Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin.

Access control are primarily driven by -

- The principle of least privilege, allowing only authorized accesses for users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

- Separation of duties, as a security principle, has as its primary objective the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users. Principally several approaches are optionally viable as partially or entirely different paradigms:

  - Sequential separation (two signatures principle)
  - Individual separation (four eyes principle)
  - Spatial separation (separate action in separate locations)
  - Factorial separation (several factors contribute to completion)