Questions IT Security

1. What are the protection objectives of information security?
   a. **Confidentiality, Integrity, Availability, Authenticity, Commitment**
   b. Accessibility, Respect, Feasibility, Probability, Prevention
   c. Recognition, Security, Encryption, Systematization, Digitization
   d. Risk reduction, reaction, damage limitation, communication, security

2. What types of encryption are there?
   a. **Symmetric and asymmetric encryption**
   b. Normal and abnormal encryption
   c. Right and left encryption
   d. Horizontal and Vertical Encryption

3. What does symmetric encryption mean?
   a. **Same key for encryption and decryption**
   b. Public key for encryption and private key for decryption
   c. Exchanging a generated session key across multiple systems
   d. Private key for encryption and public key for decryption

4. Is there an absolute saftey?
   a. **No, there is no absolute safety**
   b. Yes, there is absolute safety
   c. It depends on which people work with it
   d. It depends on which data is used

5. What do the letters R, E and S in the equation R = E * S mean?
   a. **Risk, probability, amount of the potential loss**
   b. Redundancy, Entity, Service
   c. Risk, Effect, Safety
   d. Reaction, Probability, System

6. What levels of attack are there?
   a. **Networks, applications, users**
   b. Internet, Intranet, Extranet
   c. Mobile devices, television, radio
   d. Antennas, people, computers

7. What are the classifications of security measures?
   a. **Prevention, recognition, reaction**
   b. Securing, connection, accessibility
   c. Safety, reduction, prevention
   d. Damage limitation, safety, communication

8. What does CRC mean?
   a. **Cyclic Redundancy Check**
   b. Cross-Role Check
   c. Control Redundancy Command

d. Convertible Risk Control

9. What does MAC mean?
   a. **Mandatory Access Control**
   b. Multiple Availability Control
   c. Media Authentication Control
   d. Moderate Analysis Control

10. What does DAC mean?
    a. **Discretionary Access Control**
    b. Dictionary Access Control
    c. Discretionary Availability Command
    d. Dictionary Authenticity Command

11. What does RBAC mean?
    a. **Role Based Access Control**
    b. Redundancy Based Access Control
    c. Replay Based Access Control
    d. Reaction Based Access Control

12. What are the passive attack categories?
    a. **Eavesdropping und Traffic Analysis**
    b. Masquerade und Modification
    c. Insertion und Replay
    d. Denial of Service

13. What is meant by the attack category "Denial of Service"?
    a. **The attacker interferes with the availability of communication equipment.**
    b. The attacker changes the communication, delays, changes or deletes messages.
    c. The attacker masquerades as someone else.
    d. The attacker intercepts the communication channel.

14. What is meant by the attack category "Modification"?
    a. **The attacker changes the communication, delays, changes or deletes messages.**
    b. The attacker masquerades as someone else.
    c. The attacker intercepts the communication channel.
    d. The attacker adds messages to a communication.

15. What is meant by the attack category "Masquerade"?
    a. **The attacker masquerades as someone else.**
    b. The attacker intercepts the communication channel.
    c. The attacker adds messages to a communication.
    d. The attacker sends recorded data at a later time once.

16. What is meant by the attack category "Eavesdropping"?
    a. **The attacker listens to the communication channel but does not actively intervene.**
    b. The attacker analyzes the existing data
    c. The attacker masquerades as someone else
    d. The attacker adds messages to a communication.

17. What is meant by the attack category "Insertion"?
    a. **The attacker adds messages to a communication.**
    b. The attacker masquerades as someone else.

c. The attacker sends recorded data at a later point in time once.

d. The attacker intercepts the communication channel.

18. What is meant by the attack category "Replay"?

   a. **The attacker sends recorded data once at a later time**

   b. The attacker adds messages to a communication.

   c. The attacker masquerades as someone else.

   d. The attacker modifies the communication, delays, modifies, or deletes messages.

19. Which ISO family does the security management or security process deal with?

   a. **ISO 27000**

   b. ISO 18000

   c. ISO 36000

   d. ISO 41000