6.1.4 Access Control Best Practices

This lesson covers the following topics:

- Access control best practices
- Transition best practices

Access Control Best Practices

Access control best practices take into consideration the following security principles and concepts:

Principle	Description
Principle of least privilege	The *principle of least privilege* states that users or groups are given only the access they need to do their jobs and nothing more. Common methods of controlling access include: ▪ *Implicit deny* denies access to users or groups who are not specifically given access to a resource. Implicit deny is the weakest form of privilege control. ▪ *Explicit allow* specifically identifies users or groups who have access. Explicit allow is a moderate form of access control in which privilege has been granted to a subject. ▪ *Explicit deny* identifies users or groups who are not allowed access. Explicit deny is the strongest form of access control and overrules all other privileges granted. When assigning privileges, be aware that it is often easier to give a user more access when the user needs it than to take away privileges that have already been granted. Access recertification is the process of continually reviewing a user's permissions and privileges to make sure the user has the correct level of access.
Need to know	*Need to know* describes the restriction of data that is highly sensitive and is usually referenced in government and military context. Important facts about the need to know include: ▪ Even if an individual is fully cleared, the information will not be divulged unless the person has a need to know the information to perform official duties. ▪ Need to know discourages casual browsing of sensitive materials. ▪ In a classified environment, a clearance into a top secret compartment allows access to only certain information within that compartment. This is a form of mandatory access control (MAC).
Separation of duties	*Separation of duties* is the concept of having more than one person required to complete a task. This is a preventive principle primarily designed to reduce conflicts of interest. It also prevents insider attacks because no one person has end-to-end control and no one person is irreplaceable. Important facts to know about separation of duties include: ▪ System users should have the lowest level of rights and privileges necessary to perform their work and should have those privileges only for the shortest length of time possible. ▪ To achieve a separation of duties, a business can use the principle of split knowledge. This means that no single person has total control of a system's security mechanisms; no single person can completely compromise the system. ▪ In cases of sensitive or high-risk transactions, a business can use two-man controls. This means that two operators must review and approve each other's work.
Job rotation	*Job rotation* is a technique where users are cross-trained in multiple job positions.

	Responsibilities are regularly rotated between personnel. Job rotation: - Cross trains staff in different functional areas in order to detect fraud. - Exchanges positions of two or more employees to allow for oversight of past transactions. - Can be used for training purposes.
Defense-in-depth	*Defense-in-depth* is an access control principle which implements multiple access control methods instead of relying on a single method. Multiple defenses make it harder to bypass security measures.
Identification	*Identification* is the act of claiming an identity, such as telling someone your name. Important facts to know about identification include: - In the computer world, a username is a form of identification. - Because anyone could pretend to be the user, identification by itself is not very secure. - To substantiate identity, the person must provide some form of identity verification.
Multi-Factor Authentication	*Multi-Factor Authentication* is the process of using more than one way to verify identity. In the computer world, Multi-Factor Authentication is achieved by requiring two or more methods that only the user can provide. Five categories of computer system authentication include: - Something you are, such as biometric information (e.g., fingerprint or retina scan). - Something you have, such as smart cards, RSA tokens, or security key fobs. - Something you know, such as passwords and PINs. - Somewhere you are, such as a geographical location. - Something you do, such as how you type a sentence on a keyboard.
Mutual authentication	*Mutual authentication* is when two communicating entities authenticate each other before exchanging data. It requires not only the server to authenticate the user, but the user to authenticate the server. This makes mutual authentication more secure than traditional, one-way authentication.

Transition Best Practices

Organizations should follow strict guidelines when an employee transitions out of a position or into a new position.

Creeping privileges occur when a user's job position changes and the user is granted a new set of access privileges, but the user's current access privileges are not removed or modified, resulting in privilege escalation. As a result, the user accumulates privileges that are not necessary for the current work tasks. The principle of least privilege and separation of duties are countermeasures against creeping privileges.

To avoid creeping privileges and to best protect the security of information, the following precautions should be taken in each stage of the account's life cycle:

Event	Precautions
Account creation	When an account is created, apply the appropriate access rights based on the job role as implemented in the access control system. Use the principle of least privilege and grant only the

	minimum privileges required to perform the duties of the position.
Active accounts	During the life of an account: ▪ Modify access rights as job roles and circumstances change. ▪ Monitor password resets and lockouts to ensure account security. ▪ Re-evaluate access rights on a periodic basis.
Old accounts	When an account is no longer needed, take appropriate actions to: ▪ Delete accounts that will no longer be used. ▪ Rename accounts to give new users in the same job role the same access privileges. ▪ Lock accounts that will not be used for extended periods to prevent them from being used. ▪ Remove unnecessary rights from accounts that will be kept on the system. ▪ Archive important data or files owned by the user, or assign ownership to another user. ▪ Prohibit the use of generic user accounts, such as the Guest or Administrator users on Windows systems. End-of-life procedures should include not only deactivating or deleting unused accounts, but also destroying data that might remain on storage media. This will prevent sensitive data from being accessible to unauthorized users.