

RISK ASSESSMENT METHODOLOGIES AND APPLICATIONS

Question 1

Explain the following terms with reference to Information Systems:

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

(10 Marks) (Nov 2008)

Answer

- (a) (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 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.

Question 2

"There always exist some Common threats to the computerized environment." Explain these threats. (5 Marks) (Nov 2008)

or

What are common threats to the computerized environment other than natural disasters, fire and power failure? (5 Marks) (May 2010)

or

Explain the common threats to the computerized environment of an organization.

(8 Marks) (May 2011)

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 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 3

What do you understand by “Risk Assessment”? Discuss the various areas that are to be explored to determine the risk. (5 Marks) (Nov 2008)

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 prioritize 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:
 - 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 4

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

(5 Marks) (Jun 2009)

Or

Explain the threats due to Cyber crimes.

(5 Marks) (Nov 2009)

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

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

(5 Marks) (Jun 2009)

Answer

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

- Judgment and intuition
- The Delphi Approach

- Scoring
- Quantitative Techniques

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

- 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.
- 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.
- 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 score gives the risk and exposure score of the system. System risks and exposures are then ranked according to the scores.
- 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 6

Describe Risk Management Process.

(5 Marks) (Nov 2009)

Answer

Risks are classified as systematic and unsystematic.

- **Systematic risks** are unavoidable risks - these are constant across majority of technologies and applications. These risks can be reduced by designing management control process and does not involve technological solutions.
- **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.

Risk Management Process comprises of the following:

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

Question 7

What are the two primary questions to consider when evaluating the risk inherent in a business function in the context of the risk assessment methodologies? Give the purposes of risk evaluation. (5 Marks) (May 2010)

Answer

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

- (i) 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 has to focus on the available measures that can prevent such happening.
- (ii) What is the cost if 'what can go wrong' does go wrong? (*Exposure*)

Purposes of Risk Evaluation

The purpose of risk evaluation is to:

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

Question 8

"The information system insurance policy should be a multiperil policy, designed to provide various types of coverage." Discuss the comprehensive list of items considered for coverage.

(8 Marks) (Nov 2010)

Answer

The information system insurance policy should cover the following items:

- (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 centers, 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.

Question 9

Write Short notes on Delphi technique for risk evaluation.

(4 Marks) (May 2011)

Answer**Delphi Technique for Risk Evaluation**

The Delphi Technique was first used by the Rand Corporation for obtaining a consensus opinion. Here, a panel of experts is appointed. Each expert gives his/her 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.