THE INSTITUTE OF BANKERS PAKISTAN

SAMPLE PAPER

FOR

SBP- Assistant Director- IT Security System- OG II

ENGLISH COMPOSITION

Read the following passage carefully and answer questions 1 to 3

The need for strong domestic capital market cannot be over-emphasized for a successful international financial center. The domestic depositors supply funds not only to domestic users but are willing to supply funds to foreign users.

Amongst these markets, let us discuss the mechanism of "off-shore markets", before we delve into the working of international capital markets. "When foreign depositors supply funds directly to foreign users via a market mechanism that precludes domestic participation in the transaction, the relationship is called an off-shore market." Off-shore markets are created to **mobilize** specialized financial business without exposing their residents to tax nuances and freedoms that are made available to international participants.

Q1. In the first paragraph the writer implies that for success in international financial center _____.

A. there is no need for strong domestic capital market
B. considerable emphasis on the strong domestic capital market is required
C. there is a little need for strong domestic capital market
D. slight emphasis on the strong domestic capital market is sufficient

Q2. Which of the following statements is TRUE about off-shore markets?

A. Foreign investors supply funds to both domestic and foreign borrowers
B. Foreign investors supply funds to domestic borrowers only
C. Foreign investors supply funds to foreign borrowers only
D. Domestic users supply funds to foreign borrowers

Q3. The term "mobilize" means that off-shore markets help specialized financial business to

A. flourish
B. be organized
C. expand
D. furnish

Select the most effective answer from the given options to fill in the blank to make the sentence meaningfully complete.

Q4. When _____ writing the report of the meeting?

A. have you finished
B. are you finishing
C. do you finish
D. will you finish

Q5. The police _____ the stolen property to the owner.

A. turned up
B. turned out
C. turned over
D. turned down

Select the correct synonym for the given word

Q6. CONCEALED

A. Evident
B. To prove something
C. Skillful
D. Hidden

Q7. HARSH

A. Unpleasant
B. Cheap
C. Rude
D. Momentary

Select the correct antonym for the given word

Q8. GLOOMY

A. Distressed
B. Happy
C. Confused
D. Convicted

Q9. ABUNDANCE

A. Wealth
B. Profusion
C. Large amount
D. Lack

ANALYTICAL SECTION

Q10. A total of Rs. 5,000/- worth of tickets were sold for a private show. Tickets were of two types: standard costing Rs. 50/- and gold costing Rs. 150/-. If a total of 60 tickets were sold, then the number of standard tickets sold was:

A. 20
B. 30
C. 40
D. 50

Q11. A positive integer which, when added to 100, gives a sum which is greater than when it is multiplied by 100. What is the number?

A. 5
B. 2
C. 3
D. 1

Q12. When a number is doubled, increased by 70, and then tripled, it becomes 240. What is the number?

A. 3
B. 4
C. 5
D. 6

Q13. What should come next in the sequence: 1024, 512, 256, 128, _____?

A. 48
B. 64
C. 40
D. 46

IT SECURITY SYSTEM

Q14. Which of the following entity is ultimately responsible for information security within an organization?

A. IT Security Officer
B. Senior Management
C. Project Managers
D. Department Directors

Q15. It is important that information about an ongoing computer crime investigation be _____.

A. destroyed as soon after trial as possible
B. reviewed by upper management before being released
C. replicated to a backup system to ensure availability
D. limited to as few people as possible

Q16. User Rights Management is one of the:

A. Database Security Threat
B. Normalization
C. Database Structure
D. Database Security Solutions

Q17. Real-Time Alerting and Blocking is categorized under:

A. Discovery and Assessment
B. User Rights Management
C. Monitoring and Blocking
D. Auditing

Q18. A security policy provides a way to _____.

A. establish a cost model for security activities
B. allow management to define system recovery requirements
C. identify and clarify security goals and objectives
D. enable management to define system access rules

IT SECURITY SYSTEM

Q19. A local bank has opened its operation with 500 branches all over the country and implementing new core banking application "Symbol" for more than 10,000 resources.

Unauthorized access can lead to devastating effects. Entities can become victims such as identity theft, financial fraud, theft of data (e.g. credit card data) and attacks on systems, which can be especially harmful for online businesses.
Thus, more than ever, one of the prime concerns in any audit, and for management, is the logical access to computer systems and data. The proliferation of IT, and the Internet in particular, has caused the risks associated with systems and data to explode. To mitigate the risks associated with access control, it is necessary to identify the risks and to assess the level of those risks.
The bank wants to review its, IS policies and procedures for granting authorized access to the users, user's rights and privileges while simultaneously protecting itself from unauthorized access.
Write a report highlighting the risks for the bank with regard to the following and suggest what measures should be taken by the bank.

1. Access Control Principles (Least Privilege, Logical Access)
2. Security Principles (Confidentiality, Integrity and Availability)

Possible answer

Introduction /scope

Body

1. Access Control Principles

Principle of Least Privilege: It states that if nothing has been specifically configured for an individual or the groups, he/she belongs to, the user should not be able to access that resource i.e. no access by default.

Separation of Duties: Separating any conflicting areas of responsibility so as to reduce opportunities for unauthorized or unintentional modification or misuse of organizational assets and/or information.

Need to know: It is based on the concept that individuals should be given access only to the information that they absolutely require in order to perform their job duties

Logical Access: Only authorized persons have access to data and applications (including programs, tables, and related resources) and that they can perform only specifically authorized functions (e.g., inquire, execute, update).

Access Control Criteria: The criteria for providing access to an object include

- Roles
- Groups
- Location
- Time
- Transaction Type

2. Security Principles

Fundamental Principles (Confidentiality, Integrity, Availability)

- Identification
- Authentication
- Authorization
- Non Repudiation

Identification Authentication and Authorization

Identification describes a method of ensuring that a subject is the entity it claims to be. E.g.: A user name or an account no.

Authentication is the method of proving the subject's identity. E.g.: Password, Passphrase, PIN

Authorization is the method of controlling the access of objects by the subject. E.g.: A user cannot delete a particular file after logging into the system

Note: There must be a three step process of Identification, Authentication and Authorization in order for a subject to access an object

Identification Factors

When issuing identification values to users or subjects, ensure that

- Each value should be unique, for user accountability
- A standard naming scheme should be followed
- The values should be non-descriptive of the user's position or task
- The values should not be shared between the users.

Authentication Factors

There are 3 general factors for authenticating a subject.

- Something a person knows- E.g.: passwords, PIN- least expensive, least secure
- Something a person has – E.g.: Access Card, key- expensive, secure
- Something a person is- E.g.: Biometrics- most expensive, most secure

Note: For a strong authentication to be in process, it must include two out of the three authentication factors- also referred to as two factor authentication.

Conclusion

Authentication Methods

Biometrics

- Verifies an individual's identity by analyzing a unique personal attribute or behavior
- It is the most effective and accurate method for verifying identification.
- It is the most expensive authentication mechanism
- Types of Biometric Systems
- *Finger Print*- are based on the ridge endings, bifurcation exhibited by the friction edges and some minutiae of the finger
- *Palm Scan*- are based on the creases, ridges, and grooves that are unique in each individual's palm
- Hand Geometry- are based on the shape (length, width) of a person's hand and fingers
- *Retina Scan*- is based on the blood vessel pattern of the retina on the backside of the eyeball.
- *Iris Scan*- is based on the colored portion of the eye that surrounds the pupil. The iris has unique patterns, rifts, colors, rings, coronas and furrows.
- *Signature Dynamics*- is based on electrical signals generated due to physical motion of the hand during signing a document
- *Keyboard Dynamics*- is based on electrical signals generated while the user types in the keys (passphrase) on the keyboard.
- *Voice Print*- based on human voice
- *Facial Scan*- based on the different bone structures, nose ridges, eye widths, forehead sizes and chin shapes of the face.
- *Handy Topography*- based on the different peaks, valleys, overall shape and curvature of the hand.

X --- **END OF PAPER** --- X

ANSWERS

Question Number	Key
1	B
2	C
3	B
4	D
5	C
6	D
7	A
8	B
9	D
10	C
11	D
12	C
13	B
14	B
15	D
16	D
17	C
18	C