# Lesson 2 – Access Controls

## Quiz Questions

1. Logical or technical controls involve the restriction of access to systems and the protection of information. Which of the following statements pertaining to these types of controls is correct?
   1. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks but do not include a review of vacation history, and also do not include increased supervision.
   2. Examples of these types of controls do not include encryption, smart cards, access lists, and transmission protocols.
   3. Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.
   4. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.
2. In addition to the accuracy of the biometric systems, there are other factors that must also be considered:
   1. These factors include the enrolment time and the throughput rate, but not acceptability.
   2. These factors do not include the enrolment time, the throughput rate, and acceptability.
   3. These factors include the enrolment time, the throughput rate, and acceptability.
   4. These factors include the enrolment time, but not the throughput rate, neither the acceptability.
3. What is the most critical characteristic of a biometric identifying system?
   1. Perceived intrusiveness
   2. Storage requirements
   3. Accuracy
   4. Reliability
4. Which of the following does not apply to system-generated passwords?
   1. Passwords are harder to remember for users.
   2. If the password-generating algorithm gets to be known, the entire system is in jeopardy.
   3. Passwords are more vulnerable to brute force and dictionary attacks.
   4. Passwords are harder to guess for attackers.
5. What is the main concern with single sign-on?
   1. Maximum unauthorized access would be possible if a password is disclosed.
   2. The security administrator's workload would increase.
   3. The users' password would be too hard to remember.
   4. User access rights would be increased.
6. Which access control model enables the OWNER of the resource to specify what subjects can access specific resources?
   1. Discretionary Access Control
   2. Mandatory Access Control
   3. Sensitive Access Control
   4. Role-based Access Control
7. Intrusion Detection (ID) is a:
   1. preventive control.
   2. deterrent control.(if people know it’s there)
   3. recovery control.
   4. directive control.

8) In biometrics, a “one-to-one” search to verify an individual’s claim of an identity is called:

* 1. Audit trail review
  2. Authentication
  3. Accountability
  4. Aggregation

9) Kerberos is an authentication scheme that can be used to implement:

* 1. Public key cryptography
  2. Digital signatures
  3. Hash functions
  4. Single Sign-On (SSO)

10) An attack that uses a detailed listing of common passwords and words in general to gain unauthorized access to an information system is BEST described as:

* 1. Password guessing
  2. Software exploitation
  3. Dictionary attack
  4. Spoofing