CS 413 Information Security

Course Instructor

Naushad Siddiqui

Head of IT Audit, Sui Southern Gas Company

Visiting Faculty, NED University
Director & Faculty Member, ISACA Karachi

CS413 Information Security

Fall 2020

Week 09

Agenda

- Introduction to Risk Management
- Risk Assessment
- Risk Analysis
- Attack Surface Analysis
- Risk Response

Introduction to Risk Management

Basic Terminologies in Risk Management

An **asset** (information asset) is composed of the people, property and information within our organization (anything of value).

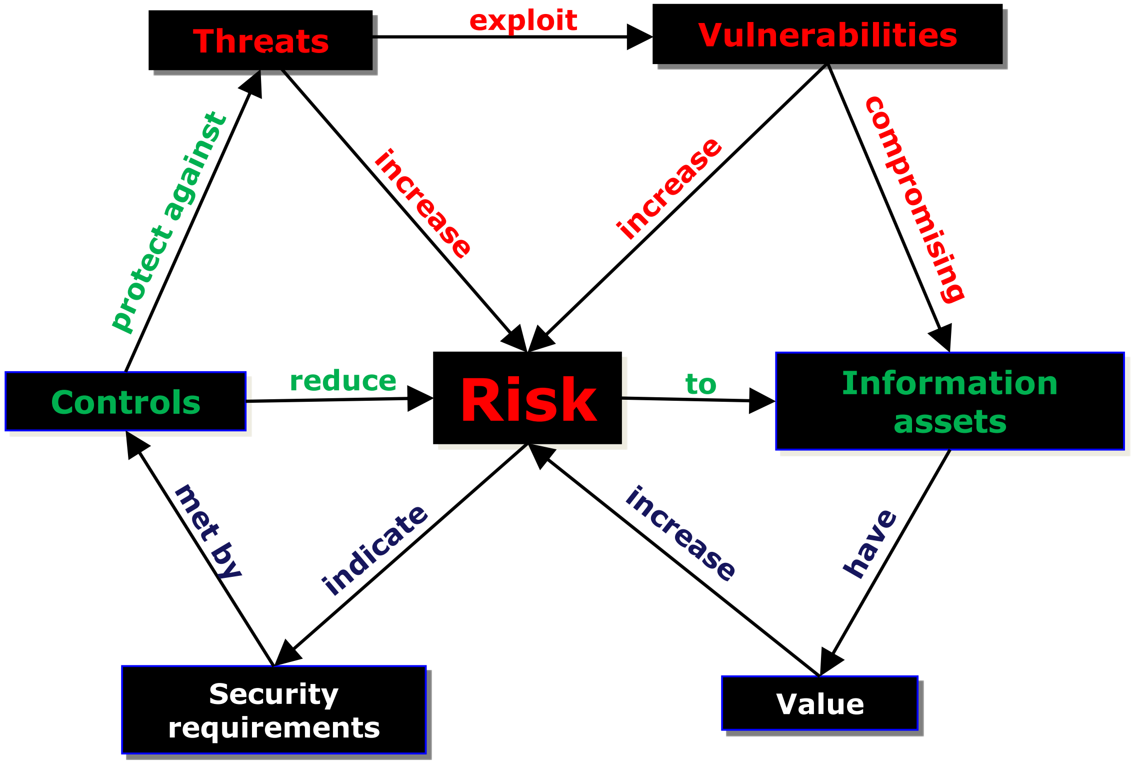
A **threat** is anything that can exploit a vulnerability, intentionally or accidently, and obtain, damage, or destroy an asset.

A **vulnerability** is a weakness of an asset that can be exploited by a threat.

A **risk** is the potential for loss, damage, or destruction of an asset when a threat exploits a vulnerability.

Introduction to Risk Management (2)

Risk Relationship



Introduction to Risk Management (3)

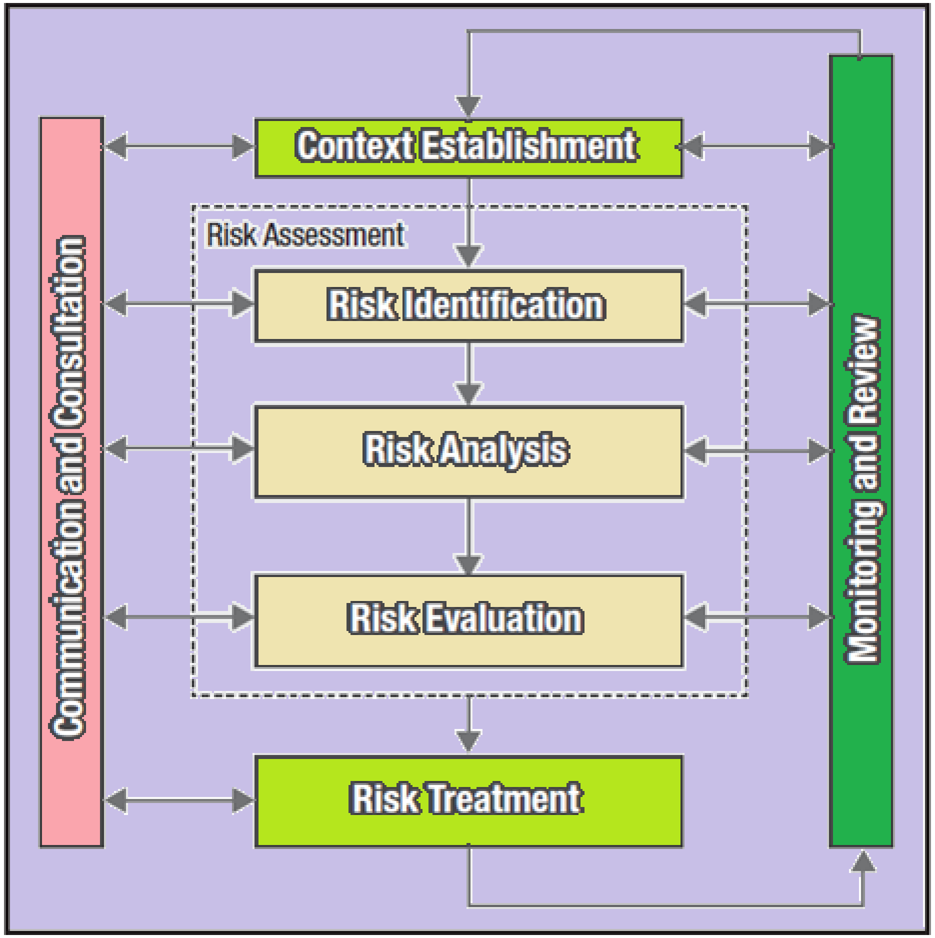
Risk Management is the process of identifying, assessing, monitoring, and limiting risk to an acceptable level.

Risk Management provides a systematic and repeatable process for *identifying*, *assessing*, *prioritizing*, *monitoring*, *tracking*, and *regularly communicating* the status of threats, risks, issues and actions items to management, stakeholders, and executive-level decision makers.

Primary Goal of Risk Management

Risks are reduced to a level that an organization will accept.

Introduction to Risk Management (4)



Introduction to Risk Management (5)

Exploring Risks, Threats and Vulnerabilities

Risks

- Monetary
- Reputation
- Loss of Asset
- Intellectual Property
- Legal

Threats

- External
  - ✓ Natural
  - ✓ Man-made
- Internal
  - ✓ Unintentional
  - ✓ Intentional

Vulnerability Areas

- Network vulnerabilities
- Physical access
- Applications
- Processes
- Equipment
- Cloud computing
- Internet of Things

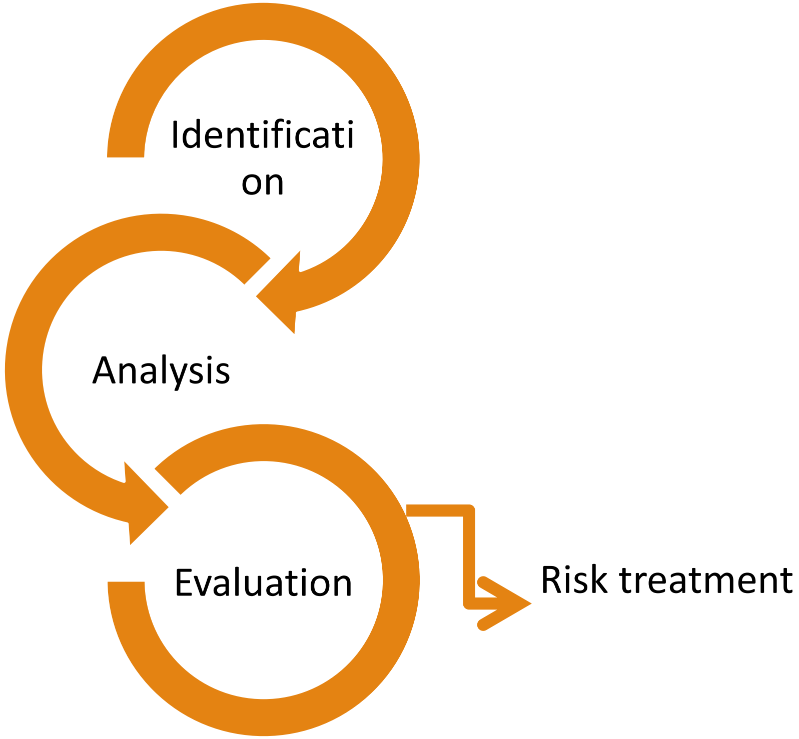
Risk Assessment

A **risk assessment**, where risks are identified and assessed, is the first step in the risk management process.

Risk Assessment Process:

1. Identify and categorize risks
2. Assess each risk’s probability and impact
3. Assign each risk a score and prioritize accordingly
4. Respond accordingly

Risk Assessment (2)



Identificati
on

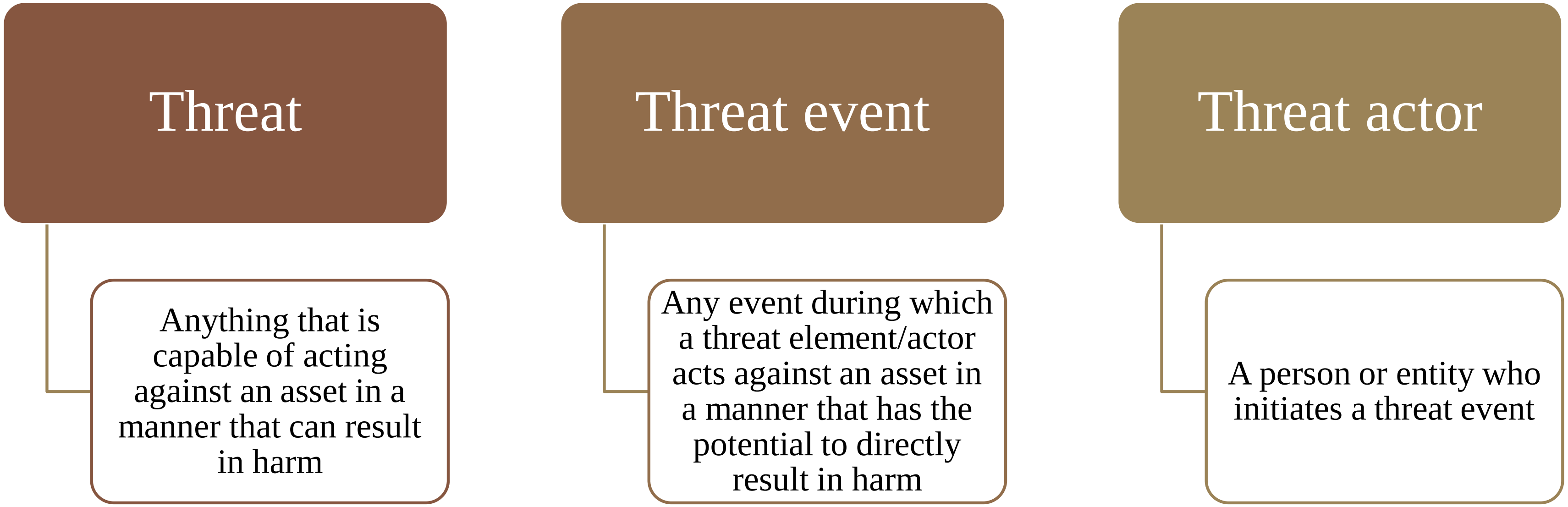
Analysis

Evaluation

Risk treatment

Risk Assessment (3)

Threats, Threat Events, Threat Actors



Threat

Anything that is capable of acting against an asset in a manner that can result in harm

Threat event

Any event during which a threat element/actor acts against an asset in a manner that has the potential to directly result in harm

Threat actor

A person or entity who initiates a threat event

Risk Assessment (4)

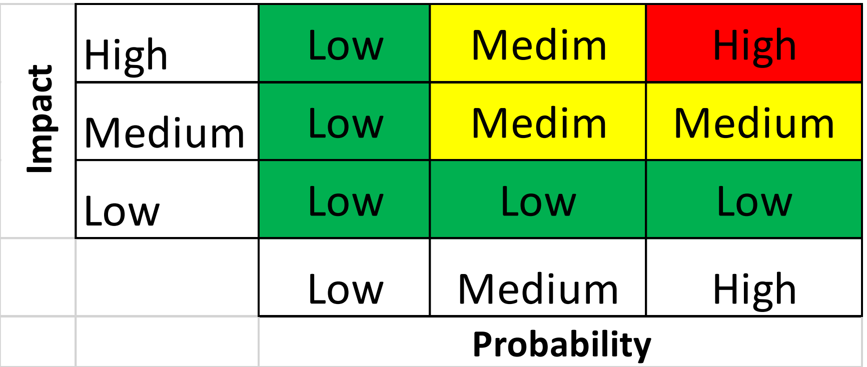
Qualitative Risk Assessment

Risk Assessment Score = Probability x Impact

Probability: The likelihood that a risk will occur.

Impact: The negative impact of a risk if it occurs.

Probability and impact are given numbers to help categorize the severity of a risk, if realized.
Based on the overall severity of risk, we can choose the appropriate risk response measure.



Impact	High	Low	Medim	High
	Medium	Low	Medim	Medium
	Low	Low	Low	Low
		Low	Medium	High
		Probability		

Knowledge Check

A security manager is preparing a report to obtain the commitment of executive management to a security program. Inclusion of which of the following items would be of MOST value:

A. Examples of genuine incidents at similar organizations

B. Statement of generally accepted good practices

C. Associating realistic threats to corporate objectives

D. Analysis of current technological exposures

Correct Answer ‘C’

Risk Analysis

Qualitative vs Quantitative Risk Analysis

- Qualitative and quantitative risk analysis are two different methods for analyzing risk:
  - **Qualitative**:
    - More Subjective
    - Perception/judgement of value
  - **Quantitative**:
    - More Objective
    - Dollar-value figures

Risk Analysis (2)

Quantitative Risk Analysis Components

Component	Definition
Asset Value (AV)	The value of an asset.
Exposure Factor (EF)	The percentage loss of a specific asset if a risk is realized.
Single Loss Expectancy (SLE)	The monetary value expected from the occurrence of a risk on an asset. **Formula**: SLE = AV x EF
Annual Rate of Occurrence (ARO)	The estimated frequency of a threat occurring in a single year.
Annualized Loss Expectancy (ALE)	The expected monetary loss that can be expected from an asset due to a risk over a one year period. **Formula**: ALE = SLE x ARO

Risk Analysis (3)

Quantitative Risk Analysis Example

Scenario: Your data center is valued at $500,000. If there is a major earthquake, you estimate 25% of the data center will be damaged. Your risk team estimated there will be major earthquake once every 10 years.

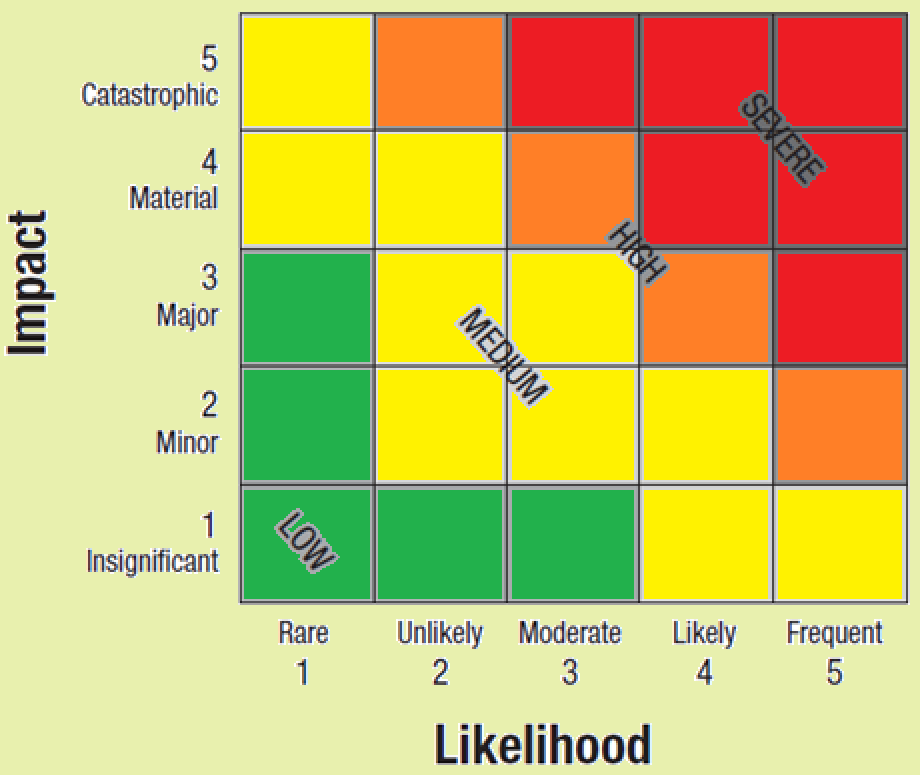
Would it be prudent to purchase earthquake insurance with an annual cost of $25,000?

- **Asset Value (AV)** = $500,000
- **Exposure Factor (EF)** = .25
- **SLE = AV x EF** = $500,000 x .25 = $125,000
- **ARO** = .10
- **ALE = SLE x ARO** = $125,000 x .10 = $12,500

No, the cost of the annual insurance premium is double the ALE, so you would be spending more than you expect to lose on an annual basis.

Risk Analysis (4)

Semi Quantitative Risk Analysis



	Rare 1	Unlikely 2	Moderate 3	Likely 4	Frequent 5
5 Catastrophic	🟨	🟧	🟥	🟥	🟥
4 Material	🟨	🟨	🟧	🟥	🟥
3 Major	🟩	🟨	🟨	🟧	🟥
2 Minor	🟩	🟨	🟨	🟨	🟧
1 Insignificant	🟩	🟩	🟩	🟨	🟨

<u>RISK VALUE</u>

1 – 3	Low
4 – 9	Medium
10 – 12	High
>12	Severe

Risk Analysis (5)

Semi Quantitative Risk Analysis – Example of Audit Planning

Audit Subject	Financial Impact		IT Risks								Score & Level (H=33~45, M=20~32, L=5~19)	
			Quality of Int. Cntrl		Availability		Integrity		Confidentiality			
	L	I	L	I	L	I	L	I	L	I		
Area 1 - IT Operations												
Backup & Recovery Process	1	1	2	2	3	3	3	3	3	3	32	Medium
DR Readiness	3	3	2	2	3	3	3	3	3	3	40	High
IT Procurement and Vendor Management	2	2	2	2	3	3	3	3	2	2	30	Medium
IT Service Delivery	1	1	2	2	3	3	3	3	3	3	32	Medium
Area 2 - ----												
	3	3	2	2	3	3	3	3	3	3	40	High
	3	3	2	2	2	2	3	3	3	3	35	High

Discussion

What are some of the reasons for using a semiquantitative approach to risk analysis? Can you think of any drawbacks?

Attack Surface Analysis

An **attack surface** is a vulnerability. It's any way an attacker can gain access to pose a security risk.

There are three common attack surfaces:

- Application
- Network
- User

The greater the overall attack surface, the greater the overall risk.

Attack Surface Analysis (2)

Application Attack Surface

When analyzing our applications for attack surfaces, we’ll commonly look at:

- The Amount of Code
- Data Inputs
- System Services
- Network Communication Ports

Attack Surface Analysis (3)

Network Attack Surface

When analyzing our network for attack surfaces, we'll commonly look at:

- Overall Network Design
- Placement of Mission Critical Servers & Systems
- Placement & Configuration of Network Firewalls
- Other Security-Related Devices & Services: IDS, IPS, VPN, etc.

Attack Surface Analysis (4)

User Attack Surface

When analyzing our users for attack surfaces, we’ll commonly look at:

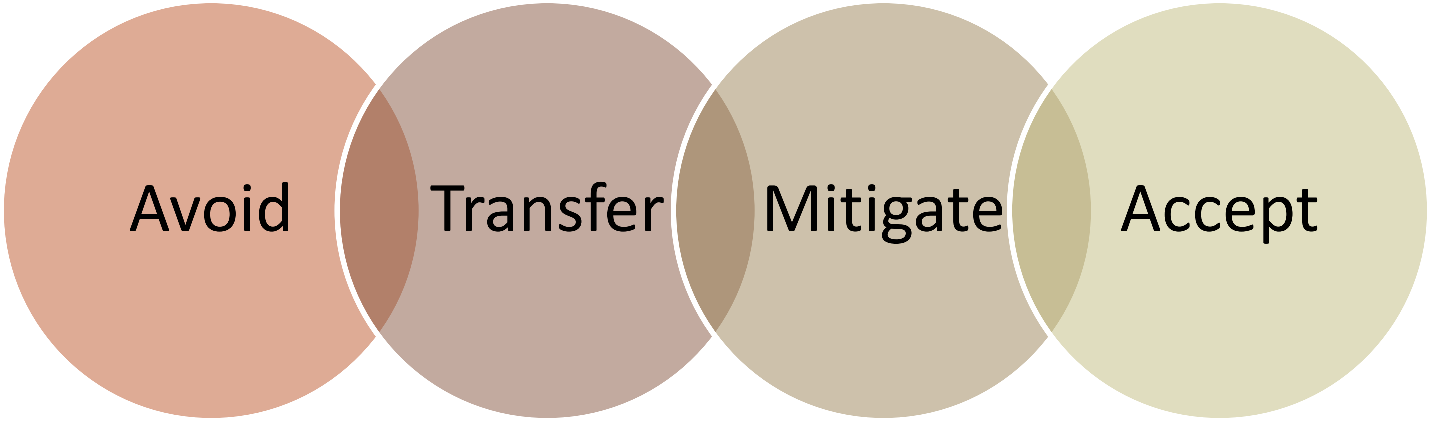
- Effectiveness of Policies, Procedures and Training
  - Risk of Social Engineering
  - Potential for Human Error
  - Risk of Malicious Behavior

Risk Response

The risk considered in the evaluation process is current risk, which is risk as it exists given current circumstances.

The decision of how to treat risk (i.e. risk response) is based on how current risk relates to the risk appetite and risk tolerance set by the organization.

There are four possible options of risk response:



Risk Response (2)

Risk Response Categories

Avoidance: The process of eliminating a risk by not engaging in an activity. We avoid a risk by eliminating its source altogether.

Acceptance: Accepting an identified risk, meaning no action will be taken when a risk assessment score is low.

Mitigation: The process of taking steps to minimize the impact of a risk. Implementing some controls or counter-measures.

Transference: Transferring the responsibility of a risk to a third party, such insurance. However, the ownership is not transferred.

Residual Risk: The risk that remains when after risk mitigation or transference activities have taken place.

Risk Response (3)

Selecting a Risk Response Category

The choice is usually straightforward.

Risk within risk appetite should be accepted.

For risk outside of the appetite:

> If value of continuing < cost of transfer/mitigation, ***avoid***.
> If value of continuing > cost of transfer/mitigation, choose most cost-effective choice

The minimum cost/cost-effective solution is the solution to adopt.

Knowledge Check

Which of the following techniques MOST clearly indicates whether specific risk-reduction controls should be implemented:

A. Cost-benefit analysis

B. Penetration testing

C. Frequent risk assessment programs

D. Annual loss expectancy calculation

Correct Answer ‘A’

End of Week 09