

Assets, Threats, Vulnerabilities, and Risks

- An **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 accidentally, 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 a potential for loss, damage, or destruction of an asset when a threat exploits a vulnerability.

Risk Equation: $\text{Risk} = \text{Threat} \times \text{Vulnerability}$

Introduction to Risk Management

The Basic Definition

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

My Expanded Definition

- **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

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

Risk Assessment

- A **risk assessment**, where risks are identified and assessed, is the first step in the risk management process.
- **Example Risk Assessment Process:**
 1. Identify and categorize your risks
 2. Assess each risk's probability and impact
 3. Assign each risk a risk score and prioritize accordingly
 4. Respond Accordingly

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 (3)	3	6	9
	Moderate (2)	2	4	6
	Low (1)	1	2	3
		Low (1)	Moderate (2)	High (3)

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.
- **Transference:** Transferring the responsibility of a risk to a third party, such as insurance.
- **Residual Risk:** The risk that remains when after risk mitigation or transference activities have taken place.