Chapter 7 - Key Terms

Term	Page	Description
Identity & Access Management (IAM)	582	A collection of policies, processes, and technology to manage identity, authentication, & authorization to organization resources.
Password Management	585	A collection of processes, policies, and technologies that helps an organization and users improve the security of their password authentication systems. It includes policies and technologies around password creation, password storage, and password reset.
One-time Password (OTP)	585	A password, randomly generated, that can be used only once.
Directory	580	Repository used by an organization to store information about users, systems, networks, and so on. Information stored in directories can be used with the purpose of identifying and authenticating users, as well to apply security policies and authorization.
Directory Service	580	A service that uses directories to provide an organization with a way to manage identity, authentication, and authorization services.
ITU-T X.500	583	A collection of standards including information on the organization of directories and protocols to access the information within the directories.
Lightweight Directory Access Protocol (LDAP)	584	Protocol—a protocol based on X.500 that maintains the same directory structure and definition. It simplifies the directory queries, and it has been designed to work with the TCP/IP stack.
Single-Sign On (SSO)	587	An authentication system that allows users to authenticate with only one system and only once to get access to organization resources.

Term	Page	Description
Federated SSO	582	A further evolution of a single sign-on (SSO) model within one organization. In this model a user could authenticate once and then obtain access to resources across multiple organizations. This type of authentication is built upon trust between two different domains that are not managed under the same IAM system. An example is when you authenticate to a website using the credentials of a social networking platform or a well-known platform such as Facebook, Google, Amazon, or GitHub.
Log Collection	584	The process of collecting and organizing logs for analysis. A log collector is software that is able to receive logs from multiple sources and in some cases offer storage capabilities and logs analysis functionality.
Security Information and Event Manager (SIEM)	587	A specialized device or software for security event management. It typically includes logs collection, normalization, aggregation and correlation capabilities, and built-in reporting.
Asset	577	Anything that has value for an organization. In simple terms an asset can be any organization resource, including personnel, hardware, software, building, and data.
Asset Management	578	In information security, policies, processes, and technologies to manage and protect organization assets during their life cycle.
Asset Inventory	578	The collection and storage of information about assets, such as location, security classification, and owner.
Asset Ownership	578	The process of assigning an owner to an asset. Each asset within the organization needs an owner. The owner is responsible for the security of the asset during its life cycle.
Asset Classification	577	In information security, the process of classifying an asset or data based on the potential damage a breach to the confidentiality, integrity, or availability of that data could cause.
Asset Handling	577	In information security, procedures and technologies that allow the secure storage, use, and transfer of an asset.

Term	Page	Description
Enterprise Mobile Management (EMM)	581	Policies, processes, and technologies that allow the secure management of mobile devices. Technologies that enable BYOD, Mobile Device Management (MDM), and Mobile Applications Management (MAM) are examples of areas covered by an organization’s EMM.
Configuration Management	579	A process concerned with all policies, processes, and technologies used to maintain the integrity of the configuration of a given asset.
Configuration Item (CI)	579	An identifiable part of the system that is the target of the configuration control process.
Configuration Record	579	A collection of attributes and relationship of a configuration item.
Configuration Management Database	579	A database that stores configuration items and configuration records.
Security Baseline Configuration	587	A set of attributes and configuration items related to a system that has been formally reviewed and approved. It can be changed only with a formal change process.
Change Management	579	A process concerned with all policies, processes, and technologies that handle a change on an asset life cycle.
Change	579	Any modification, addition, or removal of an organizational resource, for example, of a configuration item. A common categorization includes Standard, Emergency, and Normal changes.
Request For Change (RFC)	586	A formal request that usually includes a high-level description of the change, the reason for the change, and other information.
Vulnerability Management	589	The process of identifying, analyzing, prioritizing, and remediating vulnerabilities in software and hardware.
Common Vulnerabilities & Exposures (CVE)	579	A dictionary of vulnerabilities and exposures in products and systems maintained by MITRE. A CVE-ID is the industry standard method to identify vulnerabilities.
Vulnerability Scanner	589	Software that can be used to identify vulnerabilities on systems.

Term	Page	Description
Penetration Assessment	586	Also called a pen test. It is used to test an exploit of a vulnerability. Besides trying to exploit known vulnerabilities, a penetration test may also be able to find unknown vulnerabilities in a system.
Common Vulnerability Scoring System (CVSS)	579	An industry standard used to convey information about the severity of vulnerabilities.
Patch Management	585	The process of identifying, acquiring, installing, and verifying patches for products and systems.
Security, Orchestration, Automation, & Response (SOAR)	587	A system that provides automation and security orchestration capabilities for the security operations center (SOC).
Untitled		