

# Glossary terms from module 1

---

## Terms and definitions from Course 3 Module 1

**Attack vectors:** Pathways attackers use to penetrate security defenses

**Attribute-based access control (ABAC):** A security model where access is granted based on attributes, like user, resource, and environment

**Auditing:** The process of recording and reviewing system activity to ensure compliance with security policies, and identifying potential security breaches

**Authentication:** The process of verifying who someone is

**Authentication, authorization, and auditing (AAA):** A security framework that is used to verify the identity of users or groups in computer systems, and grant them access based on their privileges

**Authorization:** The concept of granting access to specific resources in a system

**Context-aware access controls:** Decisions about granting or denying access to resources are based on the user's identity and contextual information

**Discretionary access control (DAC):** A security model where the owner of the data or resource has the discretion to grant or revoke access to other users

**Identity and access management services (IAM):** A collection of processes and technologies that helps organizations manage digital identities in their environment

**Mandatory access control (MAC):** A strict security model where access is granted based on predefined security policies

**Micro-segmentation:** A security technique that divides a network into smaller, isolated segments

**Multi-factor authentication (MFA):** A security measure that requires a user to verify their identity in two or more ways to access a system or network

**Mutual Transport Layer Security (mTLS):** A protocol that provides mutual authentication and encryption between servers

**Network access control (NAC):** A security solution that enforces policy-based access control to network resources, ensuring that only authorized devices and users can access the network

**Open Authorization (OAuth):** A method that allows users to grant applications access to their information on other sites or systems, without the need to share their passwords

**OpenID:** A protocol that is used for single sign-on functionality, allowing users to authenticate once, and access multiple services

**Perimeter protection:** The security measures implemented at the edge of a network or system to defend against unauthorized access and cyber threats

**Role-based access control (RBAC):** A method of controlling access to resources based on the roles assigned to users

**Secrets:** Sensitive information like Application Programming Interface (API) keys, passwords, and certificates that are used to authenticate and authorize access to systems

**Single sign-on (SSO):** A technology that combines several different logins into one