

Risk Assessment Methodologies and Applications

Basic Concepts

1. **Risk:** A risk is the likelihood that an organization would face a vulnerability being exploited or a threat becoming harmful.
 - 1.1 **Threat:** 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.
 - 1.2 **Vulnerability:** This 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.
 - 1.3 **Exposure:** An exposure 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.
 - 1.4 **Likelihood:** Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event.
 - 1.5 **Attack:** This 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.
 - 1.6 **Residual Risk:** An organization'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. The risk can be minimized, but it can seldom be eliminated. Residual risk must be kept at a minimal, acceptable level.
2. **Threats to the Computerized Environment:** Major threats are: Power Loss, Communication Failure, Disgruntled employees, Errors, Malicious Code, Abuse of access privileges by employees, Natural disasters, Theft or destruction of computing resources, Downtime due to technology failure, Fire etc.
3. **Threats due to cyber crimes:** Major threats are: Embezzlement, Fraud, Theft of proprietary information, Denial of Service, Vandalism or sabotage, Computer Virus etc.

4. **Risk Assessment:** This 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. The areas to be focused upon are: Prioritization, Identifying critical applications, Assessing their impact on the organization, Determining recovery time frame, Assess Insurance Coverage, Identification of exposures and implications, Development of recovery plan.
 - 4.1 **Systematic Risks:** These 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.
 - 4.2 **Unsystematic Risks:** The risks 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. Thus by making additional investment one can mitigate these unsystematic risks.
5. **Techniques of Risk Evaluation:** Following are some of the techniques that are available to assess and evaluate risks: Judgment and intuition, The Delphi approach, Scoring, and Quantitative Techniques.
6. **Common Risk Mitigation Techniques:** Some of the common risk mitigation techniques are: Insurance, Outsourcing, and Service Level Agreements.

Question 1

Explain the following terms with reference to Information Systems:

- (i) Risk
- (ii) Threat
- (iii) Vulnerability
- (iv) Exposure
- (v) Attack
- (vi) Malicious Code

Answer

- (i) **Risk:** It is the likelihood that an organization 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

5.3 Information Systems Control and Audit

degree of protection applied. Some of the factors that cause gaps are widespread use of technology, Interconnectivity of systems and devolution of management and control etc.

- (ii) **Threat:** 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
- (iii) **Vulnerability:** 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.
- (iv) **Exposure:** 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.
- (v) **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.
- (vi) **Malicious Code:** It is a code such as viruses and worms which freely access the unprotected networks which may affect organizational and business networks that use these unprotected networks.

Question 2

Define the following terms:

- (i) *Likelihood*
- (ii) *Attack*
- (iii) *Residual Risk*

Answer

- (i) **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.
- (ii) **Attack:** 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.
- (iii) **Residual Risk:** Any risk still remaining after the counter measures are analyzed and

implemented is called Residual Risk. An organization'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. The risk can be minimized, but it can seldom be eliminated. 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 has been managed.

Question 3

"There always exist some Common threats to the computerized environment." Explain these threats.

Or

Discuss various threats to the computerized environment.

Answer

Any computerized environment is dependent on people. They are a critical links in making the entire enterprise computing happen and are responsible for the threats and attacks. The professionals such as analysts, programmers, data administrator, etc. are key links in ensuring that the IT infrastructure delivers to the user requirements and are target key persons who may leak the sensitive information of the enterprise. A few common threats to the computerized environment can be:

- (i) *Power Loss*: Power failure can cause disruption of entire computing equipments since computing equipments depends on power supply.
- (ii) *Communication failure*: Failure of communication lines result in inability to transfer data which is a back bone of the system. Such failures present a significant threat that will have a direct impact on operations. For example, organizations which use communication lines for e-banking, railway reservation –e-ticketing etc., failure of communication link presents a significant threat.
- (iii) *Disgruntled Employees*: Such employees presents a threat since, with access to sensitive information of the organization, they may cause intentional harm to the information processing facilities or sabotage operations.
- (iv) *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 organization network being compromised with virus attacks.
- (v) *Malicious Code*: Malicious code such as viruses and worms which freely access the unprotected networks may affect organizational and business networks that use these unprotected networks.
- (vi) *Abuse of access privileges by employees*: The security policy of the company

5.5 Information Systems Control and Audit

authorizes employees based on their job responsibilities to access and execute select functions in critical applications.

- (vii) *Natural disasters*: Natural disasters such as earthquakes, lighting, floods, tornado, tsunami, etc. can adversely affect the functioning of the IS operations due to damage to IS facilities.
- (viii) *Theft or destruction of computing resources*: Since the computing equipment forms the back-bone of information processing, any theft or destruction of the resource can result in compromising the competitive advantage of the organization.
- (ix) *Downtime due to technology failure*: IS facilities may become unavailable due to technical glitches or equipment failure. The period of downtime the facility is not available may vary in criticality depending on the nature of business and the critical business process that the technology supports.
- (x) *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.

Question 4

“Always, there exist some threats due to Cyber Crimes.” Explain these threats.

Or

Explain the threats due to Cyber crimes.

Answer

Any computerized environment is dependent on people. Though they play a critical role in success of an enterprise computing, it is a fact that threats always exist due to cyber crimes committed by people. The special skill sets of IT operational team, programmers; data administrator, etc. are key links in ensuring that the IT infrastructure delivers output as per user requirements. At the same time, 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. IT computing services are significantly dependant on various vendors and service providers for equipment supply and support, consumables, systems and program maintenance, air-conditioning, hot-site providers, utilities, etc. Following are some of the serious 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 internal 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.

- *Theft of proprietary information: It is illegal to obtain 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. Problems may erupt through internet connection or e-mail service that result 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.*
- *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: Viruses are hidden fragments of computer codes which propagates by inserting themselves into or modifying other programs.*
- *Other: Threat includes several other cases such as intrusion, 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.*

Question 5

What do you understand by "Risk Assessment"? Discuss the various areas that are to be explored to determine the risk.

Answer

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. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to priorities applications, identify exposures and develop recovery scenarios.

Various areas that are to be explored to determine the risk are briefly discussed below:

- (i) *Prioritization:* All applications are inventoried and critical ones identified. Each of the critical applications is reviewed to assess its impact on the organization, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.
- (ii) *Identifying critical applications:* It is necessary to identify critical applications of the currently running applications. 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.
- (iii) *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:

5.7 Information Systems Control and Audit

- Legal liabilities,
 - Interruptions of customer services.
 - Possible losses,
 - Likelihood of fraud and recovery procedures.
- (iv) *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.
- (v) *Assess Insurance coverage:* The information system insurance policy should be a multi-peril policy, designed to provide various types of coverage. It may cover the cost of hardware, software reconstruction, business interruption etc.
- (vi) *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.
- (vii) *Development of recovery plan:* The plan should be designed to provide for recovery from total destruction of a site.

Question 6

What do you understand by the term Risk Assessment? What areas need to be focused for risk assessment?

Answer

Risk Assessment: A risk assessment can provide an effective approach that will serve as the foundation for avoiding of disasters. Through risk analysis, it is possible to identify, assess and then mitigate the risk.

Risk Assessment is a critical step in disaster and business continuity planning. 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.

The areas to be focused upon are:

- (a) **Prioritization:** All applications are inventoried and critical ones identified. Each of the critical application is reviewed to assess its impact on the organization, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.
- (b) **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.

- (c) **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.
- (d) **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.
- (e) **Assess Insurance Coverage:** The information system insurance policy should be a multiperil policy, designed to provide various types of coverage. Depending on the individual organization and the extent of coverage required, suitable modifications may be made to the comprehensive list provided below:
- (i) **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.
 - (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, programmes 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.

5.9 Information Systems Control and Audit

- (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.

Question 7

State and explain four commonly used techniques to assess and evaluate risks.

Answer

Four most commonly used techniques to assess and evaluate risks are:

- *Judgment and intuition*
- *The Delphi Approach*
- *Scoring*
- *Quantitative Techniques*

A brief discussion on each of them is given as follows:

- (i) **Judgment and intuition:** In many situations, the auditors have to use their judgment 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, systematic education and ongoing professional updating is also required.
- (ii) **The Delphi Approach:** This technique is used for obtaining a consensus opinion. A panel of experts is engaged and each expert is asked to give his opinion in a written and independent method. They enlist the estimate of the cost benefits and the reasons why a particular system is to be chosen, the risks and exposures of the system. These estimates are then compiled together. The estimates falling within a pre-decided acceptable range are taken. The process may be repeated four times for revising estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graphs. The median is drawn and this is the consensus opinion.
- (iii) **The Scoring Approach:** In this approach, the risks in the system and their respective exposures are listed. Weights are then assigned to the risks and to the exposures depending on the severity, impact of occurrence and costs involved. The product of the risk weight with the exposure weight of every characteristic gives the weighted score. The sum of these weighted scores gives the risk and exposure score of the system. System risks and exposures are then ranked according to the scores.
- (iv) **Quantitative Techniques:** Quantitative techniques involve the calculating of an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs. This helps the organization to select cost effective solutions. It is the assessment of potential damage in the event of occurrence of unfavorable events,

keeping in mind how often such an event may occur.

Question 8

Explain the common risk mitigation techniques.

Answer

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:

- **Insurance:** *An organization 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. Under the Advanced Management Approach under Basel II norms, a bank will be allowed to recognize 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.*
- **Outsourcing:** *The organization 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. For example, 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 a failed telecommunication line. Consider the same example where the organization 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 organization has successfully mitigated the risk.*
- **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 organization 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 recognize that such availability cannot be presumed before claiming the service. 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 recognized that the organization 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 organization may find itself in a position where it is not earning adequate against the efforts and investments made.

Exercise

Question 1

An automobile spare parts production company has 10 distribution centers, each of which maintains their inventory status through the company's inventory application software on its Virtual Private Network (VPN). Managers across the distribution centers have identified different types of frauds/errors committed during data entry, transaction processing and fake user logins in the inventory system.

The manager of one of the distribution centre has asked you (IS Auditor) to prepare a report on "how the risk appraisal can be undertaken". Indicate the appropriate approach in this situation and give reasons for your answers.

Question 2

Differentiate between the Systematic and Unsystematic risks.

Question 3

Differentiate between the System Control Audit Review File (SCARF) and Continuous and Intermittent Simulation (CIS).

Question 4

An enterprise is in the process of leveraging Information and Communication Technology (ICT) for its business value chain process. As a member of ICT implementation team, prepare the risk assessment lists for the following issues:

- (a) Insurance Coverage, and*
- (b) Enterprise-wide Application Software Security.*

Question 5

Briefly explain the risk analysis and mitigation measures that a system audit and control professional should consider.