Risk Mitigate VS Risk Prevent

- Access control concept
    - Acces is based on three concept
        - Subjects
        - Objects
        - Rules
    - Defense
        - It's an information strategy that integrates people, technology & operations capabilities to establish barriers across multiple countermeasures in a layered process to fulfill security objectives.
        - And it should be implemented to prevent or deter a cyber attack
        - It's not guaranteed that an attack will not occur.
    - Privileged Access Management:
        - Reduce risk by allowing minimal usage of admin users.
        - Confirms the availability by providing administrative access when needed.
    - Understand Logical Access Controls:
        - **Discretionary access control:** A certain amount of access control is left to the discretion of the object owner.
        - **Mandatory access control:** Access control that requires the system itself to manage the access controls in accordance with the organization's security policies.
        - **Role-based access control:** An access control system that is based on user role.
        - **Logical Access control:** An automated system that controls an individual access to one or more computer resources, it requires the validation of individual identity with some authorization mechanism.
        - **ABAC (Attribute-Based Access Control):** It is an access control model that uses attributes to make access control decisions. In ABAC, access rights are granted to users based on the attributes associated with the user, the resource being accessed, and the environment in which the access attempt is made. ABAC offers a flexible and dynamic approach to access control, allowing organizations to define fine-grained access control policies based on a wide range of attributes. This model enables organizations to enforce access control policies that are aligned with their specific business requirements, regulatory compliance needs, and security objectives.
        - **Policy-Based Access Control (PBAC):** It is a component of the Policy-Based Access Control (PBAC) model, which is used for making access control decisions based on defined policies.
        - **Time-Based Access Control (TBAC):**

- **Insider Threat:** An entity with authorized access that has the potential to harm an information system through disclosure, destruction, modification of data or denial of service.
- **Layered Defense:** The use of multiple controls arranged to a series to provide consecutive control to protect an asset.

- **Principle of least privilege:** User & program should have only the minimum privilege necessary to complete the task.
- **Ransomware:** A type of malicious software that locks the computer files and prevents or limiting a user from accessing them until money is paid..
- **Segregation of Duties:** A primary idea is to distribute tasks and responsibilities among different individuals within an organization, so that no single person has too much access to the system.
- **User Provisioning:** The process of creating, maintaining and deactivating the user identities to the system.
- **PII:** Personal Identifiable Information
- **PHI:** Protected Health Information
- **PIN:** Personal Identification Number
- **Privacy:** Is the right of an individual to control the distribution of information about themselves.
- **Risk**: Risk assessment -> analysis -> mitigation -> remediation and communication

Risk Management Terminology:

- **Risk Identification:** Find The risk
- **Risk Assessment:** Risk assessment is a crucial process in the field of risk management, and it involves identifying, analyzing, and evaluating potential risks that may impact an organization's objectives. The goal of risk assessment is to provide decision-makers with information to make informed choices about how to manage or mitigate risks effectively.
- **Risk Treatment:**
    - Avoidance
    - Acceptance
    - Mitigation
    - Transfer

- **Risk Prioritization:**
    - Risk Qualitative Analysis
    - Risk Quantitative Analysis
- **Risk Tolerance:** Ability or willingness to withstand or accept the uncertainty or potential losses associated with various tasks.

Understand Security Control:

- Physical Control: Physical security
- Administrative Control: All kinds of policy, procedure, guidelines, rules & regulation.
- Technical Control: All kinds of logical access control