Lecture Two

Risk Identification and Assessment

1. Risk:

The is an object, person, or other entity that represent a danger, harm or loss to an asset.

Risk Life Cycle:

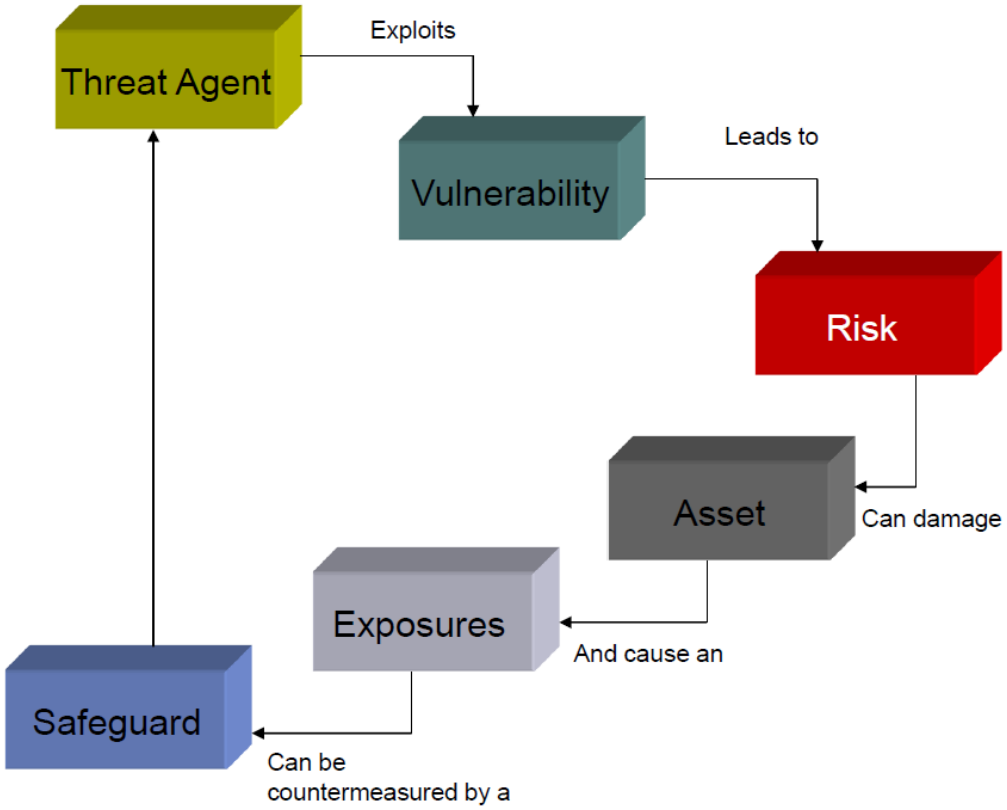

Figure 1: Risk life cycle

2. Risk Management:

Is the process of *identifying*, *assessing* and *evaluating* the level of risk facing the organization, specifically the threats to the information stored and using by organization 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 organization.

Risk Management Life Cycle

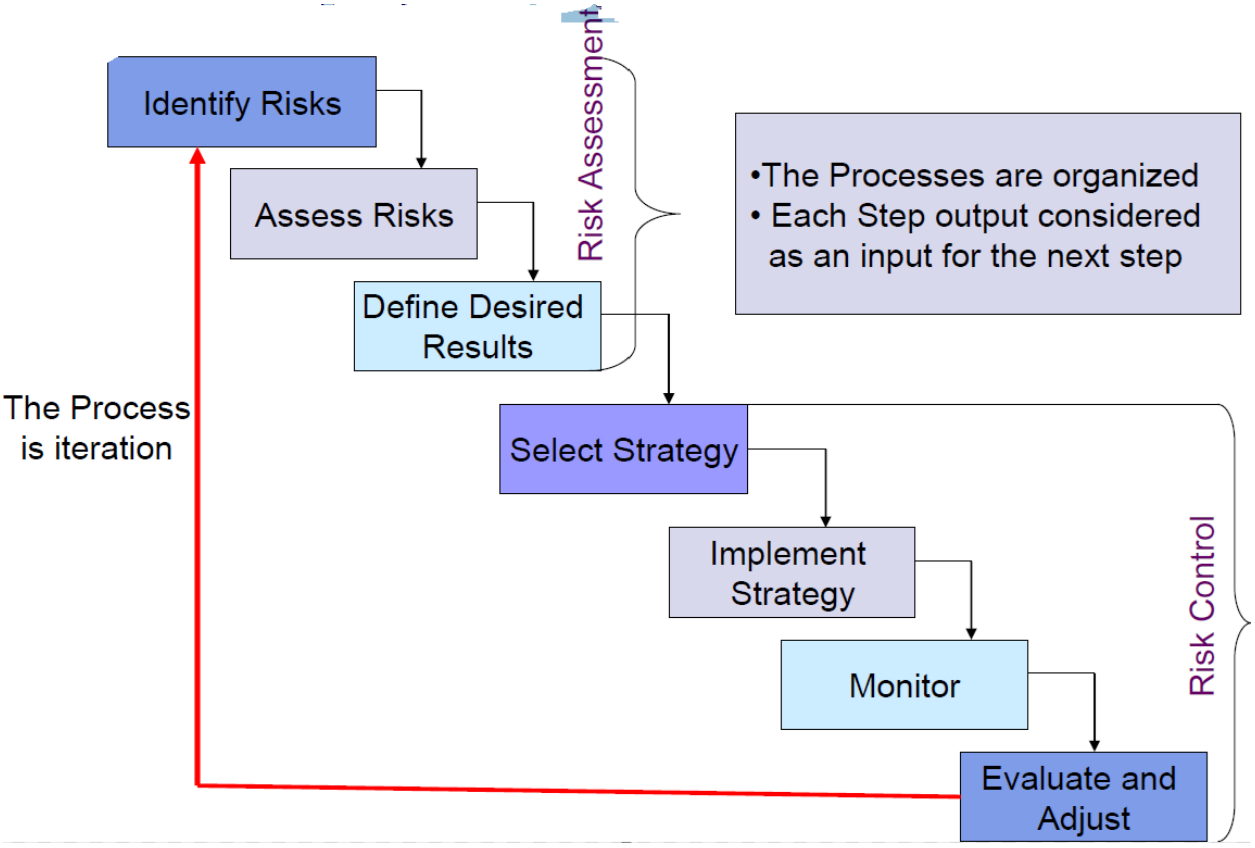

Figure 2: Risk management life cycle

3. Information Assesst:

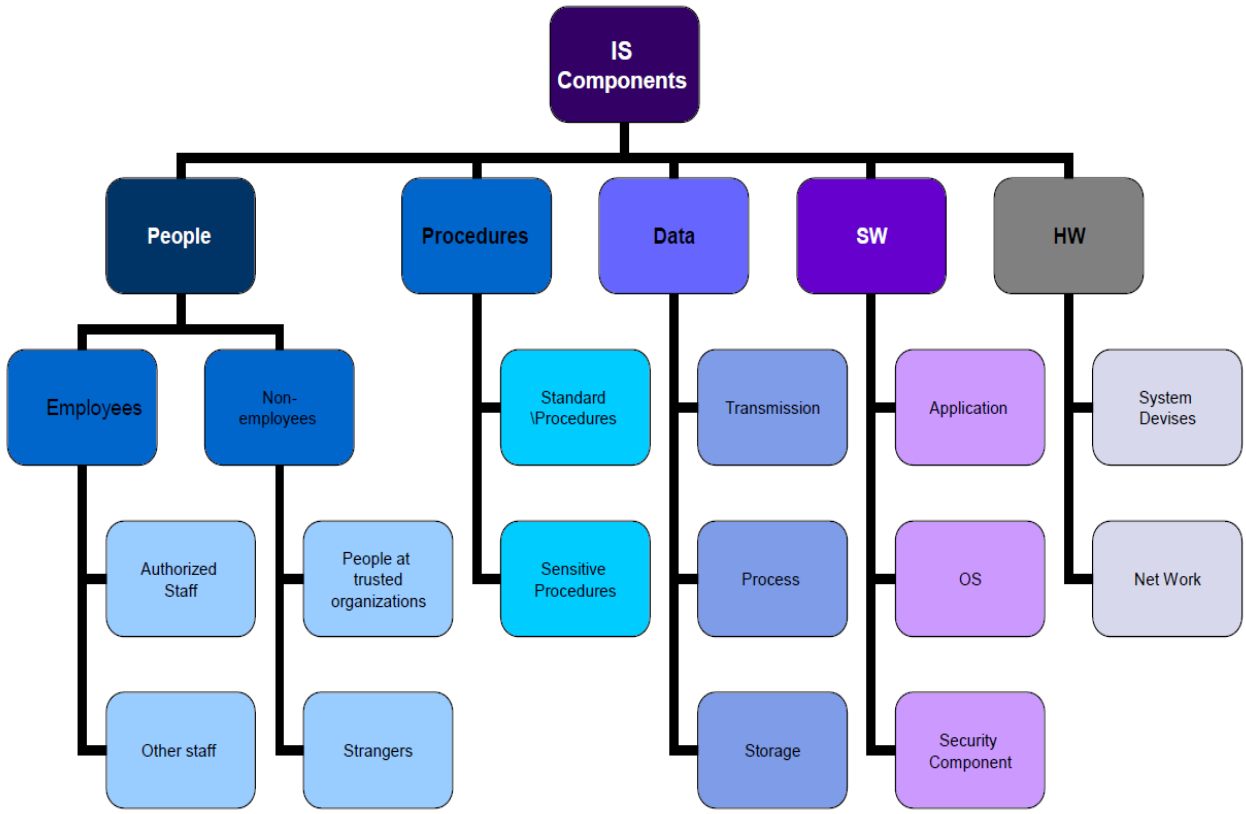

Figure 3: Information assess component

4. Primary Sources of Risk Items

They can be categorized by their origin:

✓ **Internal**:

Risks that arise from within the organization and are often more controllable.

- **Human Threats** This refers to risks caused by the actions (intentional or accidental) of employees, contractors, or anyone inside the organization. **Examples from list:** unauthorized access (e.g., by a disgruntled employee).

- **Network-Based Attacks** This category includes technical and internal environmental failures. While the *attack* may be launched from outside, the *vulnerability* is internal. **Examples from list:** virus infection (often introduced through internal user error or lack of protections), Power failure (of internal systems or backup generators), pollution (e.g., chemical contamination from an on-site source, or internal air quality issues)

✓ **External:**

Risks that originate from outside the organization and are generally less controllable.

- **Natural Threats**. Examples floods, Earthquakes, hurricanes.
- **Environmental Threats (External)** This includes broader environmental issues that originate outside the organization's premises. **Examples from list:** pollution (e.g., from a neighboring industrial accident, smog), Power failure (a widespread grid blackout).
- **Human Threats (External)**: This involves malicious actors from outside the organization targeting it. **Examples from list:** network-based attacks (e.g., by external hackers), unauthorized access (by outsiders), virus infection (from external sources like malicious websites or emails).

For the following short scenarios determine the risk source?

1. *A company's software project is delayed due to lack of skilled staff.*
2. *A government introduces new data privacy regulations affecting your business operations.*

Solutions:

1. *Internal risk source / Human threats*
2. *External risk source*

5. Methods of Risk Assessment

Methods of risk assessment include:

a) Qualitative Methods (Most Common)

These are based on *judgment*, *experience*, and *intuition*. They are faster and easier to perform but are *subjective*.

- **Risk Matrix:** The most widely used method.
- **How it works:**

  Risks are plotted on a matrix based on their **Likelihood** (e.g., Rare, Unlikely, Possible, Likely, Almost Certain) and **Impact** (e.g., Insignificant, Minor, Moderate, Major, Catastrophic).
- **Output:**

  A visual map that prioritizes risks into zones (e.g., Low, Medium, High, Extreme).
- **Best for:** General project management, workplace safety, initial screening of risks.

- **Common Risk Matrix Size:**

Matrix Size	Best For	Characteristics	Pros	Cons
3x3	Small projects, teams, or initial high-level screening.	Three levels for Likelihood & Impact (e.g., High, Medium, Low).	Very simple and fast	High clustering in the "Medium" category
4x4	Projects of moderate complexity needing a middle ground.	Four levels for Likelihood & Impact (e.g., Low, Moderate, High, Critical).	Clearer distinction between levels than 3x3	May still lack nuance for complex risks
5x5	Complex projects and larger organizations. Considered the industry standard.	Five levels for Likelihood & Impact (e.g., Rare, Unlikely, Possible, Likely, Almost Certain / Insignificant, Minor, Moderate, Major, Catastrophic).	Enables meaningful prioritization	Slightly more complex than smaller matrices
6x6 or Larger	High-risk, high-reliability industries (e.g., aerospace, nuclear, healthcare).	Highly granular scoring with six or more levels.	Allows for very fine distinctions between risks	Can be overly complex

b) <u>Quantitative Methods</u>

These rely on *numerical data* and *calculations*. They are more *objective* but require good data and can be time-consuming.

- **Monte Carlo Simulation:**
  - **How it works:**

Uses computer models to run thousands of simulations for a project, varying input parameters (like task duration or cost) based on their probability distributions.

- **Output:**

  A probability distribution of potential outcomes (e.g., "There is a 90% chance the project will finish by July 1").

- **Best for:**

  Complex project scheduling, cost estimation, and financial modeling.

c) Semi-Quantitative

d) Hybrid approach combining descriptive and numerical methods.

4.1 How to choose the best risk assessment method?

Often, the most effective approach is to start with a qualitative method (like a Risk Matrix) to screen and prioritize risks, and then apply a quantitative method (Monte Carlo) to the most critical "high-priority" risks for a deeper, more rigorous analysis.

4.2 Uses of Quantitative vs. Qualitative Risk Measurement

Quantitative risk measurement is the standard approach used in many fields such as insurance and finance; however, it is not commonly applied to measuring risk in information systems. *There are several reasons for this limitation:*

1. **Difficulty in identifying and assigning accurate numerical values** to all components involved in information system risks.
2. **Moral and human factors** (such as user behavior or intent) cannot be effectively measured using quantitative methods.
3. **Lack of sufficient statistical data** to determine the frequency or probability of specific information system incidents.

Therefore, most modern **risk assessment tools** used in information systems rely on **qualitative risk measurement**, which uses descriptive categories (such as *low, medium, or high*) instead of numerical values to evaluate risk levels.