- Security Posture: An organization's ability to manage its defenses of critical assets and data, and react to change.
- **CISSP Security Domains:**
  - **Security & Risk Management focused on defining:**
    - Security goals and Objectives.
    - Compliance.
    - Legal Regulations.
    - Risk Mitigation: the process of having the right procedures and rules in place to quickly reduce the impact of a risk.
    - Business Continuity: An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans.
  - **Asset Security focused on:**
    - Securing digital and physical assets.
    - Storage, maintenance, retention, and destruction of data.
  - **Security Architecture & Engineering focused on:**
    - Ensuring effective tools, systems, and processes are in place to protect organization's assets and data.
    - Shared responsibility: all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security.
  - **Communication & Network Security focused on**
    - Securing and managing physical networks and wireless communications.

- **Identity & Access Management (IAM):**
  - Focused on access and authorization.
  - Has 4 main components:
    - Identification.
    - Authentication
    - Authorization
    - Accountability.
- **Security Assessment & Testing focused on:**
  - Conducting security control testing
  - Collecting and analyzing data
  - Conducting security audits
- **Security Operations focused on:**
  - Conducting investigations
  - Implementing preventative measures.
- **Software Development Security focused on:**
  - Using secure coding practices.

❖ Threat is any circumstance or event that can negatively impact assets

❖ Social Engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.

❖ Risk is anything that can impact confidentiality, integrity, or availability of an asset.

❖ **Asset risk levels:**

- **Low-Level:**
  - Wouldn't harm the organization's reputation or ongoing operations.
  - Wouldn't cause financial damage if compromised.
- **Medium-Level:**
  - May cause some damage to the organization's finance, reputation, or ongoing operations.

- **High-Level:**
  - Information protected by regulations or laws.
  - If compromised, it would have a severe negative impact on an organization's finances, reputation, or ongoing operations.

❖ Vulnerability is a weakness that can be exploited by a threat.

❖ Ransomware is a malicious attack where a threat actor encrypt an organization's data and demand payment to restore access.

❖ **NIST Risk Management Framework (RMF) Steps:**

- Prepare: activities that are necessary to manage security and privacy risks before a breach occurs.
- Categorize: used to develop risk management processes and tasks.
- Select: choose, customize, and capture documentation of the controls protect an organization.
- Implement: implement security and privacy plans to the organization.
- Assess: determine if established controls are implemented correctly.
- Authorize: being accountable for the security and privacy risks that may exist in an organization.
- Monitor: be aware of how the systems are operating.