Information Security Fundamentals

Module Number: 03

Module Name: Risk Management

Version Code:IS1_Updated
Released Date:
25-Jan-2019

AIM:

To equip students with the knowledge of Information Risk Management.

Objectives

The objectives of this module are to understand:

- Risk management and its role in the SecSDLC.
- How risk is identified?
- Risk based on the likelihood of occurrence and impact on an organisation.
- The fundamental aspects of documenting risk identification and assessment.
- Risk management, risk identification, and risk control.
- How risk is identified, assessed and controlled?

Outcomes

At the end of this module, students are expected to:

- Explain the concept of information risk
- Describe the process of Identifying and Accessing Risk
- Explain the importance of documenting risk
- Summaries incident specific responses.
- Explain the various risk mitigation strategy options

Content

1. Definition of risk management
2. Risk identification, and risk control
3. Identifying and Accessing Risk, Assessing risk based on probability of occurrence and likely impact
4. Fundamental aspects of documenting risk via the process of risk assessment
5. Various risk mitigation strategy options

Introduction

- **Risk :** The is an object, person or other entity that represent a danger, harm or loss to an asset.
- **Risk Management :** Is the process of identifying, assessing and evaluating the level of risk faced by the organisation, specifically the threats to the information stored and used by organisation for achieving business objectives, and then deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organisation.

Introduction (Cont…)

- Risk management: process of identifying and controlling risks faced by an organisation.
  - Risk identification: process of examining an organisation's current information technology security situation.
  - Risk control: applying controls to reduce risks to an organisation's data and information systems.

An Overview of Risk Management

- Know yourself: identify, examine, and understand the information and systems currently in place.
- Know the enemy: identify, examine, and understand threats facing the organisation.
- Assets are targets of various threats and threat agents.
- Risk management involves identifying organisation's assets and identifying threats/vulnerabilities.
- Risk identification begins with identifying organisation's assets and assessing their value.

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.

Risk Life Cycle

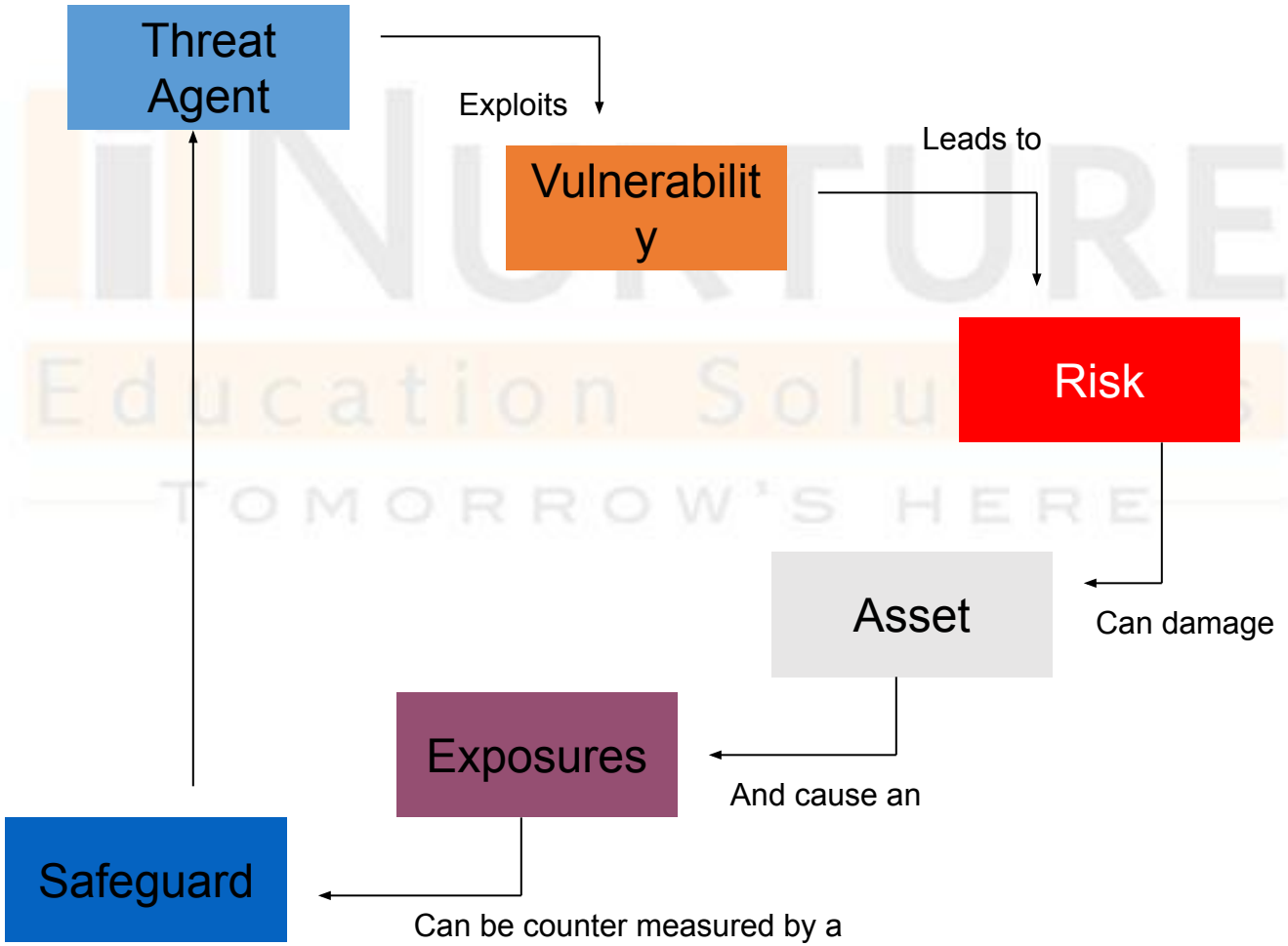
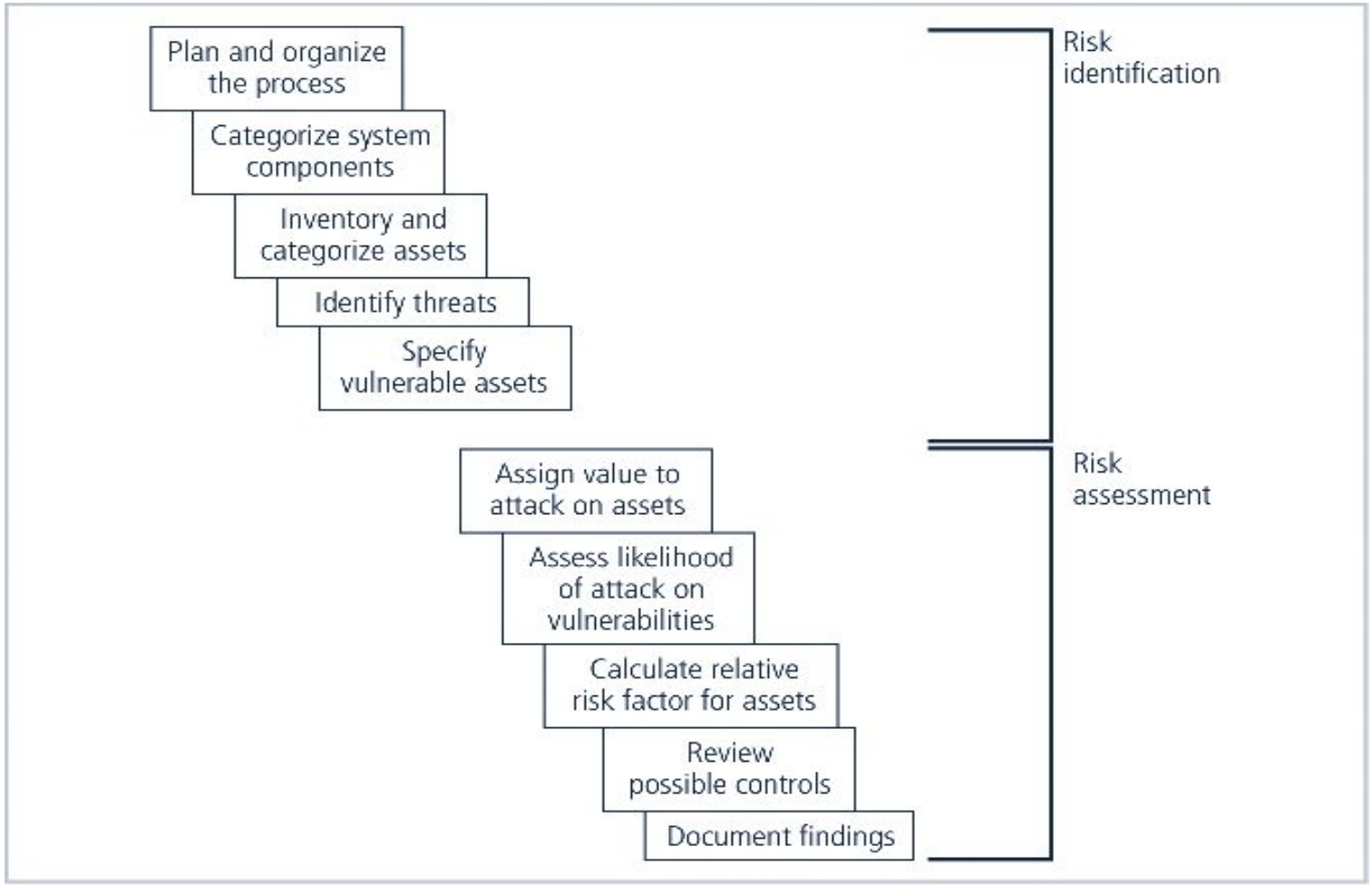


Figure: Risk Life Cycle

Component of Risk Management



Risk Identification

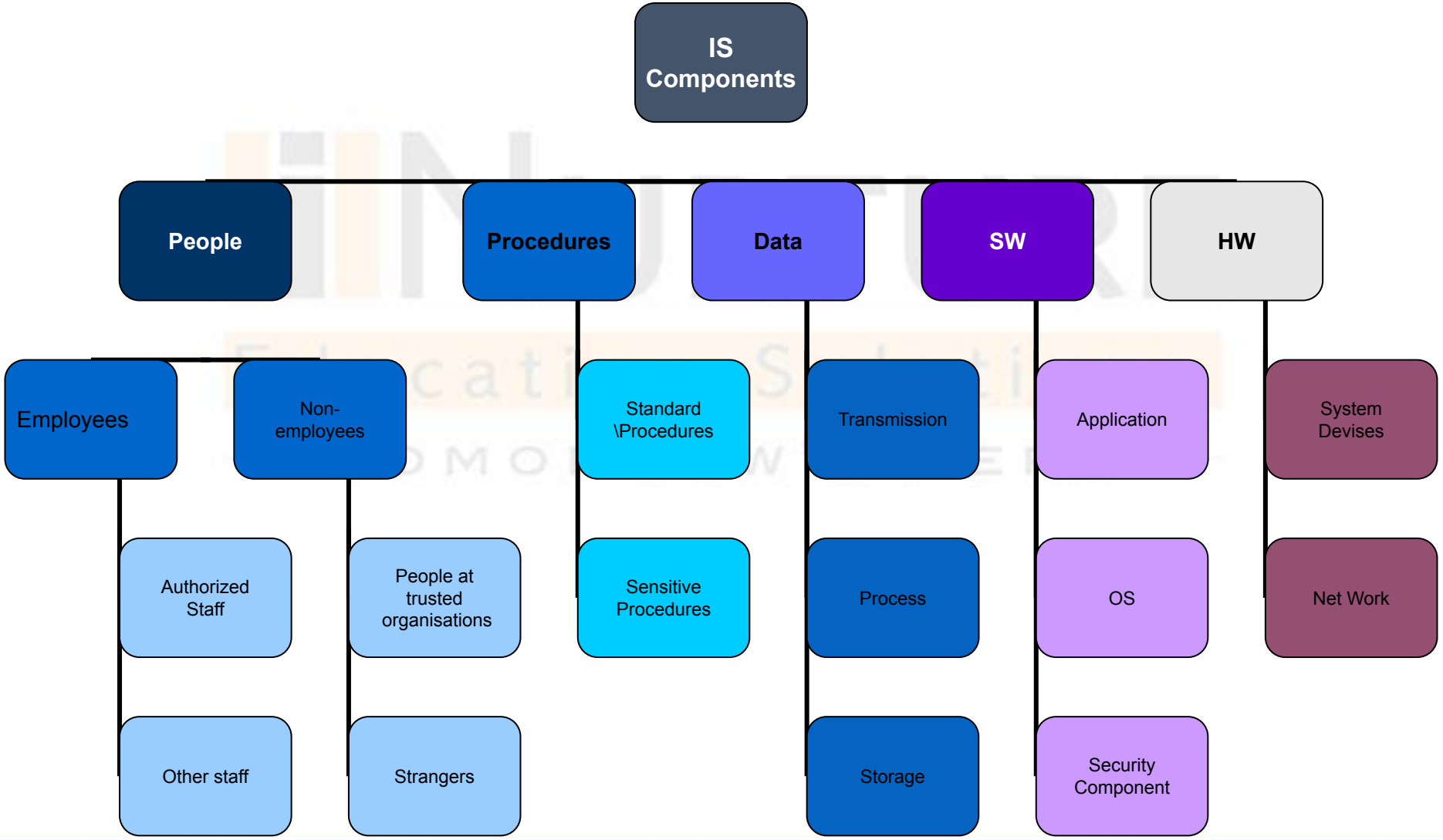
- A risk management strategy calls on us to “know ourselves” by identifying, classifying, and prioritising the organisation’s information assets.
- These assets are the targets of various threats and threat agents and our goal is to protect them from these threats.
- Next comes threat identification:
  - 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.

Risk Identification

What is the purpose of this phase ?

- The aim of this phase is to identify, classify and prioritizing the organisation's information assets (Know ourselves) and identify all important types and sources of risk and uncertainty (know our enemy), associated with each of the investment objectives.
- This is a crucial phase. If a risk is not identified it cannot be evaluated and managed.

Information Assets



Asset Identification and Valuation

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

People, Procedures, and Data Asset Identification

- Human resources, documentation, and data information assets are more difficult to identify.
- People with knowledge, experience, and good judgment should be assigned this task.
- These assets should be recorded using reliable data-handling process.
- Unlike the tangible hardware and software elements, 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

For People:

- Position name/number/ID – try to avoid names and stick to identifying positions, roles, or functions.
- Supervisor
- Security clearance level
- Special skills

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 is it located?
- Backup procedures employed

Hardware, Software, and Network Asset Identification

What information attributes to track depends on:

- Needs of organisation/risk management efforts.
- Management needs of information security/information technology communities.

- Asset attributes to be considered are: name; IP address; MAC address; element type; serial number; manufacturer name; model/part number; software version; physical or logical location; controlling entity.
- Automated tools can sometimes uncover the system elements that make up the hardware, software, and network components.
- Once created, the inventory listing must be kept current, often through a tool that periodically refreshes the data.

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

Information Asset Classification

- Categories must be comprehensive and mutually exclusive.
- Classification of components must be specific to allow determination of priority levels.
- Many organisations already have a classification scheme.

Examples of these kinds of classifications are:

  - Confidential data
  - Internal data
  - Public data

- Informal organisations may have to organise themselves to create a useable data classification model.
- The other side of the data classification scheme is the personnel security clearance structure.

Information Asset Valuation

- Each asset has to be categorised.
- 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 organisation?
  - 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?

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 organisation?

- 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.

Data Classification and Management

- Variety of classification schemes used by corporate and military organisations.
- Information owners responsible for classifying their information assets.
- Information classifications must be reviewed periodically.
- The military uses a five-level classification scheme, but most organisations do not need the detailed level of classification used by the military or federal agencies.
- However, organisations may need to classify data to provide protection.

Security Clearances

- The other side of the data classification scheme is the personnel security clearance structure.
- Each user of data in the organisation is assigned a single level of authorisation 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.

Management of Classified Data

It includes the storage, distribution, portability, and destruction of classified information.

- Must be clearly marked as such.
- When stored, it must be unavailable to unauthorised 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 organisation.

Threat Identification

- Realistic threats need investigation; unimportant threats are set aside.

Threat assessment:

- Which threats present danger to assets?
- Which threats represent the most danger to information?
- How much would it cost to recover from attack?
- Which threat requires greatest expenditure to prevent?

Identify and Prioritize Threats

- Each threat must be further examined to assess its potential to impact organisation - this is referred to as a threat assessment.

To frame the discussion of threat assessment, address each threat with a few questions:

- Which threats represent a danger to this organisation's assets in the given environment?
- Which threats represent the most danger to the organisation's information?
- How much would it cost to recover from a successful attack?
- Which of these threats would require the greatest expenditure to prevent?

Threat 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

Vulnerability Identification

- Specific avenues threat agents can exploit to attack an information asset is called as vulnerabilities.
- Examine how each threat could be perpetrated and list organisation's assets and vulnerabilities.
- Process works best when people with diverse backgrounds within organisation work iteratively in a series of brainstorming sessions.
- At the end of risk identification process, list of assets and their vulnerabilities is achieved.

Vulnerability Identification (Cont…)

- Examine how each of the threats that are possible or likely could be committed and list the organisation's assets and their vulnerabilities.
- The process works best when groups of people with diverse backgrounds within the organisation 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.

Vulnerability Identification (Cont…)

- **Identifying Vulnerabilities** : how each of the threats that are possible or likely could be committed, and list the organisation's assets and their vulnerabilities.
- **Vulnerabilities can be identified by numerous means.**

Different methodologies for identifying vulnerabilities.

- Start with commonly available vulnerability lists.
- Then, working with the system owners or other individuals with knowledge of the system or organisation, start to identify the vulnerabilities that apply to the system.
- Specific vulnerabilities can be found by reviewing vendor websites and public vulnerability archives, such as Common Vulnerabilities and Exposures (CVE) or the National Vulnerability Database (NVD).

Risk Assessment

- For each identified component and risk, which has a 'clearly significant' or 'possibly significant' position, each should be assessed to establish qualitatively and estimate the value.
- Risk assessment evaluates the relative risk for each vulnerability.
- Assigns a risk rating or score to each information asset.
- **Assessing risk is the process of determining the likelihood of the threat being exercised against the vulnerability and the resulting impact from a successful compromise.**
- **Risk assessment** assigns a risk rating or score to each specific information asset, useful in evaluating the relative risk and making comparative ratings later in the risk control process.
- Although all elements of the risk management cycle are important, risk assessments provides the foundation for other elements of the cycle. In particular, risk assessments provides a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies.

Introduction to Risk Assessment

Risk Identification Estimate Factors

- Likelihood
- Value of Information Assets
- Percent of Risk Mitigated
- Uncertainty

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

Identify Possible Controls

- 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.

Access Controls

- 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 organisation.

There are a number of approaches to controlling access. Access controls can be:

- Discretionary
- Mandatory
- Nondiscretionary

Methods of Risk Assessment

There are various methods for assessing risk

Quantitative risk assessment :

Generally estimates values of information systems components as; information, systems, business processes, recovery costs, etc.,

Risk can be measured in terms of direct and indirect costs based on:

1. The likelihood that a damaging event will occur.
2. The costs of potential losses.
3. The costs of mitigating actions that could be taken.

Methods of Risk Assessment (Cont…)

Qualitative Risk Assessment

This approach can be taken by defining:

- Risk in more subjective and general terms such as high, medium, and low.
- In this regard, qualitative assessments depends more on the expertise, experience, and judgment of those conducting the assessment.

- Qualitative risk assessments typically give risk results of “High”, “Moderate” and “Low”. However, by providing the impact and likelihood definition tables and the description of the impact, it is possible to adequately communicate the assessment to the organisation’s management.

Quantitative and Qualitative

- It is also possible to use a combination of quantitative and qualitative method.

How to assess the risks

Risk is assessed by following the following steps:

- Identifying threats
- Identifying vulnerabilities
- Relating Threats to Vulnerabilities
- Determining the likelihood
- Evaluate impact for each risk

Who does the Assessment ?

- A risk assessment is carried out by a team of people who have knowledge of specific areas of the business.
- 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 organisation.
  - Management and Users – play a part in the early detection and response process - they also ensure sufficient resources are allocated.
  - Information Technology – must assist in building secure systems and operating them safely.

Documenting the Results of Risk Assessment

- Ranked vulnerability risk worksheet is initial working document for next step in risk management process: assessing and controlling risk.
- The goal of this process has been to identify the information assets of the organisation 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.
- Final summary comprised in ranked vulnerability risk worksheet.
- Worksheet details asset, asset impact, vulnerability, vulnerability likelihood, and risk-rating factor.

Risk Control

- Once ranked vulnerability risk worksheet complete, must choose one of four strategies to control each risk:
  - Apply safeguards (avoidance)
  - Transfer the risk (transference)
  - Reduce impact (mitigation)
  - Understand consequences and accept risk (acceptance)

Avoidance

- Attempts to prevent exploitation of the vulnerability.
- Preferred approach; accomplished through countering threats, removing asset vulnerabilities, limiting asset access, and adding protective safeguards.

Three common methods of risk avoidance are:

- Application of policy
- Training and education
- Applying technology

Transference

- Control approach that attempts to shift risk to other assets, processes, or organisations.
- If lacking, organisation should hire individuals/firms that provide security management and administration expertise.
- Organisation may then transfer risk associated with management of complex systems to another organisation experienced in dealing with those risks.

Mitigation

- Attempts to reduce impact of vulnerability exploitation through planning and preparation.
- Approach includes three types of plans:
  - Incident Response Plan (IRP)
  - Disaster Recovery Plan (DRP)
  - Business Continuity Plan (BCP)

Mitigation (Cont…)

- DRP is most common mitigation procedure.
- The actions to take while incident is in progress is defined in IRP.
- BCP encompasses continuation of business activities if catastrophic event occurs.

Acceptance

- Doing nothing to protect a vulnerability and accepting the outcome of its exploitation.
- Valid only when the particular function, service, information, or asset does not justify cost of protection.
- Risk appetite describes the degree to which organisation is willing to accept risk as trade-off to the expense of applying controls.

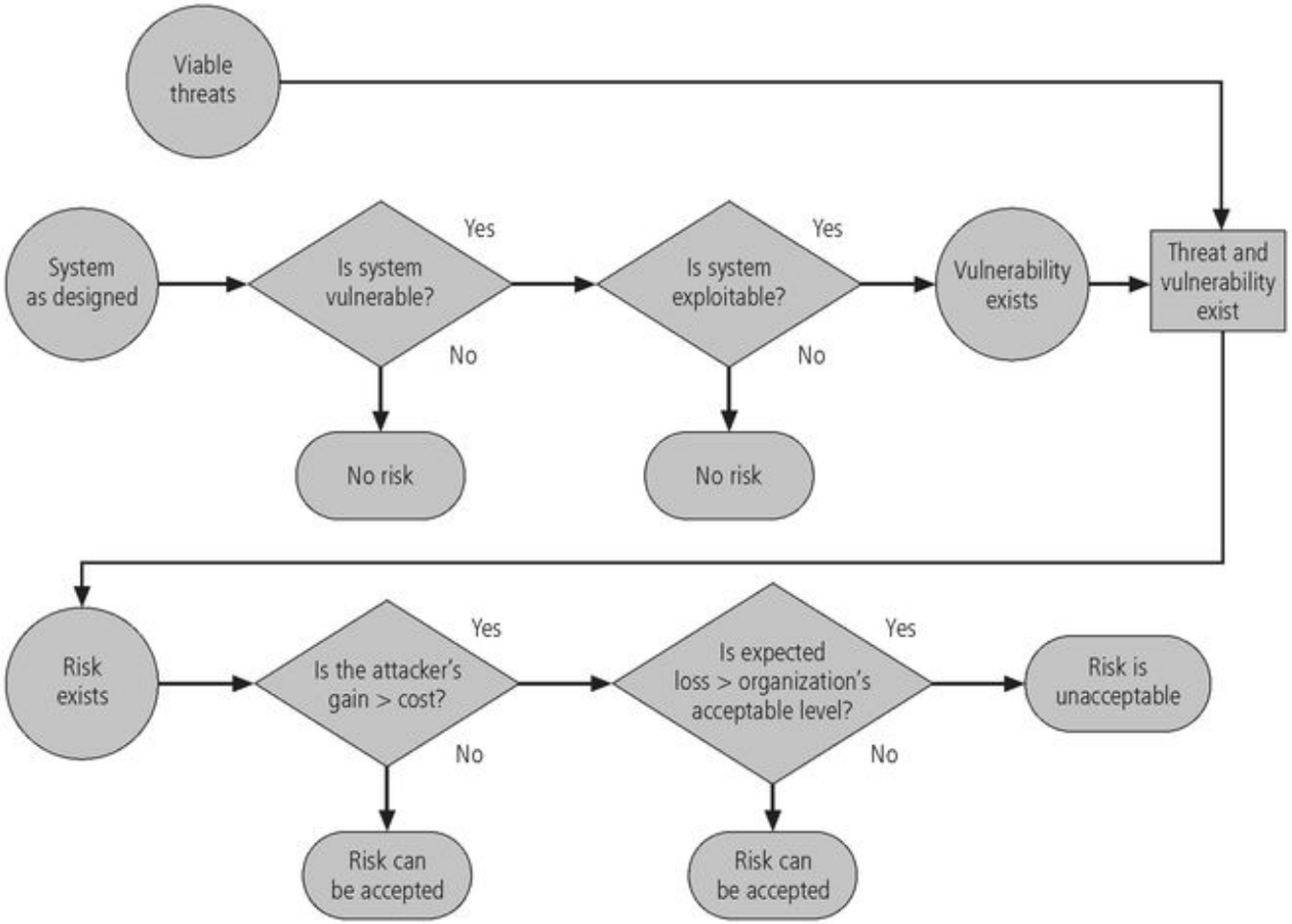
Selecting a Risk Control Strategy

- Level of threat and value of asset plays major role in selection of strategy.

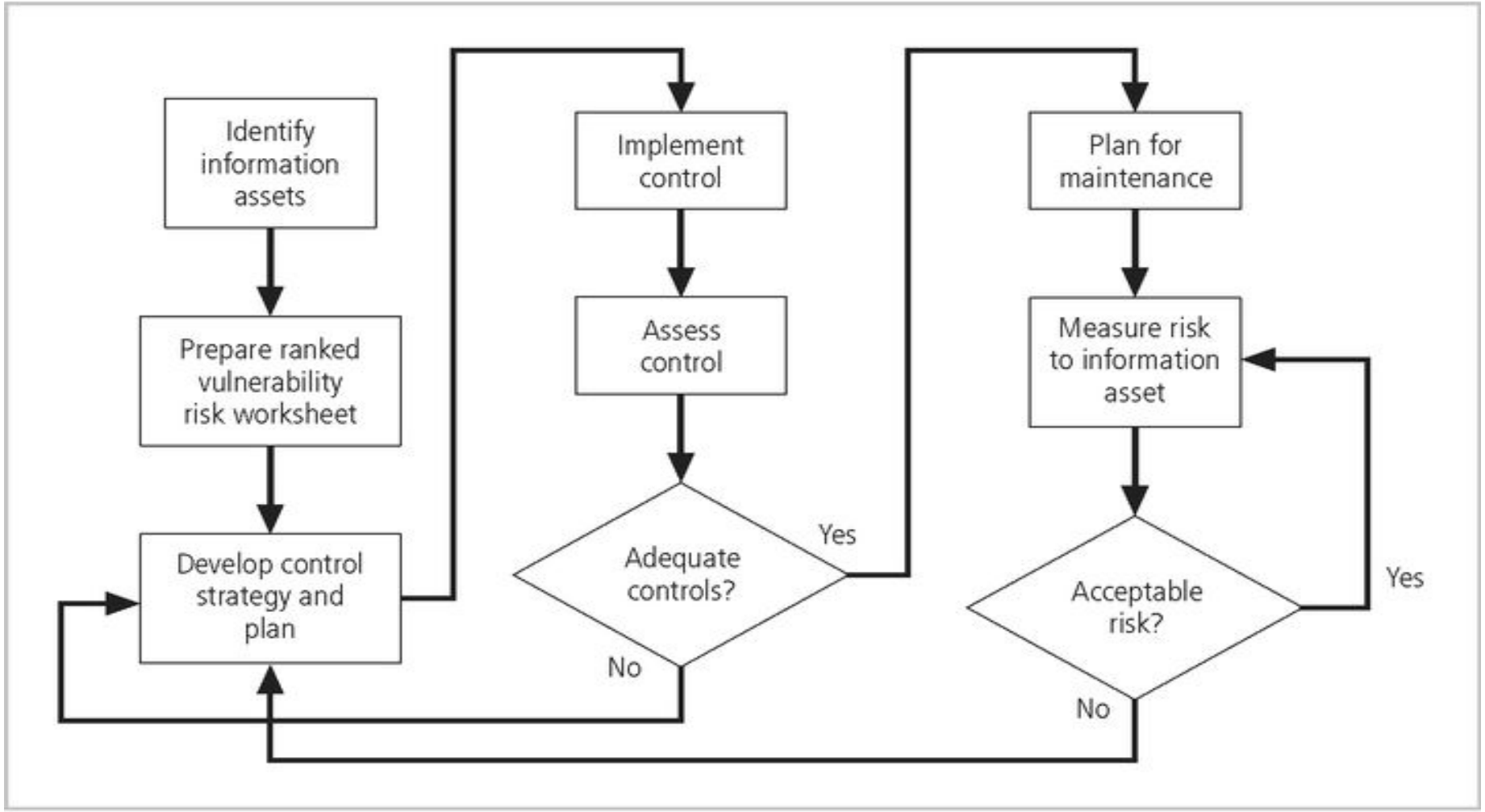
Rules of thumb on strategy selection can be applied:

- When a vulnerability exists.
- When a vulnerability can be exploited.
- When attacker's cost is less than potential gain.
- When potential loss is substantial.

Risk Handling



Risk Control Strategy



Cost Benefit Analysis (CBA)

- Most common approach for information security controls is economic feasibility of implementation.
- CBA is begun by evaluating worth of assets to be protected and the loss in value if those assets are compromised.
- The formal process to document this is called cost benefit analysis or economic feasibility study.

Cost Benefit Analysis (CBA) (Cont…)

- Items that impact cost of a control or safeguard includes: cost of development; training fees; implementation cost; service costs; cost of maintenance.
- Benefit is the value an organisation realises by using controls to prevent losses associated with a vulnerability.
- Asset valuation is process of assigning financial value or worth to each information asset; there are many components to asset valuation.

Benchmarking

An alternative approach to risk management

- Benchmarking is process of seeking out and studying practices in other organisations that one's own organisation desires to duplicate.
- One of two measures typically used to compare practices:
  - Metrics-based measures
  - Process-based measures
- Standard of due care: when adopting levels of security for a legal defense, organisation shows it has done what any prudent organisation would do in similar circumstances.

Benchmarking (Cont…)

- Due diligence: demonstration that organisation is diligent in ensuring that implemented standards continue to provide required level of protection.
- Failure to support standard of due care or due diligence can leave organisation open to legal liability.
- Best business practices: security efforts that provide a superior level protection of information.

When considering best practices for adoption in an organisation, consider:

- Does organisation resemble identified target with best practice?
- Are resources at hand similar?
- Is organisation in a similar threat environment?

Problems with Applying Benchmarking and Best Practices

- Organisations do not talk to each other (biggest problem).
- No two organisations are identical.
- Best practices are a moving target.
- Knowing what was going on in information security industry in recent years through benchmarking does not necessarily prepare for what is next.

Summary

- Risk identification: formal process of examining and documenting risk present in information systems.
- Risk control: process of taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of components in organisation's information system.

Risk identification

- A risk management strategy enables identification, classification, and prioritisation of organisation's information assets.
- Residual risk: risk that remains to the information asset even after the existing control is applied.

Summary (Cont…)

Risk control: Four strategies are used to control risks that result from vulnerabilities:

- Apply safeguards (avoidance)
- Transfer the risk (transference)
- Reduce impact (mitigation)
- Understand consequences and accept risk (acceptance)

Self Assessment Question

1. Risk is expressed in terms of probability and impact. State whether True or False.

a. True

b. False

Answer: True

Self Assessment Question

2. Which one of the following technique will ensure that impact of risk will be less?

   i. Risk avoidance technique

   ii. Risk Mitigation technique

   iii. Risk contingency technique

   a. Only i

   b. Only ii

   c. Only i and ii

   d. All i, ii and iii

Answer: All i, ii and iii

Self Assessment Question

3. Which one of the following is/are ways to deal with risk?

   i. Mitigate
   ii. Contingency
   iii. Transfer
   iv. Ignore

   a. Only i and ii
   b. Only ii and iii
   c. Only iii and iv
   d. All i, ii, iii and iv

Answer: All i, ii, iii and iv

Self Assessment Question

4. Which one of the given options is a risk?

a. Negative consequence that could occur.

b. Negative consequence that will occur.

c. Negative consequence that must occur.

d. Negative consequence that shall occur.

Answer: Negative consequence that could occur.

Self Assessment Question

5. Which one of the following is not one of the objectives of a risk management plan?

a. Create a list of threats

b. Create a list of vulnerabilities

c. Identify costs

d. Eliminate risk

Answer: Eliminate risk

Self Assessment Question

6. In the process of the risk management which one of the given options should be considered before taking the decision of risk?

a. Risk assessment

b. Risk identification

c. Risk retention

d. Risk transfer

Answer: Risk retention

Self Assessment Question

7. _____assess the risk and your plans for risk mitigation and revise these when you learn more about the risk.

a. Risk monitoring

b. Risk planning

c. Risk analysis

d. Risk identification

Answer: Risk monitoring

Self Assessment Question

8. Which one of the following risks are derived from the software or hardware technologies that are used to develop the system?

a. Managerial risks

b. Technology risks

c. Estimation risks

d. Organisational risks

Answer: Technology risks

Self Assessment Question

9. Which one of the following strategies means that the impact of the risk will be reduced?

a. Avoidance strategies

b. Minimisation strategies

c. Contingency plans

Answer: Minimisation strategies

Self Assessment Question

10. Risk management is now recognised as one of the most important project management tasks. State whether True or False.

a. True

b. False

Answer: False

Self Assessment Question

11. During which stage of risk planning, are risks prioritised based on probability and impact?

a. Perform Qualitative Risk Analysis

b. Monitor and Control Risks

c. Plan Risk Management

d. Identify Risks False

Answer: Identify Risks False

Self Assessment Question

12. Product of threat, vulnerability and asset value is

a. Compliance

b. Risk

c. Loss

d. Risk transfer

Answer: Risk

Self Assessment Question

13. Which of the following risks are derived from the organizational environment where the software is being developed?

a. People risks

b. Technology risks

c. Estimation risks

d. Organizational risks

Answer: Technology risks

Self Assessment Question

14. Which of the following risks are derived from the organizational environment where the software is being developed?

a. People risks

b. Technology risks

c. Estimation risks

d. Organizational risks

Answer: Organizational risks

Self Assessment Question

15. Which of the following term is best defined by the statement: “Derive traceability information to maximize information hiding in the design.”?

a. Underestimated development time

b. Organizational restructuring

c. Requirements changes

d. None of the mentioned

Answer: Requirements changes

Self Assessment Question

16. Which of the following term is best defined by the statement: “Derive traceability information to maximize information hiding in the design.”?

a. Underestimated development time

b. Organizational restructuring

c. Requirements changes

d. None of the mentioned

Answer: Requirements changes

Self Assessment Question

17. _____ assets are more difficult to identify

a. People

b. Network

c. Hardware

d. Software

Answer: People

Self Assessment Question

18. Automated tools can sometimes uncover the system elements that make up the hardware, software, and network components.true/false

a. True

b. False

Answer: True

Self Assessment Question

19. Information classifications must be _____ reviewed

a. Never

b. periodically

c. Once a while

d. When required

Answer: periodically

Self Assessment Question

20. Each threat must be further examined to assess its potential to impact organization - this is referred to as a _____

a. Threat classification

b. Threat assessment

c. Risk Analysis

d. Risk Mitigation

Answer: Threat assessment

Self Assessment Question

21. Access controls can't be

a. Discretionary

b. mandatory

c. nondiscretionary

d. Administrative

Answer: Administrative

Self Assessment Question

22. Which of the following term is best defined by the statement: “There will be a change in organizational management with different priorities.”?

a. Staff turnover

b. Technology change

c. Management change

d. Product competition

Answer: Management change

Self Assessment Question

23. What assess the risk and your plans for risk mitigation and revise these when you learn more about the risk?

a. Risk monitoring

b. Risk planning

c. Risk analysis

d. Risk identification

Answer: Risk monitoring

Self Assessment Question

24. When should a risk be avoided?

a. When the risk event has a low probability of occurrence and low impact

b. When the risk event is unacceptable

c. When it can be transferred by purchasing insurance

d. A risk event can never be avoided

Answer: When the risk event is unacceptable

Self Assessment Question

25. Risks are accepted when:

a. You develop a contingency plan to execute should the risk event occur

b. You accept the consequences of the risk

c. You transfer the risk to another party

d. a and b

Answer: a and b

Summary

- Due diligence is the demonstration that the organisation is diligent in ensuring that the implemented standards continue to provide the required level of protection.
- Items that impact cost of a control or safeguard includes: cost of development; training fees; implementation cost; service costs; cost of maintenance.
- Risk control: process of taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of components in organisation's information system.
- Organisation may then transfer risk associated with management of complex systems to another organisation experienced in dealing with those risks.
- Ranked vulnerability risk worksheet is initial working document for next step in risk management process: assessing and controlling risk.
- A risk management strategy calls on us to "know ourselves" by identifying, classifying, and prioritising the organisation's information assets.
- Residual risk: risk that remains to the information asset even after the existing control is applied

Assignment

1. Define risk.
2. What is risk management?
3. Explain the risk management process.
4. Explain the component of risk management.
5. Explain the importance of risk identification.
6. Discuss classification of information assets.
7. Discuss the identification of people, process and data assets.
8. Describe the asset identification of hardware, network and software.
9. Discuss information asset classification and valuation.
10. Discuss data classification and management.
11. Discuss the concept of risk assessment and the steps involved in assessing the risk.
12. Who is responsible for doing a Risk Assessment?

Document Links

Topic	URL's	Description
Risk Management	https://www.massey.ac.nz/massey/fms/PolicyGuide/Documents/Risk%20Management/Risk%20Management%20Framework.pdf	Link explains the methodology of the risk assessment.
Risk Management Process	https://www.solarwindsmsp.com/content/risk-management-process-definition	The link explains the process of the risk management.
Risk Assessment	https://www.ccohs.ca/oshanswers/hsprograms/risk_assessment.html	The link explain the concept of assessing the risk and describe the method to do it.
Risk Documentation	http://www.leoisaac.com/ris/ris008.htm	The link explain the importance of risk documentation, and provide the plan for documenting risk.
Risk mitigation strategy options	https://accendoreliability.com/4-effective-risk-mitigation-strategies/	The link explain the risk mitigation strategies

Video Links

Topic	URL's	Description
Risk Management	https://www.youtube.com/watch?v=Cp_XEhexcDw	The link explain the basic concept of the risk management.
Risk handling	https://www.youtube.com/watch?v=543TgGRUudg	The link explains the basics of risk management and how to manage the risk.
Risk assessment	https://www.youtube.com/watch?v=U6U9gXxHPIQ	The Link explain the procesdure to assess the risk
Various risk mitigation strategy options	https://www.youtube.com/watch?v=Ea7vxDngUF4	The Link explain various risk mitigation strategies

E-Book Links

Topic	URL's	Page No
Risk Management: Safeguarding Company Assets By Emmanuel Fragnière	https://books.google.co.in/books?id=_wBNqvvcavQC&printsec=frontcover&dq=risk+management&hl=en&sa=X&ved=0ahUKEwjLsLCm0oDgAhULuo8KHc05BI4Q6AEIUTAG#v=onepage&q=risk%20management&f=false	9-96
Fundamentals of Risk Management By Paul Hopkin	https://books.google.co.in/books?id=e9ilBAAAQBAJ&printsec=frontcover&dq=risk+management&hl=en&sa=X&ved=0ahUKEwjLsLCm0oDgAhULuo8KHc05BI4Q6AEISjAF#v=onepage&q=risk%20management&f=false	49-69