2.3.3 Access Control Best Practices

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

Principles	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 job (and nothing more). Common methods of controlling access include: ▪ With *implicit deny*, users or groups who are not specifically given access to a resource are denied access. 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 they need 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 they have 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 to know about need to know include: ▪ Even if an individual is fully cleared, information is still not divulged to persons who simply don't need to know the information to perform their official duties. ▪ Need to know discourages casual browsing of sensitive materials. ▪ In a classified environment, a clearance into a Top Secret compartment only allows access to 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 only have them 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, so 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, and where 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 an 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 the security measures.
Identification	*Identification* is merely 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 you, identification by itself is not very secure. ▪ To substantiate a person's identity, they need to provide some verification to prove that they are who they say they are.
Multifactor Authentication	*Multifactor authentication* is the process of proving an identity, confirming a user is who they say they are. In the computer world, authentication is achieved by providing some piece of information that only the actual user can provide. Five categories of computer system authentication include: ▪ Something you are, such as biometric information (e.g., finger print 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	*Mutual Authentication* is when two communicating entities authenticate each other before exchanging data. It requires not only

Authentication	the server to authenticate the user, but the user also to authenticate the server. This makes mutual authentication more secure than traditional, one-way authentication.
Transitive Trust	*Transitive Trust* is the concept that trust is hierarchical. That is, if A trusts B, and B trusts C, then A trusts C. An example of transitive trust use is Microsoft Active Directory, which allows authenticated users access to resources in different domains as long as the parent domain is trusted.
Authentication, Authorization, and Accounting (AAA)	*AAA* includes the following three components: - *Authentication* verifies a user's identity. - *Authorization* is the process of determining whether an authenticated user has permission to carry out a specific task or access a system resource. System administrators decide and then configure the permission scope for users and groups. - *Accounting* tracks the actions of an authenticated user, including access to files and other user activities on the system.

Creeping privileges occurs when a user's job position changes and they are granted a new set of access privileges and their previous access privileges are not removed or modified, resulting in *privilege escalation*. As a result, the user accumulates privileges over time that are not necessary for their 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 against corruption of information, the following precautions should be taken in each stage of the account's life cycle:

- 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.
- During the life of the 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.
- 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 to prevent sensitive data from being accessible to unauthorized users.

- For media intended for reuse in the same security environment, perform a *cleaning* by deleting or overwriting the data media. For magnetic media, methods might include:
  - Applying a magnetic field to render the data unreadable (known as *degaussing*). This is the least reliable means to clean or purge media.
  - Overwriting the data with zeros, such as with a tool like Microsoft's **Cipher** command. Simply deleting the files will *not* remove the data from the disk.
- For media intended for use in a different security environment, perform a *drive wipe, purge*, or *sanitization* by overwriting the media a minimum of 7 times with random data.
- For media that has reached the end of its useful life, destroy the media. Media destruction can be accomplished through:
  - Crushing (useful for CDs, DVDs, and hard drives)
  - Incineration (for paper and many other types of media)
  - Acid dipping
  - Shredding using an approved shredding process (straight-cut shredders offer little protection, cross-cut shredders provide greater security)

Because optical media (CDs and DVDs) do not have a magnetic field, they must be physically destroyed.