

# Glossary

## Cybersecurity

---



### A

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

**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

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

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

### B

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

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

## C

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

**Chronicle:** A cloud-native tool designed to retain, analyze, and search data

**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

## D

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

## E

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

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

## I

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

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

**Incident response:** An organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach

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

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

## L

**Log:** A record of events that occur within an organization's systems

## M

**Metrics:** Key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application

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

## N

**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

## O

**Open Web Application Security Project/Open Worldwide Application Security Project (OWASP):** A non-profit organization focused on improving software security

**Operating system (OS):** The interface between computer hardware and the user

## P

**Playbook:** A manual that provides details about any operational action

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

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

## R

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

**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

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

## S

**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 information and event management (SIEM):** An application that collects and analyzes log data to monitor critical activities in an organization

**Security orchestration, automation, and response (SOAR):** A collection of applications, tools, and workflows that use automation to respond to security events

**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

**Splunk Cloud:** A cloud-hosted tool used to collect, search, and monitor log data

**Splunk Enterprise:** A self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time

## T

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

## V

**Vulnerability:** A weakness that can be exploited by a threat

---