German

1. Welche Schutzziele verfolgt die Informationssicherheit?
    a. **Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Verbindlichkeit**
    b. Zugänglichkeit, Respekt, Durchführbarkeit, Wahrscheinlichkeit, Prävention
    c. Erkennung, Sicherheit, Verschlüsselung, Systematisierung, Digitalisierung
    d. Risikominderung, Reaktion, Schadensbegrenzung, Kommunikation, Sicherung

2. Welche Arten der Verschlüsselung gibt es?
    a. **Symmetrische und asymmetrische Verschlüsselung**
    b. Normale und anormale Verschlüsselung
    c. Rechts und links Verschlüsselung
    d. Waagrechte und senkrechte Verschlüsselung

3. Was bedeutet symmetrische Verschlüsselung?
    a. **Gleicher Schlüssel für Ver- und Entschlüsselung**
    b. Öffentlicher Schlüssel für Ver- und privater Schlüssel für Entschlüsselung
    c. Austausche eines generierten Sitzungsschlüssel über mehrere Systeme
    d. Privater Schlüssel für Ver- und öffentlicher Schlüssel für Entschlüsselung

4. Womit beschäftigt sich die IT-Sicherheit?
    a. **Mit ausschließlich mit elektronischer Datenverarbeitung**
    b. Mit Daten jeglicher Form (elektronisch, schriftlich, verbal)
    c. Mit rein verbalen Daten
    d. Mit ausschließlich schriftlichen Daten

5. Gibt es eine absolute Sicherheit?
    a. **Nein, es gibt keine absolute Sicherheit**
    b. Ja, es gibt eine absolute Sicherheit
    c. Es kommt darauf an, welche Personen damit arbeiten
    d. Es kommt darauf an, welche Daten verwendet werden

6. Was bedeuten die Buchstaben R, E und S in der Gleichung R = E * S?
    a. **Risiko, Wahrscheinlichkeit, Schaden**
    b. Redundanz, Entität, Service
    c. Risiko, Wirkung, Sicherheit
    d. Reaktion, Wahrscheinlichkeit, System

7. Welche Angriffsebenen gibt es?
    a. **Netzwerke, Anwendungen, Benutzer**
    b. Internet, Intranet, Extranet
    c. Mobile Geräte, Fernseher, Radio
    d. Antennen, Personen, Computer

8. Welche Klassifikationen von Sicherheitsmaßnahmen gibt es?
    a. **Prävention, Erkennung, Reaktion**
    b. Sicherung, Verbindung, Zugänglichkeit
    c. Sicherheit, Reduktion, Verhinderung
    d. Schadensbegrenzung, Sicherheit, Kommunikation

9. Was bedeutet CRC?

   a. **Cyclic Redundancy Check**
   b. Cross-Role Check
   c. Control Redundancy Command
   d. Convertible Risk Control

10. Was bedeutet MAC?
   a. **Mandatory Access Control**
   b. Multiple Availability Control
   c. Media Authentication Control
   d. Moderate Analysis Control

11. Was bedeutet DAC
   a. **Discretionary Access Control**
   b. Dictionary Access Control
   c. Discretionary Availability Command
   d. Dictionary Authenticity Command

12. Was bedeutet RBAC
   a. **Role Based Access Control**
   b. Redundancy Based Access Control
   c. Replay Based Access Control
   d. Reaction Based Access Control

13. Welche passiven Angriffskategorien gibt es?
   a. **Eavesdropping und Traffic Analysis**
   b. Masquerade und Modification
   c. Insertion und Replay
   d. Denial of Service

14. Was wird unter der Angriffskategorie „Denial of Service“ verstanden?
   a. **Der Angreifer stört die Verfügbarkeit von Kommunikationseinrichtungen.**
   b. Der Angreifer verändert die Kommunikation, verzögert, ändert oder löscht Nachrichten.
   c. Der Angreifer gibt sich als jemand anderes aus.
   d. Der Angreifer hört den Kommunikationskanal ab.

15. Was wird unter der Angriffskategorie „Modification“ verstanden?
   a. **Der Angreifer verändert die Kommunikation, verzögert, ändert oder löscht Nachrichten.**
   b. Der Angreifer gibt sich als jemand anderes aus.
   c. Der Angreifer hört den Kommunikationskanal ab.
   d. Der Angreifer fügt Nachrichten zu einer Kommunikation hinzu.

16. Was wird unter der Angriffskategorie „Masquerade“ verstanden?
   a. **Der Angreifer gibt sich als jemand anderes aus.**
   b. Der Angreifer hört den Kommunikationskanal ab.
   c. Der Angreifer fügt Nachrichten zu einer Kommunikation hinzu.
   d. Der Angreifer sendet aufgezeichnete Daten zu einem späteren Zeitpunkt einmal

17. Was wird unter der Angriffskategorie „Eavesdropping“ verstanden?
   a. **Der Angreifer hört den Kommunikationskanal ab, greift aber nicht aktiv ein**
   b. Der Angreifer analysiert die vorhandenen Daten
   c. Der Angreifer gibt sich als jemand anderes aus

d. Der Angreifer fügt Nachrichten zu einer Kommunikation hinzu.

18. Was wird unter der Angriffskategorie „Insertion“ verstanden?
    a. Der Angreifer fügt Nachrichten zu einer Kommunikation hinzu.
    b. Der Angreifer gibt sich als jemand anderes aus
    c. Der Angreifer sendet aufgezeichnete Daten zu einem späteren Zeitpunkt einmal
    d. Der Angreifer hört den Kommunikationskanal ab.

19. Was wird unter der Angriffskategorie „Replay“ verstanden?
    a. Der Angreifer sendet aufgezeichnete Daten zu einem späteren Zeitpunkt einmal
    b. Der Angreifer fügt Nachrichten zu einer Kommunikation hinzu.
    c. Der Angreifer gibt sich als jemand anderes aus.
    d. Der Angreifer verändert die Kommunikation, verzögert, ändert oder löscht Nachrichten.

20. Welche ISO-Familie behandelt das Sicherheitsmanagement bzw. den Sicherheitsprozess?
    a. ISO 27000
    b. ISO 18000
    c. ISO 36000
    d. ISO 41000