

# Glossary terms from week 2

## Terms and definitions from Course 2, Week 2

**Asset:** An item perceived as having value to an organization

**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

**Availability:** The idea that data is accessible to those who are authorized to access it

**Biometrics:** The unique physical characteristics that can be used to verify a person's identity

**Confidentiality:** The idea that only authorized users can access specific assets or data

**Confidentiality, integrity, availability (CIA) triad:** A model that helps inform how organizations consider risk when setting up systems and security policies

**Detect:** A NIST core function related to identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections

**Encryption:** The process of converting data from a readable format to an encoded format

**Identify:** A NIST core function related to management of cybersecurity risk and its effect on an organization's people and assets

**Integrity:** The idea that the data is correct, authentic, and reliable

**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

**National Institute of Standards and Technology (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

**Protect:** A NIST core function used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats

**Recover:** A NIST core function related to returning affected systems back to normal operation

**Respond:** A NIST core function related to making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process

**Risk:** Anything that can impact the confidentiality, integrity, or availability of an asset

**Security audit:** A review of an organization's security controls, policies, and procedures against a set of expectations

**Security controls:** Safeguards designed to reduce specific security risks

**Security frameworks:** Guidelines used for building plans to help mitigate risk and threats to data and privacy

**Security posture:** An organization's ability to manage its defense of critical assets and data and react to change

**Threat:** Any circumstance or event that can negatively impact assets

---

Revision #1

Created 14 June 2023 08:45:45 by naruzkurai

Updated 14 June 2023 08:45:54 by naruzkurai