

5.1 Introduction

Risk assessment seeks to identify which business processes and related resources are critical to the business, what threats or exposures exist, that can cause an unplanned interruption of business processes, and what costs accrue due to an interruption.

There are various analytical procedures that are used to determine the various risks, threats, and exposures faced by an organization. These are known by various names, such as Business Impact Analysis (BIA), Risk Impact Analysis (RIA) and so on.

5.2 Risk, Threat, Exposure and Vulnerability

Risk : A risk is the likelihood that an organisation would face a vulnerability being exploited or a threat becoming harmful.

These risks lead to a gap between the need to protect systems and the degree of protection applied. The gap is caused by:

- (a) Widespread use of technology.
- (b) Interconnectivity of systems.
- (c) Elimination of distance, time and space as constraints.
- (d) Unevenness of technological changes.
- (e) Devolution of management and control.
- (f) Attractiveness of conducting unconventional electronic attacks against organisations.
- (g) External factors such as legislative, legal and regulatory requirements or technological developments.

This means there are new risk areas that could have a significant impact on critical business operations, such as:

- (a) External dangers from hackers, leading to denial of service and virus attacks, extortion and leakage of corporate information.
- (b) Growing potential for misuse and abuse of information system affecting privacy and ethical values.
- (c) Increasing requirements for availability and robustness.

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 organisation. 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.



Fig. 5.2.1 : Risk and Vulnerabilities

Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be weakness in an information system, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat.

Here are two more vulnerability examples:

- o Leaving your front door unlocked makes your house vulnerable to unwanted visitors.
- o Short passwords (less than 6 characters) make your automated information system vulnerable to password cracking or guessing routines.

An exposure is the extent of loss the organisation has to face when a risk materialises. It is not just the immediate impact, but the real harm that occurs in the long run. For example, loss of business, loss of reputation, violation of privacy and loss of resources.

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.

Attack is a set of actions designed to compromise confidentiality, integrity, availability or any other desired feature of an information system. Simply, it is the act of trying to defeat IS safeguards. The type of attack and its degree of success will determine the consequence of the attack.

Any risk still remaining after the counter measures are analysed and implemented is called **Residual Risk**. An organisation's management of risk should consider these two areas acceptance of residual risk and selection of safeguards. Even when safeguards are applied, there is probably going to be some residual risk. Residual risk must be kept at a minimal, acceptable level.

5.3 Threats to the Computerised Environment

Any computerised environment is dependent on people. The special skill sets such as IT operational team, programmers; data administrator, etc. are key links and Social engineering risks target key persons to get sensitive information to exploit the information resources of the enterprise. Threats also arise on account of dependence on external agencies.

A few common threats to the computerised environment can be:

- (a) **Power failure** : Power failure can cause disruption of entire computing equipments since computing equipments depends on power supply.
- (b) **Communication failure**: Failure of communication lines result in inability to transfer data which primarily travel over communication lines. e.g. for e-banking, communication failure present a significant threat that will have a direct impact on operations.
- (c) **Disgruntled Employees** : A disgruntled employee presents a threat since, with access to sensitive information of the organisation, he may cause intentional harm to the information processing facilities or sabotage operations.
- (d) **Errors** : Errors which may result from technical reasons, negligence or otherwise can cause significant integrity issues. A wrong parameter setting at the firewall to “allow” attachments instead of “deny”.
- (e) **Malicious Code** : Malicious code such as viruses and worms which freely access the unprotected networks may affect organisational and business networks that use these unprotected networks.
- (f) **Abuse of access privileges by employees** : The security policy of the company authorises employees based on their job responsibilities to access and execute select functions in critical applications.
- (g) **Natural disasters** : Natural disasters such as earthquakes, lighting, floods, tornado, tsunami, etc. can adversely affect the functioning of the Information System operations due to damage to Information System facilities.
- (h) **Theft or destruction of computing resources** : Since the computing equipments form the back-bone of information processing, any theft or destruction of the resource can result in compromising the competitive advantage of the organisation.
- (i) **Downtime due to technology failure** : Information System facilities may become unavailable due to technical glitches or equipment failure and hence the computing infrastructure may not be available for short or extended periods of time.
- (j) **Fire, etc.** : Fire due to electric short circuit or due to riots, war or such other reasons can cause irreversible damage to the IS infrastructure.

5.4 Threats due to Cyber Crimes

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/her own use or purpose.

Fraud : It occurs on account of intentional misrepresentation of information or identity to deceive others, or the use of electronic means to transmit deceptive information. 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, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, and personal or financial information, usually by electronic copying.

Denial of service : There can be disruption or degradation of service that is dependent on external infrastructure. Denial of service is usually caused by events such as ping attacks, port scanning probes, and excessive amounts of incoming data.

Vandalism or sabotage: It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.

Computer virus : A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the user.

Other : Threat includes several other cases such as intrusions, breaches and compromises of the respondent's computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained as a result.

5.5 Risk Assessment

A risk assessment can provide an effective approach that will serve as the foundation for avoiding of disasters.



- 5.5.1 Risk assessment is a critical step in disaster and business continuity planning.** Risk assessment is necessary for developing a well tested contingency plan. Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster.
- Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to prioritise applications, identify exposures and develop recovery scenarios. The areas to be focused upon are:
- (a) Prioritisation :** All applications are inventoried and critical ones identified. Each of the critical applications is reviewed to assess its impact on the organisation, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.
 - (b) Identifying critical applications :** Amongst the applications critical applications are identified. Determine specific jobs in the applications which may be more critical and critical value would be determined based on its present value, future changes should not be ignored.
 - (c) Assessing their impact on the organisation :** Business continuity planning should also considered
Following areas apart from business disruption.
 - Legal liabilities.
 - Interruptions of customer services.
 - Possible losses.
 - Likelihood of fraud and recovery procedures.
 - (d) Determining recovery time-frame:** Critical recovery time period is the period of time in which business processing must be resumed before the organisation incurs severe losses.
It is essential to involve the end users in the identification of critical functions and critical recovery time period.
 - (e) Assess Insurance coverage :** The information system insurance policy should be a multi-peril policy, designed to provide various types of coverage. Depending on the individual organisation and the extent of coverage required, suitable modifications may be made to the comprehensive list provided below:
 - (i) Hardware facilities :** The equipments should be covered adequately. Provision should be made for the replacement of all equipments with a new one by the same vendor.

- (ii) **Software reconstruction:** In addition to the cost of media, programming costs for recreating the software should also be covered.
- (iii) **Extra expenses:** The cost incurred for continuing the operations till the original facility is restored should also be covered.
- (iv) **Business interruption:** This applies mainly to centres performing outsourced jobs of clients. The loss of profit caused by the damaged computer media should be covered.
- (v) **Valuable paper and records:** The actual cost of valuable papers and records stored in the insured premises should be covered.
- (vi) **Errors and omissions:** This cover is against the legal liability arising out of errors and omissions committed by system analysts, programmers and other information system personnel.
- (vii) **Fidelity coverage:** This coverage is for acts of employees, more so in the case of financial institutions which use their own computers for providing services to clients.
- (viii) **Media transportation:** The potential loss or damage to media while being transported to off-site storage/premises should be covered.
- (f) **Identification of exposures and implications:** It is not possible to accurately predict as to when and how a disaster would occur. So it is necessary to estimate the probability and frequency of disaster.
- (g) **Development of recovery plan:** The plan should be designed to provide for recovery from total destruction of a site.

5.6

Risk Management

One needs to classify the risks as systematic and unsystematic.

Systematic risks are

- unavoidable risks - these are constant across majority of technologies and applications. For example the probability of power outage is not dependant on the industry but is dependant on external factors.
- Systematic risks would remain, no matter what technology is used.
- Systematic risks can be reduced by designing management control process and does not involve technological solutions.
- For example, the solution to non availability of consumable is maintaining a high stock of the same.

Unsystematic risks are

- those which are peculiar to the specific applications or technology.
- One of the major characteristics of these risks would be that they can be generally mitigated by using an advanced technology or system.
- For example one can use a computer system with automatic mirroring to reduce the exposure to loss arising out of data loss in the event of failure of host computer.

5.6.1 Risk Management Process

The broad process of risk management will be as follows:

1. Identify the technology related risks under the scope 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. The analysis should not be restricted to the instant area of application of the technology but should be extended across the entire organisation. This is necessary since many technologies may mitigate a specific type of risk but can introduce other kinds of risks.
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.

5.6.2 The 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.

These steps are categorised into three primary functions –

- (i) Risk Identification,
- (ii) Risk Assessment and
- (iii) Risk Mitigation.

5.7 Risk Identification

A risk is anything that could jeopardize the achievement of an objective. For each of the department's objectives, risks should be identified. Asking the following questions helps to identify risks:

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we vulnerable?
- What assets do we need to protect?
- Do we have liquid assets or assets with alternative uses?

- How could someone steal from the department?
- How could someone disrupt our operations?
- How do we know whether we are achieving our objectives?
- On what information do we most rely?
- On what do we spend the most money?
- How do we bill and collect our revenue?
- What decisions require the most judgment?
- What activities are most complex?
- What activities are regulated?
- What is our greatest legal exposure?

Individuals, primarily from the business unit, are the main source of data on all aspects of business operations and assets. For this reason, identifying knowledge individuals to be interviewed and developing interview questions are critical parts of the planning process that require careful attention and close coordination between the business unit manager and senior management.

Risk Evaluation

The purpose of the risk evaluation is to identify the inherent risk of performing various business functions especially with regard to usage of information technology enabled services. Management and audit resources will be allocated to functions with highest risks. The risk evaluation will directly affect the nature, timing and extent of audit resources allocated.

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

- (1) identify the probabilities of failures and threats,
- (2) calculate the exposure, i.e., the damage or loss to assets, and
- (3) make control recommendations keeping the cost-benefit analysis in mind.

Techniques for Risk Evaluation :

Following are some of the techniques that are available to assess and evaluate risks.

- (a) In many situations the auditors have to use their **judgement and intuition** for risk assessment. This mainly depends on the personal and professional experience of the auditors and their understanding of the system and its environment. Together with it is required a systematic education and ongoing professional updating.

(b) **The Delphi Technique:**

Here a panel of experts is appointed. Each expert gives his opinion in a written and independent manner. They enlist the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposures of the system. These estimates are then compiled together. The estimates within a pre-decided acceptable range are taken. The process may be repeated four times for revising the estimates falling beyond the 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.

- (c) **In the Scoring approach** the risks in the system and their respective exposures are listed. Weights are then assigned to the **risk** and to the **exposures** depending on the severity, impact on occurrence, and costs involved. The product of the risk weight with the exposure weight of every characteristic gives us the weighted score. The sum of these weighted score gives us the risk and exposure score of the system. System risk and exposure is then ranked according to the scores obtained.

- (d) **Quantitative techniques** involve the calculating an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs. This helps the organisation to select cost effective solutions. It is the assessment of potential damage in the event of occurrence of unfavourable events, keeping in mind how often such an event may occur.

- (e) **Qualitative techniques are by far the most widely used approach to risk analysis.**

Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements:

- **Threats:** These are things that can go wrong or that can 'attack' the system. Examples, might include fire or fraud. Threats are ever present for every system.
- **Vulnerabilities:** These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire, vulnerability would be the presence of inflammable materials (e.g. paper).

Controls: These are the countermeasures for vulnerabilities. There are four types:

- i) Deterrent controls reduce the likelihood of a deliberate attack
- ii) Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact.
- iii) Corrective controls reduce the effect of an attack
- iv) Detective controls discover attacks and trigger preventative or corrective controls.

These elements can be illustrated by a simple relational model:

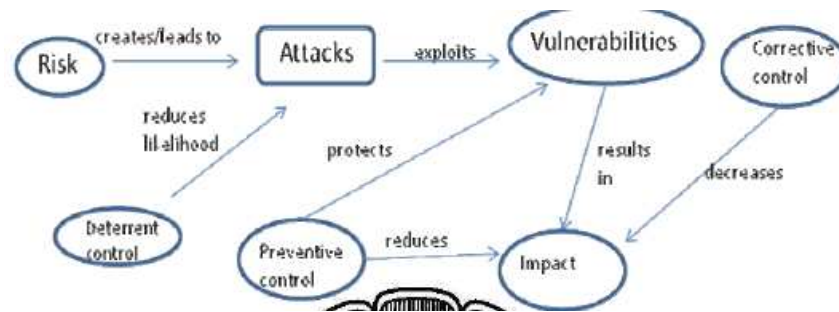


Fig. 5.7.1 : Risk evaluation

5.8 Risk Ranking

Organisations have to devise their own ranking methods. For example, the impact can be rated as: 0 = No impact or interruption in operations, 1 = Noticeable impact, interruption in operations for up to 8 hours, 2 = Damage to equipment and/or facilities, interruption in operations for 8 - 48 hours, 3 = Major damage to the equipment and/or facilities, interruption in operations for more than 48 hours. All main office and/or computer centre functions must be relocated.

Certain assumptions may be necessary to uniformly apply ratings to each potential threat.

Following are typical assumptions that can be used during the risk assessment process:

- Although impact ratings could range between 1 and 3 for any facility given a specific set of circumstances, ratings applied should reflect anticipated, likely or expected impact on each area.
- Each potential threat should be assumed to be “localised” to the facility being rated.
- Although one potential threat could lead to another potential threat (e.g., a hurricane could act off tornados), no domino effect should be assumed.
- If the result of the threat would not warrant movement to an alternate site(s), the impact should be rated no higher than a “2.”.

5.8.1 How to perform Risk Assessment : The risk assessment should be performed by facility. To measure the potential risks, a weighted point rating system can be used. Each level of probability can be assigned points as follows:

Probability	Points
High	10
Medium	5
Low	1

To obtain a weighted risk rating, probability points should be multiplied by the highest impact rating for each facility. For example, if the probability of hurricanes is high (10 points) and the impact rating to a facility is “3” (indicating that a move to alternate facilities would be required), then the weighted risk factor is 30 (10 x 3). Based on this rating method, threats that pose the greatest risk (e.g., 15 points and above) can be identified.

Considerations in analysing risk include:

1. Investigating the frequency of particular types of disasters (often versus seldom).
2. Determining the degree of predictability of the disaster.
3. Analysing 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:
 - a. Vital records are destroyed.
 - b. Vital records are not destroyed.

7. Identifying the consequences of a disaster, such as:
 - a. Personnel availability.
 - b. Personal injuries.
 - c. Loss of operating capability.
 - d. Loss of assets.
 - e. Facility damage.
8. Determining the existing and required redundancy levels throughout the organisation to accommodate critical systems and functions, including:
 - a. Hardware.
 - b. Information.
 - c. Communication.
 - d. Personnel.
 - e. Services.
9. Estimating potential loss:
 - a. Increased operating costs.
 - b. Loss of business opportunities.
 - c. Loss of financial management capability.
 - d. Loss of assets.
 - e. Negative media coverage.
 - f. Loss of stockholder's confidence.
 - g. Loss of goodwill.
 - h. Loss of income.
 - i. Loss of competitive edge.
 - j. Legal actions.
10. Estimating potential losses for each business function based on the financial and service impact and the length of time the organisation 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.

5.9 Risk Mitigation

Factor or casual analysis can help relate characteristics of an event to the probability and Severity of the operational losses. This will enable the organization to decide whether or not to Invest in information system or people (hazards) so events (frequency) or the effect of events (Severity) can be minimized.

A causal understanding is essential to take appropriate action to control and manage risks Because causality is a basis for both action and prediction. Knowing 'what causes what' gives an ability to intervene in the environment and implement the necessary controls.

Cause models help in the implementation of risk mitigation measures.

Cause analysis identifies events and their impact on losses. In addition to establishing causal relationship, other risk mitigation measures are:

- Self assessment.
- Calculating reserves and capital requirements.
- Creating culture supportive of risk mitigation.
- Strengthening internal controls, including internal and external audit of systems, processes and controls, including IS audit and assurance).
- Setting up operational risks limits (so business will have to reduce one or more of frequency of loss, severity of loss or size of operations).
- Setting up independent operational risk management departments.
- Establishing a disaster recovery plan and backup systems.
- Insurance.
- Outsourcing operations with strict service level agreements so operational risk is transferred.

5.9.1 Common risk mitigation techniques :

1. **Insurance:** An organisation may buy insurance to mitigate such risk. Under the scheme of the insurance, the loss is transferred from the insured entity to the insurance company in exchange of a premium. However while selecting such an insurance policy one has to look into the exclusion clause to assess the effective coverage of the policy.
2. **Outsourcing:** The organisation may transfer some of the functions to an outside agency and transfer some of the associated risks to the agency. One must make careful assessment of whether such outsourcing is transferring the risk or is merely transferring the management process.

3. **Service Level Agreements:** Some of risks can be mitigated by designing the service level agreement. This may be entered into with the external suppliers as well as with the customers and users. The service agreement with the customers and users may clearly exclude or limit responsibility of the organisation for any loss suffered by the customer and user consequent to the technological failure.

5.10 Risk and Controls

Risk is the probability that an event or action will adversely affect the organization. The primary categories of risk are errors, omissions, delay and fraud. In order to achieve goals and objectives, management needs to effectively balance risks and controls. Therefore, control procedures need to be developed so that they decrease risk to a level where management can accept the exposure to that risk. By performing this balancing act "reasonable assurance" can be attained. As it relates to financial and compliance goals, being out of balance can cause the following problems:

Excessive Risks	Excessive Controls
Loss of assets, donor or grants	Increased bureaucracy
Poor business decisions	Reduced productivity
Non-compliance	Increased complexity
Increased regulations	Increased cycle time
Public scandals	Increase of no-value activities

In order to achieve a balance between risk and controls, internal controls should be proactive, value-added, cost-effective and address exposure to risk.

Risk: is the likelihood that an organisation would face a vulnerability being exploited or a threat becoming harmful. 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.	Vulnerability is the weakness in the system safeguards that exposes the system to threats. Exposure is the extent of loss the organisation has to face when a risk materializes.	Attack is a set of actions designed to compromise confidentiality, integrity, availability or any other desired feature of an information system. Residual Risk: Any risk still remaining after the counter measures are analysed and implemented is called residual risk.
• THREATS TO THE COMPUTERISED ENVIRONMENT: (The <u>DEMAND Curve</u> is <u>Perfectly Fine</u>) • <u>T</u>heft or destruction of computing resources • <u>D</u>isgruntled Employees • <u>E</u>rrors • <u>M</u>alicious Code • <u>A</u>buse of access privileges by employees • <u>N</u>atural disasters • <u>D</u>owntime due to technology failure • <u>C</u>ommunication failure • <u>P</u>ower Loss • <u>F</u>ire, etc.	THREATS DUE TO CYBER CRIMES: (Due To Computer Virus Entire Fraud Slipped Off) • <u>D</u>enial of service • <u>T</u>heft of proprietary information • <u>C</u>omputer Virus • <u>E</u>mbezzlement • <u>F</u>raud • <u>S</u>abotage or Vandalism • <u>O</u>ther	RISK MANAGEMENT PROCESS: • Identify the risks • Assess the identified risk • Classify the risks • Identify various managerial actions that can reduce exposure • Look out for technological solutions • Identify the contribution of the technology in reducing the overall risk exposure. • Evaluate the technology risk premium and compare the same with the possible value of loss from the exposure. Match the analysis with the management policy

RISK MANAGEMENT: • Systematic risks • Unsystematic risks	THE RISK MANAGEMENT CYCLE: • Risk Identification • Risk Assessment • Risk Mitigation	
RISK IDENTIFICATION: • What is the probability that things can go wrong? (Probability) • What is the cost if what can go wrong does go wrong? (Exposure)	<u>The purpose of a risk evaluation is to:</u> • Identify the probabilities of failures and threats • Calculate the exposure, i.e. the damage or loss to assets • Make control recommendations keeping the cost-benefit analysis in mind	TECHNIQUES FOR RISK EVALUATION: • Judgement and intuition • The Delphi approach • Scoring • Quantitative Techniques
RISK ASSESSMENT: Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster.	<u>Various areas to determine the risk:</u> (Please Issue Anil Dhirubhai Ambani's ID) • <u>P</u>rioritisation • <u>I</u>dentifying critical applications • <u>A</u>ssessing their impact on the organisation • <u>D</u>etermining recovery time-frame • <u>A</u>ssess Insurance coverage • <u>I</u>dentification of exposures & implications • <u>D</u>evelopment of recovery plan	RISK MITIGATION: Factor or casual analysis can help related characteristics of an event to the probability and severity of the operational losses. This will enable the organisation to decide whether or not to invest in information system or people (hazards) so events (frequency) or the effect of events (severity) can be minimized.
COMMON RISK MITIGATION TECHNIQUES • Insurance • Outsourcing • Service Level Agreements		

---****---