- **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF):**
  - A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk
  - **Has 5 core functions:**
    - Identify: related to management of cybersecurity risk and its effect on an organization's people and assets
    - Protect: used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats
    - Detect: related to identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections
    - Respond: related to making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process
    - Recover: related to returning affected systems back to normal operation
- NIST Special Publication (S.P.) 800-53: A unified framework for protecting the security of information systems within the U.S. federal government

- **Open Web Application Security Project/Open Worldwide Application Security Project (OWASP):**
  - A non-profit organization focused on improving software security
  - **Has several principles:**
    - Minimize attack surface area: Attack surface refers to all the potential vulnerabilities a threat actor could exploit.
    - Principle of least privilege: Users have the least amount of access required to perform their everyday tasks.
    - Defense in depth: Organizations should have varying security controls that mitigate risks and threats.
    - Separation of duties: Critical actions should rely on multiple people, each of whom follow the principle of least privilege.
    - Keep security simple: Avoid unnecessarily complicated solutions. Complexity makes security difficult.
    - Fix security issues correctly: When security incidents occur, identify the root cause, contain the impact, identify vulnerabilities, and conduct tests to ensure that remediation is successful.
    - Establish secure defaults: the optimal security state of an application is also its default state for users; it should take extra work to make the application insecure.
    - Fail securely: means that when a control fails or stops, it should do so by defaulting to its most secure option.
    - Don't trust services: the organization shouldn't explicitly trust that their third-party partners' systems are secure.
    - Avoid security by obscurity: The security of an application should not rely on keeping the source code secret.

- Attack vectors: The pathways attackers use to penetrate security defenses
- Authentication: The process of verifying who someone is
- Authorization: The concept of granting access to specific resources in a system
- Biometrics: The unique physical characteristics that can be used to verify a person's identity
- Encryption: The process of converting data from a readable format to an encoded format