Chapter 5 - Risk Assessment methodologies And Application

ISCA

By Sumit ANAND

Risk Assessment methodologies And Applications

1. Risk Definitions
   - Risk; Threat; Exposures; Vulnerability
2. Threats to Computerized Environment
3. Threats due to cyber crimes
4. Risk Management
5. Risk Identification
6. Risk Assessment
7. Risk Ranking
8. Risk Mitigation
9. Risk and Controls

Risk Analysis and Assessment Forms

1.0 Risks: Threats, Exposure and Vulnerabilities

- Risk is a probabilistic terms it is likelihood that an organizations. For example organizations are exposed to risks of fire and theft etc so fire and theft are risks to organization which may cause harms to organization working etc.

- These risks primarily have emerged due to technological changes of information systems these changes always create gap between protection applied and protection required due to:

1. Widespread use of new technologies
2. Extensive use of network applications
3. Eliminations of distance, time and space constraints i.e. use of distributed or any time anywhere processing systems
4. Frequent technological changes

2.0 Some Important Terms

- **Threat:** An action or event which may cause harm to organization in terms of business
- continuity problems, disclosure of confidential information, data destruction &denial of
- information etc.
- **Vulnerabilities:** The weakness in the safeguard or security of the system that exposes the IS to various threats.
- **Exposure:** The extent of loss organization may face in case of risk. It is impact of
- occurrence of risk in immediate & longer term.
- **Likelihood:** The probability of occurrence of any risk.

2.0 Continue… Some Important Terms

- **Attack:** Actions which may compromise the integrity & confidentiality & other desired
- features of an IS. The type of attack & its degree of success determine the results or
- consequences of attack.
- **Residual Risk:** Any risk that still remains after all the security majors to prevent the risks
- are analyzed & implemented. Here, organization Management needs to consider two areas:
- Acceptance level of residual risk
- Selection of safeguards to be implemented to reduce overall risks to reach level of acceptance
- As long as residual risks can be minimized & kept at acceptable level, the risks are considered to be managed.

3.0 Threats to Computerized Environment

- Power loss
- Communication network failure
- Disgruntled employees
- Errors
- Malicious codes (programs)
- Abuse of access privilege by employees
- Natural disasters
- Theft & destruction of computing resources
- Downtime due to technology failure

4.0 Threats Due to Cyber Crimes

- **Cyber Crime** is the general nomenclature for "electronic offences" due to increasing use of computer network & internet & frauds thereof.

- Examples of cyber crimes:
- embezzlement
- unauthorized use of ATM/ DC/ CC
- theft of proprietary information
- denial of service
- vandalism or sabotage
- computer virus

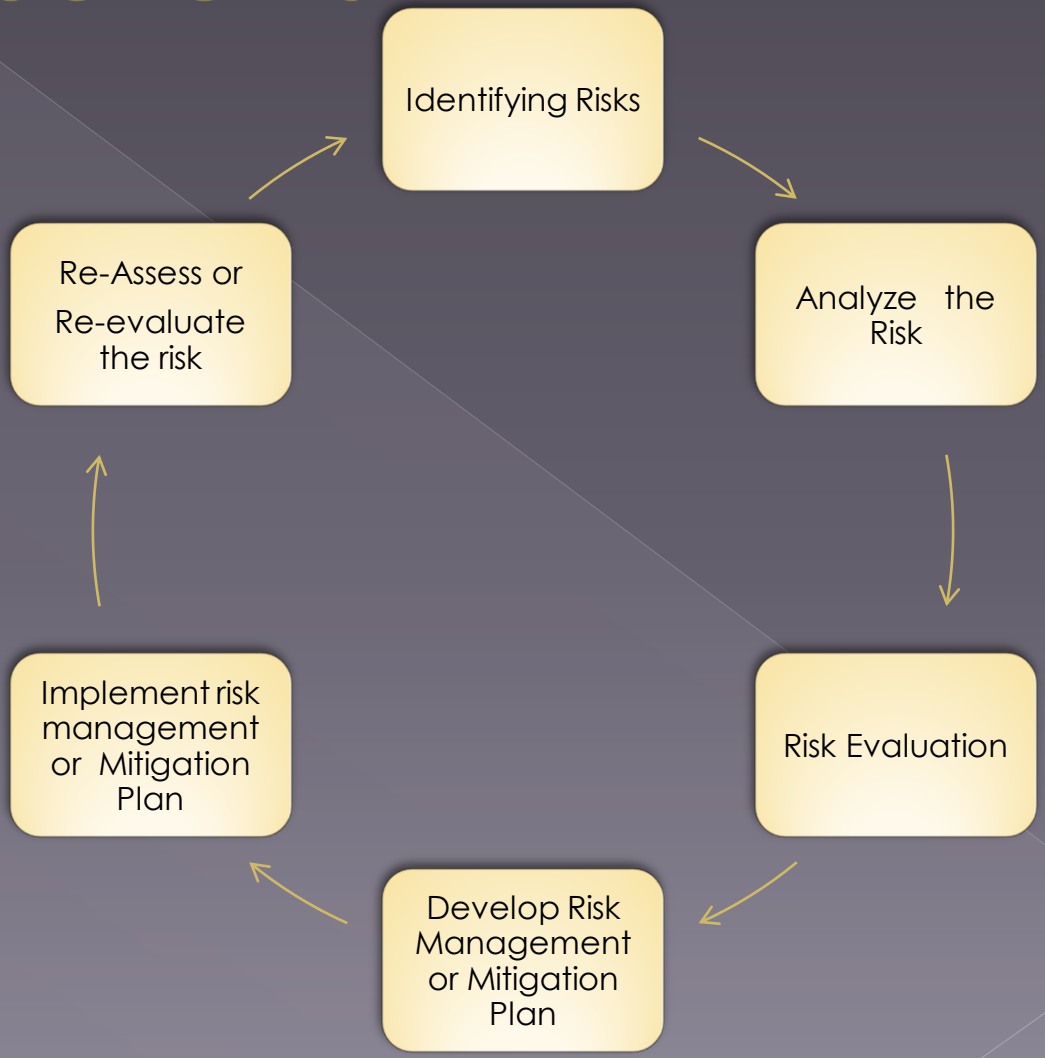
5.0 RISK MANAGEMENT

- The systematic application of management policies, procedures & practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating, monitoring & communicating risk.

Risk Management Steps:

- **Risk Identification**
- **Risk Assessment:** process of analyzing & measuring risk to quantify risks to system
- **Risk Evaluation**
- **Risk Mitigation Development:** involving implementation of measures to reduce or
- eliminate some or all risks
- **Risk Mitigation Implementation**
- **Re-assessment/ Re-evaluation of risks**

5.1 Risk Management Cycle Components



5.2 CLASSIFICATION OF RISKS

- **Systematic Risk:** normally avoidable risks; same for all organizations; primarily from
- external factors; organizations have little control over them
- **Unsystematic Risk:** specific & unavoidable risks; from specific application or technologies
-

6.0 RISK IDENTIFICATION

- Purpose is to identify various risks inherent to performing business functions, especially
- w.r.t. use of IT
- Risk identification should be comprehensive
- Risk identification should be for operations, financial objectives & compliance
- Questions to be asked:
- What assets to be protected
- What could go wrong with assets
- How could we fail to deliver
- What are various threats to A & L
- What info. to be relied upon
- What is greatest legal, financial & operational exposure

7.0 ASSESSMENT & EVALUATION TECHNIQUES

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

- What is probability that a particular thing(threat) can go wrong? (**Probability**)
- What is the cost, if particular thing(threat) can go wrong? (**Exposure**)

- Risk is the probability times the exposure.

RISK = PROBALILITY OF DISRUPTION X POSSIBILITY OF EXPOSURE

- Purpose of risk analysis & evaluation:
- Identify probability of failures & threats
- Calculate the exposure i.e. the damage or loss to assets.

7.1 Risk Assessment procedure

1. Establish the context

Preserve or increase MH's Export Sales earnings

2. Identifying the risks

Identification of risk factors

3. Analyze the Risks

Quantitative and Qualitative Analysis of identified risks

4. Evaluate the Risks

Compare the Risks against criteria to accept the risk or treat the risk

5. Treat the Risks

Identify and assess the options, and prepare treatment plan

7.2 Techniques used for Risk Analysis and Evaluation

1. Judgment and Intuition

   Auditor uses his judgment mainly depends upon his professional experience.

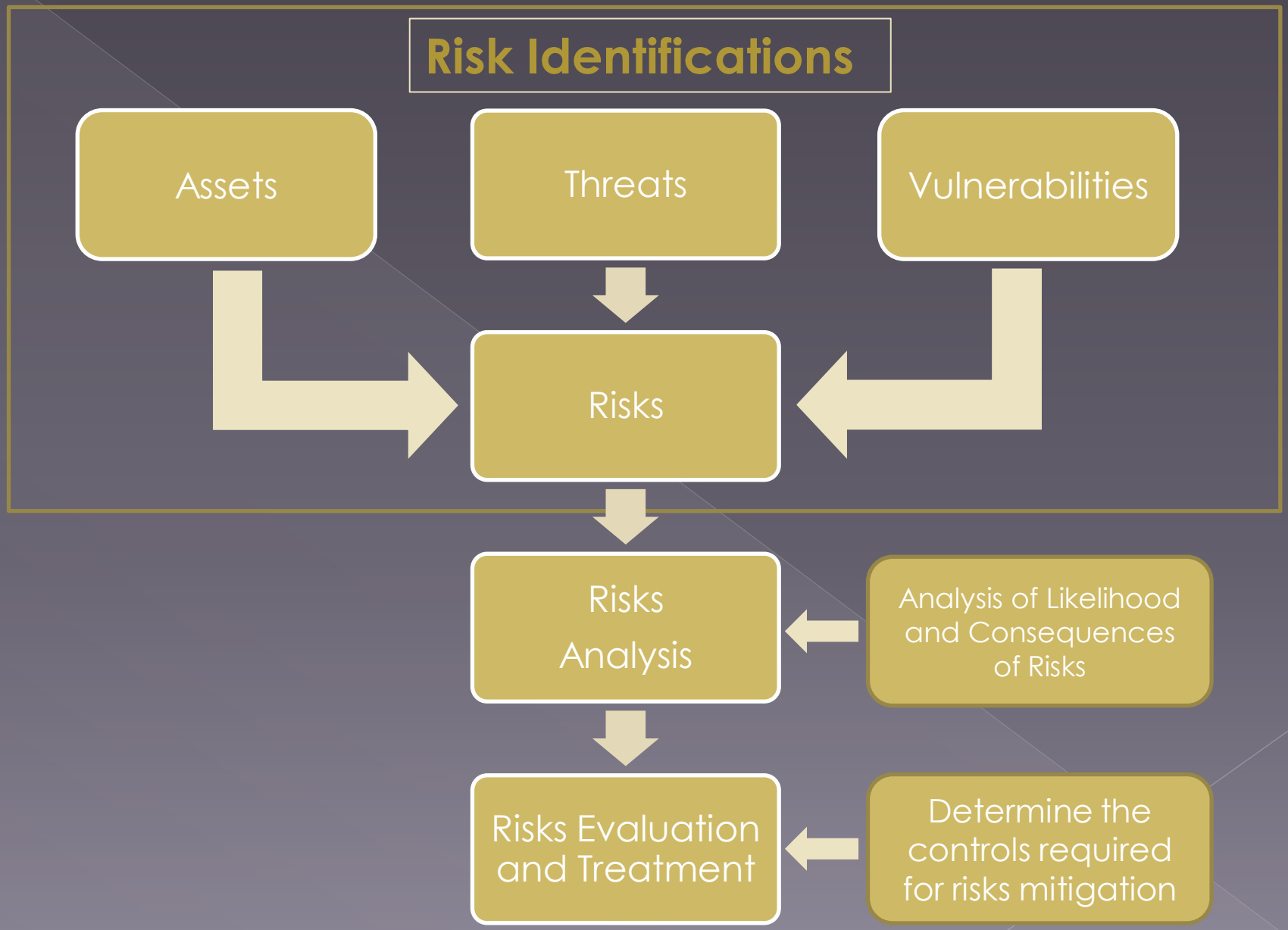
2. The Delphi Approach

3. Scoring Approach
4. Quantitative Approach
5. Qualitative Techniques

8.0 RISK ASSESSMENT

- Process used to identify risk factors, & then analyze & evaluate the identified risk factors to develop an appropriate risk mitigation plan
- Provides an effective approach that serves as foundation to avoid losses
- Helps to identify, assess & mitigate risks
- Includes development of clear summary of current situation & systematic plan to identify,
- assess & mitigate risks
- In general, includes the following for protection of an IS & its applications:
  - Prioritization
  - Identifying critical components & applications
  - Assessing their impact on organization
  - Identification of exposures & implications
  - Determination of recovery-time period
  - Assessment of Insurance coverage
  - Development of recovery plan

8.1 Risk Assessment Framework



9.0 RISK RANKING

- Technique to measure impact of potential risks
- Requires that each component & application be analyzed separately before ranking
- Two quantitative parameters used for ranking:
  - Probability of occurrence
  - Possible impact or exposure of threats

- Considering & analyzing risk impacts & probability of occurrence includes:
  - Investigating the frequencies of particular types of disaster
  - Determining the degree of predictability of disaster
  - Analyzing speed of occurring impact of disaster
  - Determining amount of forewarning associated with disaster
  - Estimating situation of disaster
  - Considering impact of disasters if vital records are destroyed/ not destroyed
  - Identifying consequences of disaster
  - Estimating potential loss
  - Determining cost of contingency planning

10.0 RISK MITIGATION

- Means avoiding risks
- Should be based on probability of occurrence of risk & severity of risk in terms of losses
- Some risk mitigation measures are:
  - Creating supportive environment
  - Strengthening internal controls
  - Establishing reserve funds
  - Setting up of operational risk limits
  - Setting up independent operational risk management departments
  - Establishing disaster recovery plan
- Common risk mitigation techniques:
  - Insurance
  - Outsourcing
  - Service Level Agreements

11.0 RISK & CONTROLS

Excessive Risk leads to:

- Loss of assets
- Poor business decisions
- Non-compliance
- Increased regulations
- Increased frauds

Excessive Control leads to:

- Increased bureaucracy
- Reduced productivity
- Increased complexity
- Increased processing cycle-time
- Increase of activities having no value