Information Technology Security and Risk Management

Introduction to Computer Security

Naercio Magaia and Imran Khan

Contents

Information Technology (IT) Security Management Overview

Is the formal process of answering the questions:

What assets need to be protected? → How are those assets threatened? → What can be done to counter those threats?

- Ensures that **critical assets are sufficiently protected** in a cost-effective manner
- Security risk assessment is needed **for each asset in the organization** that requires protection
- Provides the information necessary to decide **what management, operational, and technical controls are needed** to reduce the risks identified

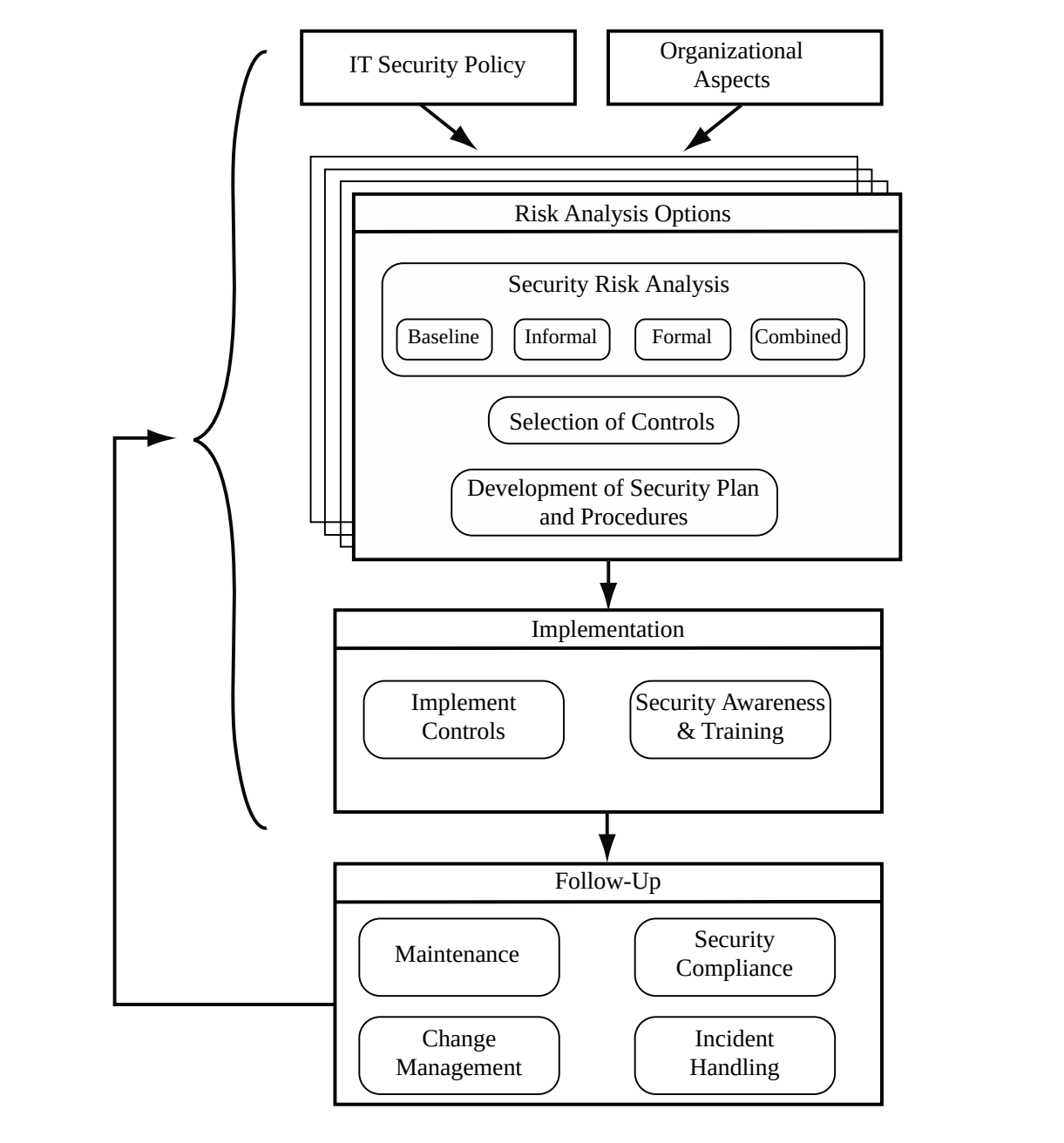
IT Security Management

A process used to **achieve and maintain appropriate levels** of confidentiality, integrity, availability, accountability, authenticity, and reliability. Its functions include:

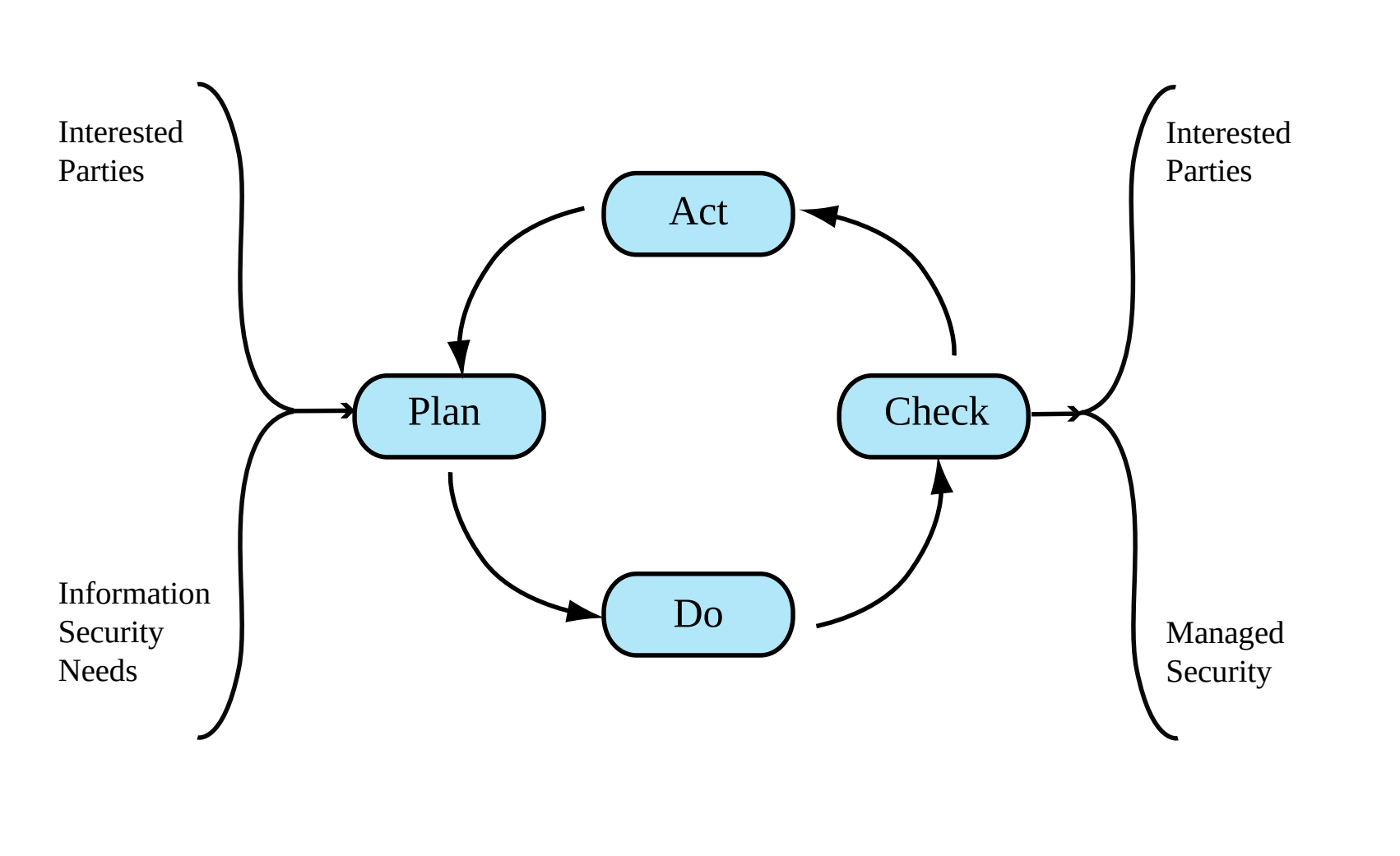
Determining organizational **IT security objectives, strategies, and policies**	Determining organizational **IT security requirements**	Identifying and analyzing **security threats to IT assets** within the organization	**Identifying and analyzing risks**	**Specifying appropriate safeguards**	Monitoring the **implementation and operation of safeguards** that are necessary in order to **cost effectively protect the information and services** within the organization	Developing and implementing **a security awareness program**	**Detecting and reacting to incidents**

IT Security Policy Flow

- IT Security is **an ongoing process**
- Policy drives the risk analysis
- Risk Analysis drives the implementation
- Implementation is regularly reviewed to tune the analysis and implementation
- Major incidents may also drive review



The Plan-Do-Check-Act Process Model



Organizational Context and Security Policy

- Maintained and updated regularly
  - Using periodic security reviews
  - Reflect changing technical/risk environments
- Examine **role and importance** of IT systems in organization

First examine organization's IT security:

Objectives - wanted IT security outcomes

Strategies - how to meet objectives

Policies - identify what needs to be done

Security Policy

Needs to address:

- **Scope and purpose** including relation of objectives to business, legal, regulatory requirements
- IT security requirements
- Assignment of **responsibilities**
- Risk management approach
- Security **awareness and training**
- General personnel issues and any legal sanctions
- Integration of security into systems development
- Information classification scheme
- **Contingency** and business **continuity** planning
- Incident detection and handling processes
- How and when policy should be reviewed, and change control to it

Management Support

- IT security policy **must be supported** by senior management
- Need IT security officer
  - To provide **consistent overall supervision**
  - Liaison with senior management
  - Maintenance of IT security objectives, strategies, policies
  - Handle incidents
  - Management of IT security awareness and training programs
  - Interaction with IT project security officers
- Large organizations need separate IT project security officers **associated with major projects and systems**
  - Manage security policies within their area

Security Risk Assessment

Critical component of process

Ideally examine every organizational asset

- Not feasible in practice

Approaches to identifying and mitigating risks to an organization's IT infrastructure:

- Baseline
- Informal
- Detailed risk
- Combined

Baseline Approach

- The goal is to **implement agreed controls** to provide protection against **the most common threats**
- Forms a good base for further security measures
- Use "industry best practice"
  - Easy, cheap, can be replicated
  - Gives no special consideration to variations in risk exposure
  - May give too much or too little security
- Generally **recommended only for small organizations** without the resources to implement more structured approaches

Informal Approach

Involves conducting an **informal, pragmatic risk analysis** on organization's IT systems

Exploits **knowledge and expertise** of analyst

Fairly quick and cheap

Judgments can be made about **vulnerabilities and risks** that baseline approach would not address

Some risks may be **incorrectly assessed**

Skewed by analyst's views, **varies over time**

Suitable for small to medium sized organizations where IT systems are not necessarily essential

Detailed Risk Analysis

Most comprehensive approach

Assess using **formal structured process**

- Number of stages
- Identify **threats and vulnerabilities** to assets
- Identify **likelihood of risk occurring** and consequences

Significant cost in time, resources, expertise

May be a legal requirement to use

Suitable for large organizations with IT systems critical to their business objectives

Combined Approach

- Combines elements of the baseline, informal, and detailed risk analysis approaches
- Aim is to provide **reasonable levels of protection as quickly as possible** then to examine and adjust the protection controls deployed on key systems over time
- Approach **starts with the implementation of suitable baseline security recommendations** on all systems
- Next, systems either **exposed to high risk levels or critical to the organization's business objectives** are identified in the high-level risk assessment
- A decision can then be made to possibly conduct an immediate informal risk assessment on key systems, with the aim of relatively quickly tailoring controls to more accurately reflect their requirements
- Lastly, an ordered process of performing detailed risk analyses of these systems can be instituted
- Over time, this can result in the **most appropriate and cost-effective security controls** being selected and implemented on these systems

Detailed Security Risk Analysis

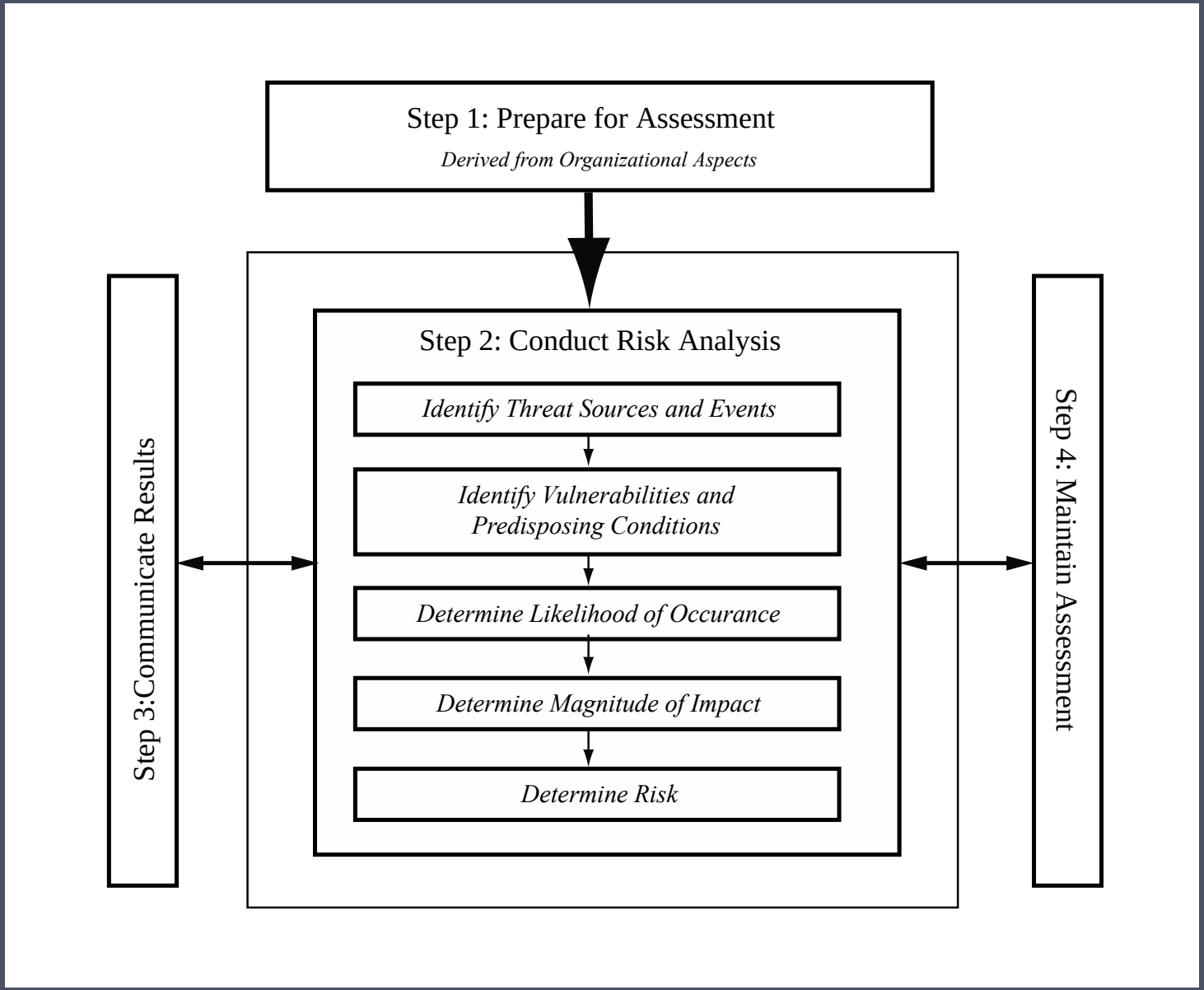
Provides **the most accurate evaluation** of an organization's IT system's security risks

Highest cost

Initially focused on addressing defense security concerns

Often mandated by government organizations and associated businesses

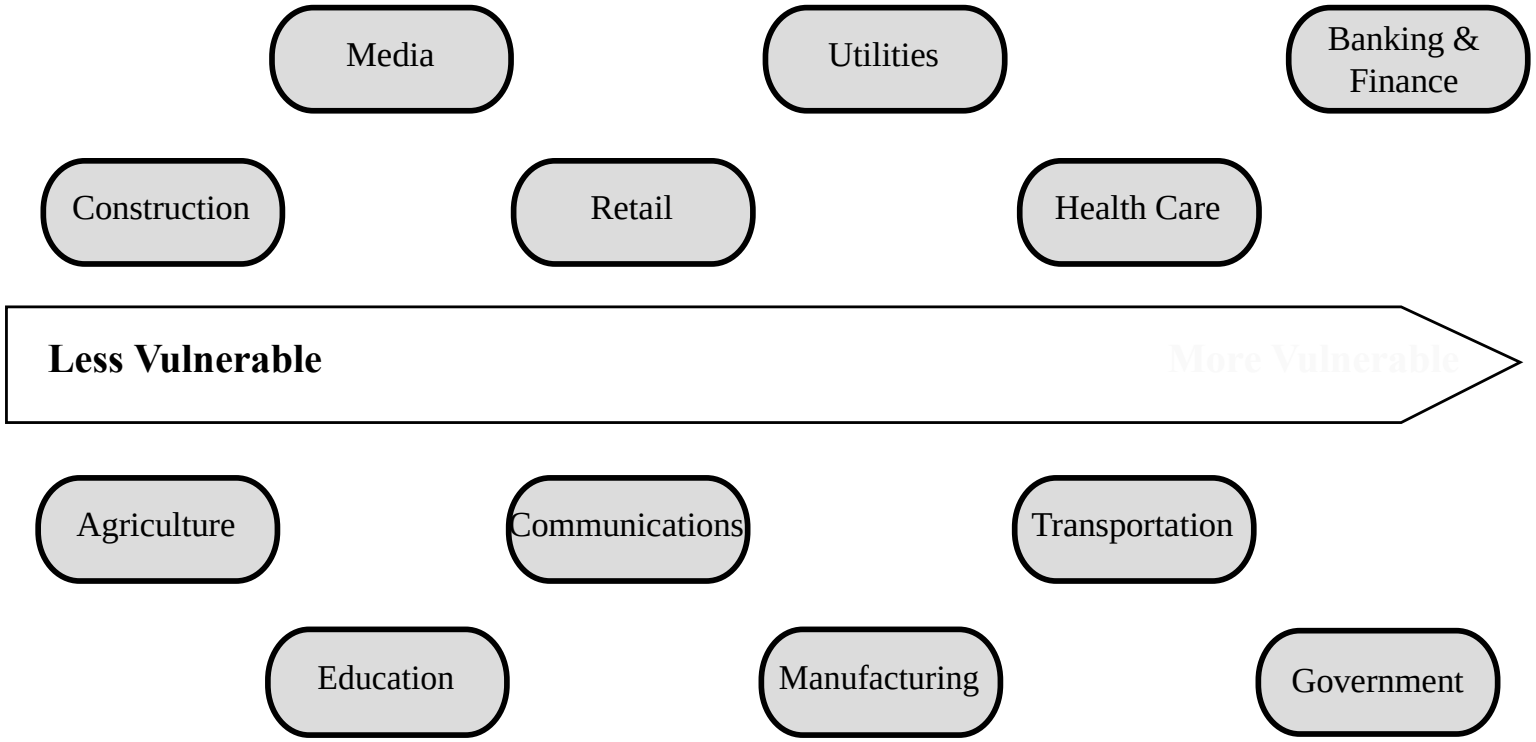
Risk Assessment Process



Establishing the Context

- Initial step
  - Determine the basic parameters of the risk assessment
  - Identify the assets to be examined
- Explores political and social environment in which the organization operates
  - Legal and regulatory constraints
  - Provide baseline for organization's risk exposure
- Risk appetite
  - The level of risk the organization views as acceptable

Generic Organizational Risk Context



Asset Identification

- Last component is to **identify assets to examine**
- Draw on expertise of people in relevant areas of organization to **identify key assets**
  - Identify and interview such personnel

Asset
• "anything that needs to be protected" because **it has value to the organization** and contributes to the successful attainment of the organization's objectives

Terminology

- **Asset**: A system resource or capability of value to its owner that **requires protection**
- **Vulnerability**: A **flaw or weakness in an asset**'s design, implementation, or operation and management that could be exploited by some threat
- **Threat**: A potential for a threat source to exploit a vulnerability in some asset, which, if it occurs, may **compromise the security of the asset** and cause harm to the asset's owner
- **Risk**: The **potential for loss** computed as the combination of the **likelihood** that a given threat exploits some vulnerability to an asset, and the magnitude of harmful **consequence** that results to the asset's owner

Threat Identification

- A threat is:

Threat Sources

- Threats may be
  - Natural "acts of God" or man-made
  - Accidental or deliberate

Evaluation of human threat sources should consider:

- Motivation
- Capability
- Resources
- Probability of attack
- Deterrence

- Any previous experience of attacks seen by the organization also needs to be considered

Vulnerability Identification

- Identify **exploitable flaws or weaknesses** in organization's IT systems or processes
  - Determines applicability and significance of threat to organization
- Need combination of threat and vulnerability to create a risk to an asset
- Outcome should be **a list of threats and vulnerabilities** with brief descriptions of how and why they might occur

Analyze Risks

- Specify **likelihood of occurrence** of each identified threat to asset given existing controls
- Specify consequence should threat occur
- **Derive overall risk rating** for each threat
  - **Risk = probability threat occurs x cost to organization**
- Hard to determine accurate probabilities and realistic cost consequences
- Use qualitative, not quantitative, ratings

Analyze Existing Controls

- Existing controls used to attempt to minimize threats need to be identified
- Security controls include **management, operational, and technical processes and procedures**
- Use checklists of existing controls and **interview key organizational staff** to solicit information

Risk Likelihood

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may be deemed as “unlucky” or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

Risk Consequences

Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify. Usually does not result in any tangible detriment to the organization.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources. Again, does not result in any tangible detriment to the organization, but may, in hindsight, show previous lost opportunities or lack of efficiency.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and will generally require management intervention, though should still be able to be dealt with at the project or team level. Will require some ongoing compliance costs to overcome. Customers or the public may be indirectly aware or have limited information about this event.
4	**Major**	Ongoing systemic security breach. Impact will likely last 4-8 weeks and require significant management intervention and resources to overcome. Senior management will be required to sustain ongoing direct management for the duration of the incident and compliance costs are expected to be substantial. Customers or the public will be aware of the occurrence of such an event and will be in possession of a range of important facts. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. A loss of customer business or other significant harm to the organization is expected. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action against personnel involved is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable. Compliance costs are likely to result in annual losses for some years, with liquidation of the organization likely.

(Table can be found on pages 476-477 in textbook)

Risk Level Determination and Meaning

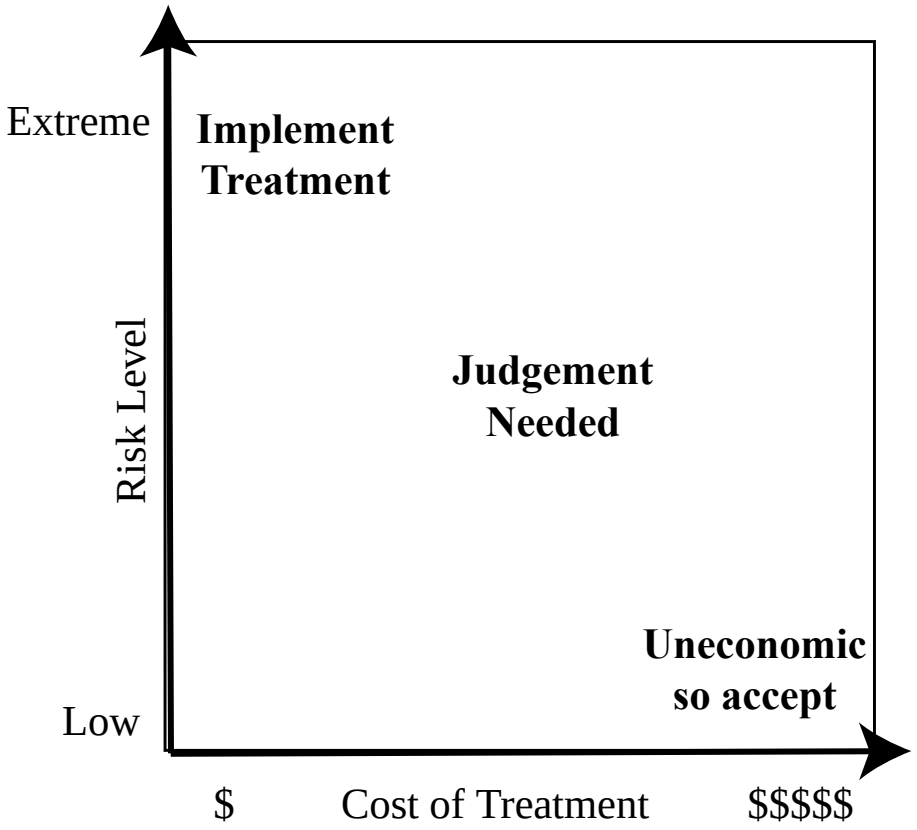
	Consequences					
Likelihood	**Doomsday**	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources.
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet router	Outside hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of data center	Accidental fire or flood	None (no disaster recovery plan)	Unlikely	Major	High	2

Judgment About Risk Treatment



Risk Treatment Alternatives

Risk acceptance	Choosing to accept a risk level greater than normal for business reasons
Risk avoidance	Not proceeding with the activity or system that creates this risk
Risk transfer	Sharing responsibility for the risk with a third party
Reduce consequence	Modifying the structure or use of the assets at risk to reduce the impact on the organization should the risk occur
Reduce likelihood	Implement suitable controls to lower the chance of the vulnerability being exploited

Summary

- IT security management
- Organizational context and security policy
- Security risk assessment
  - Baseline approach
  - Informal approach
  - Detailed risk analysis
  - Combined approach
- Detailed security risk analysis
  - Context and system characterization
  - Identification of threats/risks/vulnerabilities
  - Analyze risks
  - Evaluate risks
  - Risk treatment
- Case Study