CHAPTER 5

RISK ASSESSMENT METHODOLOGIES AND APPLICATIONS

- DEFINITION OF RISK (M'08-2 Marks)
  - **PROBABILITY** of a **THREAT** Exploiting a **VULNERBAILITY**.
  - Risk may be direct or indirect.
  - These risks lead to a gap between
    - The need to protect systems and
    - The degree of protection applied.
  - The gap is caused by
    - Widespread use of technology,
    - Elimination of distance, time and space as constraints,
    - Unevenness of technological changes,
    - Attractiveness of conducting unconventional electronic attacks against organizations
    - External factors such as legislative, legal and regulatory requirements or technological developments.
    - Interconnectivity of systems and
    - Devolution of management and control etc.
  - For e.g. Rain = Threat, Not carrying umbrella = Vulnerability, Risk= Getting drenched.

- DEFINITION OF THREAT (M'08-2 Marks)
  - A threat is an **ACTION, EVENT OR CONDITION**
  - Where there is a compromise
    - In the system,
    - its quality and
    - Ability to inflict harm to the organization.
  - Threat is any circumstance or event with the potential to cause harm to an information system in the form of
    - destruction,
    - disclosure,
    - adverse modification of data and
    - Denial of services.

- DEFINITION OF VULNERABILITY (M'08-2 Marks)
  - It is the **WEAKNESS IN THE SYSTEM SAFEGUARDS** that exposes the system to threats.
  - It may be weakness in

- ✳ an information system,
- ✳ cryptographic system,
- ✳ internal controls etc, that could be exploited by a threat.

☞ Vulnerabilities potentially "allow" a threat to harm or exploit the system

⇨ DEFINITION OF EXPOSURE (M'08-2 Marks)

☞ It is the **EXTENT OF LOSS** the organization has to face when a **RISK MATERIALIZES.**

☞ It is not just the immediate impact, but the real harm that occurs in the **LONG RUN**.

☞ For example, loss of business, failure to perform the system's mission, loss of reputation, violation of privacy, loss of resources.

⇨ DEFINITION OF LIKELIHOOD

☞ Likelihood of the threat occurring is the **ESTIMATION OF THE PROBABILITY** that the threat will succeed in achieving an undesirable event.

☞ The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring

⇨ DEFINITION OF ATTACK (M'08-2 Marks)

☞ Attack is **A SET OF ACTIONS DESIGNED** to compromise

- ✳ Confidentiality,
- ✳ integrity,
- ✳ availability or
- ✳ Any other desired feature of an information system.

☞ It is an attempt to defeat IS safeguards.

☞ The type of attack and its degree of success will determine the consequence of the attack.

⇨ DEFINITION OF RESIDUAL RISKS

☞ Any risk still remaining after the counter measures are analysized and implemented is called **RESIDUAL RISK**.

☞ An organization's management of risk should consider these two areas:

- ✳ **SELECTION OF SAFEGUARDS &**
- ✳ **ACCEPTANCE OF RESIDUAL RISK**

☞ Even when safeguards are applies there is probably going to be same residual risk.

☞ The risk can be minimized, but it can seldom be eliminated residual risk must be kept at a minimal acceptance level.

☞ A strong as it is kept at an acceptable level, the risk has been managed.

⇨ WHAT CAUSES RISK?

☞ Widespread use of technology

☞ External factors such as legislative, legal and regulatory requirements or **TECHNOLOGY DEVELOPMENT**

- ☞ **EXTERNAL DANGERS FROM HACKERS**, leading to denial of service and virus attacks, extortion and leakage of corporate information.
- ☞ Growing potential for misuse and abuse of information system **AFFECTING PRIVACY** and ethical values.
- ☞ **INCREASING REQUIREMENTS FOR AVAILABILITY** and robustness.

⇨ THREATS TO A COMPUTERIZED ENVIRONMENTS (N'08 & M'10- 5 Marks & M'11-8 Marks)

- ☞ A threat is an **ACTION, EVENT** OR **CONDITION**
- ☞ Where there is a **COMPROMISE IN THE SYSTEM** and causes **HARM TO THE ORGANIZATION.**

a) NATURAL THREATS

- ☞ **Natural Disasters:**
  Natural disasters such as earthquakes, lightings, floods, tornado, tsunami, etc can adversely affect the functioning of ARE Operations due to damage to IS facilities.
- ☞ **Power Loss:**
  Power failure can cause disruption of entire computing equipments depends on power supply.

b) TECHNOLOGICAL THREATS

- ☞ **Communication Failure:**
  Failure of communication lines result in inability to transfer data which primarily travel over communication line. E.g.: E-banking
- ☞ **Downtimes:**
  IS facilities may become unavailable due to equipment facility and hence the computing infrastructure may be available for short or extended period of time.
- ☞ **Errors:**
  Errors which may result from technical reasons, negligence or otherwise can cause significant integrity issues. (A wrong Parameter setting at a firewall)
- ☞ **Malicious Code:**
  Malicious code was such as viruses and worms which freely access the unprotected network may affect organizational & business networks that use these unprotected network.

c) OTHER THREATS

- ☞ **Disgruntled Employees:**
  A Disgruntled employee may cause intentional harm to information processing facilities or sabotage operations.
- ☞ **Abuse of access privileges by employees:**
  The security policy of company authorizes employee basis on their job responsibilities to access and executed select functions in critical application.
- ☞ **Theft or Destruction of Computing Resources:**
  Compromises the competitive advantages of the organization

⇨ THREATS DUE TO CYBER CRIMES (M'09 & N'09- 5 Marks)

- **Embezzlement:**
  It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted (typically an employee), for his or her own use or purpose
- **Fraud:**
  - It occurs on account of
    - Intentional misrepresentation of information or
    - Identity to deceive other,
    - The unlawful use of credit/debit card or ATM, or
    - Other use of electronic means to transmit deceptive information,
    - To obtain money or other things of value.
  - Fraud may be committed by someone inside or outside the company.
- **Theft of Proprietary Information:**
  It is the illegal obtaining of designs, plans, blueprints, codes, computer programs, formulas, receipts, trade secrets, graphics, copyrighted material data, forms, files lists, and personal or financial information, usually by electronic copying.
- **Denial of Services:**
  Denial of services usually caused by event such as ping attacks, port scanning probes & excessive amounts of income data (Degradation of Services)
- **Vandalism or Sabotage:**
  It is the deliberate or malicious, damage, defacement, destruction or other alternation of electronic files, data, web pages, and programs.
- **Other:**
  Threat includes several other causes such as intrusions, breaches & compromises of the respondent's computer networks (such as hacking or sniffing) regardless of whether damage or loss were sub stained as a result.

⇨ RISK ASSESSMENT (N'08- 5 Marks)

- The analysis of **PROBABILITY** of a disaster and estimating **THE IMPACT** of the same
- BCP/DRP (CO-RELATED TO RISK ASSESSMENT)
  - Risk assessment is a **CIRITICAL STEP** in disaster and business continuity planning.
  - Risk assessment is necessary for developing a well **TESTED CONTINGENCY PLAN**.
  - Risk assessment is a useful technique to assess the risks involved in the event of
    - Unavailability of information,
    - to priorities applications,
    - identify Expenses and
    - Develop Recovery Scenarios.
- The areas to be focused upon are:

1. Prioritization:
   - All applications are **INVENTORIED AND CRITICAL** ones identified.
   - Each of the critical application is reviewed to access its impact on the organization, in case a disaster occurs.
   - Subsequently, appropriate recovery plans are developed.

2. Identifying critical applications:
   - ✳ Amongst the applications currently being processed the critical applications are identified.
   - ✳ Further analysis is done to determine specific jobs in the applications which may be more critical.
   - ✳ Even though the critical value would be **DETERMINED BASED ON ITS PRESENT VALUE, FUTURE CHANGES SHOULD NOT BE IGNORED.**
3. Assessing their impact on the organization:
   - ✳ Business continuity planning should not concentrate only on business disruption but should also take into account other organizational functions which may be affected.
   - ✳ The areas to be considered include:
     - Legal liabilities,
     - Interruptions of customer services,
     - Possible losses,
     - Likelihood of fraud and recovery procedures.
4. Determining recovery time-frame:
   - ✳ Critical recovery time period is the period of time in which **BUSINESS PROCESSING MUST BE RESUMED** before the organization **INCURS SEVERE LOSSES.**
   - ✳ This critical time depends upon the nature of operations.
   - ✳ It is essential to involve the end users in the identification of critical functions and critical recovery time period.
5. Identification of exposures and implications:
   - ✳ It is not possible to accurately predict as to when and how a disaster would occur.
   - ✳ So, it s necessary to estimate the probability and frequency of disaster.
6. Development of recovery plan: The plan should be designed to provide for recovery from total destruction of a site.

⇨ RISK MANAGEMENT (N'09- 5 marks)

One needs to classify the risks as systematic and unsystematic.

a. SYSTEMATIC RISK
   - ☞ Systematic risks are the risk of being in business
   - ☞ These are generally unavoidable risk.
   - ☞ These are **CONSTANT ACROSS MAJORITY OF TECHNOLOGIES AND APPLICATION AND NOT PECULIAR TO ANY SPECIFIC APPLICATION OR TECHNOLOGY**.
   - ☞ For e.g.: The probability of power outage. The solution to power outage is having backup generator.
   - ☞ Thus, a Systematic risk can be mitigated **NOT BY TECHNOLOGY BUT BY MANAGEMENT PROCESS**.

b. UNSYSTEMATIC RISK

- ☞ Those which are **PECULIAR TO THE SPECIFIC APPLICATION** or technology.
- ☞ Generally, mitigated by advance technology: one of the major characteristics can be generally **MITIGATED BY USING AN ADVANCED TECHNOLOGY OR SYSTEM**.
- ☞ For e.g.: one can use a computer system with automatic mirroring (i.e. real time back up) to reduce the exposure to loss arising out of data loss in event of failure of host computer.

c. RISK MANAGEMENT PROCESS:

The broad Risk Management Process comprises of the following:

1. Identify the technology related risks under the gamut of operational risks.
2. Assess the identified risks in terms of probability and exposure.
3. Classify the risks as systematic and unsystematic.
4. Identify various managerial actions that can reduce exposure to systematic risks and the cost of implementing the same.
5. Look out for technological solutions available to mitigate unsystematic risks.
6. Identify the contribution of the technology in reducing the overall risk exposure.
7. Evaluate the technology risk premium on the available solutions and compare the same with the possible value of loss from the exposure.
8. Match the analysis with the management policy on risk appetite and decide on induction of the same.

⇨ RISK MANAGEMENT CYCLE

- ☞ It is a process involving the following steps:
  - ✳ Identifying assets,
  - ✳ Vulnerabilities and threats;
  - ✳ Assessing the risks;
  - ✳ Developing a risk management plan;
  - ✳ Implementing risk management actions, and
  - ✳ Re-evaluating the risks.
- ☞ The steps are categorized into 3 Primary Functions.
  1. Risk Identification
  2. Risk Assessment
  3. Risk Mitigation

⇨ RISK IDENTIFICATION

- ☞ Risk identification entails the identification of the various **THREATS** to the organization and also the underling **VULNERABILITIES**.
- ☞ Risk Identification is undertaken for critical applications, if it is not feasible to perform the study for entire organization.
- ☞ For Risk Identification, **ALL APPLICATIONS ARE INVENTORIED & CRITICAL ONES IDENTIFIED**
- ☞ Future analysis is done to determine specific jobs in the applications which may be more **CRITICAL**

⇨ PROBABILITY DETERMINATION

- To estimate the probability & frequency of disaster.
- The Presence, tenacity and strangles of threats as well as the effectiveness of safeguards must be considered while assessing the likelihood of threat occurring.
- While deciding on the class to be accorded, one has to focus on the available measures that can prevent such happing (i.e. **AVAILALB E CONTROL**)

⇨ EXPOSURE DETERMINATION

- An exposure is the **EXTENT OF LOSS** the organization has to face a risk materializes.
- It is not just the immediate impact, but the real harm that occurs in the **LONG RUN**.
- For E.g.:
  - Loss of business,
  - Failure to perform the system mission,
  - Loss of reputation,
  - Violation of privacy,
  - Loss of resources.
- Impact determination should not only include direct financial Losses, but also consider the following
  - Legal liabilities;
  - Interruption of customer services;
  - Possible Losses; and
  - Recovery Procedures
  - Availability of insurance limits the impact of the risk.
- **RISK IS THE PROBABILITY TIME OF EXPOSURE**.

⇨ TECHNIQUES FOR RISK ASSESSMENT/POLARIZATION RANKING (M'09- 5 Marks)

- **Judgment and Intuition:**
  - This is mainly depends on Personal & Professional Experience of the auditors &
  - Their understanding of the system and its environment.
  - To gather required a systematic education and ongoing professional Updating.
- **Quantitative Techniques:**
  - Involve the calculating an annual loss exposure value bases on the probability of the event and exposure in terms of estimated costs.
  - It is the assessment of Potential damage in the event of occurrence of unfavorable events, keeping in the mind often such event may occur.
- **Scoring Approach:**
  - The likelihood of risks in the system and their respective exposures are listed.
  - **WEIGHTS** are then assigned to likelihood and to the exposures depending on the severity, impact on occurrence, and cost involved.
  - The product of **LIKELYHOOD WEIGHT** with the exposure weight of every characteristic gives us the weighted score.

- ✳ System risk and exposure is **THEN RANKED** according to score obtained.

☞ **The Delphi Approach:** (M' 11- 4 Marks)

- ✳ Here a **PANEL OF EXPERTS** is appointed.
- ✳ The experts answer questionnaires in two or more rounds.
- ✳ Each expert given his opinion in a written and independent manner in each round.
- ✳ These estimates are then compiled together.
- ✳ After each round, facilitator providers an **ANONYMOUS SUMMARY** of the experts forecasts from the previous round as well as the reasons they provided for their judgments.
- ✳ Thus, experts are encouraged TO **REVISE THEIR EARLIER ANSWERS** in light of the replies of other members of their panel.
- ✳ It is believed that during this process the **RANGE OF THESE ANSWERS WILL DECREASE** and the group will coverage towards the "correct" answer.
- ✳ The estimates within pre-decided acceptance range are taken.
- ✳ The process may be repeated **FOUR TIMES** for revising the estimates falling beyond range.
- ✳ Then a **CURVE IS DRAWN** taking all the estimates as points on the graph.
- ✳ The median is drawn and this is the consensus opinion.

⇨ CONSIDERATIONS IN ANALYSING RIKS INCLUDE

1. Investigating the frequency of particular types of disasters (often versus seldom)
2. Determining the degree of predictability of the disaster.
3. Analyzing speed of onset of the disaster (sudden versus gradual).
4. Determining the amount of forewarning associated with the disaster.
5. Estimating the duration of the disaster.
6. Considering the impact of a disaster based on two scenarios:
   - ✳ Vital records are destroyed.
   - ✳ Vital records are not destroyed.
7. Identifying the consequences of a disaster, such as:
   - ✳ Personnel availability.
   - ✳ Personal injuries.
   - ✳ Loss of operating capability
   - ✳ Loss of assets.
   - ✳ Facility damage.
8. Determining the existing and required redundancy levels throughout the organization to accommodate critical systems and functions, including:
   - ✳ Hardware.
   - ✳ Information.
   - ✳ Communication.
   - ✳ Personnel.
   - ✳ Services.
9. Estimating potential loss:
   - ✳ Increased operating costs.
   - ✳ Loss of business opportunities.

- ✳ Loss of financial management capability.
- ✳ Loss of assets.
- ✳ Negative media coverage.
- ✳ Loss of stockholder's confidence.
- ✳ Loss of goodwill.
- ✳ Loss of income.
- ✳ Loss of competitive edge.
- ✳ Legal actions.

10. Estimating potential losses for each business function based on the financial and service impact and the length of time the organization can operate without this business function. The impact of a disaster related to a business function depends on the type of outage that occurs and the time that elapses before normal operations can be resumed.
11. Determining the cost of contingency planning.

⇨ RISK MITIGATION

☞ DEFINITION:

Risk Mitigation is the determination of various methods to **LOWER THE LIKELYHOOD** (Probability) or **EXPOSURE** (impact) of the risk.

☞ RISK MITIGATION THCHNIQUES:

1. Implementation of Controls
2. Insurance
3. Outsourcing
4. Service Level Agreements
5. Other Techniques

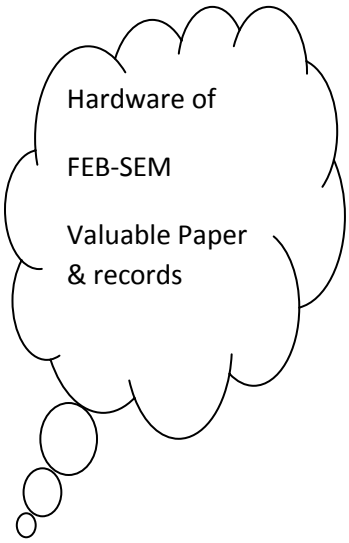
1. Implementation of Controls:

- ✳ To minimize Risks **CONTROLS PROCEDURES** need to be developed so that they decrease risk to a level where management can **ACCEPT** the exposure to that risk.
- ✳ It should be noted that excessive controls should not be implemented which may result IN
  - **INCREASED**
    - **BUREAUCRCACY**
    - **COMPLEXITY**
    - **CYCLE TIME,**
    - **NO VALUE ACTIVITIES**
  - **REDUCED**
    - **PRODUCTIVITY, ETC.**

2. Insurance:

H/W, S/W, N/W, PEOPLE & DATA TO BE PROTECTED

- ✳ An organization may buy insurance to MITIGATE such risk.
- ✳ Information system insurance policy should be a **MULTI-PERIL POLICY,** designed to provide various types of coverage.
- ✳ It should normally cover the following (N'10-8makrs)



a. Hardware and Facilities:
   - The **EQUIPMENT** should be covered adequately.
   - Provision should be made for the replacement of all equipment with a new one by the **SAME VENDOR**.

b. Software Reconstruction: In addition to the cost of media, **PROGRAMMING COSTS FOR RECREATING THE SOFTWARE** should be covered.

c. Extra Expenses: The Cost incurred for CONTINUING THE OPERATIONS TILL the original facility is restored should also be covered.

d. Business interruption:
   - This applies mainly to centre performing outsourced job of clients.
   - **THE LOSS OF PROFITS CAUSED BY THE DAMAGED COMPUTER MEDIA SHOULD BE COVERED.**

e. Valuable paper and records: The actual **COST OF VALUABLE PAPER** and record stored in the **INSURED PREMISES** should be covered.

f. Errors & Omission: This cover is against the **LEGAL LIABILITY** arising out of errors & omission committed by system analysis, programmers and other information System personnel.

g. Fidelity Coverage: This coverage is for **ACTS OF EMPLOYEES**, more so in case of financial institutions which use their own computers for providing services to clients.

h. Media Transportation: The Potential loss of damage to media while **BEING TRANSPORTED TO OFF SITE STORAGE/PREMISES SHOULD BE COVERED.**

3. Outsourcing:
   - ✳ The organization may **TRANSFER SOME OF THE FUNCTIONS** to an outside agency and transfers some of the associates risk to the agency.
   - ✳ For e.g.: Outsourcing of telecommunication line viz. subscribing to a leased line does not transfer the risk. The organization remains liable for failure to provide service because of failed telecommunication line.
   - ✳ **CAREFUL ASSESSMENT IS REQUIRED**
   - ✳ (Agreement that state the **MINIMUM SERVICE LEVEL PERFOMANCE AND A COMENSATION CLASUED** in the event failure to provide the minimum service level result in case of a loss.)

4. Service level agreements:
   - ✳ This may enter in to with the external suppliers as well as with the customers and users.
   - ✳ The service agreement with customers and user may clearly exclude or limit responsibility of the organization for any loss suffered by customer and user consequent to the technological failure.

- ✳ Thus, a bank may sate that service at ATM are subject to availability of Service.
- ✳ The delivery of service is conditional up on the system functionality, whereas the service is guaranteed if the customer visits the bank premises within the banking hours.

5. Other Techniques:
   - ✳ Creating Culture supportive of risk mitigation
   - ✳ Setting up independent operational risk management departments.
   - ✳ Establishing a disaster recovery plan & backup systems.
   - ✳ **COST BENEFI T ANALYSIS**!!

⇨ PRIMARY QUESTION TO CONSIDER WHEN EVALUATING THE RISK & PURPOSE OF RISK (N'10-5Marks)

- ☞ The two primary questions to consider when evaluating the risk inherent in a business function are:
  - ➢ What is the probability that things can go wrong? **(Probability)**
    - ✳ This view will have to be taken strictly on the technical point of view and should not be mixed up with past experience.
    - ✳ While deciding on the class to be accorded, one has to focus on the available measures that can prevent such happening.
  - ➢ What is the cost if what can go wrong does go wrong? **(Exposure)**
- ☞ The purposes of a risk evaluation is to
  - ✳ Identify the probabilities of failures and threats,
  - ✳ Calculate the exposure, i.e., the damage or loss to assets, and
  - ✳ Make control recommendations keeping the cost-benefit analysis in mind.

⇨ RISK ANALYSIS & ASSESSMENT FORM

A form may be used to list out severity of different elements passing risk. This will help in clearly assessing the overall organizational exposure and given an idea how to mitigate the risk. A typical form is given in the ICAI study material.