P.D.E.A's

Prof Ramkrishna More Arts,Commerce and Science College,Akurdi Pune-44

Introduction to Cyber Security

Practice MCQ Questions with Solutions

Module 2: Security Management

Chapter-1: Security Management Practices

1. Interest rate risk is a type of
   a) Credit risk
   b) Market risk
   c) Operational risk
   d) All the above

   Answer: B

2. A bank suffers loss due to adverse market movement of a security. The security was however held beyond the defeasance period. What is the type of the risk that the bank has suffered ?
   a) Market Risk
   b) Operational Risk
   c) Market Liquidation Risk
   d) Credit Risk

   Answer: B

3. Risk of a portfolio with over exposure in steel sector will be
   a) More than systematic risk
   b) Equal to intrinsic risk
   c) Less than intrinsic risk
   d) None of these

   Answer: A

4. A transaction where financial securities are issued against the cash flow generated from a pool of assets is called
   a. Securitization
   b. Credit Default Swaps
   c. Credit Linked Notes
   d. Total Return Swaps

   Answer: A

5. Operational Risk arises from
   i. Inadequate or failed internal processes
   ii. People and systems
   iii. External Events

iv. Defaults

Which of the above is true ?

a) All of them
b) None of them
c) **(i) , (ii) and (iii)**
d) (i) , (ii)

Answer: B

6. Systemic risk the risk of
   a) Failure of a bank, which is not adhering to regulations
   b) Failure of two banks simultaneously due to bankruptcy of one bank
   c) Where a group of banks fail due to contagion effect
   d) **Failure of entire banking system**

   Answer: D

7. Investment in Post Office time deposit is
   a) Zero risk investment
   b) Low risk investment
   c) Medium risk investment
   d) High risk investment

   Answer: A

8. What is the minimum and customary practice that constitutes "responsible protection of information assets that affects a community or societal norm"? (Information Security & Risk Management Domain)
   a) Due diligence
   b) Risk mitigation
   c) Asset protection
   d) Due care

   Answer: D

9. What type of access control is implemented where a database administrator can grant "Update" privilege in a database to specific users or group? (Application Security Domain)
   a) Supplemental
   b) **Discretionary**
   c) Mandatory
   d) System

   Answer: B

10. What is the purpose of biometrics in access control? (Access Control Domain) Certification
    a) Authorization

b) Authentication

c) Confirmation

d) none of the mentioned

Answer: B

11. What security implementation principle is used for granting users only the rights that are necessary for them to perform their work? (Information Security & Risk Management Domain)

a) Discretionary Access

b) Least Privilege

c) Mandatory Access

d) Separation of Duties

Answer: B

12. As an information systems security manager (ISSM), how would you explain the purpose a system security policy? (Information Security & Risk Management Domain)

a) A definition of the particular settings that have been determined to provide optimum security

b) A set of brief, high-level statements that defines what is and is not permitted during the operation of the system

c) A definition of those items that must be excluded on the system

d) A listing of tools and applications that will be used to protect the system

Answer: B

13. In mandatory access control, what determines the assignment of data classifications? (Information Security & Risk Management Domain)
    a) The analysis of the users in conjunction with the audit department
    b) The assessment by the information security department
    c) The user's evaluation of a particular information element
    d) **A security classification policy / guideline**

    Answer: D

14. As a security manager, how would you explain the primary goal of a security awareness program to senior management? (Information Security & Risk Management Domain)
    a) Provide a vehicle for communicating security procedures
    b) Provide a clear understanding of potential risk and exposure
    c) Provide a forum for disclosing exposure and risk analysis
    d) Provide a forum to communicate user responsibilities

    Answer: B

15. Which statement below most accurately reflects the goal of risk mitigation? (Information Security & Risk Management Domain)
    a) Defining the acceptable level of risk the organization can tolerate, then reduce risk to that level.
    b) Analyzing and removing all vulnerabilities and threats to security within the organization.
    c) Defining the acceptable level of risk the organization can tolerate, and assigning any costs associated with loss or disruption to a third party such as an insurance carrier.
    d) Analyzing the effects of a business disruption and preparing the company's response.

    Answer: A

Chapter-2: Security Laws and Standards

16. In computer security, ……. means that computer system assets can be modified only by authorized parities.
    A) Confidentiality
    B) Integrity
    C) Availability
    D) Authenticity

Answer: B

17. The kind of crime involves altering raw data just before the computer processes it and then changing it back after the processing is completed_____
    a. Data diddling
    b. Data tampering
    c. Salami attacks
    d. None of above

Answer: A

18. Information Technology Act in India was amended in _____
    a. 2000
    b. 2004
    c. 2008
    d. 2010

Answer: C

19. Which of the following are the Cyber crimes ? 1. Cyber crimes against persons. 2. Cyber crimes against property. 3. Cyber crimes against government. 4. Cyber crimes against animal?
    a. 1, 2, 3 only
    b. 2, 3, 4 only
    c. 1, 3, 4 only
    d. 2, 3 only

Answer: A