5) Explain the process of risk assessment and documenting the result of risk assessment. (MAY/JUNE 2014) Discuss the risk assessment in detail. (APRIL/MAY 2015)

Risk Assessment

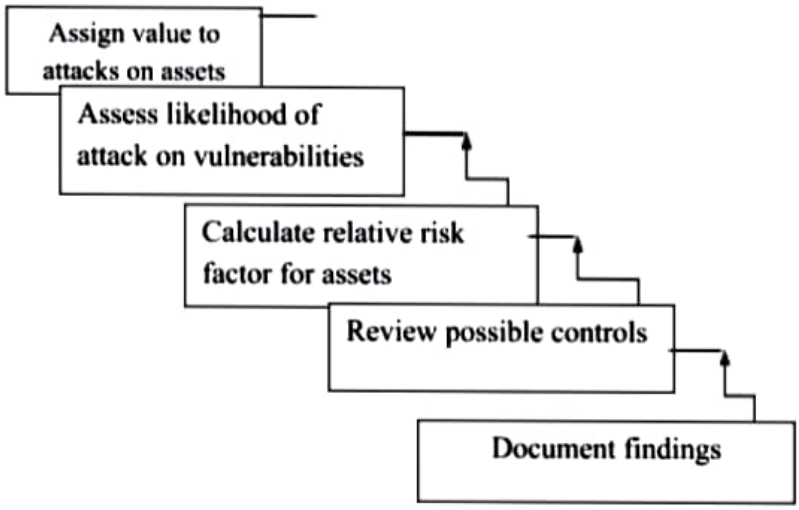
It assigns a risk rating or score to each Information asset. It is useful in gauging the relative risk to each vulnerable asset. Risk is the likelihood of the occurrence of a vulnerability multiplied by the value of the information asset minus the percentage of risk mitigated by current controls plus the uncertainty of current knowledge of the vulnerability.

Major stages of risk assessment

Valuation of Information assets

It assigns weighted scores for the value to the organization of each information asset. National Institute of Standards & Technology (NIST) gives some standards. To be effective, the values must be assigned by asking the following questions.

- Which threats present a danger to an 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 the threats would require the greatest expenditure to prevent?



Likelihood

It is the probability of specific vulnerability within an organization will be successfully attacked. NIST gives some standards.

- 0.1 = Low
- 1.0 = High

Eg: Number of network attacks can be forecast based on how many network address the organization has assigned.

Risk Determination

Risk = Likelihood of vulnerability occurrence) X (Value of information Asset) __ (% of risk mitigated by current controls) + uncertainty of current knowledge of the vulnerability.

- For the purpose of relative risk assessment, risk equals:
  - Likelihood of vulnerability occurrence TIMES value or impact
  - MINUS percentage risk already controlled
  - PLUS an element of uncertainty

Eg: Information Asset A has a value score of 50 & has one vulnerability: Vulnerability 1 has a likelihood of 1.0 with no current controls, estimate that assumptions and data are 90% accurate.

Solution:

Risk = [(1.0) x 50] – 0% + 10%

$= (50 \times 1.0) - ((50 \times 1.0) \times 0.0) + ((50 \times 1.0) \times 0.1)$

$= 50 - 0 + 5$

$= 55$

Identify Possible Controls (For Residual Risk)

The residual risk is the risk that remains to the information asset even after the existing control has been applied. The three general categories of controls are as follows:

1. Policies
2. Programs
3. Technologies

1. Policies
   - General Security Policy
   - Program Security Policy
   - Issue Specific Policy
   - Systems Specific Policy
2. Programs
   - Education
   - Training
   - Awareness
3. Security Technologies
   - Technical Implementation Policies

Access Controls

It specially addresses admission of a user into a trusted area of the organization.Eg: Computer rooms, power Rooms. It maintains the combination of policies, programs and technologies

Types of Access controls

Mandatory Access Controls (MACs)

Give users and data owner's limited control over access to information resources.

Nondiscretionary Controls

It is managed by a central authority in the organization; can be based on individual's role (role-based controls) or a specified set of assigned tasks (task-based controls)

Discretionary Access Controls (DAC)

It is implemented at discretion or option of the data user

Lattice-based Access Control

The variation of MAC shows that the users are assigned matrix of authorizations for particular areas of access.

Documenting the Results of Risk Assessment

By the end of the Risk Assessment process, you probably have a collection of long lists of information assets with data about each of them. The goal of this process is to identify the information assets that have specific vulnerabilities and list them, ranked according to those most needing protection. It should also have collected some information about the controls that are already in place. The final summarized document is the ranked vulnerability risk worksheet, a sample of which is shown in the following table.

Asset	Asset Impact or Relative value	Vulnerability	Vulnerability Likelihood	Risk Rating Factor
Customer Service Request via e-mail(inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer order via SSL -(inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL -(inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer Service Request via e-mail(inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer Service Request via e-mail(inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer order via SSL -(inbound)	100	Lost orders due to Web server denial-of-service attack	0.025	2.5
Customer order via SSL -(inbound)SSL-Secure Sockets Layer	100	Lost orders due to Web server software failure	0.01	1

c) Explain in detail about CBA and benchmarking with its metrics based measures