E. G. S. Pillay Engineering College, Nagapattinam
Computer Science and Engineering

Elective II **IT 2042 INFORMATION SECURITY** **VIII Sem CSE**

QUESTION BANK - UNIT-III

1) What is risk management?

Risk management is the process of identifying **vulnerabilities** in an organization's information systems and taking carefully reasoned steps to assure

a. **Confidentiality**
b. **Integrity**
c. **Availability**

of all the components in the organization's information systems

2) Explain the roles to be played by the communities of interest to manage the risks an organization encounters?

- It is the responsibility of each community of interest to manage risks; each community has a role to play:
  - **Information Security** - best understands the threats and attacks that introduce risk into the organization
  - **Management and Users** – play a part in the early detection and response process - they also insure sufficient resources are allocated
  - **Information Technology** – must assist in building secure systems and operating them safely

Accountability for Risk Management

- All three communities must also:
  - Evaluate the risk controls
  - Determine which control options are cost effective
  - Assist in acquiring or installing needed controls
  - Ensure that the controls remain effective

Risk Management Process

- Management reviews asset inventory
- The threats and vulnerabilities that have been identified as dangerous to the asset inventory must be reviewed and verified as complete and current
- The potential controls and mitigation strategies should be reviewed for completeness
- The cost effectiveness of each control should be reviewed as well, and the decisions about deployment of controls revisited
- Further, managers of all levels are accountable on a regular schedule for ensuring the ongoing effectiveness of every control deployed

3) What is the process of Risk Identification?

Risk Identification

- A risk management strategy calls on us to "know ourselves" by identifying, classifying, and prioritizing the organization's information assets

- These assets are the targets of various threats and threat agents and our goal is to protect them from these threats
- Next comes threat identification:
  - Assess the circumstances and setting of each information asset
  - Identify the vulnerabilities and begin exploring the controls that might be used to manage the risks

4) Explain asset identification and valuation.

Asset Identification and Valuation

- This iterative process begins with the identification of assets, including all of the elements of an organization's system: people, procedures, data and information, software, hardware, and networking elements
- Then, we classify and categorize the assets adding details as we dig deeper into the analysis

TABLE 4-1 Categorizing the Components of an Information System

Traditional system components	SecSDLC and risk management system components	
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

5) Explain in detail the process of asset identification for different categories.

People, Procedures, and Data Asset Identification

- *Unlike the tangible hardware and software elements already described, the human resources, documentation, and data information assets are not as readily discovered and documented*
- *These assets should be identified, described, and evaluated by people using knowledge, experience, and judgment*
- *As these elements are identified, they should also be recorded into some reliable data handling process*

Asset Information for People

- Position name/number/ID – try to avoid names and stick to identifying positions, roles, or functions
- Supervisor

- Security clearance level
- Special skills

Hardware, Software, and Network Asset Identification

- What attributes of each of these information assets should be tracked?
- When deciding which information assets to track, consider including these asset attributes:
  - Name
  - IP address
  - MAC address
  - Element type
  - Serial number
  - Manufacturer name
  - Manufacturer's model number or part number
  - Software version, update revision, or FCO number
  - Physical location
  - Logical location
  - Controlling entity

Asset Information for Procedures

- For Procedures:
  - Description
  - Intended purpose
  - What elements is it tied to
  - Where is it stored for reference
  - Where is it stored for update purposes

Asset Information for Data

- For Data:
  - Classification
  - Owner/creator/manager
  - Size of data structure
  - Data structure used – sequential, relational
  - Online or offline
  - Where located
  - Backup procedures employed

6) How information assets are classified?

Information Asset Classification

- Many organizations already have a classification scheme
- Examples of these kinds of classifications are:
  - confidential data
  - internal data
  - public data
- Informal organizations may have to organize themselves to create a useable data classification model
- The other side of the data classification scheme is the personnel security clearance structure

7) Explain the process of Information asset valuation.

Information Asset Valuation

- Each asset is categorized
- Questions to assist in developing the criteria to be used for asset valuation:
  - Which information asset is the most critical to the success of the organization?
  - Which information asset generates the **most revenue**?
  - Which information asset generates the **most profitability**?
  - Which information asset would be the **most expensive to replace**?
  - Which information asset would be the **most expensive to protect**?
  - Which information asset would be the most embarrassing or **cause the greatest liability if revealed?**

System Name: SLS E-Commerce
Date Evaluated: February 2003
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1 —Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2—Supplier orders (Outbound)	Confidential	High
EDI Document Set 2—Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading:
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

FIGURE 4-3 Example Worksheet for the Asset Identification of Information Systems

Information Asset Valuation

- Create a weighting for each category based on the answers to the previous questions

Which factor is the most important to the organization?

- Once each question has been weighted, calculating the importance of each asset is straightforward
- List the assets in order of importance using a weighted factor analysis worksheet

TABLE 4-2 Example of a Weighted Factor Analysis Worksheet

Information asset	Criteria 1: impact to revenue	Criteria 2: impact to profitability	Criteria 3: public image impact	Weighted score
Criterion Weight (1-100) Must total 100	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Notes: EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

8) Discuss briefly data classification and management.

Data Classification and Management

- A variety of classification schemes are used by corporate and military organizations
- Information owners are responsible for classifying the information assets for which they are responsible
- Information owners must review information classifications periodically
- The military uses a five-level classification scheme but most organizations do not need the detailed level of classification used by the military or federal agencies

Management of Classified Data

- Includes the storage, distribution, portability, and destruction of classified information
  - Must be clearly marked as such
  - When stored, it must be unavailable to unauthorized individuals
  - When carried should be inconspicuous, as in a locked briefcase or portfolio
- Clean desk policies require all information to be stored in its appropriate storage container at the end of each day
- Proper care should be taken to destroy any unneeded copies
- Dumpster diving can prove embarrassing to the organization

9) What are security clearances?

Security Clearances

- The other side of the data classification scheme is the personnel security clearance structure
- Each user of data in the organization is assigned a single level of authorization indicating the level of classification

- Before an individual is allowed access to a specific set of data, he or she must meet the need-to-know requirement
- This extra level of protection ensures that the confidentiality of information is properly maintained

10) Explain the process of threat identification?

Threat Identification

- Each of the threats identified so far has the potential to attack any of the assets protected
- This will quickly become more complex and overwhelm the ability to plan
- To make this part of the process manageable, each step in the threat identification and vulnerability identification process is managed separately, and then coordinated at the end of the process

Identify and Prioritize Threats

- Each threat must be further examined to assess its potential to impact organization - this is referred to as a threat assessment
- To frame the discussion of threat assessment, address each threat with a few questions:
  - Which threats present a danger to this organization's assets in the given environment?
  - Which threats represent the most danger to the organization's information?
  - How much would it cost to recover from a successful attack?
  - Which of these threats would require the greatest expenditure to prevent?

11) What are the different threats faced by an information system in an Organization?

TABLE 4-3 Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial of service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

©2003 ACM, Inc., Included here by permission.

12) Explain the process of vulnerability identification and assessment for different threats faced by an information security system.

Vulnerability Identification

- We now face the challenge of reviewing each information asset for each threat it faces and creating a list of the vulnerabilities that remain viable risks to the organization
- Vulnerabilities are specific avenues that threat agents can exploit to attack an information asset

- Examine how each of the threats that are possible or likely could be perpetrated and list the organization's assets and their vulnerabilities
- The process works best when groups of people with diverse backgrounds within the organization work iteratively in a series of brainstorming sessions
- At the end of the process, an information asset / vulnerability list has been developed
    - this list is the starting point for the next step, risk assessment

TABLE 4-4 Vulnerability assessment of a hypothetical DMZ router

Threat	Possible vulnerabilities
Deliberate software attacks	▪ Internet protocol is vulnerable to denial of service ▪ Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented
Act of human error or failure	▪ Employees or contractors may cause outage if configuration errors are made
Technical software failures or errors	▪ Vendor-supplied routing software could fail and cause an outage
Technical hardware failures or errors	▪ Hardware can fail and cause an outage ▪ Power system failures are always possible
Quality of service deviations from service providers	▪ Unless suitable electrical power conditioning is provided, failure is probable over time
Deliberate acts of espionage or trespass	▪ This information asset has little intrinsic value, but other assets protected by this device could be attacked if it compromised
Deliberate theft	▪ This information asset has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of sabotage or vandalism	▪ Internet protocol is vulnerable to denial of service ▪ This devise may be subject to defacement or cache poisoning
Technological obsolescence	▪ If this asset is not reviewed and periodically updated, it may fall too far behind its vendor support model to be kept in service
Forces of nature	▪ All information assets in the organization are subject to forces of nature, unless suitable controls are provided
Compromises to intellectual property	▪ This information asset has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of information extortion	▪ This information asset has little intrinsic value, but other assets protected by this device could be attacked if it is compromised

13) Explain the process of Risk assessment

Introduction to Risk Assessment

- The process you develop for risk identification should include designating what function the reports will serve, who is responsible for preparing the reports, and who reviews them
  - We do know that the ranked vulnerability risk worksheet is the initial working document for the next step in the risk management process: assessing and controlling risk

TABLE 4-6 Risk Identification and Assessment Deliverables

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns ranked value of risk rating for each uncontrolled asset-vulnerability pair

Risk Assessment

- We can determine the relative risk for each of the vulnerabilities through a process called risk assessment
- Risk assessment assigns a risk rating or score to each specific information asset, useful in gauging the relative risk introduced by each vulnerable information asset and making comparative ratings later in the risk control process
- **Risk Identification Estimate Factors**
  - Likelihood
  - Value of Information Assets
  - Percent of Risk Mitigated
  - Uncertainty

14) Explain with an example of Risk determination.

Risk Determination

For the purpose of relative risk assessment:

risk =

likelihood of vulnerability occurrence

times

value (or impact)

minus

percentage risk already controlled

Plus

an element of uncertainty

Risk Determination: Example

- Information Asset A has an value score of 50 and has one vulnerability:

- Vulnerability 1 has a likelihood of 1.0 with no current controls and you estimate that assumptions and data are 90 % accurate

- Information Asset B has an value score of 100 and has two vulnerabilities:
  - Vulnerability 2 has a likelihood of 0.5 with current control that addresses 50% of its risk
  - Vulnerability 3 has a likelihood of 0.1 with no current controls.
  - You can estimate assumptions and data are 80% accurate

Asset A: vulnerability rated as 55 = (50 * 1.0) – 0% + 10%

Asset B: vulnerability rated as 35 = (100 * 0.5) – 50% + 20%

Asset C: vulnerability rated as 12 = (100 * 0.1) – 0% + 20%

15) What is residual risk?

- For each threat and its associated vulnerabilities that have any residual risk, create a preliminary list of control ideas
- Residual risk is the risk that remains to the information asset even after the existing control has been applied

16) What is access control? Explain different types.

- One particular application of controls is in the area of access controls
- Access controls are those controls that specifically address admission of a user into a trusted area of the organization
- There are a number of approaches to controlling access
- Access controls can be
  - discretionary
  - mandatory
  - nondiscretionary

Types of Access Controls

- Discretionary Access Controls (DAC) are implemented at the discretion or option of the data user
- Mandatory Access Controls (MACs) are structured and coordinated with a data classification scheme, and are required
- Nondiscretionary Controls are those determined by a central authority in the organization and can be based on that individual's role (Role-Based Controls) or a specified set of duties or tasks the individual is assigned (Task-Based Controls) or can be based on specified lists maintained on subjects or objects

Lattice-based Control

- Another type of nondiscretionary access is lattice-based control, where a lattice structure (or matrix) is created containing subjects and objects, and the boundaries associated with each pair is contained
- This specifies the level of access each subject has to each object
- In a lattice-based control the column of attributes associated with a particular object are referred to as an access control list or ACL

- The row of attributes associated with a particular subject (such as a user) is referred to as a capabilities table

17) What is the goal of documenting results of the risk assessment?

- The goal of this process has been to identify the information assets of the organization that have specific vulnerabilities and create a list of them, ranked for focus on those most needing protection first
- In preparing this list we have collected and preserved factual information about the assets, the threats they face, and the vulnerabilities they experience
- We should also have collected some information about the controls that are already in place

18) **What are risk control strategies?**

- When risks from information security threats are creating a **competitive disadvantage**
  - the information technology and information security communities of interest **take control of the risks**
- **Four basic strategies** are used to control the risks that result from vulnerabilities:
  - Apply safeguards **(avoidance)**
  - Transfer the risk (**transference**)
  - Reduce the impact (**mitigation**)
  - Inform themselves of all of the consequences and accept the risk without control or mitigation (**acceptance**)

19) Explain in detail different risk control strategies?

Risk Control Strategies: Avoidance

- **Avoidance** attempts to prevent the exploitation of the vulnerability
- This is the preferred approach, as it seeks to avoid risk in its entirety rather than dealing with it after it has been realized
- Accomplished through countering threats
  - removing vulnerabilities in assets
  - limiting access to assets
  - adding protective safeguards
- Three areas of control:
  - Policy
  - Training and education
  - Technology

Transference

- **Transference** is the control approach that attempts to shift the risk to other assets, other processes, or other organizations
  - If an organization does not already have quality security management and administration experience, it should hire individuals or firms that provide such expertise

- This allows the organization to transfer the risk associated with the management of these complex systems to another organization with established experience in dealing with those risks

Mitigation

- **Mitigation** attempts to reduce the impact of exploitation through planning and preparation
- Three types of plans:
  - **disaster recovery planning (DRP)**
    - The most common of the mitigation procedures is the disaster recovery plan or DRP
  - **business continuity planning (BCP)**
    - Longer term issues are handled in the business continuity plan or BCP
  - **incident response planning (IRP)**
    - The actions to take while the incident is in progress are defined in the incident response plan or IRP

Acceptance

- **Acceptance** of risk is doing nothing to close a vulnerability and to accept the outcome of its exploitation
- Acceptance is valid only when:
  - Determined the level of risk
  - Assessed the probability of attack
  - Estimated the potential damage
  - Performed a thorough cost benefit analysis
  - Evaluated controls using each appropriate feasibility
  - Decided that the particular function, service, information, or asset did not justify the cost of protection
- Risk appetite describes the degree to which an organization is willing to accept risk as a trade-off to the expense of applying controls

20) Write short notes on

a) Incidence Response Plan b)Disaster Recovery Plan c)Business continuity plan

a) Incidence Response Plan

The actions an organization can perhaps should take while the incident is in progress are documented in what is known as Incident Response Plan(IRP)
IRP provides answers to questions victims might pose in the midst of the incident ,such as “What do I do now?”.
Answers to the following type of questions will be provided in IRP:

a. What should the administrator should do first?
b. Whom should they contact?
c. What should they document?

For example ,in the event of serious virus or worm outbreak,the IRP may be used to asses the likelihood of imminent damage and to inform key decision makers in the various communities of interest.

b) Disaster Recovery Plan

The most common mitigation procedure is Disaster Recovery Plan(DRP). The DRP includes the entire spectrum of activities used to recover from the incident. DRP can include strategies to limit losses before and after the disaster. These strategies are fully deployed once the disaster has stopped.

DRP usually include all preparations for the recovery process,strategies to limit losses during the disaster,and detailed steps to follow when the smoke clears,the dust settles,or the floodwaters recede.

c) Business Continuity Plan

The BCP is the most strategic and long term of the three plans. It encompasses the continuation of business activities if a catastrophic event occurs,such as the loss of an entire database,building or entire operations center. The BCP includes the planning the steps necessary to to ensure the continuation of the organization when the scope or scale of a disaster exceeds the ability of the DRP to restore operations. This can include preparation steps for activation of secondary data centers,hot sites,or business recovery sites.

21) Explain briefly the plans adopted for mitigation of risks.

TABLE 5.1 Summaries of Mitigation Plans

Plan	Description	Example	When deployed	Time frame
Incident response plan (IRP)	Actions an organization takes during incidents (attacks)	■ List of steps to be taken during disaster ■ Intelligence gathering ■ Information analysis	As incident or disaster unfolds	Immediate and real-time reaction
Disaster recovery plan (DRP)	Preparations for recovery should a disaster occur; strategies to limit losses before and during disaster; step-by-step instructions to regain normalcy	■ Procedures for the recovery of lost data ■ Procedures for the reestablishment of lost services ■ Shut-down procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business recovery plan (BCP)	Steps to ensure continuation of the overall business when the scale of a disaster requires relocation	■ Preparation steps for activation of secondary data centers ■ Establishment of a hot site in a remote location	Immediately after it is determined that the disaster affects the continued operations of the organization	Long-term recovery

22) Explain briefly how a risk control strategy can be selected?

Risk control involves selecting one of the four risk control strategies for each vulnerability. The following flowchart can be used as a guide for deciding how to proceed :

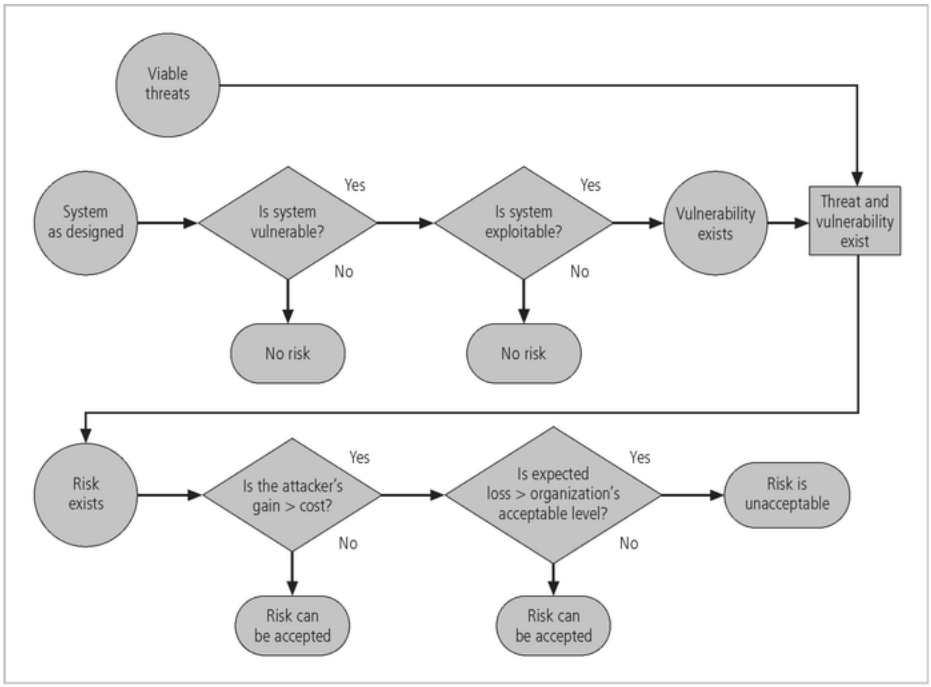

FIGURE 5-2 Risk Handling Decision Points[7]

23) Explain how the risk controls are effectively maintained in an organization?

Once a control strategy has been implemented,it should be monitored and measures on an ongoing basis to determine the effectiveness of the security controls and the accuracy of the estimate of the residual risk. The following flowchart shoes how this cyclical process is continuously used to ensure that risks are controlled.

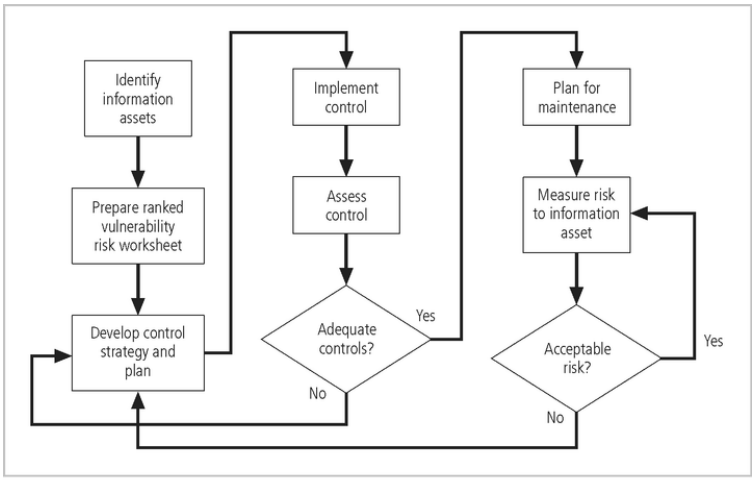

FIGURE 5-3 Risk Control Cycle[8]

24) What are different categories of controls? Explain briefly each.

Categories of controls

- **Controlling risk through avoidance, mitigation, or transference may be accomplished by implementing controls or safeguards**
- **One approach to selecting controls is by category:**
  - **Control Function**
  - **Architectural Layer**
  - **Strategy Layer**
  - **Information Security Principles**

Control Function

- Controls or safeguards designed to defend the vulnerability are either preventive or detective
- **Preventive controls** stop attempts to **exploit vulnerability** by implementing enforcement of an organizational policy or a security principle, such as **authentication** or **confidentiality**
- **Detective controls** warn of violations of security principles, organizational policies, or attempts to exploit vulnerabilities
- Detective controls use techniques such as audit trails, intrusion detection, or configuration monitoring

Architectural Layer

- Some controls apply to one or more layers of an organization's technical architecture
- Among the architectural layer designators in common use are:
  - organizational policy
  - external networks
  - extranets (or demilitarized zones)
  - Intranets (WAN and LAN)
  - network devices that interface network zones (switches, routers, firewalls, and hubs)
  - systems (computers for mainframe, server or desktop use)
  - applications

Information Security Principles

- Controls operate within one or more of the commonly accepted information security principles:
  - Confidentiality
  - Integrity
  - Availability
  - Authentication
  - Authorization
  - Accountability
  - Privacy