Glossary terms from module 1

Terms and definitions from Course 2, Module 1

Assess: The fifth step of the NIST RMF that means to determine if established controls are implemented correctly

Authorize: The sixth step of the NIST RMF that refers to being accountable for the security and privacy risks that may exist in an organization

Business continuity: An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans

Categorize: The second step of the NIST RMF that is used to develop risk management processes and tasks

External threat: Anything outside the organization that has the potential to harm organizational assets

Implement: The fourth step of the NIST RMF that means to implement security and privacy plans for an organization

Internal threat: A current or former employee, external vendor, or trusted partner who poses a security risk

Monitor: The seventh step of the NIST RMF that means be aware of how systems are operating

Prepare: The first step of the NIST RMF related to activities that are necessary to manage security and privacy risks before a breach occurs

Ransomware: A malicious attack where threat actors encrypt an organization’s data and demand payment to restore access

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

Risk mitigation: The process of having the right procedures and rules in place to quickly reduce the impact of a risk like a breach

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

Select: The third step of the NIST RMF that means to choose, customize, and capture documentation of the controls that protect an organization

Shared responsibility: The idea that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security

Social engineering: A manipulation technique that exploits human error to gain private information, access, or valuables

Vulnerability: A weakness that can be exploited by a threat