

5. Risk Assessment Methodologies and applications

Introduction

In the current interconnected world, business is highly dependent on the information systems. Computer networks have transferred our lives into a fast and comfortable one but at the same time, it has also posed various threats to the existing information systems due to open accessibility.

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 increase due to an interruption'. There are various analytical procedures that are used to determine various risks, threats and exposures faced by an organization. The purpose of risk analysis involves threat identification, risk assessment and risk mitigation.

Related Terms

(useful for short notes in exam)

- **Asset:** asset can be defined as something of value of the organization; e.g. information in electronic or physical form, software systems, employees. Irrespective the nature of the assets themselves, they all have one or more of the following characteristics:
 1. They are recognized to be a value to the organization
 2. They are not easily replaceable without costs, skill, time, resources or a combination.
 3. They form a part of the organization's corporate identity, without which, the organization may be threatened.
 4. Their data classification would normally be proprietary, hilly confidential o even top secret.

- **Vulnerability:** vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system or other components that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to ham or exploit the system, for example vulnerability could be a poor access control method allowing dishonest employees to exploit the system to adjust their own records.

Simply, vulnerability can be refereed as the weakness of the software, which can be exploited by the attacks. Vulnerabilities can organize from flaws on the software's design defects in its implementation, or problems in its operation. Some experts also define 'vulnerability' as opening doors for attacks. Normally vulnerability is a state in a computing system, which must have at least one connection, out of the following:

1. Allows an attacker to execute commands
 2. Allow an attacker to access data that is contrary to the specified access restrictions for that data
 3. Allows an attacker to pose as another entity
 4. Allows an attacker to conduct a denial or service
- **Threat:** any entity, circumstances, or event with the potential to harm the system or components through its unauthorized access. Destruction, modification, and/or denial o service called threat.

Threat has capability to attack on a system with intent to harm. It is often to start threat modeling with a list known threats and vulnerabilities found in similar systems. Every system has a data, which is considered as a fuel to drive a system, data us nothing but assets. Assets and threats are closely correlated. A threat cannot exist without a target asset. Threats are typically prevented by applying some sort of protection to asset.

- **Exposure:** an exposures is the event of loss the organization has to face when a risk materiality. 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 and loss of resources.

- **Likelihood:** likelihood of the threat occurring is the estimation of the probability that the threats will succeed in achieving an undesirable event. The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.
- **Attack:** an attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability. In software terms, an attack is a malicious internal fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system.
- **Risk:** risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset, and risk analysis is defined as the process of identifying security risks and determining their magnitude and impact on an organization. Risk assessment include the following:
 1. Identification of threats and vulnerabilities in the system
 2. Potential impact or magnitude harm that a loss of CIA (Confidentiality, integrity and availability) would have an enterprise operations or enterprise assets, should an identified vulnerability be exploited by a threat; and
 3. The identification and analysis of security controls for the information system

Information system generates direct and indirect risks. These risks lead o a gap between the need to protect systems and the degree of protection applied. The gap is cause by

1. Widespread use of technology;
 2. Interconnectivity of systems;
 3. Elimination of distance, time and space as constrains;
 4. Unevenness of technological changes;
 5. Devolution of management and control;
 6. Attractiveness of conduction unconventional electronic attacks against operations; and
 7. External factors such as legislative, legal and regulatory requirements or technological developments
- **Countermeasure:** an action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as countermeasure. For example well known threat "spoofing the user identity", has two countermeasures:
 1. Strong authentication protocols to validate users; and
 2. Password should not be stored in configuration files instead somas secure mechanism should be used.

Any risk still remaining after the counter measures are analyzed and implemented is called residual risk. An organization's management of risk should be these two areas: acceptance of residual risk and selection of safeguards.

Threats to computerized environment

1. Power failure: can cause disruption of entire computing equipments
2. Communication Failure: its result in inability to transfer data, which primarily travel over communication lines.
3. Disgruntles Employees: presents a threats as he is known is having the access to sensitive information of the organization.

4. **Errors and Omissions:** are important threats to data and system integrity. These errors are caused not only by data entry clerks, processing hundreds of transaction per day, but also by all types of users, who create and edit data.

Data entry clerks, system operators and programmers frequently make errors that contribute directly or indirectly security problems. In some case, the error is the threat, such as a data entry error or programming error that crashes a system.

5. **Malicious Code:** refers to viruses, worms, Trojan horses, logic bombs and other such software, which freely accesses the unprotected networks may affect organizational and business networks that use these unprotected networks.
6. **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 application.
7. **Natural disasters:** Natural disasters such as earthquake, lighting, floods, tornado, tsunami etc. can adversely affect the functioning of the IS operation due to damage to information system facilities.
8. **Theft or destruction of computing services:** since the computing equipments form the backbone of information processing, any theft or destruction of the resource can result in compromising the competitive advantages of the organization.
9. **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 may vary in critically depending on the nature of business and the critical business process that the technology supports.
10. **Fire etc. :** Fire due to electrical short circuit or due to riots, war or such other reasons, can cause irreversible damage to the IS infrastructure.

Threat due to cyber crimes

1. **Embezzlement:** it is unlawful misappropriation of money or other thing of value, by the person to whom it was entrusted, for his own use or purpose
2. **Fraud:** it occurs in 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.
3. **Theft or proprietary information:** it is the illegal obtaining of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrights material, data, files, lists and personal or financial information, usually by electronic copying.
4. **Denial of Services (Dos):** an action or series of actions that prevents access to a software system by its intended/authorized users or cause the delay of its time-critical operations or prevents any part of the system from sanctioning is termed as 'Dos'. There can disruption or degradation of services 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.
5. **Validation of Sabotage:** it is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and problems.
6. **Computer virus:** a computer virus is a program that can copy itself and infect a computer without the permission or knowledge of user.
7. **Others:** threats includes several other cases, such as intrusions, breaches and compromises of the respondent's computer met works regardless of whether damage or loss were sustains as a result.

Risk Assessment

Risk assessment is a step in the risk management procedures. Risk assessment is the determination of quantitative or qualitative value of the risk related to a concrete situation and a

recognized threat. Risk assessment can provide an effective approach that will serve as the foundation for avoiding of disasters. Risk assessment is a disaster and business continuity planning.

Focus areas of risk Assessment

1. 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.
2. Identifying Critical application: first critical application is identified from among current running application and further analysis is done to determine specific jobs in the application which may be more critical. Even though the critical value would be determined base on the present value, future changes should not be ignored.
3. Assessing their impact on the organization: business continuity planning should not concentrate only on business disruption but should also take into account other organizational functions which may be affected. The areas to be considered include:
 - a. Legal liabilities
 - b. Interruptions or customer services
 - c. Possible losses, and
 - d. Likelihood of fraud and recover procedures
4. Deterring recovery time-frame: critical recovery time period is the times in which business processing must be resumed before the organization incurs sever losses. This critical time depends upon the nature of operations. It is essential to involve the end users in identification of critical functions and critical recovery time period.
5. Assess insurance coverage: the IS insurance policy should be a multi-peril policy. Designed to provide various types of coverage's. Depending upon on the individual organization and the extent of coverage required, suitable modification may be made to the comprehensive list provided below:
 - Hardware facilities
 - Software reconstruction
 - Extra expenses
 - Business interruption
 - Valuable paper and records
 - Errors and omissions
 - Fidelity coverage
 - Media transportation
6. Identification of exposures and implication: 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 if disaster.
7. Development of recovery plan: the plan should be designed to provide for recovery from total destruction of site.
- 8.

Risk Management

Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and deciding what countermeasures, if any, to take in reducing risk to an acceptable level (i.e. residual risk), based on the volume of the information resources to the organization.

Risk may be classified In two category

1. Systematic risk: are unavailable risks-these are constant across majority of technologies and application. For example, the probability of power outage is not dependent on the industry but is dependent on external factors. Systematic risk can be reduced by designing management control process and does not involve technological solution.

2. Unsystematic risk: 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. Thus by making additional investment one can mitigate these unsystematic risks.

Risk Management process

This process typically involves the following steps.

1. Identifying of information assets: the assets could fall under two groups
 - a. Conceptual/Intangible assets
 - b. Physical/Tangible assets
2. Valuation of information assets: the information classification process focuses on business risk and data valuation. Not all data has the same value to an organization. Some data is more valuable to the people who are making strategic decision because it aids them in making long-range or short-range business direction decisions. The assets so identified and grouped may be categorized into different classes, which are
 - a. Top Secret
 - b. Secret
 - c. Confidential
 - d. Sensitive
 - e. Unclassified
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, and
 - Equipment/Software failure

Threats occur because of vulnerabilities associated with use of information resources. Examples of vulnerabilities are:

 - Lack of user knowledge,
 - Lack of security functionality,
 - Poor choice of passwords,
 - Untested technology, and
 - Transmission over unprotected communication medium.
4. Information risk assessment: once, the assets and corresponding potential threats have been identified, the system reviewed for weakness 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 weakness that can lead to a threat being materialized

 - a. Vulnerabilities assessment
 - b. Probability of likelihood assessment
 - c. Impact analysis
5. Developing strategies for information risk management

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

 - a. Risk avoidance
 - b. Risk mitigation/Reduction
 - c. Risk transfer
 - d. Risk retention/Acceptance

Understanding of Relationship between IS risks and Controls

A control is a check or resistant on a system, which is designed to enhance its security. Control can act to:

- a. Reduce a threat,
- b. Reduce vulnerability to a threat,
- c. Reduce impact of a threat,
- d. Detect an impact, and
- e. Recover from an impact.

The objective of IS controls is to prevent the threats from exploiting the vulnerabilities of the assets of the assets or the safeguards. In the event the threats cannot be prevented, the control should enable timely detection and trigger corrective action.

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 weakness to the auditee management along with a appropriate recommendations.

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. Benefits could be in terms of reduction of risks, or in terms of improving the effectiveness and efficiency of operations. The following rules apply in determine the use of new controls.

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

Risk Management Cycle

It is a process, involving the following steps.

- i. Risk identification
- ii. Risk assessment, and
- iii. Risk mitigation

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 factions with highest risk.

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

- What is the probability that thing can go wrong?
- What is the cost if what can go wrong does go wrong?

The purpose of a risk evolution is to:

- Identifying the probabilities of failures and threats,
- Calculate the exposures, i.e. damage or loss to assets, and
- Make control recommendations keeping the cost-benefit analysis in mind.

Technique for risk evaluation

1. Judgment and intuition: This mainly depends upon the personal and professional experience of the auditors and their understanding of the system and its environment. Together with it is required a systematic education and ongoing professional updating.

2. The Delphi Approach: the Delphi approach is defined as: 'a method for structuring a group communication process so that the process is effective in allowing a group of individuals as a whole to deal with a complex problem.

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 independent manner. They enlist the estimate of the cost, benefits and the reason 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.

3. Scoring: in the scoring approach, in the system and their respective exposures are listed. Weights are then assigned to the risk and to the exposures depending on the severity, impact on occurrence, and costs involved. The sum of the weight with the exposure weight of every characteristic gives us the weighted score. The sum of these weighted score gives us the risk and exposures score of the system. System risk and exposures is then ranked according to the scores obtained.
4. Quantitative technique: these techniques involve the calculating an annual loss exposures value based on the probability of the event and the exposures in terms of estimated costs.
5. Qualitative Approach: these techniques are most widely used approaches to risk analysis. Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements.
 - a. Threats
 - b. Vulnerabilities
 - c. Controls

Considerations in analyzing risk

1. Investigating the frequency of particular types of disaster.
2. Determining the degree of predictability of the disaster.
3. Analyzing speed of onset of the disaster.
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 organization 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 stakeholders' confidence
 - g. loss of goodwill
 - h. loss of income
 - i. loss of competitive edge
 - j. Legal actions.
10. Estimating potentials losses for each business function based on the financial and service impact and the length of time the organization can operate without this business function.
11. Determining the cost of contingency planning.

Risk mitigation

The ultimate purpose of risk identification and analysis is to prepare for risk mitigation. A systematic reduction in the extent of exposure to a risk and/or the likelihood of its occurrence is termed as risk mitigation. Typically, in case of risk mitigation, there is a particular threshold that is acceptable below which the risk is attempted to be mitigated. Factor or casual analysis can help to relate characteristic of an event to the probability and severity of the operational loss. This will enable the organization to decide whether or no to invest in information system or people so events of the effects of events can be minimized.

Common Risk mitigation Techniques

1. Insurance; however selecting such insurance policy one has to look into the exclusion clause to assess coverage of the policy. Under the Advanced management Approach (AMA) under base II norms, a bank will be allowed to recognize the risk mitigation 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: the organization may transfer some of the functions to an outside agency and transfer some of the associated risk to the agency. One must make careful assessment of whether such outsourcing is transferring the risk or is merely transferring the management process.
3. Service Level agreements (SLAs): 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.