Chapter 3 - Key Terms

Term	Page	Description
Subject	588	The active entity that requests access to an object. The subject usually performs requests on behalf of the principal.
Object	585	A passive entity that is, or contains information needed by the subject. The role of the subject or object is purely determined by the entity that requests access.
Access Control	577	The process of granting, preventing, or revoking access to an object.
Identification	582	The process of providing identity to the access control enforcer.
Authentication	578	The process of proving the identity of an entity.
Authorization	578	The process of providing access to a resource with specific access rights.
Accounting	577	The process of auditing and monitoring user operations on a resource.
Asset Classification	577	The process of classifying an asset or data based on the potential damage a breach of the confidentiality, integrity, or availability of that data could cause.
Information or Data Owner	583	The person who maintains ownership and responsibility over a specific piece or subset of data. Part of the responsibility of this role is to determine the appropriate classification of the information, ensure that the information is protected with controls, periodically review classification and access rights, and understand the risk associated with the information he or she owns. Together with senior management, the information or data owner holds the responsibility for the security on the asset.
Discretionary Access Control (DAC)	580	An access control model where the access decision and permission are decided by the object owner.
Mandatory Access Control (MAC)	584	An access control model where the access decision is enforced by the access policy enforcer (for example, OS). Uses labels.

Term	Page	Description
Role-Based Access Control (RBAC)	587	An access control model where the access decision is based on the role or function of the subject.
Attribute-Based Access Control (ABAC)	578	An access control model where the access decision is based on the attributes or characteristics of the subject, object, and environment.
Network-Based Intrusion Prevention	585	A system or software designed to detect and prevent cybersecurity threats by analyzing network traffic.
Host-Based Intrusion Prevention System (HIPS)	582	Specialized software that interacts with the host operating system to provide access control and threat protection. In most cases, it also includes network detection and protection capabilities on the host network interface cards. If there are no prevention capabilities but the system can only detect threats, it is referred to as a host-based intrusion detection system (HIDS).
Antivirus & Antimalware	577	Terms generally used interchangeably to indicate software that can be used to detect and prevent the installation of computer malware and in some cases quarantine affected computers or eradicate the malware and restore the operation of the system.
Untitled		