Which of the, following statements is not true about the new proposal of BCSPL bringing in risks?

(A) Rapid changes in information systems can change the risks relating to internal controls.

(B) Significant expansion of operations can strain controls and increase the risk of a breakdown in controls.

(C) New personnel may have the same focus on understanding of internal controls.

(D) Incorporating new technologies into information systems may change the risk associated with internal controls.

(1.2) Which of the following is an internal risk threat metric about the cyber-risk that BCSPL may face in its proposal to implement VOMS in all the computer systems?

(A) The number IT system requests emanating from unidentified IP addresses.

(B) The number of IT controls that have been self-certified as working correctly.

(C) The number of IT security incidents reported by similar organisations in the past one year.

(D) The number of social engineering attempts reported within BCSPL.

(1.3) Mr. Peter's suggestion is an example of:

(A) risk control

(B) risk avoidance

(C) risk transfer

(D) risk retention

(1.4) The proposal of BCSPL would have an impact on the stakeholders and while taking such decision, the management least likely would consider:

(A) Information about the internal and external environment.

(B) Recognition of risk and opportunity.

(C) Deploying scarce resources and recalibrates activities to changing circumstances.

(D) Risk of legal liability for damages accruing to customers.

(1.5) Before approving the term loan, if the banker 'performs an inadequate check on KYC of BCSPL and assuming that a violation is committed by BCSPL, it would be known as:

(A) Regulatory Risk

(B) Credit Risk

(C) Sanction Risk

(D) Control Risk ***(5 x 2 Marks = 10 Marks)***

Descriptive Questions

(1.6) Suggest some best practices to address the data privacy and cyber-security risks in the VOMS proposed to be implemented by BCSPL. ***(6 Marks)***

(1.7) Explain the risk management techniques that Mr. Kishore would suggest to BCSPL. ***(5 Marks)***

(1.8) Discuss the integrating of risks in the strategic planning process of BCSPL. ***(4 Marks)***

Answer

Multiple Choice Questions

1.1 (C)

1.2 (A) or (B)

1.3 (A) or (D)

1.4 (A) or (D)

1.5 (A)

Descriptive Questions

1.6 Following are some best practices to address the data privacy and cyber-security risk

- Identification of risk areas. Whether it is own or outsourced network, internet, individual computers, mobile devices etc. Prioritization of resources and effort can be managed accordingly.
- Adequately restricting access to systems is the common way to prevent cyber risk; this is done by password protection at various levels, from common user to administrator level.
- Encryption solutions on individual computers is also done in a manner that if lost, the unauthorised entity cannot download the data into an external storage device.
- There are several technology solutions that create an adequate firewall of the organisation's systems to protect them from hacking from outside.
- A regular vulnerability testing of the firewall and periodic review to upgrade it is one of the main tasks of the information security manager. Detection of a test-attack is very important part of the preventive mechanism; an attacker may attempt to cause a minor violation to test the organisation's network security before causing a major incident.
- A response strategy to a cyber-attack incident is also important as part of risk management. The measures to prevent or mitigate customer disputes, legal indemnities, assess and minimize the financial impact of a cyber-attack, and governance over decision making and investments to restore the system

functionalities to its secure state, are all important considerations. The root cause of these incidents and the impact have to be adequately documented.

Alternative Answer

Best practices to address the data privacy and cyber-security risks:

- **Disabling removable devices in the laptops:** The connecting ports and removable media such as use of pen drives are to be disabled in the laptops. The users are not allowed to install any software and access restrictions are to be in place for visiting the Internet sites.
- **Use of security measures:** The data must be encrypted during transmission. Strong firewall and anti-virus software to be installed with periodic updating of patches and updates.
- **Securing home networks:** The staff must be instructed to ensure that their home networks, in which they would be using the company provided laptops, are secured.
- **Periodical updating of security policies:** Data security policy, network policy, Internet usage policy, user security policy etc., must be periodically reviewed, updated and such updated policies must be timely communicated to the staff.
- **Personal Device Protocol:** The staff are going to use company's devices that are connected to company's network through secured Virtual Private Network (VPN). With the increase in number of devices connected, there must be a strong authentication mechanism. Personal devices of the staff must never be allowed to access the VPN. Use of personal emails in the corporate network should be discouraged.
- **Usage of video conferencing faculties:** Before selecting and implementing the services for video conferencing to be utilised, adequate study must be performed. There is a risk of data piracy with the use of weaker software.

1.7 Techniques that would be suggested by Mr. Kishore:

The Risk Enabled and Managed organisations uses the following techniques.

Technique	Description
Risk Questionnaires	Designed to identify the relevant risks and create risk history
Flow Charts with Risk Flags	Designed to identify operational risks embedded in the Processes
Identify Controls to manage risks	Recognize controls and test their adequacy and operative Effectiveness
Risk Event Maps	Identify potential events that can have a significant impact on business to avoid negative surprises

Risk Scorecards	A Monitoring tool to track progress of risk management
Capital Budgeting	A financial analysis tool to evaluate the future cash flow benefits arising from risk management actions against the costs of risk consequences
Value at Risk	A financial analysis tool to evaluate the impact of the worst case scenario of a risk event
Risk Heat Maps	A Monitoring tool to track progress of risk management using qualitative assessment of probability and impact of risk

Alternative Solution

Insurance is generally used by organisations to mitigate operational risks that can be insured. Insurance coverage is commonly available for risks arising out of fire, for instance. Depending on the cover available and opted for, other losses due to terrorist attacks, natural disasters etc. can also be covered.

Recently a new concept of Cyber risk insurance has also come up, and there are companies offering cover against the risk of damages due to lawsuits / compensation on account of being a victim of cyber-attack, due to which data of customers, vendors or any other counter-party can be leaked to an unauthorised, malevolent entity.

1.8 Integrating Risk in the Strategic Planning Process:

- BCSPL in its proposal to adopt 100% VOMS, may have to identify cyber-attack threats at the stage of business plan preparation and respond by investing in a suitable internal control such as a best in class Firewall device.
- Strategic risks might arise to affect BCSPL's strategic plan of installing and running VOMS to 100%, from internal operations or external factors. Internal factors such as resistance to change by the staff members and the external factors such as pandemic affecting the pockets of geographical regions, against which BCSPL has no control.
- New legislation that regulates the data protection in the countries/regions which would significantly impact the operations of BCSPL
- BCSPL's proposal to expand VOMS to 100%, involves a strategic objective to be achieved and the same may require a specific set of skills required for installing and running VOMS and the same may not be readily available with BCSPL.
- BCSPL's proposal to approach a cloud services provider for holding its data and running cloud-based software services may make BCSPL more vulnerable to information security breaches.

CASE STUDY: 2

About DHSS:

- *BHSS is running classes for higher secondary education in Madurai, Tamil Nadu since 1995. It is following rules and regulations, syllabus and examination of Tami Nadu Board of Higher Secondary Education (TNBHSE) under Department of Education, Government of Tamil Nadu. The school is famous for its teaching and coaching and has produced many state level rankers. The toppers got admission into prestigious engineering and medical colleges on merit. For the academic year, the school had a total strength of 1200 students.*

BHSS School Core Committee (BSCC):

BSCC, consisting of twelve committee members, is running the school. It met in April 2020 and discussed the various aspects of the pandemic situation affecting the functioning of the school and its teaching and coaching activities. Mr. Pandian is the Chairman of BSCC. The following issues were discussed at the meeting:

- *New Mode of Teaching: Because of the present pandemic situation, the students may not be able to attend the school. Therefore, it has been decided to teach the students online through Internet.*
- *A committee, viz., Online Teaching Committee (OTC) is to be formed consisting of 5 teachers and 2 committee members, to help in preparing and testing the teaching materials and conducting online classes to students. The online learning module would be named Bright Digital Learning Module (BDLM).*
- *Necessary technology infrastructure is to be created for running the online classes such as buying suitable computers, software, audio-video (AV) equipment, printers and high-speed Internet data connection and devices. Besides the above, latest anti-virus software and suitable firewall mechanism are to be installed to prevent virus attack and hacking attempts.*
- *It was also decided to conduct online examination for the students at frequent intervals. The examination content would be created by the respective class teachers and supervised by the OTC members.*
- *Training to teachers and students: Sufficient training on the preparation of teaching and examination contents to be given as well as training to be given on the delivery of content as well as handling the A V equipment.*

The teachers who are not familiar with computers are to be additionally trained.

- *A technical support team will be made ready who will support not only the teachers handling the online classes but also the technical queries received from the students. Suitable dashboards would be displayed in the interface of BDLM.*

- *Online Class Fee Collection: It is initially decided to collect ₹ 1,000 per month from each student as online class fee.*
- *It is to be ensured that the online classes are to be commenced on-time. Periodic updates would have to be given to each parent's registered mobile number and / or email account.*
- *BSCC members are aware that when hosting BDLM online, BHSS would face a variety of Internet Security Risks (ISR). Each aspect in the online BDLM can be a possible target of cyber-attack.*

Adoption of Enterprise Risk Management (ERM) approach:

- *In pursuant to the discussions, the BSCC members decided to study and adopt risk management strategies and practices throughout the operations of BHSS. They would like to engage in the process of assessing risk and acting in such a manner, or prescribing policies and procedures, to avoid or minimize loss associated with such risk.*
- *BSCC members are considering the option to prepare a list of possible risks and the proposed treatment of such risks.*

Projection of Risks:

- *BSCC members developed hypotheses based on financial projections and estimated a possibility of 30% in failing to achieve the projected collections if there is a fall in 25% in admission of students to the online classes. Different scenarios were analysed and calculations were made on the sensitivity of the projections by changing the assumed parameters, such as, the number of students who might enrol for various courses, fee collection from each student, the duration of the course etc.*

Bank Loan Proposal:

- *The committee estimated a capital expenditure of ₹ 60 Lakhs and decided to approach Cholan Bank Limited (CBL) for a term loan of ₹ 50 lakhs repayable in 5 years and a working capital loan of ₹ 10 Lakhs. The members of BSCC offered to give their personal lands and buildings as collateral to the proposed loans and would act as guarantors of the loans. The market value of the collateral offered is ₹ 2 crores. BHSS did not have any previous loans either with the bank or from others.*

You are required to answer the following questions:

Multiple Choice Questions

Choose the most appropriate answer from the given options:

(2.1) Which one of following most likely would be of some help to BHSS, if ERM approach is adopted?

(A) To define the risk appetite of the organization.

(B) Align annual performance goals with risk identification and management.

(C) *To assess the company's risk profile, risk appetite and key areas of risk.*

(D) *Define & develop risk policies, procedures, processes & other documentation as required.*

(2.2) *The primary objective of Risk Treatment methodology proposed to be adopted by BHSS would be to:*

(A) *Give a response to risks.*

(B) *Ease the pressure from parents and students.*

(C) *Comply with the guidelines relating to the pandemic situation issued by the Government.*

(D) *Conduct periodic risk assessments.*

(2.3) *In the hypotheses developed by BSCC members, there might be a risk of acceptance of hypotheses and the associated projections that should have been rejected. Such a situation is best known as:*

(A) *Design Level Error*

(B) *Transaction Level Error*

(C) *Type I Error*

(D) *Type II Error*

(2.4) *Which of the following would not be considered as an inherent risk for the ISR that would be faced?*

(A) *Identity Theft*

(B) *Inadequate Content*

(C) *Impersonation*

(D) *Inadequate Authentication*

(2.5) *By introducing BDLM, BHSS is attempting to convert negative risk events into positives by creating a focussed group of experts who brainstorm on breakthrough proposals that could help BHSS move in a positive direction. This contemporary phenomenon is commonly referred to as*

(A) *Incident Analysis*

(B) *Scenario Analysis*

(C) *Idea Funnel*

(D) *Risk Heat Maps* ***(5 x 2 Marks = 10 Marks)***

Descriptive Questions

(2.6) Discuss the risks that would be faced by BHSS in the current pandemic situation and the proposed introduction of BDLM. ***(6 Marks)***

(2.7) Explain the credit risk components that CBL would consider with specific reference to the loan proposal of BHSS. ***(5 Marks)***

(2.8) Briefly explain the difference between Scenario Analysis and Sensitivity Analysis.

(5 Marks)

Answer

Multiple Choice Questions

2.1 (B)

2.2 (A)

2.3 (D)

2.4 (B)

2.5 (C)

Descriptive Questions

2.6 Risks that would be faced by BHSS:

1. Financial Risk:
   - There may be insufficient inflow of funds, if required number of students do not join which would cause great strain on the financial operations of BHSS.
2. Liquidity Risk:
   - If sufficient fees collections are not received from the students, there would be a liquidity problem and the same may prevent BHSS from paying the loan dues within time.
3. Market Risk:
   - There are adverse changes in the present conditions due to pandemic situation. This would pose a risk to BHSS.
4. Operational Risk:
   - The external conditions prevailing in the current pandemic situation would have an impact on the day-to-day operations of BHSS.
5. Strategic Risk:
   - The decision to adopt online teaching by BHSS is a strategic one. Failure of strategies will adversely impact the business objectives and attainment of the goals.

6. Regulatory Risk:
   - The Government may change the pandemic guidelines and policies to be followed by the schools from time-to-time, such as, changes in maximum amount of fees to be collected, maximum hours per day for conducting the online classes etc. Any changes In the rules and regulations which may have a negative Impact on the activities of BHSS can be classified under this risk.
7. Reputation Risk:
   - If the quality of the online teaching is not up-to the mark, BHSS's reputation may go down and this will pose a risk
8. Staffing Risk:
   - The staff may not be experienced to handle the newly proposed online teaching system.
9. Technology Risk:
   - The technology used in the online teaching may have to be changed with the changing technologies and this would impose additional cost to BHSS.
10. Business Continuity Risk:
    - If in case, the online teaching system is hacked, BHSS may not be able to continue the operations and necessary backup and recovery controls should be in place.
11. Information (data security) Risk:
    - Risk of unauthorised data access to the online teaching system as BHSS heavily would depend on information technology. Unauthorised data access might lead to theft of resources painstakingly created by BHSS.
12. Security Risk:
    - BHSS's system may be hacked and this might pose a risk to BHSS.
13. Governance Risk:
    - If the management of the school is improperly conducted, there would arise governance risk.

Alternative Answer

The various types of risks that will be faced by BHSS during the pandemic tine and introduction of DDLM are as follows:

(i) Maintenance Cost of huge infrastructure: Since now there is a remote possibility of starting of physical classes for long period, the cost of maintenance of such infrastructure may continue for longer period.

(ii) Loss of Revenue: Since due to the situation of uncertainty, there may be a fall in the registration of new entrants.

(iii) Teacher's Salary: Despite the fact that there may be no physical classes, BHSS has to pay salary to the current teaching staff in order to retain them.

(iv) Poor Results: Due to uncertainty in conducting of Entrance Examinations it might be possible that some selected students who have been prepared by Institute may not produce the good result as expected.

(v) New IT infrastructure: Funds shall be needed to create new infrastructure.

(vi) Cyber Risk: Since the system will be connected to students on pan India basis there is risk of cyber risk.

(vii) Integrity of Examination system: Since practice examination shall be conducted online, the integrity of same shall be a big issue and it will be bit difficult to judge the performance of students.

2.7 The credit risk components that CBL would consider with specific reference to the loan proposal of BHSS are as follows:

(i) Default Risk – This risk means the missing a payment obligation (of principal or interest or both). Default Risk can be measured by probability of default. It depends on credit worthiness of a borrower which in turn depends upon various factors such as management of organization, size of business, strength and reputation of promoters etc.

- CBL would check credit worthiness of the committee members who are offering collaterals for the loans and reputation of them and of BHSS.

(ii) Exposure Risk – This implies the uncertainty associated with future level or amount of risk. In other words, this risk is mainly associated with unexpected action of other party say prepayment of loan before due date or request for refund of deposit before due date.

- The bank may even ask BHSS to repay the loan in full before the due date if the performance of BHSS is not satisfactory in the future.

(iii) Recovery Risk – This risk is related to recoveries in the event of default, which in turn depends upon various factors such as quality of guarantee provided by borrower, and other surrounding circumstances. This risk can be minimized through Collateral and Third-Party Guarantee. However, existence of these two risk management tools also carries risk.

- In the proposed loan, the members of BSCC offered to give their personal lands and buildings and the market value of the same is Rs. 2 Crores.

(iv) Collateral Risk: Although collateral reduces the credit risk but it happens only if collateral can be sold at a significant value. The quickness in realization of collateral

depends upon its nature and prevailing market conditions. In normal course, fixed asset collateral normally carries low realizable value than cash collateral. However, if in buoyant market say in case of a property even a fixed asset in the form of a house property carries a higher value.

With the use of collateral, the credit risk becomes twofold:

(a) Uncertainty related to access it and disposing encumbrances which may be legal in some cases.

- CBL will ensure that the collaterals offered by the committee members of BSCC do not have any encumbrance.

(b) Uncertainty related to the value realizable from the collateral which may be subject to various factors.

- It would be ensured by CBL that the assets offered as collateral have the capability of easily salability in the event of default of BHSS in the loan repayments.

(v) Third Party Guarantee Risk: This collateral is a kind of simple transfer of risk on Guarantor and in case guarantor defaults then risk again comes back to lender.

- CBL would ensure that the Committee members who are the guarantors for the loan have sufficient assets to cover the loan. For this purpose, CBL would obtain and scrutinize the financial statements of the Committee members.

2.8 Sensitivity analysis and Scenario analysis both help to understand the impact of the change in input variable on the outcome of the project. However, there are certain basic differences between the two.

Sensitivity analysis calculates the impact of the change of a single input variable on the outcome of the project viz., NPV or IRR. The sensitivity analysis thus enables to identify that single critical variable that can impact the outcome in a huge way and the range of outcomes of the project given the change in the input variable.

Scenario analysis, on the other hand, is based on a scenario. The scenario may be recession or a boom wherein depending on the scenario, all input variables change. Scenario Analysis calculates the outcome of the project considering this scenario where the variables have changed simultaneously. Similarly, the outcome of the project would also be considered for the normal and recessionary situation. The variability in the outcome under the three different scenarios would help the management to assess the risk a project carries. Higher deviation in the outcome can be assessed as higher risk and lower to medium deviation can be assessed accordingly.

Scenario analysis is far more complex than sensitivity analysis because in scenario analysis all inputs are changed simultaneously considering the situation in hand while in sensitivity analysis only one input is changed and others are kept constant.

CASE STUDY: 3

About the Company

Blue Hospital (BH) is a reputed chain of hospitals located in the National Capital Region (NCR). The BH package of services includes: inpatient hospital delivery services, outpatient ambulatory services, home health, drug rehabilitation and alcohol treatment and retail services including diagnostic, laboratory, sports medicine, rehabilitation and imaging. BH's trauma center is one of the NCR's busiest. In addition BH operates one of the only air ambulance services in the region and has its own health insurance company providing health benefits for its employees and others.

Review of Risk Management Function

BH's risk management function had been outsourced to a single firm named RLM for approximately eight years. Immediately after joining BH as a Chief Risk Officer (CRO), Ms. Sana commissioned an independent assessment of the risk management function as she was uncertain whether outsourcing model was an effective risk management structure for BH. The Board has asked Ms. Sana to do her own assessment also of the existing risk management practices after reviewing the findings of that independent study from the outside firm. The Board has also asked the CRO to consider Delphi and Bow-Tie techniques of risk analysis.

Observations made by CRO

1. *The studies suggested that the circumstances that led to the initial outsourcing decision no longer existed. Also, BH had grown considerably in size and complexity to warrant both a high level of direct accountability by a senior leader and their own team and a strategic approach to the management and mitigation of risks. Another issue these processes uncovered was that the outsourcing model was less effective in proactive data mining and trend analysis that could be used to create actionable risk and quality initiatives to prevent or mitigate risk events in the future.*
2. *BH did not have a forum to look across the organization to assess interrelated risks and potential impact on the organization or how multiple risks could correlate.*
3. *The CRO is also concerned that Business Continuity Plan (BCP) is not properly implemented in the organization. Also, employees think that there is no difference between Enterprise Risk Management (ERM) and BCP. One of the Audit Committee of Board (ACB) members has remarked that ERM approach and the business impact analysis approach are very similar and there is no difference.*
4. *The CRO has flagged the fact that risk culture within BH must improve and there is no narrative approach of risk management in place for those risks which cannot be adequately or accurately reflected by a numeric or quantitative method. Therefore, while developing new risk management approach narrative approach to risk management must be considered especially considering the nature of business of BH.*

Action plan

After a presentation to the Board by the CRO, BH began a three-step approach to reestablish a risk management function in the organization and create a strategic approach to management of risks.

Step one was laying the groundwork or a design-build phase to create the foundation for a high functioning internal risk management department including adding the necessary business intelligence data structure.

Step two was the introduction into the organization of an ERM framework and the establishment of an Enterprise Risk Committee (ERC) at the highest level of the organization. It was determined that an advisory group of executives should serve together as a coordinating body to look at diverse risks to the organization from whatever source. The advisory group shall be called ERC and is chartered to look more expansively and from a strategic point of view at risks in order to understand the inter-relatedness and cumulative impact on the organization. Further, the selection of key individuals who will form part of the ERC will be based on a broad parameter to be developed by the CRO after taking inputs from a consultant and after obtaining approval of the Board. They will meet regularly not only to continually reassess the critical risks faced by the hospital but also to report on progress in each of the initiatives that is associated with critical risk.

Step three is focused on the maturation of the ERM approach to risk identification and management at a strategic level as well as the expansion of and integration of ERM principles throughout the organization.

Multiple Choice Questions

Choose the most appropriate answer from the answer options:

(3.1) Which one of the following is incorrect with respect to ERM?

- *(A) It is a process effected by an entity's board of directors, management and other personnel.*
- *(B) It is applied in strategic setting and across the enterprise.*
- *(C) It manages risk to be within risk appetite.*
- *(D) It provides complete assurance regarding the achievement of entity's objective.*

(3.2) What are some examples of internal drivers of an organization's risk culture?

- *(A) Resource allocation and risk attitude*
- *(B) Risk appetite and risk tolerance*
- *(C) Employee records*
- *(D) All of the options*

(3.3) The Delphi Technique is a method that attempts to move a group of experts toward a consensus opinion. When using the Delphi technique in practice which one of the following is incorrect?

(A) Each individual expert in the group is asked a question. The answer that each expert develops individually after consulting the others in the group is reported to the entire group.

(B) Each individual expert in the group is asked a question. The answer that each expert develops individually without consulting the others in the group is reported to the entire group.

(C) The question reported at group level is posed again separately to the expert, who is instructed to consider revising their response based on the results that were reported to the group.

(D) The question and response cycle continues for a predetermined number of rounds or until a consensus is achieved.

(3.4) Which one of the following is incorrect about the bow-tie technique?

(A) The purpose of the Bow-tie technique is to demonstrate that sources of risk can lead to events that have consequences.

(B) The event shown in the centre of the bow-tie would be listed in terms of the component of the organization that is impacted by the event. These components are people, premises, processes and products

(C) The Bow-tie technique cannot be only used to illustrate the four types of controls namely preventive, detective and corrective but not directive.

(D) The Bow-tie technique can be used m many ways, including the representation of opportunity risks.

(3.5) Which one of the following is not correct in reference to the sound risk culture in a company?

(A) At all level of the organisation understand and appreciate the positive and negative results that a risk event can bring.

(B) An appropriate risk reward balance consistent with the risk appetite is achieved when taking on risks.

(C) An effective system of controls commensurate with the scale and complexity is properly put in place.

(D) Previous mistakes are not considered while shaping the right risk actions.

(5 x 2 Marks = 10 Marks)

Descriptive Questions

(3.6) While recommending selection of individuals in the ERC, if you were hired as a consultant, what should be the three broad parameters? ***(3 Marks)***

(3.7) Would you agree with the view that there is no difference between ERM and BCP? Provide reasoned answer. ***(3 Marks)***

(3.8) How could a Narrative Approach be used to better identify and assess risks that are not easily quantified? ***(4 Marks)***

(3.9) Outsourcing of services has its place in risk management. What are the five key issues you would consider to make sure that what has been outsourced meets the continuing needs of the organization and is consistent with its strategy, vision and brand promise?

(5 Marks)

Answer

Multiple Choice Questions

3.1 (D)

3.2 (D)

3.3 (A) or (D)

3.4 (C) or (D)

3.5 (D)

Descriptive Questions

3.6 Broad parameters that an individual in the ERC should possess are as follows:

(i) has a chair who is an independent director and avoids "dual-hatting" with the chair of the board, or any other committee;

(ii) includes members who are independent;

(iii) includes members who have experience with regard to risk management issues and practices;

Alternative Solution

The ERC council should be made up of key individuals who

i. understand the strategic direction of the enterprise,

ii. represent most major segments in the enterprise, and

iii. have significant decision-making and budgetary authority to make changes happen.

3.7 Although Business Continuity Plan (BCP) is now an integral part of Operational Risk Management that can be triggered as part of an overall disruption that is caused by any or a combination thereof. However, link between BCP and Enterprise Risk Management

(ERM) cannot be denied as ERM is concerned with the risks facing the whole organization and BCP takes an approach that business continuity arrangements should be in place.

The BCP approach is to ensure the continuity of operations across the whole organization and is obviously part of an ERM approach. Hence, BCP can be considered a part of ERM, but it is not the whole of ERM activity.

The basis of ERM is that the stakeholder expectations and the core processes of the organization that deliver those expectations are the focus of the risk assessment process. The continuation of core business processes is also the basis of BCP and the intention of ERM is to ensure that the core processes are maintained as it is basis of stakeholder expectations.

However, if we talk about the difference in emphasis while ERM seeks to identify the risks that could impact the core processes, BCP seeks to identify the critical business functions that need to be maintained in order to achieve continuation of the business. Thus, it can be concluded that there is a good deal of similarity between BCP and style of ERM but both approaches are complementary to each other.

Alternative Solution

Because both approaches are based on the identification of the key dependencies and functions that must be in place for the continuity and success of the business.

I do not agree with the view that there is no difference between ERM and BCP. ERM and BCP differ because the former is concerned with the management of the risks that could impact core processes, whereas BCP is concerned with actions that should be taken to maintain the continuity of individual activities. The BCP, therefore, has the very specific function of identifying actions that should be taken after the risk has materialized in order to minimize its impact. BCP relates to the damage-limitation and cost-containment components of loss control.

3.8 Narrative Analysis is a process to analyze future events by considering alternative outcomes or alternative worlds i.e. making scenarios.

Scenario making involves preparing a brief narrative or description of a hypothetical situation of how a future event or events might turn out or look like.

For each scenario, the management reflects and analyses the potential consequences and potential causes when analysing risk.

Scenario analysis can be used effectively to identify opportunities for fraud, forecasting, managing financial risks, etc.

Alternative Solution

Not all risks of an organization easily quantified. Reputation is a good example of a risk for a hospital like BH that is often viewed as an intangible and therefore difficult to

quantify and best expressed through narrative reporting when numerical expression can be unreliable. For hospitals the narrative in risk management could be constructed similarly to that of medicine.

- The first is active listening.
- The second is putting into writing what happened, beyond the basics of the incident. What was the environment at the time, were there emotional Issues that surrounded the event or incident; and what happened in the days, weeks, or moments that led to the event?
- The third is sharing the narrative with those affected by it whether it is an individual or an entire organization.

It is a myth that the narrative approach is not just for ex post facto analysis of events.

Narrative can be used to describe critical risks that the organization faces. This is important to multiple reasons. First, the narrative can more fully explain the problem and how it might produce loss. Second, many people are more attuned and responsive to stories because they help individuals to visualize the concept. Third, narratives more fully describe the circumstances of the organization and may lead management to understand risk more holistically in association with attitudes, aptitudes, and environment that may produce or exacerbate losses.

3.9 The various key issues that need to be looked into to ensure that outsourcing meets the continuing needs of the organisation and is consistent with its strategy, vision and brand

- Clearly defined objective of outsourcing; this has to be brought into the scope of work;
- Contractual documentation to be adequate to ensure the service provider does only what is assigned and to the standard mutually agreed to by all parties involved;
- Legal indemnities to the organisation to be assessed while hiring a service provider;
- In agreements where the client and the service provider are in different states or in different countries, the respective countries' or states' laws have to be complied with;
- The BCP of the service provider has to be reviewed.
- The operational risk assessment covering regulatory risks, financial risk, financial reporting risk and other risks as delivery to end customers of the client in case the service provider fails to deliver for whatever reason.
- If technology or its disaster recovery itself is outsourced, all the attention is required to ensure the business operations work as designed and agreed.

Alternative Solution

- Potential impact of outsourcing on end to end processes when making a decision to outsource?
- Need to apply operational risk management and governance practices to outsourcing arrangements including risk associated with sub-contracting
- Identification and assessment of conflict of interest with the service provider
- Due diligence of service provider
- Adequacy of responsibility and oversight over the outsourcing arrangement
- Documentation, exit strategies and BCP

CASE STUDY: 4

OE, the Company is a leading manufacturer of garments headquartered at Delhi. Its customers are located in Europe and the USA. Major portion (80%) of the revenue is from export business. OE has borrowed in foreign currency and INR as well.

The Company is exposed to the impact of interest rate changes primarily through its borrowing activities. The Company's objective is to mitigate the impact of interest rate changes on earnings and cash flows and on the market value of its borrowings. In accordance with its policy, the Company targets its fixed-rate debt as a percentage of its net debt between a minimum and maximum percentage.

As the Company transacts business globally and is subject to risks associated with changing foreign currency exchange rates. The Company's objective is to reduce fluctuations associated with foreign currency exchange rate changes in its earnings and cash flow, enabling management to focus on core business issues and challenges.

The Company enters into option and forward contracts that change in value as foreign currency exchange rates change, to protect the value of its existing foreign currency assets, liabilities, firm commitments and forecasted but not firmly committed foreign currency transactions. In accordance with policy, the company hedges its forecasted foreign currency transactions for periods generally not to exceed two years within an established minimum and maximum range of annual exposure. Cross-currency swaps are used by the company to effectively convert foreign currency-denominated borrowings into INR denominated borrowings. It's also uses swaption and zero cost collar for hedging purposes.

Despite having a robust risk management practices the management of OE is concerned about the operating forex exposure. OE has been maintaining risk-register knowing well that a well-constructed and dynamic risk register is at the heart of a successful risk management initiative. However, during a risk review process it was uncovered that senior management has started believing that attending a risk assessment workshop and producing a risk register is a risk management obligations and therefore no ongoing actions are required.

Further, considering disruption in value chain in the garment business and its strong presence in Europe and it has a plan to open a garment manufacturing unit in Birmingham UK which will be wholly owned subsidiary of OE. The management believes this would reduce delivery time and hence would help in getting more business. Also the locational advantages enjoyed by competitors from Turkey can be addressed with this strategy. Recently number of buyers from Europe has started giving orders to suppliers in Bangladesh due to labour cost advantages and faster depreciating Bangladeshi Taka. Considering this OE has also plan to open a factory in Bangladesh.

Multiple Choice Questions

Choose the most appropriate answer from the answer options:

(4.1) Suppose OE issued a callable bond two years ago and it has three more years to go before the first call date. If interest rates have fallen over the past two years and you believe rates will not stay this low and that it would be in the firm's best interest to lengthen the duration of the liabilities, which of the following is one· potential strategy to accomplish the objective of lengthening the duration while also securing the lowering interest rate.

(A) buy a payer swaption

(B) sell a payer swaption

(C) buy a receiver swaption

(D) sell a receiver swaption

(4.2) Which of the following best describes a zero cost collar within the context of interest rate derivatives?

(A) A zero cost collar is a long (short) position in an interest rate cap and a short (long) position in an interest rate floor where the cost of the cap (floor) exactly offsets the revenue from the floor (cap).

(B) A zero cost collar is a long (short) position in an interest rate cap and a short (long) position in an interest rate floor where the cost of the cap (floor) is less than the revenue from the floor (cap).

(C) A zero cost collar is a long (short) position in an interest rate cap and a short (long) position in an interest rate floor where the cost of the cap (floor) is greater than the revenue from the floor (cap).

(D) A zero cost collar is an option that pays off only if interest rates remain within a designated range.

(4.3) The modem long-term currency swap can be viewed as:

(A) a spot sale and a forward purchase.

(B) a combination of forward contracts, each of them having zero initial market value.

(C) *a combination of forward contracts, each of them having, generally, a non-zero initial market value but with a zero initial market value for all of them taken together.*

(D) *a spot transaction and a combination of forward contracts, each of them having, generally, a non-zero initial market value but with a initial market value for all of them taken together.*

(4.4) A cross-hedge

(A) *involves the use of forward contracts, a combination of spot and market and money market transactions and other techniques to protect from foreign exchange loss.*

(B) *is a technique designed to hedge exposure in one currency by the use of futures or other contracts on another currency that is correlated with the first currency.*

(C) *involves an exchange of cash flows in two different currencies between two companies.*

(D) *involves a loan contract and a source of funds to carry out that contract in order to hedge transaction exposure.*

(4.5) As the financing of a foreign project by the parent ___ relative to the financing provided by the subsidiary, the parent's exchange exposure ____.

(A) *increases; decreases*

(B) *decreases; increases*

(C) *increases; increases*

(D) *decreases; decreases* ***(5 x 2 Marks = 10 Marks)***

Descriptive Questions

(4.6) Discuss the condition under which exchange rate changes may actually reduce the risk of foreign investment. ***(3 Marks)***

(4.7) You are hired by OE to review its operating forex exposure. Discuss two determinants of forex operating exposure. Bases on the information given in the Case Study, identify any one activity of OE which is likely to address the operating forex exposure? What would be the implications of purchasing power parity for operating exposure? ***(4 Marks)***

(4.8) What are the advantages and disadvantages of financial hedging of the firm's operating exposure vis-a-vis operational hedges and what are the advantages of a currency options contract as a hedging tool compared with the forward contract? ***(4 Marks)***

(4.9) What is the purpose of risk register? What would typically a risk register would cover? Do you think there are disadvantages associated with the use of risk registers? ***(4 Marks)***

Answer

Multiple Choice Questions

4.1 (D)

4.2 (A)

4.3 (D)

4.4 (B)

4.5 (C)

Descriptive Questions

4.6 It is not always necessary that exchange rate changes need not always increase the risk of foreign investment.

If covariance between exchange rate changes and the local market returns is negative enough to offset the positive variance of exchange rate volatility, changes in exchange rate can actually reduce the risk of foreign investment.

4.7 The main determinants of a OE's operating exposure are as follows:

(1) the structure of the markets in which the firm sources its inputs, such as labor and materials, and sells its products, and

(2) the OE's ability to mitigate the effect of exchange rate changes by adjusting its markets, product mix, and sourcing.

The plan to open a factory in Bangladesh is an example of addressing operating forex exposure.

So far as implication of purchasing power parity for operating exposure is concerned if the exchange rate changes are matched by the inflation rate differential between countries, OEs' competitive positions will not be altered by exchange rate changes and OE will not subject to operating exposure.

4.8 While financial hedging can be implemented quickly and that too with relatively low costs, the operational hedges are costly, time-consuming. However, in financial hedging it is difficult to hedge against long-term, real exposure with financial contracts. Also, operating hedging is not easily reversible.

The main advantage of currency option contract is that not only option contract provide hedging against the risk but also allows to take the benefit of movement in the exchange rate because of element of choice not an obligation. Option thus provides a hedge against ex post regret that forward hedger might have to suffer. Thus, hedger can eliminate the downside risk while retaining the upside potential.

4.9 The purpose of the risk register is to form an agreed record of the significant risks that have been identified. Also, the risk register will serve as a record of the control activities

that are currently undertaken. It will also be a record of the additional actions that are proposed to improve the control of the particular risk. Other information about risks will also be included in the risk register.

Typically, the risk register will cover the significant risks facing the organization or the project. It will record the results of the risk assessment related to the process, operation, location, business unit or project under consideration.

There are disadvantages associated with the use of risk registers, including the danger that the information recorded in the risk register will not be used in a dynamic way. The risk register could become a static record of risk status, rather than the risk action plan for the organization.

Alternative Answer

The purpose of Risk Register is as follows:

- Risk register is a record of risk, risk assessments; risk mitigation and action plans prepared by the responsible parties that help to support overall ERM and controls disclosures reporting process.
- Risk register is continuously updated and has columns for risk, causes, consequences, ownership, inherent risk score, controls, residual risk score, process, action for further mitigation, action owner, due date, etc.

Typically, the risk register will cover the following:

- ❖ Risk
- ❖ Causes
- ❖ Consequences
- ❖ Ownership
- ❖ Inherent risk score
- ❖ Controls
- ❖ Residual risk score
- ❖ Process
- ❖ Action for further mitigation
- ❖ Action owner
- ❖ Due Date

So far as the disadvantage of using Risk Register is concerned it has been seen that sometimes it becomes a static i.e., a non-living document.

CASE STUDY: 5

About the Company

HC is a leading restaurant company headquartered at Mumbai. It has 500 outlets operating across India and is listed on both BSE and NSE. As a result of COVID-19 the performance of the company was not good during first half of FY 2020-21. But the company has now made started using extensively online mode of order taking, payment and delivery. The operating model has now been completely revamped. The company has now created data base of customers which helps in marketing new products This has started showing results but has also exposed the Company with new risks including cyber risks.

Recent Developments

Recently Company was attacked by malware which affected the operations of the Company for two days. Cyber security was not an agenda just six month back. But with change in the operating model this has become one of the key risk of HC. The Board believes that now the Company will have to invest in cyber security to minimize the possibility of a having a cyber loss. It is well known that even the companies with the best IT security and highest expenditure on cyber protection still suffer successful cyber-attacks. However, Companies need to have contingency plans for managing the financial impact on their balance sheet of a potential large loss from a cyber-attack. The management is aware that cyber-attacks have been responsible for many missed quarterly earnings reports, which have been punished by shareholders, credit providers and business counterparties. It is more expensive in terms of the interest rates charged to access funds through borrowing after the event has occurred, particularly if credit ratings have been impaired as a result of cyber-attack.

A recent internal assessment indicates that it is still operating at 60% of the Pre-COVID level and hence needs further fund for operations.

HC has also acquired a Company named PC which is in food delivery business. The revenue of the PC has been rising during last two years. PC however is poorly managed and the Board of HC believes that they can transform it well and this acquisition would create synergy in terms increase in revenue and saving in the operating costs. The owner would raise the fund for acquisition from own sources and a private equity investor.

Plans of the Company

Considering the revival of economy, the Company wants to expand by opening 10 more outlets by the end of March 2021. And for this also it need borrowing which is available under various scheme announced by the Government of India. The Company has started the process of making financial analysis of the performance so that the Board is fully aware about the information being sent to the lenders.

HC has a plan to open few outlets in UK to serve Indian customers. But before committing huge Capex it wants to make a proper financial viability analysis. The Board members also want this analysis to cover analysis with respect to parent in order to satisfy the shareholders of HC.

Actions taken by the Company

The Company has hired a consultant to review entire risk management practices of HC and suggest suitable and practical solution to make it cyber-resilient. The consultant has been specifically asked to cover sensitivity analysis, scenario analysis and use of Monte Carlo Analysis especially considering the high uncertainties in the external environment so that adequate steps are taken to mitigate the risks.

The Key remark of one of the Board member was: "We believe that risk management decisions should be based on objective assessments of risk and be as evidence-based as possible. You should be able to estimate how various security measures and risk mitigation processes will affect your risk profile and to justify their implementation by how much they will reduce the risk of unacceptable loss."

The Board has given general guidance with respect to risk tolerance and wants this should also be covered in the consultant's report. They are aware that some companies may tolerate the occasional minor loss from cyber-attacks. In fact, it may be too costly relative to the value to make an organization invulnerable and to prevent any cyber loss occurrence at all. But most companies want to avoid having a severe loss above a certain threshold, particularly one that will cause reputation damage, lead to missing earnings targets, materially damage the balance sheet, trigger a rating downgrade, or threaten the viability of the organization itself.

Multiple Choice Questions

Choose the most appropriate answer from the answer options:

(5.1) HC has the following balance sheet (in INR millions):

Bills Payables	*100*		*Net PPE*		*1200*
Accounts Payable	*200*		*Inventories*	*300*	
Accruals	*100*		*Accounts Receivables*	*400*	
Total Current Liabilities		*400*	*Cash*	*100*	
Long -Term Debt		*600*	*Total Current Assets*		*800*
Equity		*1000*			
Total Liabilities and Equity		***2000***	***Total Assets***		***2000***

HC's Days Sales Outstanding (DSO) on a 365-day basis is 40, which is above the industry average of 30? Assume that HC is able to reduce its DSO to the industry average without reducing sales and the Company takes the freed-up cash and uses it to reduce its outstanding long-term bonds. If this occurs, what will be the new current ratio?

(A) 1.75

(B) 1.33

(C) 2.33

(D) 1.25

(5.2) You have been asked to compare performance of HC with another Company Y. You have collected the following information:

- *The two companies have the same total assets.*
- *HC has a higher total assets turnover than Company Y.*
- *HC has a higher profit margin than Company Y.*
- *Company Y has a higher inventory turnover ratio than HC.*
- *Company Y has a higher current ratio than HC.*

Which of the following statements is the most correct?

(A) HC must have a higher net income.

(B) HC must have a higher ROE.

(C) Company Y must have a higher ROA.

(D) Company Y must have higher profit margin.

(5.3) Which of the following statements about risk analysis techniques is FALSE?

(A) In sensitivity analysis, the dependent variable is plotted on the y-axis and the independent variable on the x-axis. The steeper the slope on the resulting line the less sensitive the dependent variable is to changes in the independent variable.

(B) Sensitivity analysis is incomplete, because it fails to consider the probability distributions of the independent variables.

(C) In Monte Carlo simulation, probable future events are simulated on a computer generating estimated rates of return and risk indexes.

(D) Scenario analysis is a risk analysis technique that considers both the sensitivity of the dependent variable to changes in the independent variables and the range of likely values of these variables.

(5.4) In the case of PC, at present the investment in working capital is 22% of sales. The Board of HC believes that it can be reduced that dramatically to 20% in the first year of ownership, 18% in the second year and then finally 15% in the third year. This level of 15% will then be the stable level of working capital investment for the business. What is the acquisition value of this working capital reduction if sales remain constant at INR 100 million per annum and your cost of capital is 10%? (rounded off)

(A) INR 7 million

(B) INR 5.8 million

(C) INR 10.7 million

(D) INR 8 million

(5.5) Broad categories of malware include

(A) 'Virus' - computer code inside a host program.

(B) 'worm' - a stand-alone piece of compiled software as a program that can replicate itself.

(C) 'Trojan horse' - a program that appears to do one thing but actually does something different.

(D) All of the options ***(5 x 2 Marks = 10 Marks)***

Descriptive Questions

(5.6) What are risk capacity and risk exposure? Explain the difference between risk exposure, risk tolerance and risk appetite? ***(6 Marks)***

(5.7) What are the two defining characteristics of cyber-resilient organization?

What is reverse stress testing in case of a cyber-resilient organization? ***(2 Marks)***

(5.8) Discuss the difference between performing the capital budgeting analysis from the parent firm's perspective as opposed to the project perspective. ***(3 Marks)***

(5.9) Discuss the four types of direct pay out cost if HC suffers from the cyber-attack.

(4 Marks)

Answer

Multiple Choice Questions

5.1 (A)

5.2 (A)

5.3 (A)

5.4 (B)

5.5 (D)

Descriptive Questions

5.6 Risk capacity is the level of risk an organization considers itself capable of absorbing, based on its earnings power, without damage to its dividend paying ability, its strategic plans and, ultimately, its reputation and ongoing business viability. It is based on a combination of budgeted, forecast and historical revenues and costs, adjusted for variable compensation, dividends and related taxes.

Risk exposure is an estimate of potential loss based on current and prospective risk positions across major risk categories - primary risks, operational risk and business risk. It builds as far as possible on the statistical loss measures used in the day-to-day operating controls. Correlations are taken into account when aggregating potential losses from risk positions in various risk categories to obtain an overall estimate of the risk exposure. The risk exposure is assessed against a severe but plausible constellation of events over say a one-year time horizon to a 95 per cent confidence level or a 'once in 20 years' event.

Risk exposure is the actual risk that the organization is taking and this may not be same as the risk appetite that the board believes is appropriate for the organization.

Risk appetite is established by the board, which sets an upper boundary on aggregate risk exposure.

The concept of tolerate is normally concerned with the organization being willing to retain or tolerate a risk, even if it is higher than the organization would choose to accept. The other concept is that of risk tolerance. Many organization use risk tolerance in the engineering sense to represent the range of risk that is broadly acceptable. As with the engineering use of the word tolerance, risk tolerance zones define the boundaries within which an organization desires the level of risk to be confined. An organization may have to tolerate risks that have a current level beyond its comfort zone and its risk appetite.

On occasions, an organization may even have to tolerate risks that are beyond its actual risk capacity. However, this situation would not be sustainable, and the organization would be vulnerable during this period.

Risk tolerance relates to a specific or individual risk, rather than the more general approach represented by risk appetite. Risk appetite refers to the amount and type of risk that an organization is willing to pursue or retain.

5.7 Defining characteristics of cyber-resilient organization are as follows:

- Identification of risk areas: whether it is own or outsourced network, internet, individual computers, mobile devices etc. Prioritization of resources and effort can be managed accordingly.
- Adequately restricting access to systems is the common way to prevent cyber risk; this is done by password protection at various levels, from common user to administrator level.

- Encryption solutions on individual computers is also done in a manner that if lost, the unauthorised entity cannot download the data into an external storage device.
- There are several technology solutions that create an adequate firewall of the organisation's systems to protect them from hacking from outside.
- A regular vulnerability testing of the firewall and periodic review to upgrade it is one of the main tasks of the information security manager. Detection of a test-attack is very important part of the preventive mechanism; an attacker may attempt to cause a minor violation to test the organisation's network security before causing a major incident.
- A response strategy to a cyber-attack incident is also important as part of risk management. The measures to prevent or mitigate customer disputes, legal indemnities, assess and minimize the financial impact of a cyber-attack, and governance over decision making and investments to restore the system functionalities to its secure state, are all important considerations. The root cause of these incidents and the impact have to be adequately documented.

Like some institutions failed during global financial crises, this period represented stress to default scenario. It involves extremely unlikely events which force the companies to think about the firm's most serious vulnerabilities and design stress to default scenarios accordingly.

5.8 There exists a big difference between the project and parent cash flows due to tax rules, exchange controls. Management and royalty payments are returns to the parent firm. The basis on which a project shall be evaluated depend on one's own cash flows, cash flows accruing to the parent firm or both.

Evaluation of a project on the basis of own cash flows entails that the project should compete favourably with domestic firms and earn a return higher than the local competitors. If not, the shareholders and management of the parent company shall invest in the equity/government bonds of domestic firms. A comparison cannot be made since foreign projects replace imports and are not competitors with existing local firms. Project evaluation based on local cash flows avoid currency conversion and eliminates problems associated with fluctuating exchange rate changes.

For evaluation of foreign project from the parent firm's angle, both operating and financial cash flows actually remitted to it form the yardstick for the firm's performance and the basis for distribution of dividends to the shareholders and repayment of debt/interest to lenders. An investment has to be evaluated on basis of net after tax operating cash flows generated by the project. As both types of cash flows (operating and financial) are clubbed together, it is essential to see that financial cash flows are not mixed up with operating cash flows.

5.9 Type of direct pay-out costs include:

(i) The response and forensics costs of the IT security team, both internal personnel and typically involving external consultants, that has to diagnose what happened as quickly as possible and render the system safe from further exploitation.

(ii) New technology, equipment, software, and systems may need to be purchased to remedy vulnerabilities.

(iii) Compensation for people whose personal data is compromised, including costs of notification, managing their enquiries and providing customer support, providing credit watch services, and payouts for any losses these individuals may suffer.

(iv) Legal costs to defend any litigation that might be brought against the company, including the costs of settling the action or losing the case and paying damages or even punitive awards.