Accounts:

Information system account types include individual, shared, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

Account rights can be further broken into two categories -

- Common use accounts
- Application, system, and process account
- Elevated rights accounts (Users requiring administrative privileges on information system accounts). These accounts require additional scrutiny -
    1. During the creation process by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer).
    2. Security monitoring to evaluate appropriateness of elevated right usage.
    3. Period re-validation of continuing need for elevated rights.

Key control points are the activation request/approval and termination disabling/deletion procedures.

Authentication:

The process or action of proving or showing something to be true, genuine, or valid before establishing a local, remote, or network connection.

Individual authenticators include passwords, tokens, biometrics, PKI certificates, and key cards.

Multi-factor authentication (MFA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. MFS mechanisms require the use of items from two of the following three general things, Something the individual -

1. Knows (something the user and only the user knows
2. Possesses (something the user and only the user has)
3. Inherits (something the user and only the user is)

The key to the strength of the authentication is the requirements about authenticator content (e.g., password settings, invalid attempt limits, account lockout settings, etc.).