- Asset Management: the process of tracking assets and risks that affects them.
- Asset Inventory: A catalog of assets that need to be protected.
- Asset Classification: The practice of labeling assets based on sensitivity and importance to an organization.
    - Public: can be shared with anyone outside the organization.
    - Internal-Only: can be shared only with people inside the organization
    - Confidential: should only be accessed by those who working on a specific project.
    - Restricted: very highly sensitive and considered as need-to-know.
- Data is information that is translated, processed, or stored by a computer.
- **Data states:**
    - In use: being accessed by one or more users.
    - In transit: travelling from one point to another.
    - At rest: not currently being accessed or travelling.
- Information Security (InfoSec): The practice of keeping data in all states away from unauthorized users.
- **Elements of Security Plan:**
    - Policies: a set of rules that reduces risk and protects information.
    - Standards: references that inform how to set policies.
    - Procedures: step-by-step instructions to perform a specific security task.

- NIST Cybersecurity Framework (CSF): a voluntary framework that consists of standards, guideline, and best practices to manage security risk.
- **NIST CSF Components:**
  - Core: a simplified version of the functions (or duties), consists of 5 functions: Identify, Protect, Detect, Respond, and Recover.
  - Tiers: provide security teams with a way to measure performance across each of the five functions of the core, has 4 levels:
    - Level-1 (Passive): a function that is reaching bare minimum standards.
    - Level-4 (Adaptive): a function that is being performed at an exemplary standards.
  - Profiles: provides insight into the current state of a security plan.