5 - RISK ASSESSMENT METHODOLOGIES AND APPLICATIONS

Risk assessment seeks to identify which business processes and related resources are critical to the business, what threats or exposures exists, 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.

Risk assessment consists of two basic components they are data collection and its analysis. The data collected in risk assessment should include a comprehensive list of business processes and their resource dependencies. The purpose of risk analysis involves threat identification and risk mitigation.

5.2 RISK, THREAT, EXPOSURE, AND VULNERABILITY

1. **Risk :** A **risk** is the likelihood that an organisation would face a vulnerability being exploited or a threat becoming harmful. Information systems can generate many direct and indirect risks.

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

   (a) **W**idespread use of technology.

   (b) **I**nterconnectivity of systems.

   (c) **D**evolution of management and control.

   (d) **E**limination of distance, time and space as constraints

   (e) **U**nevenness of technological changes.

   (f) **A**ttractiveness of conducting unconventional electronic attacks against organisations.

   (g) **E**xternal 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 **D**angers from hackers, leading to denial of service and virus attacks, extortion and leakage of corporate information.

   (b) **I**ncreasing requirements for availability and robustness.

   (c) **G**rowing potential for misuse and abuse of information system affecting privacy and ethical values.

   New technology provides the potential for (i) dramatically enhanced business performance, (ii) improved and demonstrated information risk reduction and security measures.

   Thus it can add real value to the organisation by contributing to (i) Interactions with the trading partners, (ii) closer customer relations, (iii) improved competitive advantage and (iv) protected reputation.

2. **Threat** :

   (a) 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.

   (b) 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

3. **Vulnerability:**

   (a) **Vulnerability** is the weakness in the system safeguards that exposes the system to threats.

   (b) 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.

   (c) Vulnerabilities potentially "allow" a threat to harm or exploit the system.

   For example, vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records.

   Here are two more vulnerability examples:

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

   (d) Missing safeguards often determine the level of vulnerability. Determining vulnerabilities involves a security evaluation of the system including inspection of safeguards, testing, and penetration analysis.

4. **Exposure:**

   (a) 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.

   (b) For example, loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources.

5. Likelihood:

   (a) **Likelihood** of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event.

   (b) 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.

6. Attack:

   (a) **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.

   (b) The type of attack and its degree of success will determine the consequence of the attack.

7. **Residual Risk**:

   (a) Any risk still remaining after the counter measures are analysed and implemented is called **Residual Risk**.

   (b) An organisation's management of risk should consider these two areas: (i) acceptance of residual risk and (ii) selection of safeguards

   (c) Even when safeguards are applied, there is probably going to be some residual risk. The risk can be minimised, but it can seldom be eliminated.

   (d) Residual risk must be kept at a minimal, acceptable level. As long as it is kept at an acceptable level, (i.e. the likelihood of the event occurring or the severity of the consequence is sufficiently reduced) the risk can be managed.

5.3 THREATS TO THE COMPUTERISED ENVIRONMENT

1. Any computerised environment is dependent on people. They are a critical links in making the entire enterprise computing happen.
2. As such threats emanate from people themselves. The special skill sets such as IT operational team, programmers; data administrator, etc. are key links in ensuring that the IT infrastructure delivers to the user requirements.
3. 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.
4. IT computing services are significantly dependant on various vendors and service providers e.g., equipment supply and support, consumables, systems and program maintenance, air-conditioning, hot-site providers, utilities, etc.

A few common threats to the computerised environment can be: **DEMAND PF CD**

(i) **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

(ii) 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" may result in the entire organisation network being compromised with virus attacks

(iii) **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.

(iv) **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.

(v) **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.

(vi) **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. However the period for which the facilities are not available may vary in criticality depending on the nature of business and the critical business process that the technology supports

(vii) **Power failure :** Power failure can cause disruption of entire computing equipments since computing equipments depends on power supply.

(viii) **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

(ix) **Communication failure :** Failure of communication lines result in inability to transfer data which primarily travel over communication lines. Where the organisation depends on public communication lines e.g. for e-banking, communication failure present a significant threat that will have a direct impact on operations.

(x) **Destruction or Theft 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.

Fig. 5.3.1 : Types of attacks

5.4 THREATS DUE TO CYBER CRIMES

VITamins **CDEF**

1. ***Vandalism or sabotage**:* It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.
2. ***Illegal Access*** : 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.
3. ***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.
4. ***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.
5. ***Denial of service*** : There can be disruption or degradation of service that is dependent on external infrastructure. Problems may erupt through internet connection or e-mail service those results in an interruption of the normal flow of information. Denial of service is usually caused by events such as ping attacks, port scanning probes, and excessive amounts of incoming data.
6. ***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.
7. ***Fraud*** : It occurs on account of intentional misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the 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.

5.5 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.

Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan. Risk assessment helps organisation in the following way:

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

(b) Through risk analysis, it is possible to identify, assess, and then mitigate the risk. Such an analysis entails the development of a clear summary of the current situation and a systematic plan for risk identification, characterisation, and mitigation

(c) Risk assessment is a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well tested contingency plan

(d) 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

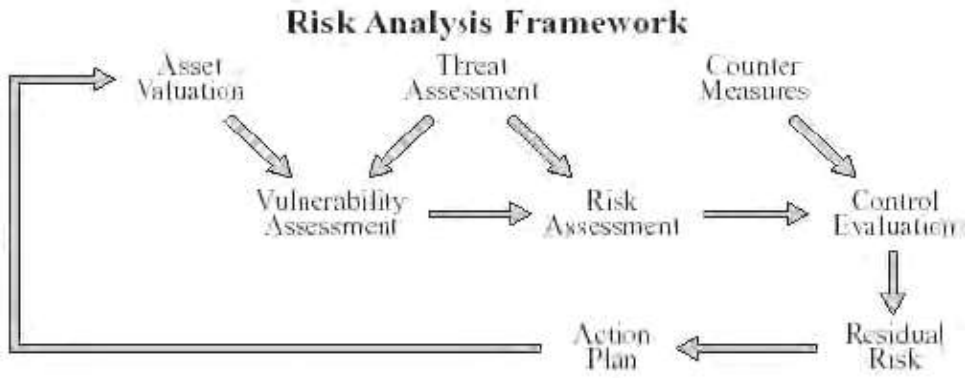


Fig. 5.5.1 : Risk analysis framework

The areas to be focused upon are:

1. ***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
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 organisation****:* Business continuity planning should not concentrate only on business disruption but should also take into account other organisational 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 organisation 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. ***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: **SAB TV ME Extra Facilities**

(a) **Storage media** : Covers the replacement of the storage media plus their contents – data files, programs, documentation.

(b) **Accounts receivable** : Covers cash-flow problems that arise because an organisation cannot collect its accounts receivable promptly.

(c) **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.

(d) **Transportation of Media :** The potential loss or damage to media while being transported to off-site storage/premises should be covered.

(e) **Valuable paper and records:** The actual cost of valuable papers and records stored in the insured premises should be covered.

(f) **Malpractice, errors***:* Covers claims against an organisation by its customers. This covers the legal liability arising out of errors and omissions committed by system analysts, programmers and other information system Personnel.

(g) **Equipment and software:** The hardware equipments should be covered adequately. Provision should be made for the repairs or replacement of all equipments with a new one by the same vendor. In addition to the cost of hardware equipments, programming costs for recreating the software should also be covered.

(h) **Extra expenses:** The cost incurred for continuing the operations till the original facility is restored should also be covered.

(i) **Facilities** : Covers items such as reconstruction of a computer room, raised floors, special furniture.

6. ***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.

7. ***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:

(a) **Systematic risks** are unavoidable risks .

(b) These are constant across majority of technologies and applications.

(c) 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.

(d) Thus effort to seek technological solution to reduce systematic risks would essentially be unfruitful activity and needs to be avoided.

(e) 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. Thus a systematic risk can be mitigated not by technology but by management process.

(f) Hence one would not make any additional payment for technological solution to the problem. To put in other words there would not be any technology linked premium that one should pay trying to reduce the exposure to systematic risk.

Unsystematic risks:

(a) Unsystematic risks are those which are peculiar to the specific applications or technology.

(b) They depend on technology and applications and are avoidable.

(c) 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.

(d) Thus by making additional investment one can mitigate these unsystematic risks.

(e) The management has to decide whether the additional payment to mitigate the risk is justifiable considering the possibility of loss that may or may not occur. The answer lies in identification of whether the overall risk exposure of the organisation is coming down because of the additional investment.

Risk Appetite:

(a) It may be noted that every business has its inherent risk - the cost of running the business. In case of a technology driven business, the risks induced by technology failure is a part of the operating risk.

(b) The issue is how much of the risk is acceptable and what should be the price that one would pay to reduce a certain part of the risk.

(c) Cardinal to this issue is the ability to measure risk. Until the organisation has developed a process of risk and exposure measurement –it will be difficult to develop a model for risk management.

(d) Following this issue will be the risk appetite of the organisation –does it wants to be risk aggressive or risk averter.

(e) The comparison will have to be made within the frame work of the industry for ensuring usage of a consistent and relevant yardstick. For example, the risk appetite of risk aggressive bank may be far lower than that of a risk averse foreign exchange dealer.

5.6.1 Risk Management Process : *(In revised material as on January 2012, para 5.6.1 is fully revised. It is old para 5.6.1. New para 5.6.1 which is replaced is given from page 7 to page 14)*

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.

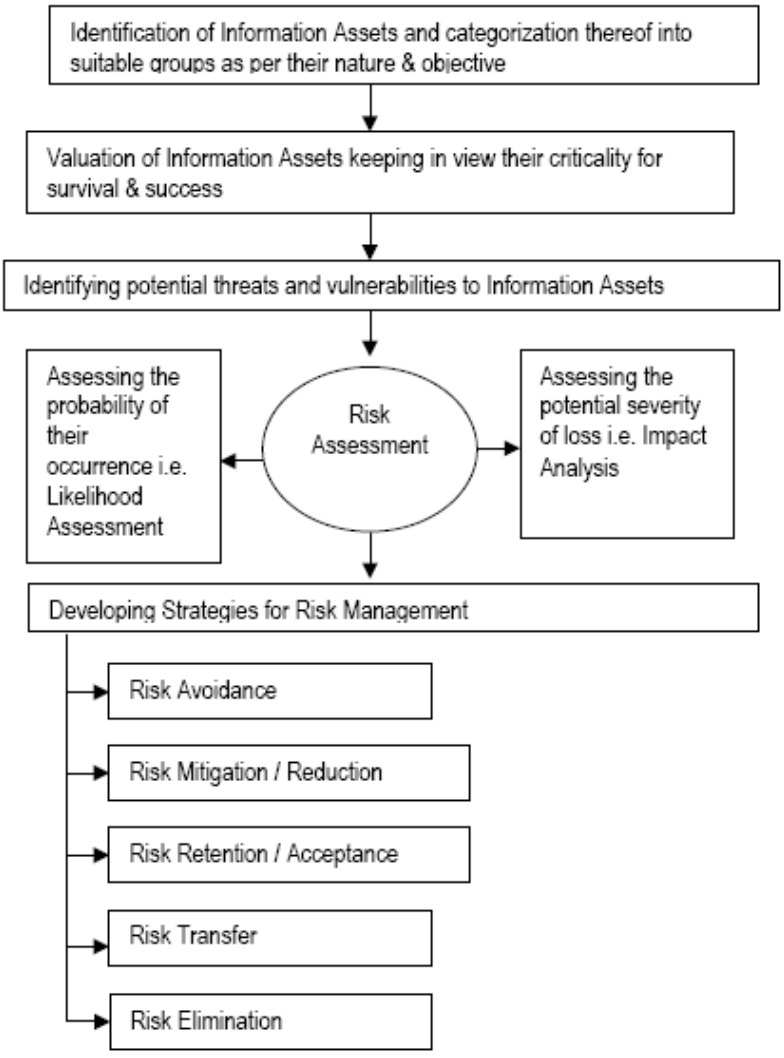
Page 7 to 14 contain Revised para 5.6.1

5.6.1 Risk Management Process:

The process of Information Risk Management typically involves the following steps:

- Identifying and classifying information assets,
- Valuation of the information and information assets as per their criticality
- Identifying threats and vulnerabilities to those assets,
- Measuring or assessing risk
- Developing strategies to manage risk

A pictorial representation of these steps is given as follows:



The detail of each step is given as follows:

Step 1: Identification of Information Assets

The first step in the information risk management process is to identify the information assets supporting critical business operations that need to be protected. The assets could fall under different groups which are:

- **Conceptual / Intangible Assets**
  - *Data and Information:* Business and related information contained in various storage devices such as hard disks or in transit may be subject to unauthorized disclosure, copying, theft, corruption or damage.
  - *Software:* It includes
    - Application software: application packages for accounting, payroll, sales etc. and
    - System software: operating system, utility programs, compiler, communication software, DBMS etc.

    Such programs may be susceptible to intentional or unintentional unauthorized modification by persons internal or external to the organization or by faulty technology processes.
- **Physical / Tangible Assets**
  - *People*: e.g. skilled users, analysts, programmers etc.
  - Hardware: e.g. mainframes, minicomputers, microcomputers, storage media, printers
  - Networking devices: e.g. communication lines, concentrators, hubs and switches etc.
  - Facilities: The computing and communication equipments such as servers could require special environment such as air-conditioned, dust free, humidity controlled facilities.
  - Documentation: e.g. printed forms, manuals, system and database documentation, IS policies & procedures

Step 2: Valuation of Information Assets

Data Valuation

(a) The information classification process focuses on business risk and data valuation. Not all data has the same value to an organization.

(b) Some data is more valuable to the people who are making strategic decisions because it aids them in making long-range or short-range business direction decisions.

(c) Some data, such as trade secrets, formulas, and new product information, are so valuable that its loss could create a significant problem for the enterprise in the marketplace by creating public embarrassment or by causing a lack of credibility.

Data Classification

(a) Information systems resources may require classifying or categorizing according to their sensitivity.

(b) This would depend upon the risks affecting such resources and impact resulting from exposure.

(c) Such classification is made for administrative convenience of implementing and maintaining access control systems and importantly optimizing the cost of security.

(d) Some information is more critical to a business than others such as production process information, formulas, strategic plans, research information.

(e) In the financial services industry, for example, information assets are very close to being financial assets. The loss of such information can jeopardize the existence of the business or create loss of goodwill and trust among stakeholders and loss of brand equity

(f) Compared to this, the organization may also have information, which is of less consequence in the event of their loss, such as a list of customers, details of employees' salaries, etc.

(g) Thus in order to ensure cost-effective controls, it is beneficial to classify the entire organizational information.

(h) This also enables fine tuning of access control mechanisms and avoids the cost of over-protecting and under protecting information.

The assets so identified and grouped may be categorized into different classes, which are:

- **Top secret:** This indicates the highest classification wherein the compromise of the confidentiality, integrity and availability can endanger the existence of the organization. Access to such information may be restricted to either a few named individuals in the organization or to a set of identified individuals.
- **Secret:** Information in this category is strategic to the survival of the organization. Unauthorized disclosure could cause severe damage to the organization and stakeholders.
- **Confidential:** Information in this category also needs high levels of protection but unauthorized disclosure may cause significant loss or damage. Such information is highly sensitive and should be well protected.
- **Sensitive:** Such information requires higher classification as compared to unclassified information. Disclosure may cause serious impact.
- **Unclassified:** Information that does not fall in any of the above categories finds place here. This also implies that the nature of the information is such that its unauthorized disclosure would not cause any adverse impact on the organization. Such information may also be made freely available to the public.

Another type of classification, popular in commercial organizations, can be: Public, Sensitive, Private and Confidential.

Step 3: Identifying the potential threats

Threat can be defined as an event that contributes to the interruption or destruction of any service, product or process. Common *classes of threats* are:

- Errors
- Malicious damage/attack
- Fraud
- Theft
- Equipment/software failure

Threats occur because of **vulnerabilities** associated with use of information resources. Vulnerabilities are characteristics of information resources that can be exploited by a threat to cause harm. *Examples of vulnerabilities* are:

- Lack of user knowledge
- Lack of security functionality
- Poor choice of passwords
- Untested technology
- Transmission over unprotected communication medium

Computer systems are vulnerable to threats that cause damage ranging from the loss of database integrity to the destruction of entire computer facilities. The sources of loss could be manifold from mere technological glitches to hackers, disgruntled or adventurous employees, data entry clerks, etc.

These threats could affect the **confidentiality, integrity or availability (CIA)** of system information or resources.

(a) **Confidentiality :** Confidentiality involves the protection of the organization's sensitive information from disclosure to unauthorized persons and processes.

Confidentiality threats in an IT environment include intentional as well as unintentional access to sensitive information. A few examples of exposures are given hereunder:

- *Improper application controls* in application software may lead to sensitive information being accessed by employees not having any need to access such information e.g. a payroll clerk may get accidental access to confidential records of management employees.
- *Unauthorized disclosure* arising from the access of confidential data on a system/network by inadvertent broadcast of data across the network, improper disposal of data etc.
- *Accidental access* to spool files used by printers may compromise sensitive information which may otherwise be protected by stringent access controls.

(b) **Integrity:** Integrity requires that the business information and related processes should not suffer any intentional or accidental unauthorized modification, which may result in serious consequences to the business.

Integrity violations in an IT environment are also common due to system errors which include: (i) corruption of files, (ii) power failures leading to unauthorized alteration in the values being transmitted or stored, (iii) erroneous program codes leading to alteration of values in data files etc.

Hence there is need to prevent the processes from performing any integrity violations.

A few examples of threats are given hereunder:

- A bank employee not having authority to credit files may tamper with the sanctioned amount of credit facilities by bypassing the application controls and making direct changes to data files or by gaining unauthorized access to the manager's login.
- Computer virus may cause corruption of data/program thereby causing loss of transactions or state of integrity of such transactions.
- Integrity violations in mission critical systems could cause irreparable damage to the business, threats to national security or loss of lives e.g. (i) corruption of tariff data files of Indian Railways, (ii) changes in values or parameter files of missile control systems, meteorological warning systems, (iii) corruption of program codes of autopilot systems used in flight control etc.

(c) **Availability:** Availability relates to whether the information and information technology processes are available to the authorized business users when required.

Availability therefore requires safeguarding the information systems and processes that are essential for supporting business processes, so as to ensure that the information systems and processes critical for conduct of business will be available to authorized users as and when required.

A few examples of exposures are given hereunder:

- The most common problems of availability occur due to improper capacity availability such as strangulated bandwidth, low computer resources as against the actual requirements such as processing capacity, storage capacity, number of terminals etc.
- Failure or improper functioning of power systems can lead to the computer systems being dysfunctional and hence not available for service e.g. power failure during banking hours.
- Intentional unavailability can also be created by hackers by launching denial-of-service attacks.

A clear idea of threats in the working environment will enable systems managers to implement the most cost-effective security measures.

Sources and Causes of Threats: Various threats can be grouped into environmental and man-made threats. Man made threats can again be categorized into internal and external threats.

Step 4: Information Risk Assessment :

Once the assets and corresponding potential threats have been identified, the systems are reviewed for weaknesses that can be exploited and the likelihood of those being exploited.

Information security professional or IS auditor here audits various systems and processes to find out vulnerabilities or weaknesses that can lead to a threat being materialized.

(a) **Vulnerability Assessment:**

- Vulnerability is a condition or weakness in (or the absence of) the safeguards, procedures, technical controls, physical controls or other controls that could be exploited by the threat.
- Sometimes the threat viewed in isolation may be misleading unless the vulnerabilities are taken into consideration.
- In most cases the threats attempt to exploit the vulnerabilities to cause loss or harm to the assets. For example, a hacker would look for loopholes in the architecture of the firewall to compromise the controls and gain unauthorized access to the networks.

(b) **Probability or Likelihood Assessment :**

- **Likelihood** is the estimation of the frequency, or the chance of a threat happening.
- A likelihood assessment considers the presence, tenacity and strength of threats, as well as, the effectiveness of safeguards.
- In general, historical information about many threats is weak, particularly with regard to human threats; hence the judgment and experience in this area is of relevance.
- Some threats affect data especially threats to physical assets such as fires, floods etc.
- Care needs to be taken in using any statistical threat data regarding the source of data; otherwise the analysis may be inaccurate or incomplete.
- In general, the greater the likelihood of a threat occurring, the greater is the risk. To some extent, the nature and value of information assets affect the likelihood of occurrence of a threat.
- If the asset is of high value, e.g. proprietary software packages, it is a prime target for piracy attempts.
- Thus, the identification and valuation of assets also assists with the identification of threats and their likelihood of occurrence.
- Periodically, the likelihood of occurrence of a threat needs to be reassessed due to changes occurring in the structure, direction, and environment of an organization.

(c) **Impact Analysis:**

- The threat that is successful in causing harm or loss to an asset results in an impact.
- Impact may be either in terms of direct loss of money or financial impact such as a hacker stealing a sensitive file containing all information about credit card customers that is used by the ATM access control system.
- Impact need not necessarily be in terms of direct impact of money; but can be, for example, disruption of operations leading to operational loss and delayed and back log processing etc.
- IT risks can also lead to significant losses in terms of damages (both monetary as well as to the reputation of the organization) such as a hacking attack leading to compromise of sensitive financial information of customers, which may be published by the hacker on the Internet resulting in both legal repercussions and loss of reputation.

Step 5: Developing Strategies for Information Risk Management

Once risks have been identified and assessed, appropriate corrections shall be made to the system, if required. Immediate action may not be taken to correct some identified vulnerabilities but the process will at least analyse these vulnerabilities, document and recognize them for risk management decisions.

Risk Management Strategies:

The strategies to manage the risk fall into one or more of these four major categories:

(a) **Risk Avoidance:** It means not doing an activity that involves risk. It involves losing out on the potential gain that accepting the risk might have provided. E.g. not using Internet / public network on a system connected to organisation's internal network, instead using a stand-alone PC for Internet usage.

(b) **Risk Mitigation / Reduction:** It involves implementing controls to protect IT infrastructure and to reduce the severity of the loss or the likelihood of the loss from occurring. E.g. using an effective anti-virus solution to protect against the risk of viruses and updating it on timely basis.

(c) **Risk Transfer:** It involves causing another party to accept the risk i.e. sharing risk with partners or insurance coverage.

(d) **Risk Retention / Acceptance:** It means formally acknowledging that the risk exists and monitoring it. In some cases it may not be possible to take immediate action to avoid/mitigate the risk.

All risks that are not identified or avoided or transferred are retained by default. These risks are called residual risks.

Risk management aims to identify, select and implement the controls that are necessary to reduce residual exposures to acceptable levels.

Risk Prioritization:

- The goals and mission of an organization should be considered in selecting any of these risk management strategies.
- It may not be practical to address all identified risks, so priority should be given to the risks that have the potential to cause significant mission impact or harm.
- In ideal information risk management, a prioritization process is followed whereby the risks with the greatest loss and the greatest probability of occurrence are handled first, and risks with lower probability of occurrence and lower loss are handled later.
- In practice the process can be very difficult, and balancing between risks with a high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

Understanding the Relationships Between IS Risks and Controls:

- Risks that threaten the IS cannot be altogether eliminated but, through appropriate decisions and actions can be mitigated.

  Threats to information system can materialize as an outcome of poor controls or absence of controls. Any threat to the system or its components could result in a loss to the company as a consequence of exploitation of the vulnerabilities.

  A control is a check or restraint on a system which is designed to enhance its security. Controls can act to

  - reduce a threat
  - reduce vulnerability to a threat
  - reduce impact of a threat
  - detect an impact
  - recover from an impact

- The objective of IS controls is to prevent the threats from exploiting the vulnerabilities of the assets or the safeguards.

  In the event the threats cannot be prevented, the controls should enable timely detection and trigger corrective action.

  In the event of failure of a control, threats could cause harm to the assets resulting in an actual impact.

- IS Auditor should be able to evaluate whether available controls are adequate and appropriate to mitigate the IS risks.

  In the case of deficiency in controls or existence of newer or uncontrolled risks, the IS auditor should report such weaknesses to the auditee management along with appropriate recommendations.

  Hence it is important for the IS auditor to understand the relationship between risks and controls. He should also be thorough with the process and procedure of reviewing and evaluating controls.

- The auditor should understand that the controls always have a *cost*, but also come with a *benefit*.

  The *cost* could be in terms of time or investment of money or sometimes even compromising with the performance of systems e.g. anti-virus software or intrusion detection systems consume the resources and might make the system slow.

  Benefits could be in terms of reduction of risk, or in terms of improving the effectiveness and efficiency of operations. In any organization, it is crucial to balance the cost vs. benefits of controls.

  The following rules apply in determining the use of new controls:

  - If control would reduce risk more than needed, then see whether a less expensive alternative exists.
  - If control would cost more than the risk reduction provided, then find something else.
  - If control does not reduce risk sufficiently, then look for more controls or a different control.
  - If control provides enough risk reduction and is cost-effective also, then use it.

.
.
.
.
.
.
.

End of Revised Para 5.6.1

Next Part is not Revised and is as per old Module

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 categorized into three primary functions–

1. Risk Identification,
2. Risk Assessment and
3. Risk Mitigation.

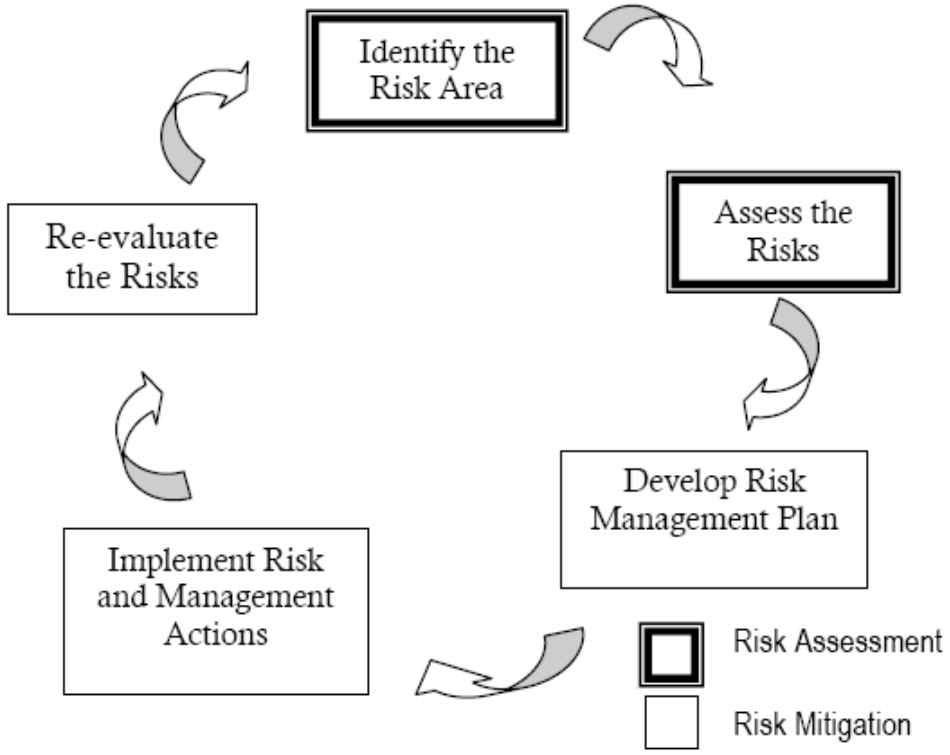


Fig. 5.6.1 : Risk management cycle

5.7 RISK IDENTIFICATION

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.

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:

1. What could go wrong?
2. How could we fail?
3. What must go right for us to succeed?
4. Where are we vulnerable?
5. What assets do we need to protect?
6. Do we have liquid assets or assets with alternative uses?

7. How could someone steal from the department?
8. How could someone disrupt our operations?
9. How do we know whether we are achieving our objectives?
10. On what information do we most rely?
11. On what do we spend the most money?
12. How do we bill and collect our revenue?
13. What decisions require the most judgment?
14. What activities are most complex?
15. What activities are regulated?
16. What is our greatest legal exposure?

It is important that risk identification be comprehensive, at the department level and at the activity or process level, for operations, financial reporting and compliance objectives. Both internal and external factors should be considered.

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.

In addition, the risk evaluation of the information technology interface would itself be a part of the audit report on information technology system.

The two primary questions to consider when evaluating the risk inherent in a business function are:

1. 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.
2. What is the cost if what can go wrong does go wrong? (**Exposure**)

Risk is evaluated by answering the above questions for various risk factors and assessing the probability of failure and the impact of exposure for each risk factor. Risk is the probability times the 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.

5.7.1 Techniques for Risk Evaluation:

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

1. Judgment and intuition
2. The Delphi approach
3. Scoring
4. Quantitative Techniques
5. Qualitative Techniques

1. **Judgement and intuition:**
   (a) In many situations the auditors have to use their **judgement and intuition** for risk assessment.
   (b) This mainly depends on the personal and professional experience of the auditors and their understanding of the system and its environment.
   (c) Together with it is required a systematic education and ongoing professional updating.
2. **Delphi Technique**
   (a) The **Delphi Technique** was first used by the Rand Corporation for obtaining a consensus opinion. Here a panel of experts is appointed.
   (b) 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.
   (c) 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.
   (d) Then a curve is drawn taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.
3. **Scoring approach**
   (a) In the **Scoring approach** the risks in the system and their respective exposures are listed.
   (b) Weights are then assigned to the risk and to the exposures depending on the severity, impact on occurrence, and costs involved.
   (c) The product of the risk weight with the exposure weight of every characteristic gives us the weighted score.
   (d) 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.
4. **Quantitative techniques**
   (a) involve the calculating an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs.
   (b) This helps the organisation to select cost effective solutions.
   (c) 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.
5. **Qualitative techniques**
   (a) are by far the most widely used approach to risk analysis.
   (b) Probability data is not required and only estimated potential loss is used.
   (c) Most qualitative risk analysis methodologies make use of a number of interrelated elements:
      (i) **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.
      (ii) **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).
      (iii) **Controls :** These are the countermeasures for vulnerabilities. There are four types:
         - *Deterrent controls* reduce the likelihood of a deliberate attack
         - *Preventative controls* protect vulnerabilities and make an attack unsuccessful or reduce its impact
         - *Corrective controls* reduce the effect of an attack

- *Detective controls* discover attacks and trigger preventative or corrective controls.

These elements can be illustrated by a simple relational model:

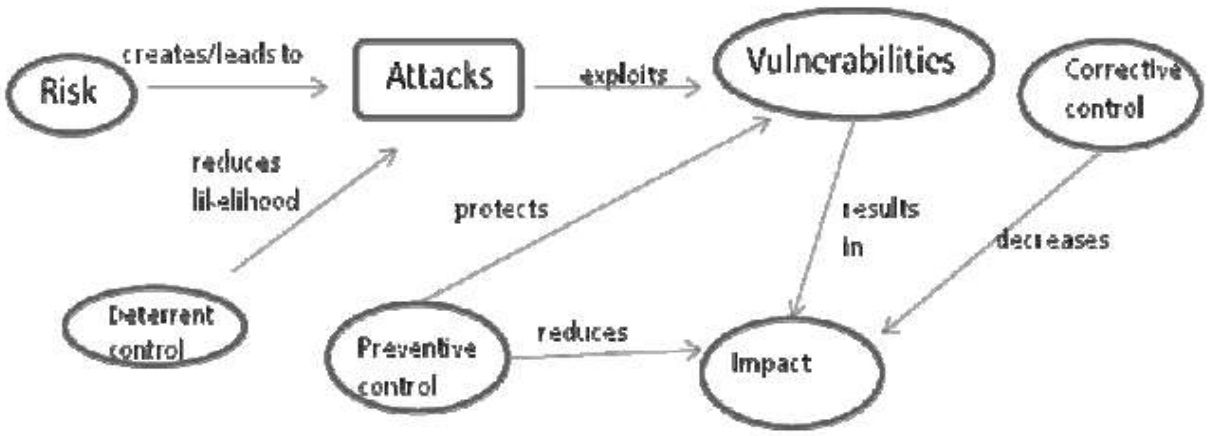


Fig. 5.7.1 : Risk evaluation

5.8 RISK RANKING

Ranking:

(a) The planning process should identify and measure the likelihood of all potential risks and the impact on the organisation if threat occurred.

(b) To do this, each department should be analysed separately.

(c) Although the main computer system may be the single greatest risk, it is not the only important concern.

(d) Even in the most automated organisations, some departments may not be computerised or automated at all. In fully automated departments, important records remain outside the system, such as legal files, computer data, software stored on diskettes, or supporting documentation for data entry.

(e) 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.

(f) All main office and/or computer centre functions must be relocated.

Assumptions

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:

(a) 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.

(b) 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 aet off tornados), no domino effect should be assumed.

(c) 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."

5.8.2 How to perform Risk Assessment :

(a) The risk assessment should be performed by facility. To measure the potential risks, a weighted point rating system can be used.

(b) Each level of probability can be assigned points as follows:

Probability	Points
High	10
Medium	5
Low	1

(c) 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).

(d) Based on this rating method, threats that pose the greatest risk (e.g., 15 points and above) can be identified.

5.7.1 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

(a) **Factor or casual analysis** can help relate 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 minimised.

(b) A causal understanding is essential to take appropriate action to control and manage risks because causality is a basis for both action and prediction.

(c) Knowing '*what causes what*' gives an ability to intervene in the environment and implement the necessary controls. Causation is different from correlation, or constant conjunction, in which two things are associated because they change in unison or are found together.

(d) Predictive models (such as loss models) often use correlation as a basis for prediction, but actions based on associations are tentative at best.

(e) Simple cause and effect relationships are known from experience, but more complex situations such as those buried in the processes of business operations may not be intuitively obvious from the information at hand. An Information System audit and control professional may be required to establish the cause.

(f) 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:

1. Self assessment.
2. Calculating reserves and capital requirements.
3. Creating culture supportive of risk mitigation.
4. Strengthening internal controls, including internal and external audit of systems, processes and controls, including IS audit and assurance).
5. 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).
6. Setting up independent operational risk management departments.

7. Establishing a disaster recovery plan and backup systems.
8. Insurance.
9. Outsourcing operations with strict service level agreements so operational risk is transferred.

5.9.1 Common risk mitigation techniques :

Mitigation and measurement techniques are applied according to the event's losses, and are measured and classified according to the loss type. Some of the common risk mitigation techniques are as under:

1. **Insurance :**
   (a) 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.
   (b) However while selecting such an insurance policy one has to look into the exclusion clause to assess the effective coverage of the policy.
   (c) Under the Advanced Management Approach under Basel II norms (AMA), a bank will be allowed to recognise the risk mitigating impact of insurance in the measures of operational risk used for regulatory minimum capital requirements. The recognition of insurance mitigation is limited to 20% of the total operational risk capital charge calculated under the AMA.
2. **Outsourcing :**
   (a) The organisation may transfer some of the functions to an outside agency and transfer some of the associated risks to the agency.
   (b) One must make careful assessment of whether such outsourcing is transferring the risk or is merely transferring the management process.
   (c) For example, outsourcing of telecommunication line viz. subscribing to a leased line does not transfer the risk. The organisation remains liable for failure to provide service because of a failed telecommunication line.
   (d) In the same example as above, where the organisation has outsourced supply and maintenance of a dedicated leased line communication channel with an agreement that states the minimum service level performance and a compensation clause in the event failure to provide the minimum service level results in to a loss. In this case, the organisation has successfully mitigated the risk.
3. **Service Level Agreements :**
   (a) 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.
   (b) 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. Thus a bank may state that services at ATM are subject to availability of service there and customers need to recognise that such availability cannot be presumed before claiming the service.
   (c) The delivery of service is conditional upon the system functionality. Whereas the service is guaranteed if the customer visits the bank premises within the banking hours.

It must be recognised that the organisation should not be so obsessed with mitigating the risk that it seeks to reduce the systematic risk - the risk of being in business.

The risk mitigation tools available should not eat so much into the economics of business that the organisation may find itself in a position where it is not earning adequate against the efforts and investments made.

5.10 RISK AND CONTROLS

1. 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.
2. In order to achieve goals and objectives, management needs to effectively balance risks and controls.
3. Therefore, control procedures need to be developed so that they decrease risk to a level where management can accept the exposure to that risk.
4. 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

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

5.11 RISK ANALYSIS AND ASSESSMENT FORM

Refer Study Material for Risk Analysis Form

Note: Mark all questions in Practise Manual, RTP, and Suggested answers in your regular study material from which you study so as to avoid referring those things again for what you have already covered. Refer those things only for what is not covered in your regular material and for presentation of answers.