(ISC)2

CISSP

CISSP CISSP CISSP CISSP CISSP CISSP CISSP CISSP CISSP

PRINTABLES

Printable Practice Questions

QUESTIONS, ANSWERS, AND DETAILED EXPLANATIONS IN AN EASY-TO-USE PRINTABLE FORMAT

PrepLogic

Be Prepared. Be Confident. Get Certified.

Table of Contents

Chapter 1
Access Control..... 2

Answer Key 250
Explanations 287

Chapter 2
Application Security..... 24

Answer Key 253
Explanations 312

Chapter 3
Business Continuity and Disaster Recovery Planning..... 49

Answer Key 257
Explanations 340

Chapter 4
Cryptography..... 76

Answer Key 261
Explanations 372

Chapter 5
Information Security and Risk Management..... 99

Answer Key 264
Explanations 398

Chapter 6
Legal, Regulations, Compliance and Investigations..... 129

Answer Key 268
Explanations 435

Chapter 7
Operations Security..... 152

Answer Key 271
Explanations 462

Chapter 8
Physical (Environmental) Security..... 172

Answer Key 274
Explanations 486

Chapter 9
Security Architecture and Design..... 197

Answer Key 278
Explanations 516

Chapter 10
Telecommunications and Network Security..... 224

Answer Key 282
Explanations 547

CISSP Printables

Product ID: 4293
Production Date: April 19, 2010
Total Questions: 750

Warning and Disclaimer
Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales
PrepLogic offers favorable discounts on all products when ordered in quantity. For more information, please contact PrepLogic directly:

1-800-418-6789
solutions@preplogic.com

Chapter 1
Access Control

1. _____ is what allows you to perform requested actions or denies such actions based on access criteria.Select the best answer.

   - ❍ A. Authorization
   - ❍ B. Identification
   - ❍ C. Authentication
   - ❍ D. Auditing

   Find the Answer p. 250

2. What type of access control is based on job description?Select the best answer.

   - ❍ A. Group-based
   - ❍ B. Role-based
   - ❍ C. Transaction-based
   - ❍ D. Discretionary

   Find the Answer p. 250

3. Which of the following is a security disadvantage of single sign-on?Select the best answer.

   - ❍ A. Simplified password management and administration
   - ❍ B. Less time required overall to perform logon and authentication
   - ❍ C. Stronger passwords are often used
   - ❍ D. Users can roam the network without restrictions

   Find the Answer p. 250

4. Which of the following is NOT an example of a single sign-on technology?Select the best answer.

- ❍ A. TACACS
- ❍ B. Kerberos
- ❍ C. SESAME
- ❍ D. KryptoKnight

Find the Answer p. 250

5. Role based access control can be labeled as what form of access control?Select the best answer.

- ❍ A. Discretionary
- ❍ B. Mandatory
- ❍ C. Nondiscretionary
- ❍ D. Recursive

Find the Answer p. 250

6. ACLs on objects are the most common implementation of what form of access control?Select the best answer.

- ❍ A. Role based
- ❍ B. Mandatory
- ❍ C. Nondiscretionary
- ❍ D. Discretionary

Find the Answer p. 250

7. What form of access control is NOT centrally managed?Select the best answer.

- ❍ A. Discretionary
- ❍ B. Mandatory
- ❍ C. Nondiscretionary
- ❍ D. Role-based

Find the Answer p. 250

8. What is the most efficient form of access control for environments with a high rate of personnel turnover?Select the best answer.

- ❍ A. Interpretive
- ❍ B. Role based
- ❍ C. Mandatory
- ❍ D. Discretionary

Find the Answer p. 250

9. Which of the following is the least appropriate technique for controlling access?Select the best answer.

- ❍ A. Encryption
- ❍ B. Rule-based access
- ❍ C. Restricted interface
- ❍ D. Capability table

Find the Answer p. 250

10. Which of the following is NOT a form of access control administration?Select the best answer.

- ❍ A. Centralized
- ❍ B. Delegated
- ❍ C. Decentralized
- ❍ D. Hybrid

Find the Answer p. 250

11. Which of the following is NOT a form of a centralized access control mechanism?Select the best answer.

- ❍ A. RADIUS (Remote Authentication Dial-in User Service)
- ❍ B. TACACS+ (Terminal Access Controller Access Control System Plus)
- ❍ C. Security domains
- ❍ D. 802.1x

Find the Answer p. 250

12. Which form of TACACS (Terminal Access Controller Access Control System) can use tokens for two-factor authentication and supports dynamic password authentication?Select the best answer.

- ❍ A. TACACS (Terminal Access Controller Access Control System)
- ❍ B. Dual-TACACS (Dual Terminal Access Controller Access Control System)
- ❍ C. XTACACS (Extended Terminal Access Controller Access Control System)
- ❍ D. TACACS+ (Terminal Access Controller Access Control System Plus)

Find the Answer p. 250

13. Which of the following is NOT an administrative access control method?Select the best answer.

- ❍ A. Work area separation
- ❍ B. Policies and procedures
- ❍ C. Personnel controls
- ❍ D. Supervisory structure

Find the Answer p. 250

14. Which of the following is an administrative access control method?Select the best answer.

- ❍ A. Data backups
- ❍ B. Security awareness training
- ❍ C. Network architecture
- ❍ D. Auditing

Find the Answer p. 250

15. Which of the following is NOT a physical access control method?Select the best answer.

- ❍ A. Network segregation
- ❍ B. Perimeter security
- ❍ C. Testing
- ❍ D. Cabling

Find the Answer p. 250

16. Which of the following is a physical access control method?Select the best answer.

- ❍ A. Restricting computer system and network access
- ❍ B. Encryption
- ❍ C. Security awareness training
- ❍ D. Computer media inventory

Find the Answer p. 250

17. Which of the following is NOT a technical/logical access control method?Select the best answer.

- ❍ A. Security awareness training
- ❍ B. Network architecture
- ❍ C. Encryption
- ❍ D. Control zones

Find the Answer p. 250

18. Which of the following is a technical/logical access control method?Select the best answer.

- ❍ A. Work area separation
- ❍ B. Auditing
- ❍ C. Data backups
- ❍ D. Policies and procedures

Find the Answer p. 250

19. What type of security control reduces the likelihood of security violations?Select the best answer.

- ❍ A. Detective
- ❍ B. Corrective
- ❍ C. Preventative
- ❍ D. Recovery

Find the Answer p. 250

20. Which of the following is the odd element in this set of items?Select the best answer.

- ❍ A. Need to know
- ❍ B. Access based on work tasks
- ❍ C. Data classification
- ❍ D. Least privilege

Find the Answer p. 250

21. Which of the following is the most secure form of password?Select the best answer.

- ❍ A. Static password
- ❍ B. Dynamic password
- ❍ C. One time password
- ❍ D. Cognitive password

Find the Answer p. 250

22. What does the False Acceptance Rate (Type II) error of a biometric device indicate?Select the best answer.

- ❍ A. The rate at which authorized users are not granted access
- ❍ B. The rate at which authorized users are granted access
- ❍ C. The rate at which unauthorized users are not granted access
- ❍ D. The rate at which unauthorized users are granted access

Find the Answer p. 250

23. What will a fail-secure access control mechanism default to?Select the best answer.

- ❍ A. No access
- ❍ B. Minimal access
- ❍ C. Least privilege
- ❍ D. Need to know access

Find the Answer p. 250

24. What is the primary disadvantage of single sign-on?Select the best answer.

- ❍ A. Password management and account administration
- ❍ B. Users can roam the network without restrictions
- ❍ C. User work task prohibitive
- ❍ D. Length of time required to perform logon

Find the Answer p. 251

25. Which of the following is usually NOT labeled as an entity that serves as either a subject or an object?Select the best answer.

- ❍ A. File
- ❍ B. Database
- ❍ C. Program
- ❍ D. Computers

Find the Answer p. 251

26. Which of the following is the act of providing the "who" of a subject, and is the first step in establishing accountability?Select the best answer.

- ❍ A. Authorization
- ❍ B. Identification
- ❍ C. Auditing
- ❍ D. Non-repudiation

Find the Answer p. 251

27. Which of the following represents the activity of verifying the claimed identity of a subject?Select the best answer.

- ❍ A. Authorization
- ❍ B. Accountability
- ❍ C. Authentication
- ❍ D. Availability

Find the Answer p. 251

28. Which of the following is NOT an example of an authorization method?Select the best answer.

- ❍ A. Need to know
- ❍ B. Access control matrix
- ❍ C. Security label
- ❍ D. Password

Find the Answer p. 251

29. Which of the following is NOT an example of a logical access control?Select the best answer.

- ❍ A. Perimeter padlocked gates
- ❍ B. Restricted database interfaces
- ❍ C. Required authentication before access
- ❍ D. Centralized remote access authentication services

Find the Answer p. 251

30. Which of the following is NOT typically considered to be used as an identification factor?Select the best answer.

- ❍ A. Smart Card
- ❍ B. Password
- ❍ C. Biometric feature
- ❍ D. Employee identification

Find the Answer p. 251

31. Which form of password may require different interactions or responses from the subject each time they attempt to logon?Select the best answer.

- ❍ A. Static password
- ❍ B. Dynamic password
- ❍ C. Cognitive password
- ❍ D. Passphrase

Find the Answer p. 251

32. Which of the following is also a dynamic password?Select the best answer.

- ❍ A. Passphrase
- ❍ B. PIN
- ❍ C. Smart card
- ❍ D. One time password

Find the Answer p. 251

33. A password is an example of what type of authentication factor?Select the best answer.

- ❍ A. Type 1
- ❍ B. Type 2
- ❍ C. Type 3
- ❍ D. Type 4

Find the Answer p. 251

34. What is a Type 3 authentication factor?Select the best answer.

- ❍ A. Something you have
- ❍ B. Something you are
- ❍ C. Something you know
- ❍ D. Something you do

Find the Answer p. 251

35. What is an example of a Type 3 authentication factor?Select the best answer.

- ❍ A. Password
- ❍ B. Signing your name
- ❍ C. Fingerprint
- ❍ D. Smart card

Find the Answer p. 251

36. Which of the following provides the greatest level of authentication security?Select the best answer.

- ❍ A. Biometric
- ❍ B. Type 2
- ❍ C. Something you do
- ❍ D. Two-factor

Find the Answer p. 251

37. Which of the following is converted to a hash value (a.k.a. a virtual password) before being sent to the authentication server for processing?Select the best answer.

- ❍ A. Passphrase
- ❍ B. Smart card swipe
- ❍ C. Fingerprint scan
- ❍ D. MAC filtering check

Find the Answer p. 251

38. What type of authentication token requires the subject to authenticate themselves to the token, and then the token authenticates to the system?Select the best answer.

- ❍ A. Synchronous dynamic password token
- ❍ B. Static password token
- ❍ C. Asynchronous dynamic password token
- ❍ D. Challenge-response token

Find the Answer p. 251

39. Biometrics can be used directly for all but which of the following purposes?Select the best answer.

- ❍ A. Identification
- ❍ B. Physical access control
- ❍ C. Accountability
- ❍ D. Authentication

Find the Answer p. 251

40. When used as an _____ method, biometrics function as a one to one function.Select the best answer.

- ❍ A. Identification
- ❍ B. Authorization
- ❍ C. Impersonation
- ❍ D. Authentication

Find the Answer p. 251

41. What is the primary use of the crossover error rate?Select the best answer.

- ❍ A. Sensitivity adjustment
- ❍ B. Comparison of similar biometric devices
- ❍ C. Configuration control
- ❍ D. Reducing enrollment time

Find the Answer p. 251

42. What is the threshold rate of subject processing per minute at which a biometric device considered to be accetable or unacceptable?Select the best answer.

- ❍ A. 50 subjects per minute
- ❍ B. 2 subjects per minute
- ❍ C. 5 subjects per minute
- ❍ D. 10 subjects per minute

Find the Answer p. 251

43. What does a Type I biometric error indicate?Select the best answer.

- ❍ A. The rate at which authorized users are not granted access
- ❍ B. The rate at which authorized users are granted access
- ❍ C. The rate at which unauthorized users are not granted access
- ❍ D. The rate at which unauthorized users are granted access

Find the Answer p. 251

44. What is the threshold point of enrollment time required at which a biometric device is generally considered unacceptable to most users?Select the best answer.

- ❍ A. 30 seconds
- ❍ B. 1 minute
- ❍ C. 2 minutes
- ❍ D. 10 minutes

Find the Answer p. 251

45. A biometric scanner for facility access is considered all but which of the following types of access control?Select the best answer.

- ❍ A. Preventative
- ❍ B. Detective
- ❍ C. Corrective
- ❍ D. Recovery

Find the Answer p. 251

46. Which of the following is not considered a detective security control?Select the best answer.

- ❍ A. Monitoring
- ❍ B. Separation of duties
- ❍ C. Job rotation
- ❍ D. Intrusion detection

Find the Answer p. 251

47. Which of the following is an example of a recovery security control?Select the best answer.

- ❍ A. Intrusion detection
- ❍ B. Encryption
- ❍ C. Anti-virus software
- ❍ D. Smart cards

Find the Answer p. 251

48. Which of the following is NOT an example of a preventative administrative access control?Select the best answer.

- ❍ A. Background checks
- ❍ B. Controlled termination process
- ❍ C. Data classification
- ❍ D. Alarms

Find the Answer p. 251

49. Which of the following is NOT an example of a preventative technical/logical access control?Select the best answer.

- ❍ A. Passwords
- ❍ B. Motion detectors
- ❍ C. Constrained user interfaces
- ❍ D. Firewalls

Find the Answer p. 252

50. Which of the following is NOT a preventative physical access control?Select the best answer.

- ❍ A. Biometrics
- ❍ B. fences
- ❍ C. Call back systems
- ❍ D. CCTV (Closed-Circuit TV)

Find the Answer p. 252

51. Which of the following is used to ensure that users are held responsible for their actions?Select the best answer.

- ❍ A. Auditing
- ❍ B. Authentication
- ❍ C. Identificaiton
- ❍ D. Accountability

Find the Answer p. 252

52. Auditing allows for all but which of the following?Select the best answer.

- ❍ A. Controlling data classifications
- ❍ B. Reconstruction of events
- ❍ C. Evidence for legal action
- ❍ D. Producing problem reports

Find the Answer p. 252

53. Which of the following is NOT considered an audit analysis tool?Select the best answer.

- ❍ A. Malicious code scanning tool
- ❍ B. Data reduction tool
- ❍ C. Variance detection tool
- ❍ D. Attack signature detection tool

Find the Answer p. 252

54. Which of the following is a method by which accountability can be enforced?Select the best answer.

- ❍ A. Data backups
- ❍ B. Keystroke logging
- ❍ C. Bandwidth throttling
- ❍ D. Trusted recovery

Find the Answer p. 252

55. What is the act of a hacker cleaning out all traces of their activities from audit logs known as?Select the best answer.

- ❍ A. Spoofing
- ❍ B. Masquerading
- ❍ C. Scrubbing
- ❍ D. Data diddling

Find the Answer p. 252

56. Audit logs can be used for all but which of the following?Select the best answer.

- ❍ A. Legal evidence
- ❍ B. Predicting the source of the next intrusion attempt
- ❍ C. Demonstrate the means by which an attack was waged
- ❍ D. Corroborate and verify the story of a suspect

Find the Answer p. 252

57. Which of the following is a means by which data is disclosed intentionally?Select the best answer.

- ❍ A. Social engineering
- ❍ B. Malicious code
- ❍ C. Espionage
- ❍ D. Object/media reuse

Find the Answer p. 252

58. What is TEMPEST?Select the best answer.

- ❍ A. A centralized remote access authentication service
- ❍ B. A security domain authorization system
- ❍ C. A vulnerability scanner
- ❍ D. The study and control of stray electrical signals

Find the Answer p. 252

59. Which of the following is NOT a valid countermeasure against the interception of radio frequency and other electromagnetic radiation signals by unauthorized individuals?Select the best answer.

- ❍ A. Sound dampening insulation
- ❍ B. TEMPEST equipment
- ❍ C. White noise generation
- ❍ D. Control zones

Find the Answer p. 252

60. Without _____ there is no security.Select the best answer.

- ❍ A. Removable media usage controls
- ❍ B. Physical access controls
- ❍ C. Access control lists
- ❍ D. Firewalls

Find the Answer p. 252

61. Which of the following is NOT considered a monitoring or reconnaisance technique?Select the best answer.

- ❍ A. Intrusion Detection
- ❍ B. Probing
- ❍ C. Proximity detectors
- ❍ D. Dumpster Diving

Find the Answer p. 252

62. What is a clipping level?Select the best answer.

- ❍ A. The point at which a monitoring device is unable to process further data due to saturation
- ❍ B. The point at which normal activity is distinguished from abnormal
- ❍ C. The point at which a device experiences a power surge and thus an operational failure
- ❍ D. The rate at which a firewalls access ports are scanned when under attack

Find the Answer p. 252

63. An audit log should contain all but which of the following?Select the best answer.

- ❍ A. Time and date of violation
- ❍ B. Location (physical or logical) of incident
- ❍ C. What event violated the security policy
- ❍ D. Biometric profile of the offending user account

Find the Answer p. 252

64. Which of the following is used to locate significant or relevant information within audit trails?Select the best answer.

- ❍ A. Scavenging
- ❍ B. Data diddling
- ❍ C. Data mining
- ❍ D. Random access

Find the Answer p. 252

65. Which of the following is NOT an example of a technical or logical security control?Select the best answer.

- ❍ A. Encryption
- ❍ B. Personnel screening
- ❍ C. Identification
- ❍ D. Access Control Lists

Find the Answer p. 252

66. Of the following methods of encryption, which involves the process of completely encrypting the volume upon which all data is stored?

- ❍ A. Manual Encryption.
- ❍ B. Transparent Encryption.
- ❍ C. Semi-Transparent Encryption.
- ❍ D. Solid State Encryption.

Find the Answer p. 252

Chapter 2
Application Security

1. Which of the following methods is effective in maintaining the integrity of stored audit logs?Select the best answer.

   - ❍ A. Use of optical versus magnet storage media
   - ❍ B. Periodic manual inspection
   - ❍ C. Storage in binary rather than text format
   - ❍ D. Digital signatures

   Find the Answer p. 253

2. In what level of the software capability maturity model are security requirements institutionalized?Select the best answer.

   - ❍ A. Initiating
   - ❍ B. Repeatable
   - ❍ C. Defined
   - ❍ D. Managed

   Find the Answer p. 253

3. Which of the following is most susceptible to insertion of malicious code?Select the best answer.

   - ❍ A. Assembly language
   - ❍ B. Compiled language
   - ❍ C. Commercial software
   - ❍ D. CGI scripts

   Find the Answer p. 253

4. Within the realm of object oriented programming, what is the communications sent to an object in order to instruct it to perform some operation known as?Select the best answer.

- ❍ A. Method
- ❍ B. Behavior
- ❍ C. Delegation
- ❍ D. Message

Find the Answer p. 253

5. Within the realm of object oriented programming, what is the code that defines the actions that an object performs in response to an instruction known as?Select the best answer.

- ❍ A. Method
- ❍ B. Behavior
- ❍ C. Delegation
- ❍ D. Message

Find the Answer p. 253

6. Which of the following is NOT one of the elements of the software maintenance phase and change control process?Select the best answer.

- ❍ A. Risk control
- ❍ B. Request control
- ❍ C. Change control
- ❍ D. Release control

Find the Answer p. 253

7. What programming language can be used directly by computers?Select the best answer.

- ❍ A. Assembly language
- ❍ B. Artificial intelligence language
- ❍ C. Machine language
- ❍ D. Interpreted language

Find the Answer p. 253

8. What are objects in an object-oriented programming environment, created on-the-fly by software as it executes known as?Select the best answer.

- ❍ A. Dynamic lifetime objects
- ❍ B. Transient elements
- ❍ C. Volatile agents
- ❍ D. Distributed computing applets

Find the Answer p. 253

9. What does encapsulation mean, in the context of an object-oriented programming environment?Select the best answer.

- ❍ A. Objects can produce multiple outputs from the same input
- ❍ B. Objects are self-contained
- ❍ C. Objects are more secure than compiled programs
- ❍ D. Objects are transient

Find the Answer p. 253

10. Within the realm of object oriented programming, what is the ability for one object to be removed from a system and be replaced with another object known as?Select the best answer.

- ❍ A. Polymorphism
- ❍ B. Data diddling
- ❍ C. Substitution property
- ❍ D. Normalization

Find the Answer p. 253

11. Within the realm of object oriented programming, what is the forwarding of an instruction from one object to another known as?Select the best answer.

- ❍ A. Method
- ❍ B. Behavior
- ❍ C. Delegation
- ❍ D. Message

Find the Answer p. 253

12. Within the realm of object oriented programming, what is the result exhibited by an object upon receipt of an instruction known as?Select the best answer.

- ❍ A. Method
- ❍ B. Behavior
- ❍ C. Delegation
- ❍ D. Message

Find the Answer p. 253

13. Within the realm of object oriented programming, what is the ability for an object to produce different behaviors from the same message known as?Select the best answer.

- ❍ A. Method
- ❍ B. Data diddling
- ❍ C. Electronic vaulting
- ❍ D. Polymorphism

Find the Answer p. 253

14. What type of computer system exhibits the same reasoning capabilities as those of a human?Select the best answer.

- ❍ A. Expert system
- ❍ B. Neural network
- ❍ C. Object-oriented system
- ❍ D. Artifical intelligence system

Find the Answer p. 253

15. What type of computer system mimics the functioning of biological neurons?Select the best answer.

- ❍ A. Expert system
- ❍ B. Neural network
- ❍ C. Object-oriented system
- ❍ D. Artifical intelligence system

Find the Answer p. 253

16. Expert systems function without using?Select the best answer.

- ❍ A. If-then statement rule databases
- ❍ B. Fuzzy logic
- ❍ C. Delta rule
- ❍ D. Inference engine

Find the Answer p. 253

17. Which of the following is NOT one of the steps used by expert systems when performing fuzzy logic operations?Select the best answer.

- ❍ A. Fuzzification
- ❍ B. Inference
- ❍ C. Composition
- ❍ D. Normalization

Find the Answer p. 253

18. Which of the following is considered the most common example of a distributed computing environment(DCE)?Select the best answer.

- ❍ A. Client/server
- ❍ B. Terminal/host
- ❍ C. Stand alone desktop system
- ❍ D. Portable computers

Find the Answer p. 253

19. Which of the following is NOT an example of a mobile code language used in a distributed computing environment?Select the best answer.

- ❍ A. ActiveX
- ❍ B. Fortran
- ❍ C. Java
- ❍ D. Macromedia Flash

Find the Answer p. 253

20. Which of the following are true regarding ActiveX?1. Platform independent2. Platform dependent3. Language independent4. Language dependentSelect the best answer.

- ❍ A. 1 and 3
- ❍ B. 2 and 4
- ❍ C. 2 and 3
- ❍ D. 1 and 4

Find the Answer p. 253

21. Which of the following are true regarding Java?1. Platform independent2. Platform dependent3. Language independent4. Language dependentSelect the best answer.

- ❍ A. 1 and 3
- ❍ B. 2 and 4
- ❍ C. 2 and 3
- ❍ D. 1 and 4

Find the Answer p. 253

22. What is the primary security flaw of ActiveX?Select the best answer.

- ❍ A. It stores controls to the hard drive
- ❍ B. It uses a sandbox
- ❍ C. It is specific to Windows OSes
- ❍ D. It is not language dependant

Find the Answer p. 253

23. Which of the following statements is FALSE about Java?Select the best answer.

- ❍ A. It uses a sandbox
- ❍ B. It is stored on the hard drive
- ❍ C. It is multithreaded
- ❍ D. It is temporarily stored in memory

Find the Answer p. 253

24. Which of the following is NOT one of the three primary models of databases?Select the best answer.

- ❍ A. Hierarchical
- ❍ B. Distributed
- ❍ C. Relational
- ❍ D. Dynamic

Find the Answer p. 254

25. A relational database provides for what types of relationships?Select the best answer.

- ❍ A. One-to-one
- ❍ B. One-to-many
- ❍ C. Many-to-many
- ❍ D. Many-to-one

Find the Answer p. 254

26. When a program or operating system experiences a failure state, what should it do?Select the best answer.

- ❍ A. Save a memory dump
- ❍ B. Revert to a secure state
- ❍ C. Restart in privilege mode
- ❍ D. Automatically reboot

Find the Answer p. 254

27. In regards to a database, what is an attribute?Select the best answer.

- ❍ A. A table stored in a database
- ❍ B. A column that has a unique value in each row
- ❍ C. A column in a database
- ❍ D. The data that describes the database

Find the Answer p. 254

28. What database model provides for many-to-many relationships?Select the best answer.

- ❍ A. Relational data model
- ❍ B. Heirarchical data model
- ❍ C. Networked data model
- ❍ D. Distributed data model

Find the Answer p. 254

29. An indication that the integrity of the database has been violated occurs when which of the following includes a null value?Select the best answer.

- ❍ A. Primary key
- ❍ B. Cell
- ❍ C. Tuple
- ❍ D. Relation

Find the Answer p. 254

30. Environmental controls and hardware devices can NOT prevent problems created by which of the following?Select the best answer.

- ❍ A. Bad program coding
- ❍ B. Unrestricted physical access
- ❍ C. Lack of boundary controls
- ❍ D. Poor air quality

Find the Answer p. 254

31. A reliable and controlled software development, design, and coding process is necessary to ensure which of the following?Select the best answer.

- ❍ A. Marketability
- ❍ B. Security
- ❍ C. Interoperability
- ❍ D. Compatibility

Find the Answer p. 254

32. Buffer overflows are caused by a programmer failing to compensate for all but which of the following?Select the best answer.

- ❍ A. Input data block size
- ❍ B. ASCII vs. Binary input
- ❍ C. English vs. Spanish
- ❍ D. Alpha vs. numeric

Find the Answer p. 254

33. Failing to compensate for invalid or extensive values of data types, formats, or lengths in input to programs can cause which of the following?Select the best answer.

- ❍ A. Time of check/time of use attack
- ❍ B. Aggregation
- ❍ C. Unauthorized alterations of a configuration item
- ❍ D. Buffer overflows

Find the Answer p. 254

34. Which of the following is NOT true about out-of-the-box security?Select the best answer.

- ❍ A. Security and functionality are directly proportional
- ❍ B. Security is usually disabled for installation
- ❍ C. Security must be configured for the environment
- ❍ D. Security is often a tradeoff for ease of use

Find the Answer p. 254

35. What characteristic of newly deployed software is considered a security failure or downfall?Select the best answer.

- ❍ A. Platform dependence
- ❍ B. A wide range of features or functionality
- ❍ C. Interpreted vs. compiled language
- ❍ D. Implementation within a distributed computing environment

Find the Answer p. 254

36. What is the primary reason software is unable to handle failures or errors in a secure fashion?Select the best answer.

- ❍ A. Use of interpreted languages
- ❍ B. Designed to be used in a distributed computing environment
- ❍ C. Circumstances of use are difficult to predict and plan for
- ❍ D. Lack of software change management

Find the Answer p. 254

37. Since all circumstances of use are difficult to predict and plan for, what should programmers do?Select the best answer.

- ❍ A. Not produce software
- ❍ B. Use only fifth generation programming languages
- ❍ C. Avoid CGI scripts
- ❍ D. Design a general method for handling unexpected failures

Find the Answer p. 254

38. If a system should fail for any reason, it should always perform a _____.Select the best answer.

- ❍ A. fail safe operation
- ❍ B. self-diagnostic
- ❍ C. fail over maneuver
- ❍ D. privileged restart function

Find the Answer p. 254

39. If a system encounters a failure and it is prevented from rebooting, what will this help avoid?Select the best answer.

- ❍ A. Denial of service
- ❍ B. Initial program load vulnerabilities
- ❍ C. Time of check/time of use attacks
- ❍ D. Inference

Find the Answer p. 254

40. _____ is most effective if it is planned and managed throughout the lifecycle of a system or application.Select the best answer.

- ❍ A. Capability
- ❍ B. Functionality
- ❍ C. Security
- ❍ D. Marketability

Find the Answer p. 254

41. _____ keeps the development project on target and moving toward the goal of a completed product.Select the best answer.

- ❍ A. Business continuity planning
- ❍ B. Change control management
- ❍ C. Facility design and construction
- ❍ D. Project management

Find the Answer p. 254

42. Which of the following is NOT one of the standard phases in a system life cycle?Select the best answer.

- ❍ A. Penetration testing
- ❍ B. Project initiation
- ❍ C. System design specifications
- ❍ D. Maintenance

Find the Answer p. 254

43. Which of the following is NOT one of the standard phases in a the system life cycle?Select the best answer.

- ❍ A. Functional design analysis and planning
- ❍ B. Risk assessment
- ❍ C. Software development
- ❍ D. Installation

Find the Answer p. 254

44. Which of the following is a means by which to incorporate improvements in the software/system development process?Select the best answer.

- ❍ A. Disaster recovery planning
- ❍ B. Software capability maturity model
- ❍ C. Waterfall model
- ❍ D. Change and control management

Find the Answer p. 254

45. The waterfall models allows for what?Select the best answer.

- ❍ A. Improved management
- ❍ B. Greater control over project progress toward objective completion
- ❍ C. Creation of multiple prototypes
- ❍ D. Modification only to the immediately previous stage of the life cycle process

Find the Answer p. 254

46. Which of the following life cycle phase models allows for the intiation through software development phases of the life cycle process to be repeated?Select the best answer.

- ❍ A. Spiral model
- ❍ B. Waterfall model
- ❍ C. Modified waterfall model
- ❍ D. Information security and life cycle model

Find the Answer p. 254

47. Which life cycle model provides mechanisms for back verification and validation against defined baselines?Select the best answer.

- ❍ A. Spiral model
- ❍ B. Modified waterfall model
- ❍ C. Clark Wilson model
- ❍ D. Information security and life cycle model

Find the Answer p. 254

48. According to the Information Security and Life Cycle Model, security implemented early in the life cycle process results in all but which of the following?Select the best answer.

- ❍ A. Greater chance for success
- ❍ B. Lower costs
- ❍ C. Greater granularity
- ❍ D. Reduced work

Find the Answer p. 254

49. When testing a newly developed software, system, or solution, all but which of the following should be true?Select the best answer.

- ❍ A. All aspects of the system should be testable
- ❍ B. Testing should examine how incorrect values are handled
- ❍ C. Testing should probe boundary conditions
- ❍ D. Testing should use real or live data

Find the Answer p. 255

50. An intersection of a row and a column in a relational database is known as?Select the best answer.

- ❍ A. File
- ❍ B. Tuple
- ❍ C. Cell
- ❍ D. Attribute

Find the Answer p. 255

51. A column in a relational database table is known as?Select the best answer.

- ❍ A. File
- ❍ B. Tuple
- ❍ C. Cell
- ❍ D. Attribute

Find the Answer p. 255

52. A collection of records of the same type is known as?Select the best answer.

- ❍ A. File
- ❍ B. Tuple
- ❍ C. Cell
- ❍ D. Attribute

Find the Answer p. 255

53. A row in a relational database table is known as?Select the best answer.

- ❍ A. File
- ❍ B. Tuple
- ❍ C. Cell
- ❍ D. Attribute

Find the Answer p. 255

54. The attribute that makes each tuple unique in relational database is?Select the best answer.

- ❍ A. Domain
- ❍ B. Candidate key
- ❍ C. Primary key
- ❍ D. Foreign key

Find the Answer p. 255

55. In order to link the contents of two relational databases, the unique attribute from the second table is used in the first table as a?Select the best answer.

- ❍ A. Domain
- ❍ B. Candidate key
- ❍ C. Primary key
- ❍ D. Foreign key

Find the Answer p. 255

56. A hierarchical database provides for what types of relationships?Select the best answer.

- ❍ A. One-to-one
- ❍ B. One-to-many
- ❍ C. Many-to-many
- ❍ D. Many-to-one

Find the Answer p. 255

57. The range of allowable or valid values for attributes is known as?Select the best answer.

- ❍ A. Domain
- ❍ B. Candidate key
- ❍ C. Primary key
- ❍ D. Foreign key

Find the Answer p. 255

58. An attribute in a relational database that provides an additional unique identifier for tuples is known as?Select the best answer.

- ❍ A. Domain
- ❍ B. Candidate key
- ❍ C. Primary key
- ❍ D. Foreign key

Find the Answer p. 255

59. The number of rows in a relational database is known as?Select the best answer.

- ❍ A. Schema
- ❍ B. Data dictionary
- ❍ C. Cardinality
- ❍ D. Degree

Find the Answer p. 255

60. The number of columns in a relational database is known as?Select the best answer.

- ❍ A. Schema
- ❍ B. Data dictionary
- ❍ C. Cardinality
- ❍ D. Degree

Find the Answer p. 255

61. The data that defines the structure of the database is known as?Select the best answer.

- ❍ A. Schema
- ❍ B. Data dictionary
- ❍ C. Cardinality
- ❍ D. Degree

Find the Answer p. 255

62. The central repository for the data elements and their relationships is known as?Select the best answer.

- ❍ A. Schema
- ❍ B. Data dictionary
- ❍ C. Cardinality
- ❍ D. Degree

Find the Answer p. 255

63. Which of the following is NOT one of the steps or elements in data normalization?Select the best answer.

- ❍ A. Eliminating repeating groups
- ❍ B. Eliminating redundant data
- ❍ C. Eliminating the possibility of corrupted data by locking cells while they are being edited
- ❍ D. Eliminating attributes that are not dependant on the primary key

Find the Answer p. 255

64. Semantic integrity rules ensure that all structural and semantic rules of the database are not violated. Which of the following is NOT something that these rules would examine?Select the best answer.

- ❍ A. Data type
- ❍ B. Logical value
- ❍ C. Uniqueness constraints
- ❍ D. Relevance

Find the Answer p. 255

65. The mechanism that ensures that every tuple has a primary key and that that primary key is related to an existing record is known as?Select the best answer.

- ❍ A. Referential integrity mechanism
- ❍ B. Concurrency
- ❍ C. Semantic integrity rules
- ❍ D. Transaction management

Find the Answer p. 255

66. All but which of the following is a part of database transaction management?Select the best answer.

- ❍ A. Rollback statement
- ❍ B. Normalization
- ❍ C. Commit statement
- ❍ D. Checkpoints

Find the Answer p. 255

67. SQL server is not vulnerable to which of the following types of attacks?Select the best answer.

- ❍ A. Aggregation
- ❍ B. Inference
- ❍ C. Salami technique
- ❍ D. Dead lock

Find the Answer p. 255

68. When a database system supports transaction management, which of the following is it still vulnerable to, because users have access to data cells?Select the best answer.

- ❍ A. Inference
- ❍ B. Deadlock
- ❍ C. Denial of service
- ❍ D. Data integrity loss

Find the Answer p. 255

69. The user interface for a database enforces indirect access. This type of restricted interface or controlled view provides all but which of the following?Select the best answer.

- ❍ A. Support for confidentiality
- ❍ B. Providing availability
- ❍ C. Protection from unauthorized disclosure
- ❍ D. Maintaining integrity

Find the Answer p. 255

70. Hiding specific cells in a database to prevent against inference attacks is known as?Select the best answer.

- ❍ A. Polyinstantiation
- ❍ B. Database partitioning
- ❍ C. Cell suppression
- ❍ D. Perturbation

Find the Answer p. 255

71. A centralized repository of normalized information from various databases that is made available to users to perform queries against is known as?Select the best answer.

- ❍ A. Data mining
- ❍ B. Data mart
- ❍ C. Data dictionary
- ❍ D. Data warehouse

Find the Answer p. 255

72. What type of virus requires just a host program to replicate and distribute itself?Select the best answer.

- ❍ A. Common virus
- ❍ B. Boot virus
- ❍ C. Multi-part virus
- ❍ D. Macro virus

Find the Answer p. 255

73. Which of the following is NOT considered a valid safeguard against viruses?Select the best answer.

- ❍ A. Hash signature file verification
- ❍ B. Biometric authentication
- ❍ C. Strong DAC access controls
- ❍ D. Scanning for e-mail born viruses on e-mail gateway systems

Find the Answer p. 255

74. The purpose of an audit trail is to?Select the best answer.

- ❍ A. Detect normal activity
- ❍ B. Test system security
- ❍ C. Validate trust
- ❍ D. Recreate events

Find the Answer p. 256

75. Which of the following is FALSE in regards to superzap?Select the best answer.

- ❍ A. It can bypass system security mechanisms
- ❍ B. It is is not easily detected
- ❍ C. Its use is usually logged by the system
- ❍ D. It is used to recover from system freezes

Find the Answer p. 256

76. Initial program load vulnerabilities include all but which of the following?Select the best answer.

- ❍ A. Booting from a CD
- ❍ B. Turning off the power
- ❍ C. Using an alternate boot menu
- ❍ D. Accessing CMOS

Find the Answer p. 256

77. When a buffer overflow occurs, the extra data may flow into the CPU and cause what?Select the best answer.

- ❍ A. Elevation of privileges
- ❍ B. The system to drop the extra data
- ❍ C. An error event log is written
- ❍ D. Execution of malicious code in privileged mode

Find the Answer p. 256

Chapter 3
Business Continuity and Disaster Recovery Planning

1. Failing to properly address which of the following in the design and programming phases of software development has the greatest risk of allowing buffer overflows?Select the best answer.

   - ❍ A. Data input block size
   - ❍ B. ASCII vs. binary input
   - ❍ C. Alpha vs. numeric input
   - ❍ D. Data input length of numerals (i.e., number of digits)

   Find the Answer p. 257

2. Which of the following is NOT a goal of disaster recovery planning?Select the best answer.

   - ❍ A. Maintaining critical functions through a minor disruptive event
   - ❍ B. Protecting an organization from major IT failure
   - ❍ C. Minimizing the risk to an organization from the interruption of mission critical processes
   - ❍ D. Maintaining reliable backup and restoration solutions through testing and simulation

   Find the Answer p. 257

3. Which of the following is the best type of leadership that should assume control while the disaster recovery plan is being carried out?Select the best answer.

   - ❍ A. Committee
   - ❍ B. Procedural
   - ❍ C. Interactive
   - ❍ D. Democratic

   Find the Answer p. 257

4. The primary goal of the data processing continuity aspect of disaster recovery planning is?Select the best answer.

- ❍ A. Maintaining data integrity throughout the disaster
- ❍ B. Maintaining functional networking access throughout the disaster
- ❍ C. Ensuring workers can complete their work tasks
- ❍ D. Moving the entire IT infrastructure over to a secondary location

Find the Answer p. 257

5. Which of the following is NOT a valid option for alternate site selection within disaster recovery planning?Select the best answer.

- ❍ A. Mutual aid agreements
- ❍ B. Subscription services
- ❍ C. Service bureaus
- ❍ D. Adjacent building rental

Find the Answer p. 257

6. What is a mutual aid agreement?Select the best answer.

- ❍ A. Two parties agreeing to support each other's critical business functions in the event of a disaster
- ❍ B. Two parties agreeing to share the cost of maintaining an alternate site
- ❍ C. Two parties agreeing to work together in building secondary locations
- ❍ D. An insurance company agreeing to pay for IT relocation services

Find the Answer p. 257

7. Which of the following is the most cost effective alternate site location, but which is most likely to be useless when actually needed?Select the best answer.

- ❍ A. Hot site
- ❍ B. Mutial aid agreements
- ❍ C. Portable warm site
- ❍ D. Service bureau contract

Find the Answer p. 257

8. Which of the following is an advantage of a hot site?Select the best answer.

- ❍ A. Having a duplicate copy of sensitive data
- ❍ B. Cost
- ❍ C. Fully configured systems with all supporting utilities and infrastructure
- ❍ D. Requires constant maintenance

Find the Answer p. 257

9. Which of the following is an advantage of a warm site as compared to a hot site?Select the best answer.

- ❍ A. Applications may not be fully installed
- ❍ B. Systems are not fully configured
- ❍ C. Communications links are not installed
- ❍ D. Moderate administrative and maintenance costs

Find the Answer p. 257

10. What type of site can make adequate recovery impossible?Select the best answer.

- ❍ A. Cold site
- ❍ B. Service bureaus
- ❍ C. Multiple production centers
- ❍ D. A mobile hot backup site

Find the Answer p. 257

11. What is the most common but least effective selection or type of an alternate backup site?Select the best answer.

- ❍ A. Service bureau
- ❍ B. Cold site
- ❍ C. Mobile backup site
- ❍ D. Multiple processing centers

Find the Answer p. 257

12. Which of the following is FALSE about cold sites?Select the best answer.

- ❍ A. Equipment will need to be brought in
- ❍ B. Communication lines may not be installed
- ❍ C. A duplicate copy of critical data is hosted there
- ❍ D. HVAC (Heating, Ventilation, Air Conditioning) is probably installed

Find the Answer p. 257

13. What is the primary benefit of using multiple processing centers?Select the best answer.

- ❍ A. Each location is owned and managed by a different entity
- ❍ B. Each location is within a small geographic area
- ❍ C. If a location is compromised, the remaining locations may not have sufficient capabilities to handle the additional load
- ❍ D. The mission critical applications of an organization are spread among numerous physical locations

Find the Answer p. 257

14. Which of the following is a disadvantage to a service bureau contract for an alternate processing site?Select the best answer.

- ❍ A. Resource contention during a large emergency
- ❍ B. Testing is often possible
- ❍ C. Cost effective
- ❍ D. Offer quick response and reasonable availability

Find the Answer p. 257

15. Vendor re-supply of hardware is an acceptable practice for all forms of alternate site locations except for?Select the best answer.

- ❍ A. Rolling mobile backup sites
- ❍ B. Hot site
- ❍ C. Multiple processing centers
- ❍ D. Service bureau contracts

Find the Answer p. 257

16. Which of the following should NOT be true regarding an alternate site?Select the best answer.

- ❍ A. It should have sufficient capacity to support all critical business functions
- ❍ B. The facility should be far enough away not to be affected by the same disaster
- ❍ C. It should be located very close to the primary site
- ❍ D. It should support the mission critical processes of the organization

Find the Answer p. 257

17. Another name for the backup strategy of electronic vaulting is?Select the best answer.

- ❍ A. Remote journaling
- ❍ B. Parallel processing
- ❍ C. Database shadowing
- ❍ D. Batch processing

Find the Answer p. 257

18. As a backup strategy, the act of parallel processing of transactions is also known as?Select the best answer.

- ❍ A. Remote journaling
- ❍ B. Electronic vaulting
- ❍ C. Batch processing
- ❍ D. Database shadowing

Find the Answer p. 257

19. Which form of a disaster recovery test performs all activities of the disaster recovery plan up to, but not including, the point where processing at the alternate site begins?Select the best answer.

- ❍ A. Full interruption test
- ❍ B. Structured walk through test
- ❍ C. Simulation test
- ❍ D. Parallel test

Find the Answer p. 257

20. Which of the following is NOT a reason to test a disaster recovery plan?Select the best answer.

- ❍ A. Testing verifies the accuracy of the procedures
- ❍ B. Testing minimizes legal liability
- ❍ C. Testing trains personnel
- ❍ D. Testing verifies the processing capability of the alternate site

Find the Answer p. 257

21. When designing the test document (i.e., the procedure for the test) for a disaster recovery plan, all but which of the following must be included?Select the best answer.

- ❍ A. The length of the test
- ❍ B. The participants in the test
- ❍ C. The cost in productivity of the test
- ❍ D. The resources or services to be included in the test

Find the Answer p. 257

22. Which of the following types of disaster recovery plan tests should be performed first to discover any omissions or modifications that may be needed for your plan?Select the best answer.

- ❍ A. Structured walk through test
- ❍ B. Simulation test
- ❍ C. Parallel test
- ❍ D. Checklist test

Find the Answer p. 257

23. Which type of disaster recovery tests is performed by individuals separately rather than by a group of personnel working together as a team?Select the best answer.

- ❍ A. Checklist test
- ❍ B. Simulation test
- ❍ C. Structured walk through test
- ❍ D. Parallel test

Find the Answer p. 257

24. Which of the following disaster recovery tests can be performed simultaneously with any of the other tests?Select the best answer.

- ❍ A. Simulation test
- ❍ B. Structured walk through test
- ❍ C. Parallel test
- ❍ D. Full interruption test

Find the Answer p. 258

25. Which form of disaster recovery test performs all activities of the plan but processing at the primary facility does not stop?Select the best answer.

- ❍ A. Full interruption test
- ❍ B. Structured walk through test
- ❍ C. Simulation test
- ❍ D. Parallel test

Find the Answer p. 258

26. Which disaster recovery test performs all activities of the plan, including terminating processing at the primary site?Select the best answer.

- ❍ A. Full interruption test
- ❍ B. Structured walk through test
- ❍ C. Simulation test
- ❍ D. Parallel test

Find the Answer p. 258

27. Which of the following is NOT one of the three primary goals of a business impact analysis?Select the best answer.

- ❍ A. Criticality Prioritization
- ❍ B. Downtime Estimation
- ❍ C. Risk Mitigation
- ❍ D. Resource Requirements

Find the Answer p. 258

28. Which of the following data processing facility continuity plans is the least expensive?Select the best answer.

- ❍ A. Prefabricated buildings
- ❍ B. Warm sites
- ❍ C. Rolling backup sites
- ❍ D. Mutual aid agreement

Find the Answer p. 258

29. Which of the following transaction redundancy implementations duplicates data on multiple servers?Select the best answer.

- ❍ A. Database shadowing
- ❍ B. Remote journaling
- ❍ C. Electronic vaulting
- ❍ D. Periodic backups

Find the Answer p. 258

30. Which of the following is a disaster recovery plan test that walks through the entire plan but does not implement alternate processing?Select the best answer.

- ❍ A. Checklist test
- ❍ B. Simulation test
- ❍ C. Parallel test
- ❍ D. Full interruption test

Find the Answer p. 258

31. After a disaster, when should the salvage team return to the primary facility site?Select the best answer.

- ❍ A. As soon as alternate processing is initiated
- ❍ B. Only after the disaster is completely over
- ❍ C. Once personnel safety can be assured
- ❍ D. As soon as data remaining at the primary site is needed for business continuity

Find the Answer p. 258

32. The security issue that addresses ongoing processing activity in the face of minor disruptive events is known as?Select the best answer.

- ❍ A. Business continuity planning
- ❍ B. Disaster recovery planning
- ❍ C. Mission critical relocation planning
- ❍ D. Redundancy development planning

Find the Answer p. 258

33. Which of the following is NOT a goal or objective of business continuity planning?Select the best answer.

- ❍ A. Reducing the risks associated with a disruptive event
- ❍ B. Minimizing costs associated with recovering from a disruptive event
- ❍ C. Maintaining business capability during a disruptive event
- ❍ D. Providing a procedural guide so no decisions are necessary during a disruptive event

Find the Answer p. 258

34. Which of the following should be accomplished first when acting out a business continuity plan?Select the best answer.

- ❍ A. Restoring critical functions
- ❍ B. Restoring non-critical functions
- ❍ C. Maintaining personnel safety
- ❍ D. Locating an alternate site

Find the Answer p. 258

35. What is the primary difference between a disaster recovery plan and a business continuity plan?Select the best answer.

- ❍ A. The severity of the damage to the area caused by a disaster
- ❍ B. The use of a secondary site
- ❍ C. The cost of maintenance
- ❍ D. The interruption of mission critical processes

Find the Answer p. 258

36. Although the activities themselves can be delegated, who is ultimately responsible for all phases of business continuity planning?Select the best answer.

- ❍ A. Senior management
- ❍ B. InfoSec teams
- ❍ C. Systems auditor
- ❍ D. Department managers

Find the Answer p. 258

37. Business continuity planning should address all but which of the following?Select the best answer.

- ❍ A. Local area network components
- ❍ B. Telecommunications
- ❍ C. Employee personal possessions
- ❍ D. Applications and software

Find the Answer p. 258

38. Which of the following is not one of the four aspects or elements of a business continuity plan?Select the best answer.

- ❍ A. Business impact assessment
- ❍ B. Scope and plan initiation
- ❍ C. Business continuity plan development
- ❍ D. Alternate site location

Find the Answer p. 258

39. Which of the following is NOT a goal of business impact assessment?Select the best answer.

- ❍ A. Criticality prioritization
- ❍ B. Establishing resource requirements
- ❍ C. OS migration
- ❍ D. Downtime estimation

Find the Answer p. 258

40. The business continuity planning task of identifying key business processes, ordering those processes, and evaluating event impact is known as?Select the best answer.

- ❍ A. Criticality prioritization
- ❍ B. Business impact assessment
- ❍ C. Vulnerability assessment
- ❍ D. Quantative analysis

Find the Answer p. 258

41. Which of the following is considered an essential element of due care and due diligence?Select the best answer.

- ❍ A. Creation of InfoSec teams
- ❍ B. Business continuity and disaster recovery planning
- ❍ C. Delegating implementation tasks to subordinates
- ❍ D. Senior management must participate in all security planning activities

Find the Answer p. 258

42. Which of the following is NOT an event that would be considered to trigger application of the business continuity plan?Select the best answer.

- ❍ A. Fire in the data center
- ❍ B. Earthquake resulting in broken communication lines
- ❍ C. Floods affecting the basement levels only
- ❍ D. An intrusion attack that defaces the Web server

Find the Answer p. 258

43. Which of the following is NOT an event that would be considered to trigger application of the business continuity plan?Select the best answer.

- ❍ A. A ruptured gas line explosion that destroys most of your primary site
- ❍ B. A wind storm that completely severs your power and communications
- ❍ C. A hurricane that floods your data center
- ❍ D. A rupture in a gas main near your primary facility

Find the Answer p. 258

44. A disaster recovery plan may be triggered by all but which of the following?Select the best answer.

- ❍ A. A mud slide burying your primary site
- ❍ B. Intermittent loss of access to a resource Web site
- ❍ C. A fire that destroys your entire data center
- ❍ D. A robbery where your primary servers are stolen

Find the Answer p. 258

45. The scope of the business continuity plan should include which of the following?Select the best answer.

- ❍ A. People, infrastructure, supplies, equipment
- ❍ B. Media relations, human resources, people, facilities
- ❍ C. Office supplies, people, infrastructure, facilities
- ❍ D. Infrastructure (IT), facilities, supplies and equipment

Find the Answer p. 258

46. When updating or maintaining a business continuity plan, which of the following is most important?Select the best answer.

- ❍ A. Only a single copy of the plan should exist throughout the organization
- ❍ B. Each department should develop and maintain their own plan
- ❍ C. The business continuity plan cannot make recommendations outside of the organization's security policy
- ❍ D. Keeping the cost of the plan to a minimum

Find the Answer p. 258

47. The process of making employees aware of the business continuity plan is found in what stage or element of the business continuity plan development process?Select the best answer.

- ❍ A. Business impact assessment
- ❍ B. Plan approval and implementation
- ❍ C. Business continuity plan development
- ❍ D. Scope and plan initiation

Find the Answer p. 258

48. The Maximum Tolerable Downtime estimation is an indication of what?Select the best answer.

- ❍ A. How long the business continuity plan takes to develop
- ❍ B. How long the business continuity plan takes to implement
- ❍ C. How long the migration to the secondary site will take
- ❍ D. How long can mission critical processes be down and still allow the organization to recover

Find the Answer p. 258

49. When performing a business impact analysis, which of the following is the LEAST useful assessment material item to gather?Select the best answer.

- ❍ A. Organizational chart
- ❍ B. Mission statement
- ❍ C. Definition of business units
- ❍ D. Outline of relationships within the organization

Find the Answer p. 259

50. When a business impact analysis is completed, what is the result?Select the best answer.

- ❍ A. A risk analysis report
- ❍ B. An auditor's final report
- ❍ C. A business continuity plan
- ❍ D. An organizational security policy

Find the Answer p. 259

51. Which of the following is NOT an element of the vulnerability assessment process of business impact analysis?Select the best answer.

- ❍ A. Quantitative analysis
- ❍ B. Qualitative analysis
- ❍ C. Defining critical areas and dependencies
- ❍ D. Selecting countermeasures

Find the Answer p. 259

52. Which form of disaster recovery test is an on-paper only walk through of the plan in a group meeting?Select the best answer.

- ❍ A. Full interruption test
- ❍ B. Structured walk through test
- ❍ C. Simulation test
- ❍ D. Parallel test

Find the Answer p. 259

53. The best method to test that a disaster recovery plan is fully capable of handling a serious disaster is to use which of the following testing methods?Select the best answer.

- ❍ A. Simulation test
- ❍ B. Structured walk through test
- ❍ C. Full interruption test
- ❍ D. Parallel test

Find the Answer p. 259

54. According to a disaster recovery plan, the recovery team is responsible for which of the following?Select the best answer.

- ❍ A. Returning to the primary site
- ❍ B. Getting non-critical processing operations up at the primary site
- ❍ C. Ensuring that threat to personnel at the primary site has been eliminated
- ❍ D. Implementing the disaster recovery plan

Find the Answer p. 259

55. Which of the following is a responsibility of the salvage team?Select the best answer.

- ❍ A. Return primary site back to normal operating conditions
- ❍ B. Implement the disaster recovery plan to get business functions operational at the alternate site
- ❍ C. Ensure personnel safety at the alternate site
- ❍ D. Minimize the risk of disaster effect at the primary site

Find the Answer p. 259

56. Which of the following represent the true scope of threats to an organization that may trigger the use of a business continuity plan or a disaster recovery plan?Select the best answer.

- ❍ A. Man-made, technical, accidental
- ❍ B. Natural, technical, circumstantial
- ❍ C. Man-made, natural, technical
- ❍ D. Natural, mythical, theoretical

Find the Answer p. 259

57. The most critical part of a disaster recovery plan to ensure that it will be effective in restoring the organization is?Select the best answer.

- ❍ A. Vulnerability assessment
- ❍ B. Project initiation
- ❍ C. Senior management signoff
- ❍ D. Ongoing maintenance

Find the Answer p. 259

58. Testing a business continuity plan performs all but which of the following?Select the best answer.

- ❍ A. Personnel training
- ❍ B. Staff awareness
- ❍ C. Design improvements
- ❍ D. Viability testing

Find the Answer p. 259

59. When should the salvage team return to the primary site?Select the best answer.

- ❍ A. As soon as critical processes are operating at the alternate site
- ❍ B. After threat to personal safety is eliminated
- ❍ C. Immediately to recover the backup media
- ❍ D. Within 24 hours of the disaster

Find the Answer p. 259

60. Once the disaster recovery plan has been activated, when is the emergency considered over?Select the best answer.

- ❍ A. When mission critical operations are functioning at the alternate site
- ❍ B. When the threat to human safety is eliminated
- ❍ C. When all operations are back at the primary site
- ❍ D. When the organization has maintained viability for three months after the disaster

Find the Answer p. 259

61. Why is an emergency NOT considered over until the organization fully returns to the primary site?Select the best answer.

- ❍ A. Human safety is not protected until the primary site is restored
- ❍ B. Legal requirements for insurance mandate this
- ❍ C. The alternate site can never fully support the operations of the organization
- ❍ D. Because a vulnerability exists when shifting mission critical applications from the alternate back to the primary site

Find the Answer p. 259

62. When returning to the primary site after the alternate site has been used for mission critical processing, what is the first step?Select the best answer.

- ❍ A. Return non-mission critical functions to the primary site
- ❍ B. Interrupt all operations at the alternate site
- ❍ C. Return mission critical functions to the primary site
- ❍ D. Verify safety of the alternate site

Find the Answer p. 259

63. Which arrangement does NOT need to be done before a disaster occurs?Select the best answer.

- ❍ A. Establish an alternate or backup site
- ❍ B. Establish a media contact at each of the major news agencies
- ❍ C. Make preparations to continue writing paychecks
- ❍ D. Create a rendezvous point for all employees

Find the Answer p. 259

64. Which of the following is the least important activity to perform once a disaster recovery plan is developed?Select the best answer.

- ❍ A. Post the plan on the public Web server
- ❍ B. Test the plan for viability
- ❍ C. Train staff on using the plan
- ❍ D. Retain only a single version of the plan

Find the Answer p. 259

65. When seeking senior management signoff on the final version of a disaster recovery plan, which of the following is least important?Select the best answer.

- ❍ A. Whether the plan is sufficient to recover all aspects of the organization
- ❍ B. The details of disaster recovery plans from other organizations
- ❍ C. Whether the plan has been tested for viability
- ❍ D. The level of detail the procedures include for recovering

Find the Answer p. 259

66. What is the most important element or aspect of business continuity planning or disaster recovery planning?Select the best answer.

- ❍ A. Vulnerability assessment
- ❍ B. Criticality prioritization
- ❍ C. Maintaining critical processes across any disruptive event
- ❍ D. Management support

Find the Answer p. 259

67. In the event of a minor disaster, which of the following activities should occur to restore systems and recover data files?Select the best answer.

- ❍ A. Initiate the business continuity plan
- ❍ B. Restore files from backup
- ❍ C. Initiate a full interruption test
- ❍ D. Perform a vulnerability analysis

Find the Answer p. 259

68. Qualitative and quantitative elements can be found in which of the following?Select the best answer.

- ❍ A. Senior management approval
- ❍ B. Business impact analysis
- ❍ C. Simulation testing
- ❍ D. Criticality prioritization

Find the Answer p. 259

69. When designing a business continuity plan to prevent single points of failure, which of the following is the most important?Select the best answer.

- ❍ A. Use RAID
- ❍ B. Test backups
- ❍ C. Establish redundancy
- ❍ D. Install surge protectors

Find the Answer p. 259

70. The owner of the business continuity plan and the disaster recovery plan in your organization is?Select the best answer.

- ❍ A. CIRT (Computer Incident Response Team)
- ❍ B. Internal auditor
- ❍ C. Departmental network administrator
- ❍ D. Senior management

Find the Answer p. 259

71. When performing a business impact analysis, which of the following is necessary?Select the best answer.

- ❍ A. Outlining critical operation dependencies
- ❍ B. Contracting with a service bureau
- ❍ C. Selecting countermeasures
- ❍ D. Defining staff responsibilities

Find the Answer p. 259

72. Which of the following provides the most useful or meaningful information?Select the best answer.

- ❍ A. Testing a disaster recovery plan and learning whether it passed or failed overall
- ❍ B. Testing a disaster recovery plan and learning what aspects failed
- ❍ C. Testing a business continuity plan and learning which staff members failed to follow procedure
- ❍ D. Testing a business continuity plan and restoring files from the most recent full backup

Find the Answer p. 259

73. A business continuity plan should address which sets of threats?Select the best answer.

- ❍ A. Intrusion attacks and man-made disasters
- ❍ B. Hardware failures and natural disasters
- ❍ C. Natural and man-made disasters
- ❍ D. Technical failures and human error

Find the Answer p. 259

74. When selecting an alternate site for a disaster recovery plan, which of the following is the most important consideration factor?Select the best answer.

- ❍ A. Location
- ❍ B. Size
- ❍ C. Cost
- ❍ D. Capability of supporting business processing

Find the Answer p. 260

75. The best location for a data center in an alternate site is?Select the best answer.

- ❍ A. Ground floor
- ❍ B. Center of building
- ❍ C. Sub-basement
- ❍ D. Penthouse

Find the Answer p. 260

76. Which of the following is the most often overlooked aspect of disaster recovery?Select the best answer.

- ❍ A. Maintaining employee compensation mechanisms
- ❍ B. Protecting human safety
- ❍ C. Restoring and maintaining critical business functions
- ❍ D. Alternate site selection

Find the Answer p. 260

77. To control costs while maintaining a reasonable level of protection against the failure of hardware, you should?Select the best answer.

- ❍ A. Know the locations of several hardware vendors in your city
- ❍ B. Maintain a hot site duplicate facility
- ❍ C. Obtain a service level agreement with a hardware vendor
- ❍ D. Store replacement parts on site

Find the Answer p. 260

78. Which of the following is NOT a commonly used backup tape management scheme?Select the best answer.

- ❍ A. Grandfather, father, son
- ❍ B. Six-cartridge weekly backup principle
- ❍ C. Pillar of Absolom
- ❍ D. Tower of Hanoi

Find the Answer p. 260

79. Which of the following backup methods does not reset the archive bit and backs up all data changed since the last full or incremental backup?Select the best answer.

- ❍ A. Full
- ❍ B. Daily
- ❍ C. Incremental
- ❍ D. Differential

Find the Answer p. 260

80. What is always true about using a periodic backup media system for protecting data?Select the best answer.

- ❍ A. Some amount of data is always lost when the primary source fails
- ❍ B. Transfer rates are always faster than normal network connectivity
- ❍ C. The time required to perform backups decreases as the amount of data increases
- ❍ D. The number of backup medias needed to perform a backup decreases as the amount of data increases

Find the Answer p. 260

Chapter 4
Cryptography

1. What form of single sign-on technology employs symmetric key cryptography and DES encryption to provide end-to-end security?Select the best answer.

   - ❍ A. Scripting
   - ❍ B. Kerberos
   - ❍ C. SESAME
   - ❍ D. KryptoKnight

   Find the Answer p. 261

2. The time, effort, and/or cost involved in breaking a cryptographic system is known as?Select the best answer.

   - ❍ A. Algorithm
   - ❍ B. Key length
   - ❍ C. Work function
   - ❍ D. Key space

   Find the Answer p. 261

3. The strength of a cryptosystem is dependant upon all but which of the following?Select the best answer.

   - ❍ A. Algorithm
   - ❍ B. Secrecy of the key
   - ❍ C. Initialization vector
   - ❍ D. Length of ciphertext

   Find the Answer p. 261

4. The goals or benefits of a cryptosystem include protection or support for all but which of the following?Select the best answer.

- ❍ A. Availability
- ❍ B. Confidentiality
- ❍ C. Integrity
- ❍ D. Non-repudiation

Find the Answer p. 261

5. A polyalphabetic cipher is vulnerable to what form of attack?Select the best answer.

- ❍ A. Birthday attack
- ❍ B. Frequency analysis
- ❍ C. Period analysis
- ❍ D. Collision

Find the Answer p. 261

6. In addition to polyalphabetic ciphers, what other crypotgraphic system is also vulnerable to frequency analysis?Select the best answer.

- ❍ A. Vernam cipher
- ❍ B. Running key cipher
- ❍ C. Substitution cipher
- ❍ D. Code ciphers

Find the Answer p. 261

7. A vernam cipher is an example of what type of cryptographic system?Select the best answer.

- ❍ A. Transposition cipher
- ❍ B. Running key cipher
- ❍ C. Polyalphabetic substitution cipher
- ❍ D. One-time pad

Find the Answer p. 261

8. The Escrowed Encryption Standard (EES) is embodied in which of the following?Select the best answer.

- ❍ A. Clipper chip
- ❍ B. Data Encryption Standard (DES)
- ❍ C. A symmetric cryptographic system
- ❍ D. Digital Signature Standard (DSS)

Find the Answer p. 261

9. The skipjack algorithm used in the clipper chip used what length of key?Select the best answer.

- ❍ A. 56
- ❍ B. 80
- ❍ C. 128
- ❍ D. 256

Find the Answer p. 261

10. Which of the following terms is out of place when compared to the others?Select the best answer.

- ❍ A. Symmetric key cryptography
- ❍ B. Secret key
- ❍ C. Public key
- ❍ D. Shared common key

Find the Answer p. 261

11. Which of the following terms is out of place when compared to the others?Select the best answer.

- ❍ A. Asymmetric cryptography
- ❍ B. Public key infrastructure
- ❍ C. Key pairs
- ❍ D. Bulk encryption

Find the Answer p. 261

12. Triple Data Encryption Standard (3DES) offers what key bit length strength?Select the best answer.

- ❍ A. 168
- ❍ B. 56
- ❍ C. 124
- ❍ D. 256

Find the Answer p. 261

13. What encryption system was selected to replace Triple Data Encryption Standard (3DES)?Select the best answer.

- ❍ A. TwoFish
- ❍ B. Advanced Encryption System (AES)
- ❍ C. IDEA
- ❍ D. RC5

Find the Answer p. 261

14. Which of the following is a symmetric block cipher?Select the best answer.

- ❍ A. MD5
- ❍ B. Haval
- ❍ C. TwoFish
- ❍ D. El Gamal

Find the Answer p. 261

15. Which of the following is NOT a valid key length for Advanced Encryption System (AES)?Select the best answer.

- ❍ A. 256
- ❍ B. 192
- ❍ C. 128
- ❍ D. 64

Find the Answer p. 261

16. The IDEA cipher uses what key length?Select the best answer.

- ❍ A. 128
- ❍ B. 108
- ❍ C. 64
- ❍ D. 56

Find the Answer p. 261

17. The cryptographic system that uses key pairs, where one key is kept secret and one is freely and publicly distributed, is known as?Select the best answer.

- ❍ A. Symmetric cryptosystem
- ❍ B. Asymmetric cryptosystem
- ❍ C. Digital signature cryptosystem
- ❍ D. Message digest cryptosystem

Find the Answer p. 261

18. Which of the following is NOT a benefit of a public key cryptographic system?Select the best answer.

- ❍ A. No need to exchange secret keys
- ❍ B. The private key cannot be derived from the public key
- ❍ C. No need to perform key distribution
- ❍ D. When one of the keys in a key pair is used to encrypt a message, only the key's partner can be used to decrypt that message

Find the Answer p. 261

19. What cryptographic system is dependant upon the use of a trapdoor one-way function?Select the best answer.

- ❍ A. Symmetric key cryptography
- ❍ B. Message digest algorithms
- ❍ C. Cryptosystems relying upon key exchange
- ❍ D. Asymmetric key cryptography

Find the Answer p. 261

20. What asymmetric cryptographic system is based upon the product of two very large prime numbers?Select the best answer.

- ❍ A. RSA (Rivest, Shamir, and Addleman)
- ❍ B. Diffie-Hellman
- ❍ C. Merkle-Hellman Knapsack
- ❍ D. El Gamal

Find the Answer p. 261

21. What cryptographic system includes a method by which secret keys can be exchanged securely over an insecure medium?Select the best answer.

- ❍ A. Haval
- ❍ B. Diffie-Hellman
- ❍ C. Rijndael
- ❍ D. El Gamal

Find the Answer p. 261

22. All but which of the following are true regarding elliptic curve cryptosystems (ECC)?Select the best answer.

- ❍ A. Can be used to implement Diffie-Hellman, El Gamal, or Schnorr public key algorithms
- ❍ B. Smaller key sizes used in ECC can result in higher levels of security than larger non-ECC algorithms
- ❍ C. Not suitable for hardware applications
- ❍ D. Can be used for digital signatures, encryption, and key management

Find the Answer p. 261

23. A certificate issued by a publicly trusted CA will usually contain all but which of the following?Select the best answer.

- ❍ A. Serial number
- ❍ B. Identity information
- ❍ C. Signature of issuing authority
- ❍ D. IP address

Find the Answer p. 261

24. Which of the following is FALSE in regards to a Registration Authority system in a PKI solution?Select the best answer.

- ❍ A. It issues new certificates
- ❍ B. It confirms the identity of a subject
- ❍ C. It distributes the certificate revocation list (CRL)
- ❍ D. It helps share the workload with the certificate authority (CA)

Find the Answer p. 262

25. A message digest provides for which of the following?Select the best answer.

- ❍ A. Confidentiality
- ❍ B. Integrity
- ❍ C. Authentication
- ❍ D. Non-repudiation

Find the Answer p. 262

26. Which of the following is FALSE in regards to hash functions?Select the best answer.

- ❍ A. Its secrecy and security is in its one-way-ness
- ❍ B. The hash function algorithm is publicly known
- ❍ C. The original plaintext can be reconstructed from the hash value or message digest
- ❍ D. Produces a fixed length hash value no matter what the length of the inputted plaintext

Find the Answer p. 262

27. The strength of a crypto system is based on all but which of the following?Select the best answer.

- ❍ A. Algorithm
- ❍ B. Size of keyspace
- ❍ C. Intialization vector
- ❍ D. Length of key

Find the Answer p. 262

28. Which of the following is not a goal of cryptography?Select the best answer.

- ❍ A. Confidentiality
- ❍ B. Non-repudiation
- ❍ C. Availability
- ❍ D. Integrity

Find the Answer p. 262

29. What type of cipher is subject to cracking by means of period analysis?Select the best answer.

- ❍ A. Transposition cipher
- ❍ B. Vernam cipher
- ❍ C. Running key cipher
- ❍ D. Polyalphabetic cipher

Find the Answer p. 262

30. The cryptography mechanism that hides information within images is known as?Select the best answer.

- ❍ A. Steganography
- ❍ B. Coding
- ❍ C. Substitution
- ❍ D. Tuple

Find the Answer p. 262

31. Which of the following was selected to replace Triple DES (3DES) in 2001?Select the best answer.

- ❍ A. Twofish Algorithm
- ❍ B. Advanced Encryption Standard (AES)
- ❍ C. IDEA cipher
- ❍ D. RC5

Find the Answer p. 262

32. The set of mathematical rules that dictate how enciphering and deciphering take place is known as the?Select the best answer.

- ❍ A. Key
- ❍ B. Ciphertext
- ❍ C. Code
- ❍ D. Algorithm

Find the Answer p. 262

33. What must be kept secret in order for a cryptosystem to provide any form of protection for messages?Select the best answer.

- ❍ A. Key
- ❍ B. Algorithm
- ❍ C. Keyspace
- ❍ D. Block size

Find the Answer p. 262

34. The strength of a cryptosystem is based on all but which of the following?Select the best answer.

- ❍ A. Algorithm
- ❍ B. The length of the plaintext
- ❍ C. Secrecy of the keys
- ❍ D. Initialization vectors

Find the Answer p. 262

35. Which of the following is NOT a goal of cryptosystems?Select the best answer.

- ❍ A. Confidentiality
- ❍ B. Non-repudiation
- ❍ C. Availability
- ❍ D. Integrity

Find the Answer p. 262

36. The action of dividing a plaintext message into fixed length segments and applying the same algorithm to each segment to hide the message is known as?Select the best answer.

- ❍ A. Clustering
- ❍ B. End-to-end encryption
- ❍ C. Encryption streaming
- ❍ D. Block ciphering

Find the Answer p. 262

37. An unintelligible message is also called what?Select the best answer.

- ❍ A. Cryptogram
- ❍ B. Cipher
- ❍ C. Code
- ❍ D. Algorithm

Find the Answer p. 262

38. When the same ciphertext is produced when a single plaintext is encrypted using two different keys, this is known as?Select the best answer.

- ❍ A. Collusion
- ❍ B. Clustering
- ❍ C. Polyinstantiation
- ❍ D. Scavenging

Find the Answer p. 262

39. A cryptographic transformation that operates at the word or phrase level is known as?Select the best answer.

- ❍ A. Cipher
- ❍ B. Block cipher
- ❍ C. Code cipher
- ❍ D. Streaming cipher

Find the Answer p. 262

40. When data is encrypted for the entire trip across an untrusted network, from source to destination, this is known as?Select the best answer.

- ❍ A. Work factor encryption
- ❍ B. Link encryption
- ❍ C. Streaming encryption
- ❍ D. End-to-end encryption

Find the Answer p. 262

41. Which of the following mechanisms always encrypts the entire message or data packet, including the header?Select the best answer.

- ❍ A. Link encryption
- ❍ B. End-to-end encryption
- ❍ C. IPSec in transport mode
- ❍ D. PPTP tunnels with CHAP

Find the Answer p. 262

42. When using end-to-end encryption, the actual process of encryption occurs at what level of the OSI model?Select the best answer.

- ❍ A. Physical layer
- ❍ B. Application layer
- ❍ C. Nework layer
- ❍ D. Session layer

Find the Answer p. 262

43. When using link encryption, the actual process of encryption occurs at what level of the OSI model?Select the best answer.

- ❍ A. Application layer
- ❍ B. Session layer
- ❍ C. Physical layer
- ❍ D. Network layer

Find the Answer p. 262

44. The most common mathematical Boolean operation performed by cryptographic systems is?Select the best answer.

- ❍ A. Eliptical curve
- ❍ B. Discrete algorithm
- ❍ C. ANDing
- ❍ D. Exlusive OR

Find the Answer p. 262

45. Which of the following is NOT true in regards to a one-time pad?Select the best answer.

- ❍ A. Extremely suitable for modern applications
- ❍ B. Often used as a stream cipher
- ❍ C. True random codes makes one-time pads unbreakable
- ❍ D. The key length is the same as the length of the original message

Find the Answer p. 262

46. All but which of the following is an example of steganongraphy?Select the best answer.

- ❍ A. Micro dots
- ❍ B. Hiding data in a bad sector on a hard drive
- ❍ C. Watermarks
- ❍ D. Hiding a text message in a visual image

Find the Answer p. 262

47. The art and science of hiding the meaning of communications from unintended recipients is known as?Select the best answer.

- ❍ A. Cryptanalysis
- ❍ B. Stenanography
- ❍ C. Cryptography
- ❍ D. Ciphering

Find the Answer p. 262

48. The art of obtaining the plaintext (i.e., the original message) or the key from ciphertext is known as?Select the best answer.

- ❍ A. Stenanography
- ❍ B. Cryptography
- ❍ C. Ciphering
- ❍ D. Cryptanalysis

Find the Answer p. 262

49. Which of the following is different than the others?Select the best answer.

- ❍ A. Cryptology
- ❍ B. Cryptography
- ❍ C. Cryptanalysis
- ❍ D. Cryptographic algorithm

Find the Answer p. 263

50. The process of hiding the meaning of a message by using a mechanism which shifts each letter of the alphabet by three letters is known as?Select the best answer.

- ❍ A. Polyalphabetic cipher
- ❍ B. Monoalphabetic substitution cipher
- ❍ C. Transposition cipher
- ❍ D. Running key cipher

Find the Answer p. 263

51. A cryptosystem is comprised of all but which of the following?Select the best answer.

- ❍ A. Plaintext
- ❍ B. Key
- ❍ C. A one way mathematical function
- ❍ D. Algorithm

Find the Answer p. 263

52. Which of the following is NOT true?Select the best answer.

- ❍ A. A message can be encrypted for confidentiality.
- ❍ B. A message can be digitally signed for authentication and integrity.
- ❍ C. A message can be encrypted and digitally signed for confidentiality, integrity, and authentication.
- ❍ D. A message can be hashed for confidentiality.

Find the Answer p. 263

53. Which of the following hash functions results in a default 160-bit hash value?Select the best answer.

- ❍ A. SHA-1
- ❍ B. Haval
- ❍ C. MD5
- ❍ D. MD2

Find the Answer p. 263

54. Which of the following hash algorithms supports a variable hash value length output?Select the best answer.

- ❍ A. HAVAL
- ❍ B. SHA
- ❍ C. HMAC (Hash Message Authenticating Code)
- ❍ D. MD4

Find the Answer p. 263

55. All but which of the following statements are true?Select the best answer.

- ❍ A. Key length should be long enough to provide the necessary level of protection for the encrypted data.
- ❍ B. Keys need not be stored and transmitted securely if they are long enough.
- ❍ C. Keys should be truly random and use the full spectrum of the key space.
- ❍ D. The more often a key is used, the shorter its lifetime should be.

Find the Answer p. 263

56. Which of the following is NOT a primary goal of e-mail security based on encryption?Select the best answer.

- ❍ A. Non-repudiation
- ❍ B. Authentication of the message source
- ❍ C. Guarantee of availability
- ❍ D. Delivery verification

Find the Answer p. 263

57. Which of the following is NOT an encryption system designed to provide security for Internet based e-mail?Select the best answer.

- ❍ A. Privacy Enhanced Mail (PEM)
- ❍ B. MIME Object Security Services (MOSS)
- ❍ C. Pretty Good Privacy (PGP)
- ❍ D. Secure Electronic Transaction (SET)

Find the Answer p. 263

58. Which of the following used IDEA for encryption?Select the best answer.

- ❍ A. Pretty Good Privacy (PGP)
- ❍ B. MIME Object Security Services (MOSS)
- ❍ C. Privacy Enhanced Mail (PEM)
- ❍ D. Secure Electronic Transaction (SET)

Find the Answer p. 263

59. Which of the following is similar to a cyclic redundancy check (CRC) that is appended to a message prior to transmission to ensure integrity?Select the best answer.

- ❍ A. Secure Electronic Transaction (SET)
- ❍ B. Financial Institution Message Authentication Standard (FIMAS)
- ❍ C. MIME Object Security Services (MOSS)
- ❍ D. Transaction Layer Security (TLS)

Find the Answer p. 263

60. _____ authenticates the server to the client using RSA public key cryptography and digital certificates, uses 3DES and MD5 hash functions, and can be used to provide security communications for Telnet, FTP, HTTP, and e-mail.Select the best answer.

- ❍ A. MONDEX
- ❍ B. Message Authentication Code (MAC)
- ❍ C. Secure Sockets Layer (SSL)
- ❍ D. Secure Multipurpose Internet Mail Extensions (S/MIME)

Find the Answer p. 263

61. Which of the following are the two protocols that comprise IPSec?Select the best answer.

- ❍ A. RARP and ARP
- ❍ B. IGMP and RIP
- ❍ C. TCP and UDP
- ❍ D. AH and ESP

Find the Answer p. 263

62. IPSec is able to provide all but which of the following?Select the best answer.

- ❍ A. Availability
- ❍ B. Encryption
- ❍ C. Non-repudiation
- ❍ D. Authentication

Find the Answer p. 263

63. In which IPSec mode is the data of the IP packet encrypted but the original header is not?Select the best answer.

- ❍ A. Tunnel mode
- ❍ B. Transport mode
- ❍ C. VPN mode
- ❍ D. Link mode

Find the Answer p. 263

64. Which of the following is NOT a protocol used by IPSec for key management?Select the best answer.

- ❍ A. ISAKMP (Internet Security Association and Key Management Protocol)
- ❍ B. Oakley Key Determination Protocol
- ❍ C. Merkle-Hellman Knapsack
- ❍ D. SKEME (Secure Key Exchange Mechanism)

Find the Answer p. 263

65. Which of the following is an alternative to SSL to provide secure Web transactions?Select the best answer.

- ❍ A. Internet Key Exchange (IKE)
- ❍ B. Internet Open Trading Protocol (IOTP)
- ❍ C. Financial Institution Message Authentication Standard (FIMAS)
- ❍ D. Secure Hypertext Transfer Protocol (S-HTTP)

Find the Answer p. 263

66. The birthday attack is primarily focused on what types of cryptography?Select the best answer.

- ❍ A. Asymmetric keys
- ❍ B. Symmetric keys
- ❍ C. Hash values
- ❍ D. Digital signatures

Find the Answer p. 263

67. What form of commonly named cryptographic attack attempts to break a cryptosystem by trying every possible key pattern?Select the best answer.

- ❍ A. Known key attack
- ❍ B. Key space attack
- ❍ C. Sequential referenced attack
- ❍ D. Brute force attack

Find the Answer p. 263

68. What attack attempts to break double encryption schemes by comparing the results of a single encrypting of a known plaintext with a single decryption of a ciphertext?Select the best answer.

- ❍ A. Meet-in-the-middle
- ❍ B. Known plaintext
- ❍ C. Linear cryptanalysis
- ❍ D. Chosen ciphertext

Find the Answer p. 263

69. The primary goal of cryptographic attacks is to?Select the best answer.

- ❍ A. Explore the key space
- ❍ B. Discover the key
- ❍ C. Discover the algorithm
- ❍ D. Transmit faked encrypted messages

Find the Answer p. 263

70. What single sign-on mechanisms uses (or used) DES as its encryption scheme?Select the best answer.

- ❍ A. SEASAME
- ❍ B. KryptoKnight
- ❍ C. NetSP
- ❍ D. Kerberos

Find the Answer p. 263

Chapter 5
Information Security and Risk Management

1. Which of the following is NOT an element of personnel controls?Select the best answer.

   - ❍ A. Separation of duties
   - ❍ B. Handling non-compliance
   - ❍ C. Stipulating laws and regulations
   - ❍ D. Rotation of duties

   Find the Answer p. 264

2. What security control method is used to ensure confidentiality and integrity?Select the best answer.

   - ❍ A. Network access control
   - ❍ B. Encryption
   - ❍ C. Data backups
   - ❍ D. Perimeter security

   Find the Answer p. 264

3. Auditing is not dependant upon?Select the best answer.

   - ❍ A. Identification
   - ❍ B. Accountability
   - ❍ C. Authorization
   - ❍ D. Authentication

   Find the Answer p. 264

4. _____ operations should be restricted to authorized individuals whose work tasks specifically require greater than normal capabilities.Select the best answer.

- ❍ A. Privileged
- ❍ B. Backup
- ❍ C. E-mail client
- ❍ D. Productivity software

Find the Answer p. 264

5. Auditing is a mechanism to?Select the best answer.

- ❍ A. Improve the security policy
- ❍ B. Detect networking anomalies
- ❍ C. Create audit trails
- ❍ D. Test a security system's design

Find the Answer p. 264

6. The goal of an audit trail is to?Select the best answer.

- ❍ A. Check compliance with security policy
- ❍ B. Evaluate the cost effectiveness of safeguards
- ❍ C. Provide a risk analysis treatment of an environment
- ❍ D. Keep security administrators busy

Find the Answer p. 264

7. Which of the following is NOT a safeguard against collusion?Select the best answer.

- ❍ A. Rotation of duties
- ❍ B. Trusted recovery
- ❍ C. Separation of duties
- ❍ D. Auditing

Find the Answer p. 264

8. What is the primary purpose of mandatory vacations?Select the best answer.

- ❍ A. Job rotation
- ❍ B. Background checking
- ❍ C. Testing recovery plans
- ❍ D. Auditing

Find the Answer p. 264

9. Administrative controls for personnel security should include all but which of the following?Select the best answer.

- ❍ A. Background checks
- ❍ B. Enrollment in biometric authentication systems
- ❍ C. Mandatory vacations
- ❍ D. Job action warnings

Find the Answer p. 264

10. Security controls should be _____ to the authorized user.Select the best answer.

- ❍ A. Obstructive
- ❍ B. Accessible
- ❍ C. Transparent
- ❍ D. Inhibiting

Find the Answer p. 264

11. Which of the following is FALSE?Select the best answer.

- ❍ A. The secrecy of a security control is not a valid measure of the strength of the protection it offers.
- ❍ B. Dependancy on the secrecy of a security control should be avoided.
- ❍ C. Defense in depth is more important than the secrecy of security controls.
- ❍ D. Controls provide the most or best security when they are secret.

Find the Answer p. 264

12. What type of security controls are used to encourage compliance with other security controls?Select the best answer.

- ❍ A. Directive
- ❍ B. Recovery
- ❍ C. Application
- ❍ D. Transaction

Find the Answer p. 264

13. When no single person has total control over a system's security mechanisms, this is called?Select the best answer.

- ❍ A. Split knowledge
- ❍ B. Rotation of duties
- ❍ C. Mandatory vacations
- ❍ D. Strong access controls

Find the Answer p. 264

14. Another term for a security control that employees split knowledge is?Select the best answer.

- ❍ A. Mandatory vacations
- ❍ B. Separation of duties
- ❍ C. Rotation of duties
- ❍ D. Background checks

Find the Answer p. 264

15. The security mechanism that requires that users have the minimum amount of access that is absolutely required by their job tasks, and that they have that access for the shortest amount of time, is known as?Select the best answer.

- ❍ A. Due diligence
- ❍ B. Two-man controls
- ❍ C. Principle of Least Privilege
- ❍ D. Rotation of duties

Find the Answer p. 264

16. Which of the following is an example of a split knowledge security control?Select the best answer.

- ❍ A. Mandatory vacations
- ❍ B. Auditing
- ❍ C. Rotation of duties
- ❍ D. Two-man control

Find the Answer p. 264

17. When should the final report from an auditor be issued?Select the best answer.

- ❍ A. After interim reports
- ❍ B. During the exit conference
- ❍ C. At the beginning of the auditing process
- ❍ D. After the exit conference

Find the Answer p. 264

18. Which of the following identifies the goals of auditing?Select the best answer.

- ❍ A. Problem identification and violator identification
- ❍ B. Problem identification and problem resolution
- ❍ C. Problem identification and normal activity identification
- ❍ D. Problem identification and safeguard selection

Find the Answer p. 264

19. Reviews and evaluations of the security solutions of an environment are often performed by?Select the best answer.

- ❍ A. Senior management
- ❍ B. End users
- ❍ C. The risk assessment team
- ❍ D. External consultants

Find the Answer p. 264

20. What is the purpose of interim reports by security auditors?Select the best answer.

- ❍ A. Used to communicate regarding items that need immediate attention
- ❍ B. Used to keep the length of the final report to a minimum
- ❍ C. Used to provide progress reports to management
- ❍ D. Used to request additional clarifications on audit objectives

Find the Answer p. 264

21. What is the purpose of the exit conference?Select the best answer.

- ❍ A. Place blame for security deficiencies
- ❍ B. Recommendation of countermeasures
- ❍ C. Discuss issues with all relevant and effected parties
- ❍ D. Rebuttle of auditing objectives

Find the Answer p. 264

22. Who is responsible for implementing the changes recommended in the findings report from an external auditor?Select the best answer.

- ❍ A. Senior management
- ❍ B. End users
- ❍ C. Internal auditors
- ❍ D. System managers

Find the Answer p. 264

23. Once auditing discovers a problem, what is the next step?Select the best answer.

- ❍ A. Countermeasure selection
- ❍ B. Problem management
- ❍ C. Risk analysis
- ❍ D. Security policy modification

Find the Answer p. 264

24. Which of the following is NOT a primary goal of problem management?Select the best answer.

- ❍ A. Reduce failures to a reasonable level
- ❍ B. Prevent re-occurrence of discovered problems
- ❍ C. Maintain cost effectiveness of countermeasures
- ❍ D. Mitigate the negative impact of problems

Find the Answer p. 265

25. _____ means subjects are granted only the minimal amount of access required for them to complete their assigned work tasks.Select the best answer.

- ❍ A. Need to know
- ❍ B. Separation of duties
- ❍ C. Least privilege
- ❍ D. Privilege elevation

Find the Answer p. 265

26. The purpose of a safeguard is to?Select the best answer.

- ❍ A. Remove a threat agent
- ❍ B. Enhance an exposure
- ❍ C. Update a security policy
- ❍ D. Reduce or remove a vulnerability

Find the Answer p. 265

27. What is the primary goal of risk management?Select the best answer.

- ❍ A. Remove all risk
- ❍ B. Perform a qualitative analysis of risk
- ❍ C. Remove liability from senior management
- ❍ D. Reduce risk to an acceptable level

Find the Answer p. 265

28. Which of the following is NOT an example of a risk?Select the best answer.

- ❍ A. Physical damage
- ❍ B. Blocking ports
- ❍ C. Misuse of data
- ❍ D. Buffer overflow

Find the Answer p. 265

29. Which of the following is NOT a method by which risk is reduced or eliminated?Select the best answer.

- ❍ A. Applying a safeguard
- ❍ B. Waiting
- ❍ C. Removing the vulnerability
- ❍ D. Blocking the threat agent

Find the Answer p. 265

30. An instance of being exposed to losses from a threat is known as?Select the best answer.

- ❍ A. Vulnerability
- ❍ B. Single loss expectancy
- ❍ C. Exposure
- ❍ D. Breach

Find the Answer p. 265

31. Which of the following is NOT an example of a threat?Select the best answer.

- ❍ A. Intruder access through a firewall
- ❍ B. Activities that violate the security policy
- ❍ C. A biometric device failing to authenticate a valid user
- ❍ D. A natural disaster that destroys the IT infrastructure

Find the Answer p. 265

32. Which of the following is an example of a threat?Select the best answer.

- ❍ A. Blocking all attachments at the e-mail gateway
- ❍ B. Scanning for malicious code
- ❍ C. Performing penetration testing without senior management approval
- ❍ D. An authorized user destroying confidential data

Find the Answer p. 265

33. Which of the following is NOT an example of a risk?Select the best answer.

- ❍ A. Failing to review audit logs
- ❍ B. Failing to enforce password policy
- ❍ C. Not updating anti-virus software
- ❍ D. Not filtering traffic on border communication links

Find the Answer p. 265

34. Which of the following is NOT an example of a safeguard?Select the best answer.

- ❍ A. Relaxing the filters on a firewall
- ❍ B. Imposing strong password management
- ❍ C. Deploying security guards
- ❍ D. Enable BIOS passwords

Find the Answer p. 265

35. The top down approach to security management provides for all but which of the following?Select the best answer.

- ❍ A. Provides for policy initiation, support, and direction
- ❍ B. Provides for assignment of responsibility to down-level administrators
- ❍ C. Provides for development and implementation of standards, guidelines, and procedures
- ❍ D. Provides for development of security control configurations

Find the Answer p. 265

36. Which of the following is NOT true in regards to a strategic security plan?Select the best answer.

- ❍ A. Useful for 5 years with annual updates
- ❍ B. Defines overall mission, goals, and objectives
- ❍ C. Identifies, schedules, manages and controls the tasks necessary to accomplish resource activities
- ❍ D. Includes risk assessment

Find the Answer p. 265

37. Which of the following is true about a tactical security plan?Select the best answer.

- ❍ A. A tactical security plan does not include maintenance and technical support plans
- ❍ B. It includes a risk analysis
- ❍ C. It defines projects and completion milestones
- ❍ D. It includes staffing and budgeting plans

Find the Answer p. 265

38. Which of the following is NOT true regarding an operational security plan?Select the best answer.

- ❍ A. It includes maintenance and technical support plans
- ❍ B. It integrates the elements of other plans
- ❍ C. It defines short term tasks necessary to the accomplishing of objectives
- ❍ D. It prescribes a logical sequence of initiatives

Find the Answer p. 265

39. The purpose of risk management is?Select the best answer.

- ❍ A. Safeguard evaluation
- ❍ B. Risk mitigation
- ❍ C. Loss estimation
- ❍ D. Remove all risk

Find the Answer p. 265

40. The objectives of risk analysis include all but which of the following?Select the best answer.

- ❍ A. Identify risk
- ❍ B. Quantify the impact of each risk
- ❍ C. Evaluate the cost effectiveness of safeguards
- ❍ D. Select countermeasures to implement

Find the Answer p. 265

41. The first step in risk analysis is?Select the best answer.

- ❍ A. Countermeasure selection
- ❍ B. Cost/benefit analysis
- ❍ C. Asset valuation
- ❍ D. Qualitative analysis of risk

Find the Answer p. 265

42. Which of the following represent the primary security factors that a private sector organization is concerned about?Select the best answer.

- ❍ A. Data confidentiality and integrity
- ❍ B. Data availability and integrity
- ❍ C. Data non-repudiation and encryption
- ❍ D. Data availability and confidentiality

Find the Answer p. 265

43. The most important aspect of security to military organizations is?Select the best answer.

- ❍ A. Integrity
- ❍ B. Non-repudiation
- ❍ C. Confidentiality
- ❍ D. Availability

Find the Answer p. 265

44. Risk management attempts to reduce risk to an acceptable level by performing all but which of the following activities?Select the best answer.

- ❍ A. Track down intruders for prosecution
- ❍ B. Analyze the probability of attack occurrence
- ❍ C. Predict the impact of a breach
- ❍ D. Evaluate safeguards

Find the Answer p. 265

45. Which of the following is NOT an example of a risk?Select the best answer.

- ❍ A. Human error
- ❍ B. Equipment malfunction
- ❍ C. Replacing human security guards with dogs
- ❍ D. Disgruntled insider

Find the Answer p. 265

46. Risk is the _____ of something happening that will damage assetsSelect the best answer.

- ❍ A. Certainty
- ❍ B. Evalutation
- ❍ C. Prevention
- ❍ D. Possibility

Find the Answer p. 265

47. When will risk be totally eliminated?Select the best answer.

- ❍ A. When the organization ceases to exist
- ❍ B. When the security policy is properly implemented
- ❍ C. When all systems are powered down
- ❍ D. When all users have completed security awareness training

Find the Answer p. 265

48. Risk analysis is used to determine whether safeguards are all but which of the following?Select the best answer.

- ❍ A. Cost effective
- ❍ B. Relevant
- ❍ C. Exhaustive
- ❍ D. Timely

Find the Answer p. 265

49. An effective safeguard, when evaluated via risk analysis, should?Select the best answer.

- ❍ A. Cost less than the loss possible via the risk
- ❍ B. Offer a complete solution for an individual specified risk
- ❍ C. Be invisible to the user
- ❍ D. Allow itself to be removed easily

Find the Answer p. 266

50. All but which of the following apply to senior management in relation to risk analysis?Select the best answer.

- ❍ A. Directs and supports risk analysis
- ❍ B. Is a member of the Risk Assessment team
- ❍ C. Acts appropriately upon the results
- ❍ D. Reviews the outcome of the analysis

Find the Answer p. 266

51. Who is ultimately responsible and liable if the security perimeter of an organization is violated by an intruder and asset losses occur?Select the best answer.

- ❍ A. Senior management
- ❍ B. Network or system administrators
- ❍ C. Security guards
- ❍ D. End users

Find the Answer p. 266

52. Which of the following is not one of the fundamental principles of security included in the CIA triad?Select the best answer.

- ❍ A. Confidentiality
- ❍ B. Integrity
- ❍ C. Accountability
- ❍ D. Availability

Find the Answer p. 266

53. The ability of a computer system to provide adequate capacity for predictable performance represents which of the fundamental security principles of the CIA triad?Select the best answer.

- ❍ A. Confidentiality
- ❍ B. Integrity
- ❍ C. Accountability
- ❍ D. Availability

Find the Answer p. 266

54. The likelihood of a threat taking advantage of a vulnerability is known as?Select the best answer.

- ❍ A. Risk
- ❍ B. Exposure
- ❍ C. Mitigation
- ❍ D. Attack

Find the Answer p. 266

55. The security administration team should be responsible for all but which of the following?Select the best answer.

- ❍ A. Creation of a clear and efficient reporting process
- ❍ B. Monitoring the security of an organization
- ❍ C. Approve the security policy
- ❍ D. Identify the strengths and weaknesses of a security solution

Find the Answer p. 266

56. Which of the following is NOT a task assigned to senior management?Select the best answer.

- ❍ A. Assign classifications or values to data
- ❍ B. Dictate how information is to be protected
- ❍ C. Delegate security responsibilities to data custodians
- ❍ D. Implement security controls

Find the Answer p. 266

57. A security administrator may employ all but which of the following types of controls to implement a security solution?Select the best answer.

- ❍ A. Executive
- ❍ B. Administrative
- ❍ C. Technical
- ❍ D. Physical

Find the Answer p. 266

58. Which of the following is an example of an administrative security control?Select the best answer.

- ❍ A. Security guards
- ❍ B. Policies
- ❍ C. Locks
- ❍ D. Intrusion detection systems

Find the Answer p. 266

59. Which of the following is NOT an example of an administrative security control?Select the best answer.

- ❍ A. Standards
- ❍ B. Guidelines
- ❍ C. Identification
- ❍ D. Personnel screening

Find the Answer p. 266

60. Which of the following is an example of a technical security control?Select the best answer.

- ❍ A. Procedures
- ❍ B. Awareness training
- ❍ C. Perimeter lighting
- ❍ D. Encryption

Find the Answer p. 266

61. Which of the following is NOT an example of a technical security control?Select the best answer.

- ❍ A. Fire detection and suppression
- ❍ B. Access control matrix
- ❍ C. Authorization
- ❍ D. Traffic filtering

Find the Answer p. 266

62. Which of the following is NOT an example of a valid activity of security management?Select the best answer.

- ❍ A. Evaluating the loss of productivity due to restrictions imposed by the security solution
- ❍ B. Manage user complaints of access restrictions or resource unavailability, by fine tuning least privilege access
- ❍ C. Proposing to senior management the alteration or rescinding of a security policy
- ❍ D. Deploy a new security control in a mission critical environment

Find the Answer p. 266

63. For a security policy to be effective and comprehensive, it must thoroughly address the three fundamental principles of security, which are?Select the best answer.

- ❍ A. Confidentiality, Integrity, Availability
- ❍ B. Confinement, Integrity, Accessibility
- ❍ C. Corroboration, Interrogation, Authorization
- ❍ D. Continuity, Intelligence, Authentication

Find the Answer p. 266

64. Which of the following is an example of a security control that focuses on maintaining confidentiality?Select the best answer.

- ❍ A. Restricted access
- ❍ B. Network traffic padding
- ❍ C. Input validity verification
- ❍ D. Backups

Find the Answer p. 266

65. Which of the following is NOT an example of a security control that focuses on maintaining confidentialitySelect the best answer.

- ❍ A. Data encryption
- ❍ B. Access control
- ❍ C. Change restrictions
- ❍ D. Personnel training

Find the Answer p. 266

66. Which of the following is an example of a security control that focuses primarily on maintaining integrity?Select the best answer.

- ❍ A. Trusted recovery
- ❍ B. Denial of service attack protection
- ❍ C. Data classification
- ❍ D. Hashing of data in transit

Find the Answer p. 266

67. Which of the following is NOT an example of a security control that focuses on maintaining integrity?Select the best answer.

- ❍ A. Network monitoring
- ❍ B. Managing alterations to data in a database
- ❍ C. Validating input data
- ❍ D. Preventing of unauthorized access

Find the Answer p. 266

68. Which of the following is an example of a security control that focuses on maintaining availability?Select the best answer.

- ❍ A. Encrypted transport of data
- ❍ B. Quick recovery from faults
- ❍ C. Fixed packet length transmissions
- ❍ D. User awareness training

Find the Answer p. 266

69. Which of the following is NOT an example of a security control that focuses on maintaining availability?Select the best answer.

- ❍ A. Secured state machines
- ❍ B. Avoiding single points of failure
- ❍ C. Implementing need to know access controls
- ❍ D. Controlling the environmental characteristics

Find the Answer p. 266

70. What is a vulnerability?Select the best answer.

- ❍ A. The likelihood that a system will experience a security breach
- ❍ B. Instance of being exposed to losses from a threat agent
- ❍ C. A potential danger to information or systems
- ❍ D. A weakness or the absence of a safeguard that could be exploited

Find the Answer p. 266

71. Which of the following is NOT an example of a vulnerability?Select the best answer.

- ❍ A. Assigning all users access based on job descriptions
- ❍ B. Modems on clients
- ❍ C. Open ports
- ❍ D. Easy access to the server room

Find the Answer p. 266

72. Which of the following is an example of a vulnerability?Select the best answer.

- ❍ A. Restricting access to authorized users
- ❍ B. Failing to enforce the password policy
- ❍ C. Filtering traffic at all communication borders
- ❍ D. Implementing physical access restrictions

Find the Answer p. 266

73. A quantitative risk analysis approach employs which of the following?Select the best answer.

- ❍ A. A specific dollar value is assigned to each risk
- ❍ B. Opinions about risks are collected from various departments
- ❍ C. Scenarios are used to evaluate safeguards
- ❍ D. Guesswork

Find the Answer p. 266

74. Which of the following is NOT true?Select the best answer.

- ❍ A. Quantitative analysis assigns real numbers and concrete probability percentages.
- ❍ B. A purely quantitative risk analysis is possible.
- ❍ C. Quantitative analysis can be automated.
- ❍ D. Qualitative analysis involves significantly less time and effort than a quantitative approach.

Find the Answer p. 267

75. An exposure factor is?Select the best answer.

- ❍ A. The amount of loss that would be incurred due to the compromise of an asset.
- ❍ B. The instance of being exposed to losses from a threat agent.
- ❍ C. Percentage of loss that a realized threat event would cause against a specific asset.
- ❍ D. The likelihood that a system will experience a security breach.

Find the Answer p. 267

76. The annualized loss expectancy can be calculated using which of the following equations?Select the best answer.

- ❍ A. Exposure factor multiplied by annualized rate of occurrence
- ❍ B. Asset value multiplied by exposure factor
- ❍ C. Asset value multiplied by risk probability multiplied by safeguard benefit
- ❍ D. Asset value multiplied by exposure factor multiplied by annualized rate of occurrence

Find the Answer p. 267

77. What calculation or value serves a dual purpose as an element in risk analysis cost/benefit calculations as well as a descriptive value in business impact analysis?Select the best answer.

- ❍ A. Single loss expectancy
- ❍ B. Exposure factor
- ❍ C. Annualized rate of occurrence
- ❍ D. Annualized loss expectancy

Find the Answer p. 267

78. Which of the following is NOT an accepted response to the results of risk analysis?Select the best answer.

- ❍ A. Reduce
- ❍ B. Reject
- ❍ C. Assign
- ❍ D. Accept

Find the Answer p. 267

79. Which response to risk can be implemented by purchasing insurance against loss?Select the best answer.

- ❍ A. Reduce
- ❍ B. Reject
- ❍ C. Assign
- ❍ D. Accept

Find the Answer p. 267

80. Which of the following is NOT a valid example of assigning risk?Select the best answer.

- ❍ A. Purchasing insurance
- ❍ B. Implementing offsite backups
- ❍ C. Crafting a disaster recovery plan
- ❍ D. Delegating security policy implementation responsibilities

Find the Answer p. 267

81. What security mechanism is primarily responsible for implementing security controls that protect data in the most cost-effective manner?Select the best answer.

- ❍ A. Need to know
- ❍ B. Data classification
- ❍ C. Traffic filtering
- ❍ D. Intrusion detection

Find the Answer p. 267

82. What level of private sector data classification represents assets that, if disclosed, will not cause an adverse impact?Select the best answer.

- ❍ A. Confidential
- ❍ B. Private
- ❍ C. Sensitive
- ❍ D. Public

Find the Answer p. 267

83. Which of the following is NOT a method used in qualitative risk analysis?Select the best answer.

- ❍ A. Focus group
- ❍ B. Automated software
- ❍ C. One-on-one meeting
- ❍ D. Checklist

Find the Answer p. 267

84. The value of a safeguard to an organization can be calculated using a formula which includes all but which of the following factors?Select the best answer.

- ❍ A. Annual loss expectancy before safeguard
- ❍ B. Annual loss expectancy after implementing the safeguard
- ❍ C. Residual risk
- ❍ D. Annual cost of safeguard

Find the Answer p. 267

85. What is the difference between total risk and residual risk?Select the best answer.

- ❍ A. One can be completely eliminated
- ❍ B. One cannot be managed with safeguards
- ❍ C. One is not directly quantifiable
- ❍ D. One is calculated by knowing the controls gap

Find the Answer p. 267

86. Acceptable risk is?Select the best answer.

- ❍ A. The amount of risk an organization is willing to shoulder
- ❍ B. Residual risk
- ❍ C. Any risk that cannot be addressed by safeguards
- ❍ D. All risks that have an exposure factor of less than 10%

Find the Answer p. 267

87. What element in a formalized security infrastructure consists of documents that are not compulsory in nature?Select the best answer.

- ❍ A. Procedures
- ❍ B. Guidelines
- ❍ C. Standards
- ❍ D. Policies

Find the Answer p. 267

88. Which of the following does NOT describe the formalized security infrastructure document type of guideline?Select the best answer.

- ❍ A. Defines recommended actions
- ❍ B. Used when specific standards do not apply
- ❍ C. Serves as operational guides for IT staff
- ❍ D. Details step-by-step activities

Find the Answer p. 267

89. If _____, managers can be held liable for negligence and held accountable for asset losses.Select the best answer.

- ❍ A. a company does not practice due care and due diligence
- ❍ B. a company properly implements a security policy
- ❍ C. a senior manager does not sign off on a change to the security policy
- ❍ D. an analysis team does not update the business continuity plan

Find the Answer p. 267

90. Which of the following is NOT one of the five standard data classifications used by the military?Select the best answer.

- ❍ A. Confidential
- ❍ B. Secret
- ❍ C. Private
- ❍ D. Sensitive

Find the Answer p. 267

91. Determining the value of an asset can be useful in all but which of the following requirements or activities?Select the best answer.

- ❍ A. Cost/benefit analysis of safeguards
- ❍ B. Avoiding negligence by confirming due care
- ❍ C. Insurance inventory
- ❍ D. Assigning classifications to subjects

Find the Answer p. 267

92. What form of qualitative risk analysis employs a group of people who reach a consensus through an anonymous means of voting and exchanging ideas?Select the best answer.

- ❍ A. Delphi technique
- ❍ B. Brainstorming
- ❍ C. Storyboarding
- ❍ D. Surveys

Find the Answer p. 267

93. The value of an asset helps to determine?Select the best answer.

- ❍ A. Length of time committed to performing qualitative analysis
- ❍ B. Whether or not to perform a quantitative analysis
- ❍ C. Whether a logical or a technical control is evaluated
- ❍ D. The relative strength and cost of the safeguard

Find the Answer p. 267

94. Which of the following is NOT considered an element in determining the cost of an asset?Select the best answer.

- ❍ A. Cost to train personnel to employ the asset
- ❍ B. Cost to develop
- ❍ C. Cost to acquire
- ❍ D. Cost to maintain

Find the Answer p. 267

95. Which of the following is NOT considered an element in determining the cost of an asset?Select the best answer.

- ❍ A. Cost to protect
- ❍ B. Amount in GB of hard drive storage requirements for a single asset
- ❍ C. Value to owners and users
- ❍ D. Value to competitors

Find the Answer p. 267

96. Which of the following is NOT considered an element in determining the cost of an asset?Select the best answer.

- ❍ A. Cost to replace
- ❍ B. Cost in productivity if the asset is unavailable
- ❍ C. The file formats used by the asset
- ❍ D. Liability if asset is compromised

Find the Answer p. 267

Chapter 6
Legal, Regulations, Compliance and Investigations

1. Which of the following laws addresses confidentiality, integrity, and availability for both data and systems and encourages other countries to adopt the same framework?Select the best answer.

   - ❍ A. U.S. Privacy Act of 1974
   - ❍ B. Paperwork Reduction Act of 1995
   - ❍ C. U.S. National Information Infrastructure Protection Act of 1996
   - ❍ D. Gramm Leach Bliley Act of 1999

   Find the Answer p. 268

2. Which of the following requires Federal Agencies to assess the security of their non-classified information systems, to provide a risk assessment, and to report the security needs of its systems?Select the best answer.

   - ❍ A. U.S. Privacy Act of 1974
   - ❍ B. U.S. Computer Fraud and Privacy Act of 1986
   - ❍ C. U.S. National Information Infrastructure Protection Act of 1996
   - ❍ D. Paperwork Reduction Act of 1995

   Find the Answer p. 268

3. Which of the following defines the trafficking in computer passwords as a federal crime if that activity affects interstate or foreign commerce or permits unauthorized access to government computers?Select the best answer.

   - ❍ A. U.S. Computer Fraud and Privacy Act of 1986
   - ❍ B. Paperwork Reduction Act of 1995
   - ❍ C. U.S. National Information Infrastructure Protection Act of 1996
   - ❍ D. Gramm Leach Bliley Act of 1999

   Find the Answer p. 268

4. Which form of intellectual property law protects original works of authorship for 50+ years?Select the best answer.

- ❍ A. Trademark
- ❍ B. Patent
- ❍ C. Copyright
- ❍ D. Trade secret

Find the Answer p. 268

5. Which form of intellectual property law protects or establishes a word, name, symbol, etc. as an identifying mark for an organization or a product?Select the best answer.

- ❍ A. Trademark
- ❍ B. Patent
- ❍ C. Copyright
- ❍ D. Trade secret

Find the Answer p. 268

6. Which of the following is an amendment to the U.S. Computer Fraud and Privacy Act of 1986?Select the best answer.

- ❍ A. U.S. Privacy Act of 1974
- ❍ B. U.S. National Information Infrastructure Protection Act of 1996
- ❍ C. Paperwork Reduction Act of 1995
- ❍ D. Gramm Leach Bliley Act of 1999

Find the Answer p. 268

7. Which form of intellectual property law defines data that is confidential and proprietary to a specific organization?Select the best answer.

- ❍ A. Trademark
- ❍ B. Patent
- ❍ C. Copyright
- ❍ D. Trade secret

Find the Answer p. 268

8. Which form of intellectual property law provides the owner with 17 years of exclusive use rights?Select the best answer.

- ❍ A. Trademark
- ❍ B. Patent
- ❍ C. Copyright
- ❍ D. Trade secret

Find the Answer p. 268

9. Which of the following statements is true?Select the best answer.

- ❍ A. European privacy laws are less restrictive than those of the United States.
- ❍ B. European privacy laws are just as restrictive as those of the United States.
- ❍ C. European privacy laws are more restrictive than those of the United States.
- ❍ D. European privacy laws are completely different than those of the United States.

Find the Answer p. 268

10. Which of the following is NOT a tenant of the European privacy laws?Select the best answer.

- ❍ A. Data must be collected in accordance with the law.
- ❍ B. Collected information cannot be disclosed to others without the consent of the individual.
- ❍ C. Records kept about an individual must be accurate and timely.
- ❍ D. Data can only be collected with the consent of the individual.

Find the Answer p. 268

11. Which of the following is FALSE in regards to the European privacy laws?Select the best answer.

- ❍ A. Data can be retained indefinitely
- ❍ B. Individuals can correct errors in the data collected about them
- ❍ C. Data can only be used for the original purpose for which it was collected
- ❍ D. Individuals are entitled to a report detailing the information retained about them

Find the Answer p. 268

12. Which of the following is NOT a common problem with the storage of personal health and medical data?Select the best answer.

- ❍ A. Access granted to a wide range of users, such as outside partners, members, and vendors
- ❍ B. A high level of granular access control on most systems
- ❍ C. Internet connectivity increases vulnerabilities to integrity and privacy of data
- ❍ D. Misuse of personal medical data can have a significant negative impact on the public perception of an organization

Find the Answer p. 268

13. Which of the following is NOT an information privacy principle that health care organizations should adhere to?Select the best answer.

- ❍ A. Grant individuals the means to monitor and correct the data collected about them
- ❍ B. Restrict the uses of data to those outlined when the data was originally collected
- ❍ C. Maintain the secrecy of their personal information database
- ❍ D. Organizations that gather data should provide adequate protection for that data

Find the Answer p. 268

14. Which of the following is FALSE about the Health Insurance Portability and Accountability Act (HIPAA)?Select the best answer.

- ❍ A. It establishes the rights for individuals who are subjects of individually identifiable health information.
- ❍ B. It defines uses and disclosures of individually identifiable health information that should be authorized or required.
- ❍ C. It requires an information security officer.
- ❍ D. It defines specific products, standards, guidelines, and procedures for protecting individually identifiable health information.

Find the Answer p. 268

15. Which of the following is NOT a recommended practice for the monitoring of e-mail on a company network?Select the best answer.

- ❍ A. Establish different levels of monitoring for each organizational staff level
- ❍ B. Inform all users that monitoring is occurring via a clearly visible and frequent banner or similar warning system
- ❍ C. Monitoring should be performed in a lawful and consistent manner
- ❍ D. Detail who will be accessing and viewing the archived data and for how long the data will be retained

Find the Answer p. 268

16. The U.S. Federal Sentencing Guidelines provides for a punishment for convicted senior management for the crime of failing to properly secure assets with a legally regonized obligation that can include?Select the best answer.

- ❍ A. Imprisonment
- ❍ B. Fines up to $290 million
- ❍ C. Confiscation of assets
- ❍ D. Seizure of public stock offerings

Find the Answer p. 268

17. For negligence to be proven in court, what must be demonstrated or proved?Select the best answer.

- ❍ A. Lack of due diligence
- ❍ B. Failure to comply with recognized standards
- ❍ C. Legally recognized obligation
- ❍ D. Proximate causation

Find the Answer p. 268

18. Which of the following is NOT visible proof that due care is being practiced by an organization in regards to security?Select the best answer.

- ❍ A. Physical access controls
- ❍ B. Hardware backups
- ❍ C. Security awareness training
- ❍ D. Use of plenum cabling

Find the Answer p. 268

19. Which of the following statements is true in regards to a well-organized and legitimate monitoring solution that records all e-mail on a business network?Select the best answer.

- ❍ A. Does not provide a means to track down violations of security policy
- ❍ B. Does not provide a guarantee of personal privacy
- ❍ C. Does not clearly inform all users of the monitoring activity
- ❍ D. Does not make employees aware of the acceptable use of e-mail

Find the Answer p. 268

20. Which of the following treats the unauthorized possession of information, without the intent to profit from it, as a crime?Select the best answer.

- ❍ A. U.S. Computer Fraud and Privacy Act of 1986
- ❍ B. Paperwork Reduction Act of 1995
- ❍ C. 1991 U.S. Federal Sentencing Guidelines
- ❍ D. Gramm Leach Bliley Act of 1999

Find the Answer p. 268

21. All of the following are true regarding the 1991 U.S. Federal Sentencing Guidelines, except for?Select the best answer.

- ❍ A. The guidelines treat the unauthorized possession of information, without the intent to profit from it, as a crime
- ❍ B. The guidelines apply to both individuals and organizations
- ❍ C. The guidelines make the degree of punishment a function of the extent to which the organization has demonstrated due diligence in establishing security
- ❍ D. The guidelines make the use of information that causes $1,000 or more in damages, or which impairs medical treatment, a federal crime

Find the Answer p. 268

22. The 1991 U.S. Federal Sentencing Guidelines invokes the _____ that requires that senior management of an organization perform their duties with the same care that any normal person would exercise in the same circumstances.Select the best answer.

- ❍ A. Prudent man rule
- ❍ B. Principle of least privilege
- ❍ C. Tenant of due care
- ❍ D. Separation of duties requirement

Find the Answer p. 268

23. Which of the following is NOT visible proof that due care is being practiced by an organization in regards to security?Select the best answer.

- ❍ A. Deploying high-speed networking devices
- ❍ B. Telecommunications encryption
- ❍ C. Disaster recovery plans
- ❍ D. Development of formalized security infrastructure documentation

Find the Answer p. 268

24. Which of the following is NOT a responsibility of the Computer Incident Response Team?Select the best answer.

- ❍ A. Managing public relations
- ❍ B. Designing security policies
- ❍ C. Investigating intrusions
- ❍ D. Reporting incidents

Find the Answer p. 269

25. Which of the following is not technically a crime according to the law?Select the best answer.

- ❍ A. Espionage
- ❍ B. Fraud
- ❍ C. Piracy
- ❍ D. Resource waste

Find the Answer p. 269

26. Evidence should be all but which of the following in order to be used in court?Select the best answer.

- ❍ A. Reliable
- ❍ B. Sufficient
- ❍ C. Relevant
- ❍ D. Permissible

Find the Answer p. 269

27. Which of the following is NOT a valid means to identify or label computer evidence?Select the best answer.

- ❍ A. Writing on printouts with permanent markers
- ❍ B. Recording serial numbers
- ❍ C. Writing a contents and ID tag file to a hard drive
- ❍ D. Photographing the contents displayed on the monitor

Find the Answer p. 269

28. What type of evidence proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?Select the best answer.

- ❍ A. Hearsay evidence
- ❍ B. Circumstantial evidence
- ❍ C. Secondary evidence
- ❍ D. Direct evidence

Find the Answer p. 269

29. Which of the following is NOT an element in the (ISC)^2 code of ethics that all CISSP candidates must adhere to?Select the best answer.

- ❍ A. Conduct themselves with high standards of moral, ethical, and legal behavior
- ❍ B. Do not commit any unlawful act
- ❍ C. Do not write malicious code
- ❍ D. Report all discovered unlawful activity

Find the Answer p. 269

30. Which of the following is NOT supported by the ISC2's CISSP code of ethics?Select the best answer.

- ❍ A. Promote understanding of security
- ❍ B. Provide competent service
- ❍ C. Do not disclose confidential information from clients
- ❍ D. Report crimes to ISC2

Find the Answer p. 269

31. Which of the following is NOT considered a violation of computer ethics?Select the best answer.

- ❍ A. Working overtime on an IT project
- ❍ B. Browsing files on the file server
- ❍ C. Using proprietary software without compensation
- ❍ D. Employing another's intellectual property without acknowledgement

Find the Answer p. 269

32. Which of the following is NOT defined as unacceptable and inappropriate by the Internet Activities Board of Ethics and the Internet?Select the best answer.

- ❍ A. Seeking to gain unauthorized access to resources
- ❍ B. Conducting commercial activities over the Internet
- ❍ C. Destroying the integrity of computer stored information
- ❍ D. Wasting resources

Find the Answer p. 269

33. Which of the following laws requires that federal agencies protect information about private individuals that is stored in government databases?Select the best answer.

- ❍ A. U.S. Privacy Act of 1974
- ❍ B. U.S. Computer Fraud and Privacy Act of 1986
- ❍ C. Paperwork Reduction Act of 1995
- ❍ D. Gramm Leach Bliley Act of 1999

Find the Answer p. 269

34. Which of the following laws defines the use of a federal interest computer in a crime as a federal offense and reduces the minimum damage required to declare a crime a federal offence?Select the best answer.

- ❍ A. U.S. Privacy Act of 1974
- ❍ B. U.S. Computer Fraud and Privacy Act of 1986
- ❍ C. U.S. National Information Infrastructure Protection Act of 1996
- ❍ D. Gramm Leach Bliley Act of 1999

Find the Answer p. 269

35. The U.S. Department of Health, Education, and Welfare Code of Fair Information Practices requires which of the following?Select the best answer.

- ❍ A. People must be able to remove any information about themselves from databases containing personal data
- ❍ B. Organizations maintaining personal data do not need to ensure that data isn't misused
- ❍ C. Data stored about people must be timely
- ❍ D. The existence of systems that maintain records of a personal nature cannot remain secret

Find the Answer p. 269

36. Which of the following is considered a crime committed using a computer?Select the best answer.

- ❍ A. Illegally transferring money from one bank account to another over the Internet
- ❍ B. Erasing a hard drive using a degaussing magnet
- ❍ C. Setting fire to a building
- ❍ D. Theft of a notebook from an airport security checkpoint

Find the Answer p. 269

37. Which of the following is NOT a computer crime?Select the best answer.

- ❍ A. Social engineering
- ❍ B. Surfing pornographic Web sites
- ❍ C. Password sniffing
- ❍ D. Spoofing IP addresses

Find the Answer p. 269

38. Which of the following is a crime against a computer?Select the best answer.

- ❍ A. Intercepting wireless network communications
- ❍ B. Installing software that has not been properly purchased
- ❍ C. Causing a blackout of the local power grid by damaging a power station
- ❍ D. Testing an intrusion script against a competitor's Web site

Find the Answer p. 269

39. Which of these computer crimes is NOT like the others?Select the best answer.

- ❍ A. Spoofing
- ❍ B. Social engineering
- ❍ C. Masqurading
- ❍ D. Data diddling

Find the Answer p. 269

40. Which of the following is NOT considered a computer crime?Select the best answer.

- ❍ A. Espionage
- ❍ B. Theft by taking
- ❍ C. Fraud
- ❍ D. Embezzlement

Find the Answer p. 269

41. Which of the following is NOT one of the types of laws found in the United States that can be used in a court of law?Select the best answer.

- ❍ A. Statutory law
- ❍ B. Administrative law
- ❍ C. Islamic law
- ❍ D. Common law

Find the Answer p. 269

42. The code of federal regulations is also known as?Select the best answer.

- ❍ A. Statutory law
- ❍ B. Common law
- ❍ C. Case digests
- ❍ D. Administrative law

Find the Answer p. 269

43. Which category of common law allows for punishments to include financial penalties but NOT imprisonment for a conviction?Select the best answer.

- ❍ A. Civil law
- ❍ B. Criminal law
- ❍ C. Administrative law
- ❍ D. Regulatory law

Find the Answer p. 269

44. Which form of law focuses on the violation of government laws focused on the protection of the public?Select the best answer.

- ❍ A. Civil law
- ❍ B. Criminal law
- ❍ C. Administrative law
- ❍ D. Regulatory law

Find the Answer p. 269

45. What form of common law is also known as tort?Select the best answer.

- ❍ A. Administrative law
- ❍ B. Criminal law
- ❍ C. Civil law
- ❍ D. Regulatory law

Find the Answer p. 269

46. Which of the following laws requires that banks give customers the option to prohibit the distribution of personal information with non-affiliated third parties?Select the best answer.

- ❍ A. U.S. Privacy Act of 1974
- ❍ B. U.S. Computer Fraud and Privacy Act of 1986
- ❍ C. U.S. National Information Infrastructure Protection Act of 1996
- ❍ D. Gramm Leach Bliley Act of 1999

Find the Answer p. 269

47. The act of an investigation can often have numerous negative consequences for an organization. Which of the following is NOT an example of one of these?Select the best answer.

- ❍ A. Prevention of the compromise of individual privacy
- ❍ B. The subject committing retaliatory acts
- ❍ C. Negative publicity
- ❍ D. Interruption of business processes

Find the Answer p. 269

48. Who has jurisdiction over computer crimes committed in the U.S.?Select the best answer.

- ❍ A. Local law enforcement and FBI
- ❍ B. Secret Service and NIST
- ❍ C. FBI and Secret Service
- ❍ D. NSA and CIA

Find the Answer p. 269

49. If a computer crime is suspected, which of the following is the most important activity to perform?Select the best answer.

- ❍ A. Generate post incident reports
- ❍ B. Trigger the emergency response team
- ❍ C. Restore non-critical business processes
- ❍ D. Do not alert the suspect

Find the Answer p. 270

50. When an investigation of a computer crime incident occurs, which of the following is FALSE?Select the best answer.

- ❍ A. There is a compressed time frame within which to conduct the investigation
- ❍ B. The investigation may interfere with the normal operations of business
- ❍ C. Evidence is usually tangible
- ❍ D. Evidence may be co-mingled with data needed for normal business activities

Find the Answer p. 270

51. When an investigation of a computer crime incident occurs, which of the following is FALSE?Select the best answer.

- ❍ A. Evidence can be difficult to gather
- ❍ B. Evidence may be damaged or altered by the normal operations of business
- ❍ C. Jurisdictional responsibility may be cloudy
- ❍ D. An expert or specialist is usually not required

Find the Answer p. 270

52. Which of the following is FALSE?Select the best answer.

- ❍ A. In an interview, the goal is to gather information as well as to discern the subject's credibility
- ❍ B. In an interview, a subject becomes a witness
- ❍ C. In an interrogation, a witness becomes a suspect
- ❍ D. In an interrogation, a subject becomes a witness

Find the Answer p. 270

53. Which of the following is NOT an element of the chain of custody?Select the best answer.

- ❍ A. Whether the evidence is relevant
- ❍ B. Time and location the evidence was gathered
- ❍ C. Who discovered the evidence
- ❍ D. Who maintained possession of the evidence

Find the Answer p. 270

54. Which of the following represents the proper order of the chain of evidence or the evidence life cycle?1. Collection2. Discovery3. Identification4. Presentation5. Preservation6. Protection7. Recording8. Return9. TransportationSelect the best answer.

- ❍ A. 1,2,3,4,5,6,7,8,9
- ❍ B. 8,4,2,9,5,1,3,7,6
- ❍ C. 2,6,7,1,3,5,9,4,8
- ❍ D. 6,5,8,3,4,1,9,7,2

Find the Answer p. 270

55. To present evidence in court, it must be all but which of the following?Select the best answer.

- ❍ A. Relevant
- ❍ B. Permissible
- ❍ C. Reliable
- ❍ D. Sufficient

Find the Answer p. 270

56. Aspects of the relevance of evidence include all but which of the following?Select the best answer.

- ❍ A. It has not been altered
- ❍ B. It must show that a crime has been committed
- ❍ C. It shows some aspect of the perpetrator's motives
- ❍ D. It verifies or demonstrates what has occurred

Find the Answer p. 270

57. Which of the following is NOT an exception to the hearsay rule?Select the best answer.

- ❍ A. Evidence made during the normal process of business activity
- ❍ B. Evidence in the custody of the witness on a regular basis
- ❍ C. Evidence made at or near the time of the incident being investigated
- ❍ D. Evidence produced as a result of the incident and exclusively for court presentation

Find the Answer p. 270

58. The oral testimony of a witness is known as?Select the best answer.

- ❍ A. Best evidence
- ❍ B. Direct evidence
- ❍ C. Hearsay evidence
- ❍ D. Conclusive evidence

Find the Answer p. 270

59. What type of evidence is generally inadmissible in court?Select the best answer.

- ❍ A. Best evidence
- ❍ B. Direct evidence
- ❍ C. Hearsay evidence
- ❍ D. Expert opinion

Find the Answer p. 270

60. Which of the following is NOT a valid means of identification that will allow evidence to be admissible in court?Select the best answer.

- ❍ A. Writing on paper printouts with a permanent marker
- ❍ B. Writing a identification file to a storage media
- ❍ C. A recording of serial numbers from devices
- ❍ D. Placing evidence in sealed and marked containers

Find the Answer p. 270

61. Which of the following is NOT a valid action to take when preserving evidence for admissibility in court?Select the best answer.

- ❍ A. Avoiding smoke and dust
- ❍ B. Write protecting media
- ❍ C. Storing electronic media in plastic bags
- ❍ D. Avoiding magnetic fields

Find the Answer p. 270

62. When attempting to preserve evidence for admissibility in court, which of the following is a valid action to take?Select the best answer.

- ❍ A. Run tripwire on the system
- ❍ B. Use AES to encrypt the entire storage device
- ❍ C. Defragment the storage device
- ❍ D. Create a message digest using SHA

Find the Answer p. 270

63. The original or primary evidence is also known as?Select the best answer.

- ❍ A. Best evidence
- ❍ B. Direct evidence
- ❍ C. Secondary evidence
- ❍ D. Conclusive evidence

Find the Answer p. 270

64. The standard discriminator to determine whether a subject may be the person who committed a crime is to evaluate whether that person had all but which of the following?Select the best answer.

- ❍ A. Intention
- ❍ B. Means
- ❍ C. Motive
- ❍ D. Opportunity

Find the Answer p. 270

65. The goal of an _____ is to find the answers to who, what, when, where, why, and how.Select the best answer.

- ❍ A. interrogation
- ❍ B. interview
- ❍ C. investigation
- ❍ D. interpretation

Find the Answer p. 270

66. The goal of an _____ is to establish enough evidence to consider a subject a witness.Select the best answer.

- ❍ A. investigation
- ❍ B. interview
- ❍ C. interrogation
- ❍ D. interpretation

Find the Answer p. 270

67. Which of the following is NOT a valid means to collect evidence according to the rules of evidence or the evidence life cycle?Select the best answer.

- ❍ A. Gather all relevant storage media
- ❍ B. Use degaussing equipment
- ❍ C. Image the hard drive
- ❍ D. Print out the screen

Find the Answer p. 270

68. What form of security policy outlines the laws and industry restrictions placed upon an organization?Select the best answer.

- ❍ A. Advisory
- ❍ B. Regulatory
- ❍ C. Informative
- ❍ D. Organizational

Find the Answer p. 270

Chapter 7
Operations Security

1. What is the primary element in the supervisory structure access control method?Select the best answer.

   - ❍ A. Only end users are audited
   - ❍ B. All employees need performance reviews
   - ❍ C. Senior management is always liable
   - ❍ D. Every employee has a boss

Find the Answer p. 271

2. What is a clipping level?Select the best answer.

   - ❍ A. The threshold of unauthorized activity
   - ❍ B. A baseline of normal activity
   - ❍ C. The collection of abnormal activity
   - ❍ D. The saturation point above which only violations occur

Find the Answer p. 271

3. At what point are violation records recorded?Select the best answer.

   - ❍ A. Only below the clipping level
   - ❍ B. At the clipping level
   - ❍ C. When the clipping level is exceeded
   - ❍ D. At all times

Find the Answer p. 271

4. Which of the following is NOT a repetitive mistake that will exceed clipping levels?Select the best answer.

- ❍ A. Exceeding the authority assigned to a user account
- ❍ B. Too many users with unrestricted access
- ❍ C. Repeated high-volume intrusion detection attempts
- ❍ D. Failing to submit logon credentials to access resources

Find the Answer p. 271

5. What means can be used to protect the confidentiality of audit logs?Select the best answer.

- ❍ A. Encryption
- ❍ B. Storage on write-once media
- ❍ C. Redundant event recording
- ❍ D. Digital signatures

Find the Answer p. 271

6. Which of the following will never result in data remanence?Select the best answer.

- ❍ A. Using the native OS tools to erase data
- ❍ B. Cremation of media
- ❍ C. Degaussing media
- ❍ D. Performing a single format of the media

Find the Answer p. 271

7. What is the act of recycling a backup tape for another purpose known as?Select the best answer.

- ❍ A. Disclosure
- ❍ B. Remanence
- ❍ C. Cost effective resource management
- ❍ D. Object reuse

Find the Answer p. 271

8. The process of removing data from media so it can be reused within the same security environment is known as?Select the best answer.

- ❍ A. Clearing
- ❍ B. Purging
- ❍ C. Overwriting
- ❍ D. Destruction

Find the Answer p. 271

9. Which of the following is NOT a responsibility of the Computer Incident Response Team?Select the best answer.

- ❍ A. Managing network logs
- ❍ B. Resolving vulnerabilities
- ❍ C. Risk assessment
- ❍ D. Minimizing costs of incidents

Find the Answer p. 271

10. Which of the following is a FALSE statement according to the Generally Accepted Systems Security Principles (GASSP)?Select the best answer.

- ❍ A. Computer security supports the mission of an organization
- ❍ B. Computer security should be cost effective
- ❍ C. Computer security is not restrained by society
- ❍ D. Computer security should be periodically reassessed

Find the Answer p. 271

11. Emergency response should be planned out before an incident occurs. Which of the following is not an aspect of this type of planning?Select the best answer.

- ❍ A. How an incident should be reported
- ❍ B. When should management be informed of an incident
- ❍ C. What action should be taken when an incident is detected
- ❍ D. Where should the facility be located for the greatest security

Find the Answer p. 271

12. Emergency response should be planned out before an incident occurs. Which of the following is NOT an aspect of this type of planning?Select the best answer.

- ❍ A. What constitutes a federal crime
- ❍ B. What is considered an incident
- ❍ C. To whom should incidents be reported
- ❍ D. Who should handle the response to an incident

Find the Answer p. 271

13. Which of the following actions or decisions should be made BEFORE an incident occurs?Select the best answer.

- ❍ A. Determine how much damage was caused
- ❍ B. Determine what backup solutions should be deployed
- ❍ C. Determine whether remedial safeguards are required
- ❍ D. Determine if recovery procedures should be triggered to recover from an incident

Find the Answer p. 271

14. A committee to help with the investigation of computer crime incidents should be established. This committee should perform all but which of the following?Select the best answer.

- ❍ A. Establish a liaison with law enforcement
- ❍ B. Create post-incident reports for use as evidence in court
- ❍ C. Design a procedure for reporting IT crimes
- ❍ D. Inform senior management and affected parties of the progress of an investigation

Find the Answer p. 271

15. _____ controls focus on day to day activities for the protection of IT and the support of the security policy.Select the best answer.

- ❍ A. Procedural security
- ❍ B. Oversight security
- ❍ C. Operations security
- ❍ D. Physical security

Find the Answer p. 271

16. What type of resources need NOT be included in the resource protection scheme for the organization?Select the best answer.

- ❍ A. Hardware resources
- ❍ B. Software resources
- ❍ C. Data resources
- ❍ D. Transitive resources

Find the Answer p. 271

17. Which of the following is NOT a common requirement for maintaining security while hardware undergoes maintenance or repair?Select the best answer.

- ❍ A. Recertification of security label
- ❍ B. Trusted offsite technicians
- ❍ C. Bonded escorts
- ❍ D. Accredited supervision

Find the Answer p. 271

18. Vendor maintenance accounts are considered a threat to security since they may be used as an access means for unauthorized individuals. What are vendor maintenance accounts?Select the best answer.

- ❍ A. Any account that has administrative level privileges
- ❍ B. Supervisory level factory installed accounts
- ❍ C. Accounts used by hardware repair technicians that are created and maintained by your IT staff
- ❍ D. Those administrator accounts involved in the daily support of user accounts and access

Find the Answer p. 271

19. Which of the following is an invalid countermeasure against the unauthorized use of maintenance accounts?Select the best answer.

- ❍ A. Change password
- ❍ B. Disable accounts
- ❍ C. Network traffic logging
- ❍ D. Maintain physical access control over devices

Find the Answer p. 271

20. Which of the following is NOT considered an operational security software control?Select the best answer.

- ❍ A. Software testing
- ❍ B. Managed storage of software media
- ❍ C. Backups
- ❍ D. Diagnostic port controls

Find the Answer p. 271

21. What is the primary goal of media security controls?Select the best answer.

- ❍ A. Control inventory of backup media
- ❍ B. Prevent loss or disclosure of sensitive data while it is stored on removable media
- ❍ C. Maintain chain of custody information just in case media must be used in a legal action
- ❍ D. Prevent users from accessing removable media

Find the Answer p. 271

22. Which of the following is NOT considered an element of maintaining media security controls?Select the best answer.

- ❍ A. Logging
- ❍ B. Chain of custody
- ❍ C. Deploying security guards
- ❍ D. Inventory management

Find the Answer p. 271

23. When a removable media is labeled with a security classification (i.e. a sensitivity level), which of the following is true?Select the best answer.

- ❍ A. Only users with the same or lower clearance can use the removable media.
- ❍ B. The removable media can only store data that is lower than the labeled clearance level.
- ❍ C. Availability is maintained through classification labeling of removable media.
- ❍ D. The removable media must be protected under the same restrictions as data with the same classification.

Find the Answer p. 271

24. At the end of the useful lifetime of a removable media with a high security classification level, what should occur to the media?Select the best answer.

- ❍ A. It should be incinerated
- ❍ B. It should be purged for re-use
- ❍ C. It should be cleaned for use in any security domain
- ❍ D. It should be stored in a retention vault

Find the Answer p. 272

25. Which of the following is NOT considered a monitoring or reconnaisance technique?Select the best answer.

- ❍ A. Penetration Testing
- ❍ B. Demon (war) Dialing
- ❍ C. Sniffing
- ❍ D. Use of static firewall rules

Find the Answer p. 272

26. Which of the following is NOT considered a monitoring or reconnaisance technique?Select the best answer.

- ❍ A. Biometrics
- ❍ B. Scanning
- ❍ C. Violation Analysis
- ❍ D. Social Engineering

Find the Answer p. 272

27. When an activity crosses or exceeds the clipping level, what occurs?Select the best answer.

- ❍ A. Access is denied
- ❍ B. The intruder is moved to a padded cell
- ❍ C. A violation report is generated
- ❍ D. The firewall disables further communications

Find the Answer p. 272

28. Clipping levels are useful for detecting all but which of the following?Select the best answer.

- ❍ A. Repetitive mistakes
- ❍ B. Individuals exceeding their authorized privileges
- ❍ C. Serious intrusion attempts
- ❍ D. Slow low-traffic attacks

Find the Answer p. 272

29. Monitoring should begin after all but which of the following is completed?Select the best answer.

- ❍ A. User logon
- ❍ B. Application installation
- ❍ C. System configuration
- ❍ D. Operating system patching

Find the Answer p. 272

30. Monitoring should focus on all but which of the following?Select the best answer.

- ❍ A. Violation tracking
- ❍ B. Violation resolution
- ❍ C. Violation processing
- ❍ D. Violation analysis

Find the Answer p. 272

31. What is the first activity that must be performed when evaluating the effectiveness of your security perimeter through penetration testing?Select the best answer.

- ❍ A. Develop an attack plan
- ❍ B. Obtain management approval
- ❍ C. Collect the attack tools
- ❍ D. Produce a results report

Find the Answer p. 272

32. The goal of penetration testing is?Select the best answer.

- ❍ A. Altering the security policy
- ❍ B. Placing blame for security violations
- ❍ C. Evaluating the existing security protection
- ❍ D. Tricking management into purchasing new security solutions

Find the Answer p. 272

33. What is the primary goal of configuration or change management?Select the best answer.

- ❍ A. Enable rollback to a previous system state
- ❍ B. Duplicate changes on multiple systems
- ❍ C. Prevent changes from diminishing security
- ❍ D. Informing users of changes

Find the Answer p. 272

34. Which of the following is NOT a form of monitoring?Select the best answer.

- ❍ A. Biometric enrollment
- ❍ B. Port scanning
- ❍ C. Intrusion detection
- ❍ D. Penetration testing

Find the Answer p. 272

35. The act of examining traffic patterns, rather than the contents of packets, is known as?Select the best answer.

- ❍ A. Transaction processing
- ❍ B. Trend analysis
- ❍ C. Sniffing
- ❍ D. Port scanning

Find the Answer p. 272

36. Which of the following is NOT one of the five generally recognized procedural steps to implement configuration or change control management?Select the best answer.

- ❍ A. Implementing the change
- ❍ B. Applying to introduce a change
- ❍ C. Updating the security policy
- ❍ D. Cataloging the intended change

Find the Answer p. 272

37. One of the most important features or mechanisms of configuration or change control management is?Select the best answer.

- ❍ A. Updating new employee training materials
- ❍ B. Revising the organization's security policy
- ❍ C. Compliance with due care requirements
- ❍ D. The ability to rollback changes to a previous state

Find the Answer p. 272

38. What is the purpose of trusted recovery?Select the best answer.

- ❍ A. To ensure that security is not breached during the recovery of a system failure
- ❍ B. To maintain the accreditation of a system
- ❍ C. To guarantee that files can be restored from backup media
- ❍ D. To provide a means to return to the primary site after a disaster occurs

Find the Answer p. 272

39. Which of the following is NOT an element of trusted recovery?Select the best answer.

- ❍ A. Rebooting into a single user mode
- ❍ B. Revalidating the trusted computer base (TCB)
- ❍ C. Recovering all file systems that were active at the time of failure
- ❍ D. Verifying the integrity of system level security critical files

Find the Answer p. 272

40. Which of the following is NOT a primary function of configuration or change control management?Select the best answer.

- ❍ A. Providing a means to track and audit changes to a system
- ❍ B. Ensuring formalized testing of all system changes
- ❍ C. Analyzing the effects of changes on a system
- ❍ D. Keeping users from learning about changes to a system

Find the Answer p. 272

41. The top priority of configuration or change control management is?Select the best answer.

- ❍ A. To prevent changes from diminishing security
- ❍ B. To analyze the effects of changes on a system
- ❍ C. To provide a means to track and audit changes to a system
- ❍ D. To ensure formalized testing of all system changes

Find the Answer p. 272

42. Which of the following is NOT one of the five generally recognized procedural steps to implement configuration or change control management?Select the best answer.

- ❍ A. Applying to introduce a change
- ❍ B. Updating the configuration item
- ❍ C. Scheduling the change
- ❍ D. Reporting the change to the appropriate parties

Find the Answer p. 272

43. If you want to discover how much data can be learned about your environment by external hackers, what level of knowledge of the penetration attack team would provide this most accurately?Select the best answer.

- ❍ A. Partial
- ❍ B. Disclosed
- ❍ C. Full
- ❍ D. Zero

Find the Answer p. 272

44. Which of the following is NOT considered a standard step or element in the process of penetration testing?Select the best answer.

- ❍ A. Safeguard tuning
- ❍ B. Discovery
- ❍ C. Enumaration
- ❍ D. Exploitation

Find the Answer p. 272

45. When performing a penetration attack on your own system, which of the following activities would NOT be performed during the discovery phase?Select the best answer.

- ❍ A. Footprinting
- ❍ B. Social engineering
- ❍ C. Scavenging
- ❍ D. Dumpster diving

Find the Answer p. 272

46. The final step in penetration testing is?Select the best answer.

- ❍ A. Deploying new safeguards
- ❍ B. Performing risk analysis
- ❍ C. Reporting findings
- ❍ D. Exploiting discovered vulnerabilities

Find the Answer p. 272

47. Which of the following is NOT considered an important security issue related to audit trails?Select the best answer.

- ❍ A. Purging of audit media
- ❍ B. Retention and protection of audit media
- ❍ C. Protection against alteration
- ❍ D. Support of availability of audit media

Find the Answer p. 272

48. Oral reports can be used instead of written reports for which of the following?Select the best answer.

- ❍ A. Findings report
- ❍ B. Interim reports
- ❍ C. Final report
- ❍ D. Objectives definition report

Find the Answer p. 272

49. Which of the following is NOT considered a browsing attack?Select the best answer.

- ❍ A. Viewing another user's files
- ❍ B. Shoulder surfing
- ❍ C. Going through someone's trash
- ❍ D. Extracting data from a purged media

Find the Answer p. 273

50. Which of the following is appropriate activity when using company equipment during your work shift?Select the best answer.

- ❍ A. Viewing and sharing controversial political content while at work
- ❍ B. Using company resources to sell personal items on eBay
- ❍ C. Accessing resources for which you have no legitimate work task requirements
- ❍ D. Consuming all of the bandwidth of a WAN connection performing a required data transfer

Find the Answer p. 273

51. Violating the confidentiality of sensitive data is what type of inappropriate activity?Select the best answer.

- ❍ A. Abuse of privileges
- ❍ B. Waste of corporate resources
- ❍ C. Use of inappropriate content
- ❍ D. Vandalism

Find the Answer p. 273

52. Which of the following is NOT a computer crime even though it can result in a serious financial loss to your organization?Select the best answer.

- ❍ A. Fraud
- ❍ B. Input error or omission
- ❍ C. Eavesdropping
- ❍ D. War dialing

Find the Answer p. 273

53. Which of the following is NOT a countermeasure to traffic or trend analysis?Select the best answer.

- ❍ A. Message padding
- ❍ B. Transmission of noise
- ❍ C. Covert channel analysis
- ❍ D. Encrypting individual messages

Find the Answer p. 273

54. Traffic or trend analysis is primarily concerned with?Select the best answer.

- ❍ A. The amount of data traveling to another system
- ❍ B. The content of network packets
- ❍ C. The application used in a communication
- ❍ D. The user account and password associated with a communication session

Find the Answer p. 273

55. Hardware components should be replaced when?Select the best answer.

- ❍ A. Every year
- ❍ B. Immediately after their second failure
- ❍ C. On every instance of a failure
- ❍ D. Before their mean time between failure time period expires

Find the Answer p. 273

56. The hardware component rating of mean time to repair (MTTR) is used for what purpose?Select the best answer.

- ❍ A. To determine how often to expect to repair a device.
- ❍ B. To determine when to replace a device.
- ❍ C. To determine how long it takes to repair a device.
- ❍ D. To determine the length of time after the first failure before a device must be replaced.

Find the Answer p. 273

57. When should hardware be replaced to maintain availability?Select the best answer.

- ❍ A. At the mean time to repair
- ❍ B. Every two years
- ❍ C. When capacity reaches 65% utilization
- ❍ D. Before the mean time between failures

Find the Answer p. 273

58. Information on magnetic media can be reliably destroyed by all but which of the following?Select the best answer.

- ❍ A. Degaussing
- ❍ B. OS based deletion
- ❍ C. Overwriting the media seven times
- ❍ D. Purging

Find the Answer p. 273

59. The only way to absolutely prevent data remenance from being extracted from electronic media is to?Select the best answer.

- ❍ A. Purge
- ❍ B. Format
- ❍ C. Destroy by incineration
- ❍ D. Overwrite at least seven times

Find the Answer p. 273

60. When a media is to be re-used in the same environment, which of the following is minimally sufficient to prevent unnecessary disclosure?Select the best answer.

- ❍ A. Purging
- ❍ B. Destroying by cremation
- ❍ C. Overwriting at least seven times
- ❍ D. Clearing

Find the Answer p. 273

61. What RAID level is basic mirroring?Select the best answer.

- ❍ A. RAID 1
- ❍ B. RAID 3
- ❍ C. RAID 5
- ❍ D. RAID 6

Find the Answer p. 273

Chapter 8
Physical (Environmental) Security

1. Which of the following directly protects against physical computer theft?Select the best answer.

   - ❍ A. Notebook cable locks
   - ❍ B. Work area separation
   - ❍ C. Lighting
   - ❍ D. Control zones

   Find the Answer p. 274

2. Which of the following is NOT an example of a preventative access control?Select the best answer.

   - ❍ A. Backups
   - ❍ B. Locks
   - ❍ C. Lighting
   - ❍ D. Security guards

   Find the Answer p. 274

3. Which of the following is NOT an example of a preventative physical access control?Select the best answer.

   - ❍ A. Clipping levels
   - ❍ B. Badges
   - ❍ C. Dogs
   - ❍ D. Mantraps

   Find the Answer p. 274

4. Which of the following is an example of piggybacking?Select the best answer.

- ❍ A. Cutting through a wire fence
- ❍ B. Re-transmitting intercepted packets
- ❍ C. Passing through a door opened by another person who used a key
- ❍ D. Decrypting the content of secured communication sessions

Find the Answer p. 274

5. Which of the following is NOT considered an adequate protection means for a mission critical server?Select the best answer.

- ❍ A. Uninterruptible power supply
- ❍ B. Surge protector
- ❍ C. Alternate power supply
- ❍ D. Backup generator

Find the Answer p. 274

6. A momentary loss of power is known as?Select the best answer.

- ❍ A. Brownout
- ❍ B. Spike
- ❍ C. Fault
- ❍ D. Sag

Find the Answer p. 274

7. What is the short duration of an interfering disturbance in the power line known as?Select the best answer.

- ❍ A. Transient noise
- ❍ B. Spike
- ❍ C. Noise
- ❍ D. Sag

Find the Answer p. 274

8. The radiation generated by the difference in power of the hot and neutral wires of a circuit is known as?Select the best answer.

- ❍ A. Transient noise
- ❍ B. Traverse mode noise
- ❍ C. Common mode noise
- ❍ D. Brownout

Find the Answer p. 274

9. Which of the following is NOT an effective means to eliminate or reduce power line noise?Select the best answer.

- ❍ A. Move power lines away from strong magnetic sources
- ❍ B. Ensure proper grounding
- ❍ C. Use cables with fewer twists
- ❍ D. Add cable shielding

Find the Answer p. 274

10. According to the ANSI standard, at what point of a drop in power between the power source and the meter is a brownout declared?Select the best answer.

- ❍ A. 1.2% loss
- ❍ B. 10% loss
- ❍ C. 3.5% loss
- ❍ D. 8% loss

Find the Answer p. 274

11. Which is NOT a Water-based Fire protection system?Select the best answer.

- ❍ A. Oxygen displacement
- ❍ B. Preaction System
- ❍ C. Deluge System
- ❍ D. Dry Pipe System

Find the Answer p. 274

12. What is the ideal operating humidity for a data center room?Select the best answer.

- ❍ A. 20 - 40%
- ❍ B. 40 - 60%
- ❍ C. 60 - 80%
- ❍ D. 80 - 100%

Find the Answer p. 274

13. Static electricity discharges over _____ volts are possible on low-static carpeting in an environment with very low humidity.Select the best answer.

- ❍ A. 1,000
- ❍ B. 5,000
- ❍ C. 20,000
- ❍ D. 150,000

Find the Answer p. 274

14. A static discharge of 1,000 volts is sufficient to cause which of the following forms of damage?Select the best answer.

- ❍ A. A system shutdown
- ❍ B. Destroy data on a hard drive
- ❍ C. Permenantly damage microchips
- ❍ D. Scramble a CRT monitor display

Find the Answer p. 274

15. A static discharge of only _____ volts is sufficient to cause a printer jam or serious malfunction?Select the best answer.

- ❍ A. 4,000
- ❍ B. 1,000
- ❍ C. 55,000
- ❍ D. 17,000

Find the Answer p. 274

16. Radio frequency interference (RFI) can be caused by all but which of the following?Select the best answer.

- ❍ A. Electric cables
- ❍ B. Cement walls
- ❍ C. Fluorescent lights
- ❍ D. Space heaters

Find the Answer p. 274

17. A pre-employment screening process should include all but which of the following?Select the best answer.

- ❍ A. Reference checks
- ❍ B. Drug screening
- ❍ C. Supervisor review
- ❍ D. Education history verification

Find the Answer p. 274

18. Which of the following is NOT an element that should be a part of on-going employee security compliance checks?Select the best answer.

- ❍ A. Security clearance verification
- ❍ B. Supervisor reviews
- ❍ C. Drug testing
- ❍ D. Termination of physical access

Find the Answer p. 274

19. The termination procedure may include all but which of the following?Select the best answer.

- ❍ A. Issuing of photo ID
- ❍ B. Escorting off the premises
- ❍ C. Reviewing of non-disclosure agreements
- ❍ D. Returning of equipment

Find the Answer p. 274

20. Which of the following is NOT an administrative control for maintaining physical security?Select the best answer.

- ❍ A. Fire drills
- ❍ B. Assigning a user account logon rights
- ❍ C. Exit interview
- ❍ D. Employment record verification

Find the Answer p. 274

21. When maintaining administrative controls to protect physical security in the event of a disaster or emergency, all but which of the following should be performed?Select the best answer.

- ❍ A. Clearly document the steps of the procedures
- ❍ B. Personnel training and drills
- ❍ C. Perform a detailed risk analysis
- ❍ D. Periodic review of the recovery plan

Find the Answer p. 274

22. Which of the following is NOT a human threat to physical security?Select the best answer.

- ❍ A. Vandalism
- ❍ B. Strikes
- ❍ C. Utility loss
- ❍ D. Sabotage

Find the Answer p. 274

23. The most important factor when designing and implementing physical security solutions is?Select the best answer.

- ❍ A. Cost effectiveness of mechanisms
- ❍ B. Efficiency of solutions
- ❍ C. Automation of controls
- ❍ D. Personnel safety

Find the Answer p. 274

24. The second most important aspect of a physical security mechanism, after protecting human safety, is?Select the best answer.

- ❍ A. Cost benefits
- ❍ B. Compliance with industry standards
- ❍ C. Similarity with existing solutions
- ❍ D. User training required

Find the Answer p. 275

25. Physical security mechanisms should always?Select the best answer.

- ❍ A. Be invisible to the user
- ❍ B. Comply with laws and regulations
- ❍ C. Be automated
- ❍ D. Be approved by all levels of management

Find the Answer p. 275

26. The momentary increase in power often experienced at the moment when a device or a power system is turned on is known as?Select the best answer.

- ❍ A. Surge
- ❍ B. Spike
- ❍ C. Noise
- ❍ D. Inrush

Find the Answer p. 275

27. When evaluating the security of a new facility or site, which of the following is the least important?Select the best answer.

- ❍ A. Cost
- ❍ B. Location
- ❍ C. Fire rating
- ❍ D. Local emergency services

Find the Answer p. 275

28. Which of the following is the least important aspect of a secured server room?Select the best answer.

- ❍ A. Fire suppression system
- ❍ B. Human compatibility
- ❍ C. Temperature control system
- ❍ D. Efficient use of space (such as stacking machines)

Find the Answer p. 275

29. When evaluating, selecting, and deploying physical security access controls, what is always the most important?Select the best answer.

- ❍ A. Cost
- ❍ B. Ease of maintenance
- ❍ C. Protection of human safety
- ❍ D. Reliability

Find the Answer p. 275

30. Critical path analysis is useful in the area of physical security in what way?Select the best answer.

- ❍ A. It is used to establish a hierarchy of subject classification levels.
- ❍ B. It is used to develop a system of control zones used to manage access to resources.
- ❍ C. It is used to determine the value of each element of infrastructure.
- ❍ D. It is used to test whether or not a security solution is sufficient.

Find the Answer p. 275

31. Which of the following is NOT an example of a physical security administrative control?Select the best answer.

- ❍ A. Training
- ❍ B. Facility management
- ❍ C. Emergency response procedures
- ❍ D. Alarms

Find the Answer p. 275

32. Which of the following is an example of a physical security administrative control?Select the best answer.

- ❍ A. Facility construction design
- ❍ B. Fencing
- ❍ C. Man traps
- ❍ D. Security guards

Find the Answer p. 275

33. Which of the following is an example of a physical security physical control?Select the best answer.

- ❍ A. Security guards
- ❍ B. CCTV monitoring
- ❍ C. Power supply management
- ❍ D. Intrusion detection

Find the Answer p. 275

34. Which of the following is the least important aspect to consider when selecting a security facility location?Select the best answer.

- ❍ A. Surrounding terrain
- ❍ B. Cost
- ❍ C. Access to emergency services
- ❍ D. Proximity to residential areas

Find the Answer p. 275

35. Which of the following is the least important aspect to consider when selecting a security facility location?Select the best answer.

- ❍ A. Access to means of transportation
- ❍ B. Frequency of earthquakes
- ❍ C. Size suitable for future growth
- ❍ D. Direction of door openings

Find the Answer p. 275

36. Which of the following is the least important aspect to consider when designing the interior of a security facility?Select the best answer.

- ❍ A. Load rating
- ❍ B. Fire resistance
- ❍ C. Accessibility
- ❍ D. Number of offices with doors

Find the Answer p. 275

37. Which of the following is NOT an important physical security factor when considering the security of exterior windows?Select the best answer.

- ❍ A. UV reflection or blocking
- ❍ B. Translucency vs. opaqueness
- ❍ C. Shatterproofness
- ❍ D. Placement

Find the Answer p. 275

38. Which of the following is not an important physical security factor when considering the security of flooring?Select the best answer.

- ❍ A. Load rating
- ❍ B. Texture
- ❍ C. Conductivity of the surface
- ❍ D. Combustibility

Find the Answer p. 275

39. Internal partitions are useful for creating?Select the best answer.

- ❍ A. Division of work from visitor spaces
- ❍ B. Fire barriers
- ❍ C. Separation between individual work spaces and desks
- ❍ D. Distinction between areas of different sensitivity

Find the Answer p. 275

40. Which of the following should be used to provide sufficient security and separation of areas with various levels of sensitivity and confidentiality?Select the best answer.

- ❍ A. Partitions
- ❍ B. Windows
- ❍ C. Boundaries outlined by colored tape
- ❍ D. Floor to ceiling permanent walls

Find the Answer p. 275

41. Which of the following is NOT considered a physical control for protecting physical security?Select the best answer.

- ❍ A. Fencing
- ❍ B. Dogs
- ❍ C. Lighting
- ❍ D. CCTV (Closed-Circuit TV)

Find the Answer p. 275

42. Which of the following is NOT an example of a physical security technical control?Select the best answer.

- ❍ A. Biometric door locks
- ❍ B. Visitor sign-in sheet
- ❍ C. Intrusion detection
- ❍ D. Digital HVAC monitoring

Find the Answer p. 275

43. Which of the following is an example of a physical security technical control?Select the best answer.

- ❍ A. Lighting
- ❍ B. Facility construction materials
- ❍ C. Fire detection and suppression
- ❍ D. Facility selection

Find the Answer p. 275

44. Which of the following is NOT an example of a physical security physical control?Select the best answer.

- ❍ A. Guard dogs
- ❍ B. Man traps
- ❍ C. Fencing
- ❍ D. Data backups

Find the Answer p. 275

45. To protect the mission critical data center from threats to physical security, what should be done?Select the best answer.

- ❍ A. It should be placed in the center or core of the facility
- ❍ B. It should be located off site
- ❍ C. It should be placed in the basement
- ❍ D. It should be distributed throughout the facility

Find the Answer p. 275

46. When designing a facility to provide protection for sensitive electrical equipment, what is the most important factor?Select the best answer.

- ❍ A. Load rating of the floor
- ❍ B. Electrical conductance of the flooring material
- ❍ C. Whether or not raised flooring is used
- ❍ D. The physical dimensions of the data center room

Find the Answer p. 275

47. Secure and protected computer rooms or data centers should be all but which of the following?Select the best answer.

- ❍ A. Restricted access
- ❍ B. Equipped with an electronic equipment compatible fire suppression system
- ❍ C. Human compatible
- ❍ D. Located in the center or core of the facility

Find the Answer p. 275

48. Which of the following represents a threat to confidentiality, integrity AND availability?Select the best answer.

- ❍ A. Theft of a notebook
- ❍ B. Physical destruction of access terminals
- ❍ C. Unauthorized publication of a trade secret to a public Web site
- ❍ D. Termination of power to the supporting systems

Find the Answer p. 275

49. Which of the following is a direct threat to maintaining the integrity of hosted data?Select the best answer.

- ❍ A. Unauthorized disclosure
- ❍ B. Termination of power to the supporting systems
- ❍ C. A USB drive found in the break room being plugging into the access console
- ❍ D. Severe physical damage to an access terminal

Find the Answer p. 276

50. Which of the following is NOT considered a physical security emergency?Select the best answer.

- ❍ A. Toxic material release
- ❍ B. Intrusion attempts through communication links
- ❍ C. Facility fire
- ❍ D. Flooding

Find the Answer p. 276

51. What is the most effective suppressant for electrical fires?Select the best answer.

- ❍ A. CO2
- ❍ B. Soda acid
- ❍ C. Water
- ❍ D. Soda ash

Find the Answer p. 276

52. When selecting a fire extinguisher to use against burning liquids, you should not select one which uses?Select the best answer.

- ❍ A. CO2
- ❍ B. Soda acid
- ❍ C. Halon
- ❍ D. Water

Find the Answer p. 276

53. In a data center, where there is a risk of electrical fires, what is the best choice for a hand-held fire extinguisher?Select the best answer.

- ❍ A. A bucket of sand
- ❍ B. Type C
- ❍ C. A bucket of water
- ❍ D. Type B

Find the Answer p. 276

54. Fire detectors respond to a fire through a sensor that detects one of all but which of the following?Select the best answer.

- ❍ A. Heat
- ❍ B. Light
- ❍ C. Sound
- ❍ D. Smoke

Find the Answer p. 276

55. What type of flame or fire detector is considered the most expensive but also the fastest in detecting fires?Select the best answer.

- ❍ A. Smoke actuated
- ❍ B. Fixed temperature, heat actuated
- ❍ C. Rate of rise heat actuated
- ❍ D. Flame actuated

Find the Answer p. 276

56. What form of water-based fire suppression systems is considered the most inappropriate for data centers?Select the best answer.

- ❍ A. Deluge
- ❍ B. Preaction
- ❍ C. Dry pipe
- ❍ D. Wet pipe

Find the Answer p. 276

57. The most appropriate form of fire suppression mechanism for data centers is?Select the best answer.

- ❍ A. Preaction
- ❍ B. Gas discharge
- ❍ C. Deluge
- ❍ D. Dry pipe

Find the Answer p. 276

58. A gas discharge system suppresses fires by what means?Select the best answer.

- ❍ A. Heat reduction
- ❍ B. Fuel removal
- ❍ C. Oxygen displacement
- ❍ D. Interrupting the chemical reaction of burning

Find the Answer p. 276

59. Why is Halon being replaced whenever possible and not being used when new fire suppression gas-discharge systems are installed?Select the best answer.

- ❍ A. Halon is not effective against electrical fires.
- ❍ B. Halon is expensive.
- ❍ C. Halon is too difficult to manage in most data center environments.
- ❍ D. Halon degrades into toxic chemicals at 900 degrees.

Find the Answer p. 276

60. The most commonly used ecological replacement for Halon in a gas discharge systems is?Select the best answer.

- ❍ A. FM-200
- ❍ B. Low pressure water mists
- ❍ C. CO2
- ❍ D. Halon 1301

Find the Answer p. 276

61. Which of the following is NOT an ecological replacement for Halon in gas discharge fire suppression systems?Select the best answer.

- ❍ A. Argon
- ❍ B. Neon
- ❍ C. Inergen
- ❍ D. NAF-S-III

Find the Answer p. 276

62. When a Halon or equivalent gas discharge fire suppression system is triggered to stop a fire, which of the following is responsible for causing the least amount of damage to the computer equipment?Select the best answer.

- ❍ A. Smoke
- ❍ B. Combustion
- ❍ C. Suppression medium
- ❍ D. Heat

Find the Answer p. 276

63. The benefits of security guards include all but which of the following?Select the best answer.

- ❍ A. They are able to respond to changing situations
- ❍ B. They are able to detect unique intrusions and attacks
- ❍ C. They can make value judgments in the midst of an incident
- ❍ D. They can be socially engineered

Find the Answer p. 276

64. A benefit of security guards is what?Select the best answer.

- ❍ A. They offer discriminating judgment
- ❍ B. They are not appropriate in all environments
- ❍ C. They may include fraudulent information on the job application or resume
- ❍ D. They are susceptible to illness

Find the Answer p. 276

65. What is the most suitable replacement for security guards when the primary need is prevention of tressspassing?Select the best answer.

- ❍ A. Lighting
- ❍ B. Dogs
- ❍ C. Fencing
- ❍ D. Proximity detectors

Find the Answer p. 276

66. The main benefit of guards dogs is?Select the best answer.

- ❍ A. Cost
- ❍ B. Maintenance
- ❍ C. Perimeter security control
- ❍ D. Insurance and liability issues

Find the Answer p. 276

67. What physical security mechanism is the most recognized means of defining the outer perimeter of a secured or controlled area?Select the best answer.

- ❍ A. Lighting
- ❍ B. Proximity detectors
- ❍ C. Locked doors
- ❍ D. Fencing

Find the Answer p. 276

68. Casual trespassers are usually deterred by what?Select the best answer.

- ❍ A. A fence 3 to 4 feet high
- ❍ B. A lighted perimeter
- ❍ C. A wooden fence 6 feet high
- ❍ D. Posted "authorized entry only" signs

Find the Answer p. 276

69. The most effective means to contain a subject while the authentication process is performed, so that in the event of a failure a security guard response can result in the capture of the subject, is what?Select the best answer.

- ❍ A. A gate
- ❍ B. A mantrap
- ❍ C. A turnstile
- ❍ D. A proximity detector

Find the Answer p. 276

70. The most commonly deployed form of perimeter protection is?Select the best answer.

- ❍ A. Fencing
- ❍ B. Guard dogs
- ❍ C. Lighting
- ❍ D. CCTV (Closed-Circuit TV)

Find the Answer p. 276

71. The use of closed circuit television (CCTV) for monitoring live events is considered what form or type of security control?Select the best answer.

- ❍ A. Preventative
- ❍ B. Detective
- ❍ C. Responsive
- ❍ D. Corrective

Find the Answer p. 276

72. Which of the following is correct?Select the best answer.

- ❍ A. The NIST standard for perimeter protection provided by light is that critical areas should be illuminated by 8 candle feet power at 2 feet in height.
- ❍ B. The NIST standard for perimeter protection provided by fencing is that critical areas should be bounded by chain link fencing 3 to 4 feet tall without barbed wire.
- ❍ C. The NIST standard for perimeter protection provided by fencing is that critical areas should be bounded by chain link fencing 8 feet tall with 3 strands of barbed wire.
- ❍ D. The NIST standard for perimeter protection provided by light is that critical areas should be illuminated by 2 candle feet power at 8 feet in height.

Find the Answer p. 276

73. Which of the following is an example of a physical security control?Select the best answer.

- ❍ A. Rules based access controls
- ❍ B. CCTV (Closed-Circuit TV)
- ❍ C. Exit interviews
- ❍ D. Traffic tunneling

Find the Answer p. 276

74. Which of the following is NOT an example of a physical security control?Select the best answer.

- ❍ A. Dogs
- ❍ B. Fencing
- ❍ C. Biometric authentication
- ❍ D. Badge IDs

Find the Answer p. 277

75. Why should plenum cable be used when wiring a new secure facility?Select the best answer.

- ❍ A. It prevents wire tapping
- ❍ B. It won't produce toxic fumes when burned
- ❍ C. It increases the throughput capacity of the IT infrastructure
- ❍ D. It is less expensive than other alternatives

Find the Answer p. 277

Chapter 9
Security Architecture and Design

1. What is the act of using a bad sector on a hard drive to store data that can be located and used by an unauthorized recipient known as?Select the best answer.

   - ❍ A. Data remanence
   - ❍ B. Data diddling
   - ❍ C. Data hiding
   - ❍ D. Data reduction

Find the Answer p. 278

2. Which of the following is the least effective means to mitigate the threat of malicious code in a distributed computing environment?Select the best answer.

   - ❍ A. Screen applets at firewalls
   - ❍ B. Configure browsers to accept code from trusted servers only
   - ❍ C. Avoid using FTP
   - ❍ D. Train users regarding mobile code

Find the Answer p. 278

3. Which of the following TCSEC (Trusted Computer System Evaluation Criteria) rating levels does not require configuration and change control management?Select the best answer.

   - ❍ A. C2
   - ❍ B. A1
   - ❍ C. B2
   - ❍ D. B3

Find the Answer p. 278

4. The Orange Book defines two types of assurance. Which of the following are they?Select the best answer.

- ❍ A. Life cycle and Development
- ❍ B. Operational and Life cycle
- ❍ C. Development and Improvement
- ❍ D. Functional and Efficiency

Find the Answer p. 278

5. Which of the following is NOT an element of operational assurance as defined by the Orange Book?Select the best answer.

- ❍ A. System architecture
- ❍ B. Covert channel analysis
- ❍ C. Security testing
- ❍ D. Trusted recovery

Find the Answer p. 278

6. Which of the following is NOT an element of life cycle assurance as defined by the Orange Book?Select the best answer.

- ❍ A. Design specification and testing
- ❍ B. Configuration management
- ❍ C. Trusted distribution
- ❍ D. System architecture

Find the Answer p. 278

7. Which of the following is NOT one of the three hierarchical types of trusted recovery as defined by the Common Criteria?Select the best answer.

- ❍ A. Automated recovery without undo loss
- ❍ B. Manual recovery
- ❍ C. Asynchronous assisted recovery
- ❍ D. Automated recovery

Find the Answer p. 278

8. Resource isolation provides for all but which of the following?Select the best answer.

- ❍ A. Only auditing and tracking of major events
- ❍ B. Subject and object are clearly identified
- ❍ C. Enforced accountability
- ❍ D. Independent assignment of permissions and rights

Find the Answer p. 278

9. The separation of memory physically instead of just logically is an example of and a requirement for what?Select the best answer.

- ❍ A. Trusted computing base
- ❍ B. Hardware segmentation
- ❍ C. A division between user mode and kernel mode
- ❍ D. Data classification levels

Find the Answer p. 278

10. The method used to restrict communications so that they only occur through controlled interfaces in order to maintain the security of a system is?Select the best answer.

- ❍ A. Data diddling
- ❍ B. Data hiding
- ❍ C. Abstraction
- ❍ D. Layering

Find the Answer p. 278

11. The absence of a communication interface between security layers in order to prevent subjects from obtaining knowledge of a confidential resource is known as what?Select the best answer.

- ❍ A. Data hiding
- ❍ B. Layering
- ❍ C. Data classification
- ❍ D. Abstraction

Find the Answer p. 278

12. Which of the following is NOT true of a state machine model?Select the best answer.

- ❍ A. It is secure in every instance of its existence
- ❍ B. It executes commands but not transactions securely
- ❍ C. It boots into a secure state, even after an error is encountered
- ❍ D. It restricts subjects to access resources

Find the Answer p. 278

13. The columns of an access control matrix are known as?Select the best answer.

- ❍ A. Capability lists
- ❍ B. Tuples
- ❍ C. Access control lists
- ❍ D. Ordinal sets

Find the Answer p. 278

14. The security model that defines the relationships that allow a subject to transfer rights to objects is known as?Select the best answer.

- ❍ A. The Bell-LaPadula model
- ❍ B. The Biba model
- ❍ C. The Clark-Wilson model
- ❍ D. The Take-Grant model

Find the Answer p. 278

15. The Bell-LaPadula security model is primarily concerned with protecting?Select the best answer.

- ❍ A. Confidentiality
- ❍ B. Integrity
- ❍ C. Non-repudiation
- ❍ D. Accountability

Find the Answer p. 278

16. The primary regulation of the Bell-LaPadula security model is?Select the best answer.

- ❍ A. * (star) integrity axiom
- ❍ B. * (star) property rule
- ❍ C. No write up
- ❍ D. No read down

Find the Answer p. 278

17. The Bell-LaPadula's simple security rule is what?Select the best answer.

- ❍ A. No write up
- ❍ B. No write down
- ❍ C. No read up
- ❍ D. No read down

Find the Answer p. 278

18. Which of the following is NOT a weakness, flaw, or oversight of the Bell-LaPadula security model?Select the best answer.

- ❍ A. It does not address covert channels
- ❍ B. It does not address file sharing
- ❍ C. It does not specifically define what a secure state transition actually is
- ❍ D. It does not address a multilevel security policy

Find the Answer p. 278

19. The Biba security model is primarily concerned with protecting?Select the best answer.

- ❍ A. Integrity
- ❍ B. Disclosure
- ❍ C. Availability
- ❍ D. Confidentiality

Find the Answer p. 278

20. The * (star) integrity axiom of the Biba security model is what?Select the best answer.

- ❍ A. No write down
- ❍ B. No write up
- ❍ C. No read down
- ❍ D. No read up

Find the Answer p. 278

21. What security model was developed as the integrity analog to the Bell-LaPadula security model?Select the best answer.

- ❍ A. Take-Grant
- ❍ B. Clark-Wilson
- ❍ C. Biba
- ❍ D. Information Flow

Find the Answer p. 278

22. A security model that employs the boundary controls of least upper bound (LUB) and greatest lower bound (GLB) is commonly referred to as?Select the best answer.

- ❍ A. The Clark Wilson model
- ❍ B. The non-interference model
- ❍ C. The integrity model
- ❍ D. A lattice model

Find the Answer p. 278

23. Which security model is focused on preventing authorized users from making unauthorized modifications to data?Select the best answer.

- ❍ A. Clark-Wilson
- ❍ B. Bell-LaPadula
- ❍ C. Biba
- ❍ D. Take-Grant

Find the Answer p. 278

24. Which of the following is not an element of the Clark-Wilson security model?Select the best answer.

- ❍ A. Subjects can access resources only through authorized interfaces
- ❍ B. The classifications or levels of access are defined
- ❍ C. Separation of duties is compulsory
- ❍ D. Auditing is mandatory

Find the Answer p. 279

25. The management of the movement of data between classification levels is the primary concern of which security model?Select the best answer.

- ❍ A. Biba
- ❍ B. Clark-Wilson
- ❍ C. Information Flow
- ❍ D. Noninterference

Find the Answer p. 279

26. What security model is concerned with preventing the actions of subjects at one security level from being noticed by or affecting subjects at a different security level.Select the best answer.

- ❍ A. Biba
- ❍ B. Clark-Wilson
- ❍ C. Information Flow
- ❍ D. Noninterference

Find the Answer p. 279

27. What security mode is represented by the state when all users have the clearance and need to know for all information stored on a system?Select the best answer.

- ❍ A. Dedicated security mode
- ❍ B. System-high security mode
- ❍ C. Compartmented security mode
- ❍ D. Multilevel security mode

Find the Answer p. 279

28. What security mode is represented by the state when users are limited to resource access based on need to know and formal access approval, but are only able to process data at a single level of classification?Select the best answer.

- ❍ A. Multilevel security mode
- ❍ B. Compartmentalized security mode
- ❍ C. System-high security mode
- ❍ D. Dedicated security mode

Find the Answer p. 279

29. Within what security mode does the system function at a single security level and all users have all of the need to know for all data on the system?Select the best answer.

- ❍ A. System-high security mode
- ❍ B. Multilevel security mode
- ❍ C. Dedicated security mode
- ❍ D. Compartmented security mode

Find the Answer p. 279

30. A system is labeled as having _____ when all of the security protection mechanism work in concert to process and handle sensitive data without violating the trusted computer base or the applicable security policy.Select the best answer.

- ❍ A. Assurance
- ❍ B. Certification
- ❍ C. Accreditation
- ❍ D. Trust

Find the Answer p. 279

31. The European standards for security evaluation criteria is known as?Select the best answer.

- ❍ A. Information Technology Security Evaluation Criteria (ITSEC)
- ❍ B. Common Criteria (CC)
- ❍ C. European Union Trusted Computer System Evaluation Criteria (EU TCSEC)
- ❍ D. Trusted Computer System Evaluation Criteria (TCSEC)

Find the Answer p. 279

32. If the operating system fails to establish boundaries for the size and type of data that can be inputted, what malicious event or activity can occur?Select the best answer.

- ❍ A. Denial of service
- ❍ B. Logic bomb
- ❍ C. Buffer overflow
- ❍ D. Virus infection

Find the Answer p. 279

33. Which operating state represents a process in normal execution?Select the best answer.

- ❍ A. Ready state
- ❍ B. Wait state
- ❍ C. Supervisory state
- ❍ D. Problem state

Find the Answer p. 279

34. The act of positioning data in one security division that is not accessible by a subject of another security division is called what?Select the best answer.

- ❍ A. Data hiding
- ❍ B. Layering
- ❍ C. Data diddling
- ❍ D. Abstraction

Find the Answer p. 279

35. Which of the following security models is focused on protecting confidentiality?Select the best answer.

- ❍ A. Biba model
- ❍ B. Bell-LaPadula model
- ❍ C. Take-Grant model
- ❍ D. Clark-Wilson model

Find the Answer p. 279

36. Which of the books from the Rainbow series is concerned with the interactions of computers over a communication medium?Select the best answer.

- ❍ A. Orange
- ❍ B. Tan
- ❍ C. Red
- ❍ D. Purple

Find the Answer p. 279

37. For security to be effective, which of the following must NOT be true?Select the best answer.

- ❍ A. Security is added to a product after its initial development
- ❍ B. Security is integrated into a product at the design stage
- ❍ C. Security is engineered into the product
- ❍ D. Security is implemented by default in the product

Find the Answer p. 279

38. Once security is implemented into the design of a product, it should also be all but which of the following?Select the best answer.

- ❍ A. Tested
- ❍ B. Disabled
- ❍ C. Certified
- ❍ D. Audited

Find the Answer p. 279

39. If the operating system or an application fails to set boundaries on input data, what problem can occur?Select the best answer.

- ❍ A. Session hijacking
- ❍ B. Access grabbing
- ❍ C. Buffer overflow
- ❍ D. Information disclosure

Find the Answer p. 279

40. A buffer overflow can cause all but which of the following?Select the best answer.

- ❍ A. Network throttling
- ❍ B. System freezing
- ❍ C. System rebooting
- ❍ D. Data corruption

Find the Answer p. 279

41. Once data has been processed by the CPU for a program, it is moved into memory areas known as?Select the best answer.

- ❍ A. Primary storage
- ❍ B. Real storage
- ❍ C. Secondary storage
- ❍ D. Virtual storage

Find the Answer p. 279

42. The collection of mechanisms within a computer system that work in harmony to enforce and support a security policy is known as?Select the best answer.

- ❍ A. Ring 0
- ❍ B. An assurance package
- ❍ C. White box system
- ❍ D. Trusted computing base

Find the Answer p. 279

43. What type of memory storage requires constant updates because the data it stores dissipates and decays?Select the best answer.

- ❍ A. Static RAM or Random Access Memory
- ❍ B. ROM or Read Only Memory
- ❍ C. Dyanmic RAM or Random Access Memory
- ❍ D. EPROM or Erasable and Programmable Read Only Memory

Find the Answer p. 279

44. Which of the following is the fastest form of memory?Select the best answer.

- ❍ A. Secondary
- ❍ B. Virtual
- ❍ C. Real
- ❍ D. Cache

Find the Answer p. 279

45. What component of a computer system is the most trusted element?Select the best answer.

- ❍ A. CPU
- ❍ B. Memory
- ❍ C. Storage devices
- ❍ D. Network interface

Find the Answer p. 279

46. Why is an access control layer between software and memory established using a kernel level memory mapper/manager?Select the best answer.

- ❍ A. It prevents buffer overflows
- ❍ B. Software is not trusted
- ❍ C. It helps to minimize the use of secondary storage
- ❍ D. It's required by D1 TCSEC certification

Find the Answer p. 279

47. In a trusted computer which employs the concept of protection rings, in which ring are hardware drivers typically located?Select the best answer.

- ❍ A. Ring 0
- ❍ B. Ring 1
- ❍ C. Ring 2
- ❍ D. Ring 3

Find the Answer p. 279

48. If a process in a higher protection ring number needs to communicate with a process or resource in a lower protection ring number, what must occur?Select the best answer.

- ❍ A. Buffer overflow
- ❍ B. Execution priority shift
- ❍ C. The process must be moved to a lower ring number
- ❍ D. System call

Find the Answer p. 279

49. Which of the four possible operating states is exemplified by a process that will resume execution as soon as its print job is fully sent to the print server?Select the best answer.

- ❍ A. Wait state.
- ❍ B. Ready state.
- ❍ C. Problem state.
- ❍ D. Supervisory state.

Find the Answer p. 280

50. The ability for a computer system to execute more than one process simultaneously is known as?Select the best answer.

- ❍ A. Multithreading
- ❍ B. Multitasking
- ❍ C. Multiprocessing
- ❍ D. Multiplexing

Find the Answer p. 280

51. The _____ a security system, the _____ it provides.Select the best answer.

- ❍ A. less complex, less assurance
- ❍ B. less complex, more assurance
- ❍ C. more complex, less assurance
- ❍ D. more complex, more assurance

Find the Answer p. 280

52. Trusted computing base is important for all but which of the following reasons?Select the best answer.

- ❍ A. TCB ensures that a properly designed system is fully secured.
- ❍ B. If the TCB meets specific requirements, it can be said to provide a specific level of trust.
- ❍ C. TCB can be built into a system, evaluated, and certified.
- ❍ D. TCB certification provides a standardized system to compare the security capabilities between different systems and to provide a standardized label of the level of security it provides.

Find the Answer p. 280

53. The orange book (TCSEC) from the rainbow series addresses what?Select the best answer.

- ❍ A. Auditing
- ❍ B. Stand-alone systems
- ❍ C. Interactions of computers over a communication medium
- ❍ D. Development of production-quality formal verification systems

Find the Answer p. 280

54. Which of the following is NOT true in regards to security domains?Select the best answer.

- ❍ A. Interactions between a security domain and a TCB must be strictly regulated and controlled to maintain security.
- ❍ B. A security domain contains the objects and resources that a specific subject can access.
- ❍ C. The O/S, when operating in user mode, has access to a larger security domain than when operating in kernel mode.
- ❍ D. Security domains must be clearly identified, separated, and enforced.

Find the Answer p. 280

55. Which of the following is NOT true in regards to an application executing in user mode?Select the best answer.

- ❍ A. It cannot access hardware directly
- ❍ B. Memory access is handled by a mediator
- ❍ C. It can access resources only within its own security domain
- ❍ D. It should be closely monitored since it is directly interacting with sensitive resources

Find the Answer p. 280

56. Which Trusted Computer System Evaluation Criteria (TCSEC) security label is the lowest level that requires mandatory protection mechanisms and controls?Select the best answer.

- ❍ A. A
- ❍ B. B
- ❍ C. C
- ❍ D. D

Find the Answer p. 280

57. Which of the following Trusted Computer System Evaluation Criteria (TCSEC) security labels represents those systems with the least degree of trust?Select the best answer.

- ❍ A. A1
- ❍ B. B2
- ❍ C. B1
- ❍ D. B3

Find the Answer p. 280

58. Which of the following is NOT an evaluation criteria for establishing TCSEC security labels?Select the best answer.

- ❍ A. Continuous protection
- ❍ B. Identificaiton
- ❍ C. Accountability
- ❍ D. Task based access controls

Find the Answer p. 280

59. What security label from the Trusted Computer System Evaluation Criteria (TCSEC) represents those systems with the most secure configurations?Select the best answer.

- ❍ A. A
- ❍ B. B
- ❍ C. C
- ❍ D. D

Find the Answer p. 280

60. Which TCSEC security label represents systems that employ security domains?Select the best answer.

- ❍ A. C1
- ❍ B. B3
- ❍ C. C2
- ❍ D. B2

Find the Answer p. 280

61. What is the minimum Trusted Computer System Evaluation Criteria (TCSEC) security level that directly addresses covert channels?Select the best answer.

- ❍ A. C2
- ❍ B. B1
- ❍ C. B2
- ❍ D. A1

Find the Answer p. 280

62. Which of the following is NOT an effective countermeasure against buffer overflows?Select the best answer.

- ❍ A. Port blocking
- ❍ B. Verifying input data
- ❍ C. Auditing
- ❍ D. Host based intrusion detection system

Find the Answer p. 280

63. The Information Technology Security Evaluation Criteria (ITSEC) evaluates what two attributes separately that Trusted Computer System Evaluation Criteria (TCSEC) evaluates together?Select the best answer.

- ❍ A. Confidentialty and integrity
- ❍ B. Functionality and assurance
- ❍ C. Availability and authentication
- ❍ D. Accountability and non-repudiation

Find the Answer p. 280

64. Which of the following is NOT true in regards to Trusted Computer System Evaluation Criteria (TCSEC)?Select the best answer.

- ❍ A. Addresses confidentiality
- ❍ B. Works with government data classifications
- ❍ C. Employs only a few specific ratings
- ❍ D. Addresses network connectivity

Find the Answer p. 280

65. Which of the following is NOT true in regards to the Red book from the rainbow series?Select the best answer.

- ❍ A. Addresses centralized and distributed networks with one or more accreditation authorities
- ❍ B. Addresses network connectivity
- ❍ C. Rates confidentiality and integrity
- ❍ D. Addresses denial of service protection

Find the Answer p. 280

66. An information path that is not normally used to communicate information and therefore unprotected by the system's security mechanisms is known as?Select the best answer.

- ❍ A. TEMPEST
- ❍ B. Backdoor
- ❍ C. Covert channel
- ❍ D. Data remanence

Find the Answer p. 280

67. Which of the following is an example of a multi-level security model?Select the best answer.

- ❍ A. Bell-LaPadula
- ❍ B. Information flow
- ❍ C. Clark-Wilson
- ❍ D. Take-Grant

Find the Answer p. 280

68. Which of the following is secure in each and every instance of its existence?Select the best answer.

- ❍ A. Expert system
- ❍ B. State machine model
- ❍ C. Neural network
- ❍ D. Trusted computing base

Find the Answer p. 280

69. Which of the following is NOT an example of a covert channel being used to transmit data or a signal?Select the best answer.

- ❍ A. A blinking light on a device
- ❍ B. A fraudulently marked bad sector on a hard drive
- ❍ C. A network packet sent repeatedly for a specific length of time
- ❍ D. A dedicated VPN link between the local LAN and a remote client

Find the Answer p. 280

70. Which of the following is NOT one of the three types of NIACAP (National Information Assurance Certification and Accreditation Process) accreditations?Select the best answer.

- ❍ A. Domain
- ❍ B. Site
- ❍ C. Type
- ❍ D. System

Find the Answer p. 280

71. All but which of the following is a classification evaluation criteria for the B1 level of Trusted Computer System Evaluation Criteria (TCSEC)?Select the best answer.

- ❍ A. Each object must have a classification label.
- ❍ B. Each subject must have a clearance label.
- ❍ C. Restrictions against covert channels.
- ❍ D. Data leaving the system must have an accurate security label.

Find the Answer p. 280

72. What level of Trusted Computer System Evaluation Criteria (TCSEC) certification has a requirement of verified protection?Select the best answer.

- ❍ A. C2
- ❍ B. B2
- ❍ C. B3
- ❍ D. A1

Find the Answer p. 280

73. The B2 Trusted Computer System Evaluation Criteria (TCSEC) security label is roughly equivalent to which of the following Information Technology Security Evaluation Criteria (ITSCE) security labels?Select the best answer.

- ❍ A. E3
- ❍ B. E4
- ❍ C. E5
- ❍ D. E6

Find the Answer p. 280

74. Which of the security evaluation methods employs protection profiles to specify security requirements?Select the best answer.

- ❍ A. Trusted Computer System Evaluation Criteria (TCSEC)
- ❍ B. Information Technology Security Evaluation Criteria (ITSEC)
- ❍ C. Common Criteria (CC)
- ❍ D. European Union Trusted Computer System Evaluation Criteria (EU TCSEC)

Find the Answer p. 281

75. _____ must be rechecked or reverified after a specific period of time or after significant changes occur.Select the best answer.

- ❍ A. Certification
- ❍ B. Accreditation
- ❍ C. Neither Certification nor Accreditation
- ❍ D. Both Certification and Accreditation

Find the Answer p. 281

76. The formalized certification and accreditation method employed by the department of defense is known as?Select the best answer.

- ❍ A. Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)
- ❍ B. National Information Assurance Certification and Accreditation Process (NIACAP)
- ❍ C. Commercial Information Security Analysis Process (CIAP)
- ❍ D. Common Criteria (CC)

Find the Answer p. 281

77. Which of the following is NOT true in regards to closed systems?Select the best answer.

- ❍ A. Proprietary
- ❍ B. Published specifications for easy 3rd party component development
- ❍ C. Offers some level of security through obscurity
- ❍ D. Not exemplified by Microsoft, Apple, or UNIX operating systems

Find the Answer p. 281

78. What is the most effective way to prevent the use of covert channels?Select the best answer.

- ❍ A. Firewalls
- ❍ B. Vulnerability scanners
- ❍ C. Anti-virus software
- ❍ D. Noise

Find the Answer p. 281

79. A means by which a hacker can gain access to an operating system by planting a piece of software or opening a hole in the security is known as?Select the best answer.

- ❍ A. Maintenance hook
- ❍ B. Back door
- ❍ C. Trojan horse
- ❍ D. Covert channel

Find the Answer p. 281

80. Which of the following is not an effective countermeasure against backdoors and maintenance hooks?Select the best answer.

- ❍ A. Encryption
- ❍ B. Network based intrusion detection system
- ❍ C. Strong authentication
- ❍ D. Strong access controls

Find the Answer p. 281

Chapter 10
Telecommunications and Network Security

1. At what layer of the OSI model does SQL, as a service protocol, operate?Select the best answer.

   - ❍ A. Layer 3
   - ❍ B. Layer 4
   - ❍ C. Layer 5
   - ❍ D. Layer 6

   Find the Answer p. 282

2. Which of the following is considered a secure replacement for telnet?Select the best answer.

   - ❍ A. Secure Shell (SSH-2)
   - ❍ B. Secure Multipurpose Internet Mail Extensions (S/MIME)
   - ❍ C. Secure Electronic Transaction (SET)
   - ❍ D. Secure Wide Area Network(S/WAN)

   Find the Answer p. 282

3. The Wireless Transport Layer Security Protocol (WTLS) provides for all but which of the types of authentication?Select the best answer.

   - ❍ A. Anonymous authentication
   - ❍ B. Challenge-response authentication
   - ❍ C. Two-way client and server authentication
   - ❍ D. Server authentication

   Find the Answer p. 282

4. Which of the following is FALSE?Select the best answer.

   - ❍ A. Data moving across a Wireless Application Protocol (WAP) gateway will be converted from WTLS to SSL.
   - ❍ B. Data is temporarily in the clear on a Wireless Application Protocol (WAP) gateway.
   - ❍ C. The Wireless Application Protocol (WAP) protocol stack includes IPSec.
   - ❍ D. Authentication and authorization can be performed by wireless devices through PKI enabled transactions.

Find the Answer p. 282

5. IEEE 802.11b wireless standard designates that _____ is to be used to encrypt traffic and provide authentication services.Select the best answer.

   - ❍ A. Wireless Application Protocol (WAP)
   - ❍ B. Wireless Transport Layer Security Protocol (WTLS)
   - ❍ C. Wireless Datagram Protocol (WDP)
   - ❍ D. Wired Equivalent Privacy (WEP)

Find the Answer p. 282

6. The Wired Equivalent Privacy (WEP) algorithm was selected to protect wireless communications for all but which of the following reasons?Select the best answer.

   - ❍ A. It is a mandatory element of 802.11b
   - ❍ B. It is reasonably strong
   - ❍ C. It is self-synchronizing
   - ❍ D. It is computationally efficient

Find the Answer p. 282

7. Which form of authentication, supported by the 802.11 specification, is also known as null authentication?Select the best answer.

- ❍ A. Anonymous authentication
- ❍ B. Open system authentication
- ❍ C. Shared key authentication
- ❍ D. Closed system authentication

Find the Answer p. 282

8. What network device can be used to link two or more networks together even if they use different protocols?Select the best answer.

- ❍ A. Gateway
- ❍ B. Hub
- ❍ C. Bridge
- ❍ D. Router

Find the Answer p. 282

9. Which of the following is NOT true in regards to a screened-host or sacrificial-host firewall?Select the best answer.

- ❍ A. It uses packet filtering
- ❍ B. It provides network and transport layer filtering
- ❍ C. It uses a bastion host
- ❍ D. It is a first generation firewall

Find the Answer p. 282

10. Which of the following is NOT a valid name or designation for an application level firewall?Select the best answer.

- ❍ A. Proxy server
- ❍ B. Circuit level firewall
- ❍ C. A dynamic firewall
- ❍ D. Second generation firewall

Find the Answer p. 282

11. What type of firewall creates a virtual circuit between the workstation/client system and the server?Select the best answer.

- ❍ A. A static packet filtering firewall
- ❍ B. A stateful inspection firewall
- ❍ C. A kernel proxy firewall
- ❍ D. A second generation firewall

Find the Answer p. 282

12. Which of the following is FALSE about third generation firewalls?Select the best answer.

- ❍ A. They offer significantly increased performance
- ❍ B. They are stateful inspection firewalls
- ❍ C. They operate at the network layer
- ❍ D. They examine the state and content of data

Find the Answer p. 282

13. A dynamic packet filtering firewall is known as what generation of firewall?Select the best answer.

- ❍ A. Fifth
- ❍ B. Fourth
- ❍ C. Third
- ❍ D. Second

Find the Answer p. 282

14. A host system can be a firewall if all but which of the following are true?Select the best answer.

- ❍ A. Two NICs are present, each in a different network
- ❍ B. The same protocol is used on both networks
- ❍ C. The same network topology is used on both networks
- ❍ D. IP forwarding is disabled

Find the Answer p. 282

15. A DMZ, or demilitarized zone, is used in a networking context for what primary purpose?Select the best answer.

- ❍ A. To allow systems in the DMZ to be easily accessed by Internet users
- ❍ B. To provide a means by which a private network can be connected to the Internet
- ❍ C. To enable VPN connections from remote users
- ❍ D. To provide a high level of security for the private network

Find the Answer p. 282

16. What networking mechanism is used to allow communications from a private network to the Internet to occur without enabling Internet users to initiate communications or extract internal network configuration information from the interactions?Select the best answer.

- ❍ A. Network address translation
- ❍ B. Router
- ❍ C. Firewall
- ❍ D. Virtual private networking

Find the Answer p. 282

17. A benefit of using network address translation is?Select the best answer.

- ❍ A. Proxy services
- ❍ B. Private IP addresses
- ❍ C. Traffic throttling
- ❍ D. Packet filtering

Find the Answer p. 282

18. Network address translation can also be referred to as?Select the best answer.

- ❍ A. Redirection
- ❍ B. Traffic routing
- ❍ C. IP masking
- ❍ D. Virtual circuits

Find the Answer p. 282

19. Which of the following is not one of the seven original top level domain names used on the Internet?Select the best answer.

- ❍ A. .edu
- ❍ B. .mil
- ❍ C. .org
- ❍ D. .biz

Find the Answer p. 282

20. The country codes or geographic top-level domain names are standardized _____ character names.Select the best answer.

- ❍ A. 2
- ❍ B. 3
- ❍ C. 4
- ❍ D. 5

Find the Answer p. 282

21. Which of the following is NOT a valid remote access security method for authenticating connecting users?Select the best answer.

- ❍ A. Caller ID
- ❍ B. Digital signatures
- ❍ C. Callback
- ❍ D. Restricted Access

Find the Answer p. 282

22. Synchronous Optical Network (SONET) is commonly used for metropolitan area networks (MAN). SONET offers the benefit of self-healing because of?Select the best answer.

- ❍ A. Its use of fiber optic cable
- ❍ B. Its use of redundant rings
- ❍ C. Its use of token passing
- ❍ D. Its support of numerous protocol types

Find the Answer p. 282

23. Which of the following is NOT true for circuit switching networks?Select the best answer.

- ❍ A. Uses physical permanent connections from one point to another
- ❍ B. Has a single switched communication path
- ❍ C. Routes data based on best path available
- ❍ D. Is primarily voice oriented

Find the Answer p. 282

24. Which of the following is NOT true for packet switching networks?Select the best answer.

- ❍ A. Transmit bursty or inconsistent levels of traffic
- ❍ B. Incorporates variable delays in the transmission of data
- ❍ C. Is sensitive to the loss of data
- ❍ D. Is connection oriented

Find the Answer p. 283

25. The Internet's switching mechanisms can overall be described as?Select the best answer.

- ❍ A. Switched virtual circuits
- ❍ B. Circuit switching
- ❍ C. Packet switching
- ❍ D. Permanent virtual circuits

Find the Answer p. 283

26. The first packet switching network was?Select the best answer.

- ❍ A. Frame relay
- ❍ B. X.25
- ❍ C. ATM
- ❍ D. SMDS

Find the Answer p. 283

27. In what mode of a VPN is the data contained in the IP packet encrypted but the header of the IP packet is not encrypted?Select the best answer.

- ❍ A. Tunnel
- ❍ B. Header throughput
- ❍ C. Transport
- ❍ D. Link hop

Find the Answer p. 283

28. Which of the following is FALSE in regards to the Layer 2 Tunneling Protocol (L2TP)?Select the best answer.

- ❍ A. Enables a single point to point connection
- ❍ B. Operates at the Data Link layer
- ❍ C. Supports the encryption of multiple protocols
- ❍ D. Uses PPP authentication and encryption services

Find the Answer p. 283

29. Which of the following is NOT true about IPSec?Select the best answer.

- ❍ A. It's built into all versions of TCP/IP
- ❍ B. It encrypts and authenticates IP data
- ❍ C. It is used to establish network to network connectivity
- ❍ D. It supports multiple simultaneous tunnels

Find the Answer p. 283

30. In order to provide the most secure remote access authentication method for dial-up clients, which of the following mechanisms should you configure and enforce?Select the best answer.

- ❍ A. No callback
- ❍ B. Callback to a user provided number
- ❍ C. Callback to a predetermined number
- ❍ D. Multilink callback

Find the Answer p. 283

31. Password Authentication Protocol (PAP) is an authentication mechanism supported by most remote access services. However, why should PAP be avoided?Select the best answer.

- ❍ A. Its wide range of compatibility
- ❍ B. It is used only by remote access systems
- ❍ C. It requires a certificate authority to function
- ❍ D. It transmits logon credentials in plain text

Find the Answer p. 283

32. Which of the following is not a true or valid characteristic of the TCP protocol?Select the best answer.

- ❍ A. Connectionless
- ❍ B. Full duplex
- ❍ C. Uses acknowledgements
- ❍ D. Sequenced segments

Find the Answer p. 283

33. At what layer of the TCP/IP model is data called a segment?Select the best answer.

- ❍ A. Application layer
- ❍ B. Host-to-Host or Transport layer
- ❍ C. Internet or Network layer
- ❍ D. Network Access layer

Find the Answer p. 283

34. The occurrence of electronic signals spilling over from one wire to another is known as?Select the best answer.

- ❍ A. Attenuation
- ❍ B. Noise
- ❍ C. Crosstalk
- ❍ D. superzaping

Find the Answer p. 283

35. Ethernet is an example of what type of LAN transmission protocol?Select the best answer.

- ❍ A. Broadband
- ❍ B. CSMA
- ❍ C. CSMA/CA
- ❍ D. CSMA/CD

Find the Answer p. 283

36. What type of firewall is able to self-modify its traffic filters?Select the best answer.

- ❍ A. Dynamic packet filtering
- ❍ B. Kernel proxy
- ❍ C. Stateful inspection
- ❍ D. Application level

Find the Answer p. 283

37. Which of the following uses acknowledgements to ensure that data is delivered to the recipient?Select the best answer.

- ❍ A. UDP
- ❍ B. IP
- ❍ C. TCP
- ❍ D. TFTP

Find the Answer p. 283

38. Which of the following can NOT be used to exchange files?Select the best answer.

- ❍ A. FTP
- ❍ B. NFS
- ❍ C. TFTP
- ❍ D. Telnet

Find the Answer p. 283

39. Which of the following protocols is used for e-mail?Select the best answer.

- ❍ A. SMTP
- ❍ B. LPD
- ❍ C. SNMP
- ❍ D. BootP

Find the Answer p. 283

40. Logical communication between peer layers of the OSI model are made possible through the use of?Select the best answer.

- ❍ A. Encapsulation
- ❍ B. Remote procedure calls
- ❍ C. Direct addressing
- ❍ D. Broadcasts

Find the Answer p. 283

41. What is the abstract protocol model that is widely used as the standard framework for designing applications and network protocols and describing how they function?Select the best answer.

- ❍ A. Clark-Wilson model
- ❍ B. OSI model
- ❍ C. NetBIOS
- ❍ D. MAC addressing

Find the Answer p. 283

42. Starting counting from the Physical layer, the third layer of the OSI model is?Select the best answer.

- ❍ A. Session
- ❍ B. Transport
- ❍ C. Network
- ❍ D. Data Link

Find the Answer p. 283

43. SSL (secure sockets layer) and NFS (network file system) operate at what level of the OSI model?Select the best answer.

- ❍ A. Network
- ❍ B. Transport
- ❍ C. Data Link
- ❍ D. Session

Find the Answer p. 283

44. Which of the following is NOT a security service used to protect OSI communications?Select the best answer.

- ❍ A. Auditing
- ❍ B. Authenticaiton
- ❍ C. Data integrity
- ❍ D. Non-repudiation

Find the Answer p. 283

45. TCP provides for all but which of the following?Select the best answer.

- ❍ A. Full-duplex communications
- ❍ B. Connectionless communications
- ❍ C. Data flow management through sliding windows
- ❍ D. Reliable virtual circuits

Find the Answer p. 283

46. What is the last communication between two systems over a TCP/IP connection before actual data can be exchanged?Select the best answer.

- ❍ A. FIN
- ❍ B. ACK
- ❍ C. SYN/ACK
- ❍ D. SYN

Find the Answer p. 283

47. Which of the following is NOT a valid reason to deploy a network?Select the best answer.

- ❍ A. Share resources
- ❍ B. Enable communications between systems
- ❍ C. Increase security
- ❍ D. Centralize administration

Find the Answer p. 283

48. What category of twisted pair cabling is rated to support 1Gbps of throughput?Select the best answer.

- ❍ A. CAT 1
- ❍ B. CAT 3
- ❍ C. CAT 5
- ❍ D. CAT 7

Find the Answer p. 283

49. A network engineer creates a single network by connecting the hub of one office floor to another hub on another floor using a heavily insulated CAT5 cable. One office is on the first floor, the other is on the 48th floor. The systems are fully compatible, but communications between the two floors over the network connection is very poor. What is most likely the cause of this?Select the best answer.

- ❍ A. Attenuation
- ❍ B. Noise
- ❍ C. Crosstalk
- ❍ D. Protocol mismatch

Find the Answer p. 284

50. Which of the following statements is NOT true regarding asynchronous transmissions?Select the best answer.

- ❍ A. The receiver must always be in the ready to receive state
- ❍ B. It is used primarily for small amounts of data
- ❍ C. It is timed to a clocking mechanism
- ❍ D. It often uses stop and start delimiter bits

Find the Answer p. 284

51. Which of the following technologies is baseband instead of broadband?Select the best answer.

- ❍ A. ATM
- ❍ B. ISDN
- ❍ C. DSL
- ❍ D. Ethernet

Find the Answer p. 284

52. The type of network transmission that originates from a single source but is directed toward multiple specific destinations is known as?Select the best answer.

- ❍ A. Multicast
- ❍ B. Broadcast
- ❍ C. Unicast
- ❍ D. Polling

Find the Answer p. 284

53. What LAN media access method can be used to connect systems up to 2 km apart, support transmission rates up to 100Mbps, is highly resistant to electromagnetic and radio frequency interference, and is often used to connect several different types of networks?Select the best answer.

- ❍ A. Gigabit Ethernet
- ❍ B. Fiber Distributed Data Interface (FDDI)
- ❍ C. Copper Distributed Data Interface (CDDI)
- ❍ D. Asynchronous Transfer Mode (ATM)

Find the Answer p. 284

54. What network device is used specifically to safeguard against attenuation?Select the best answer.

- ❍ A. Hub
- ❍ B. Bridge
- ❍ C. Repeater
- ❍ D. Router

Find the Answer p. 284

55. Which of the following network devices operates exclusively at layer 3 of the OSI model?Select the best answer.

- ❍ A. Bridge
- ❍ B. Repeater
- ❍ C. Switch
- ❍ D. Router

Find the Answer p. 284

56. Which of the following is not a form of server fault tolerance?Select the best answer.

- ❍ A. DNS round robin pointing to duplicate servers
- ❍ B. Automated remote journaling to an offline server
- ❍ C. A mirrored pair of servers with hot rollover capability
- ❍ D. Server clustering

Find the Answer p. 284

57. What is the most common cabling failure for twisted pair cabling?Select the best answer.

- ❍ A. Termination
- ❍ B. Excess cable length
- ❍ C. Audio interference
- ❍ D. Installation

Find the Answer p. 284

58. Which of the following network topologies is the least fault tolerant?Select the best answer.

- ❍ A. Ethernet
- ❍ B. FDDI
- ❍ C. Token Ring
- ❍ D. Frame Relay

Find the Answer p. 284

59. Which of the following types of network abuses is not primarily focused on compromising authentication?Select the best answer.

- ❍ A. Attempted logon break-ins
- ❍ B. Masquerading
- ❍ C. Identity theft
- ❍ D. Eavesdropping

Find the Answer p. 284

60. The use of false source identity, using a debugging account, and gaining access to a secured area using someone else's credentials are examples of what type of network abuse?Select the best answer.

- ❍ A. Eavesdropping
- ❍ B. Network resource saturation and Denial of Service
- ❍ C. Spoofing, Piggybacking, and Backdoors
- ❍ D. Sniffing and Probing a Network

Find the Answer p. 284

61. Which of the following denial of service attacks requires three components (source site, bounce site, and target site) to launch the attack?Select the best answer.

- ❍ A. Smurf
- ❍ B. Ping of Death
- ❍ C. SYN flood
- ❍ D. Teardrop

Find the Answer p. 284

62. When a switch is proving communiction services between VLANs, it is performing operations at what layer of the OSI model?Select the best answer.

- ❍ A. Layer 3
- ❍ B. Layer 2
- ❍ C. Layer 4
- ❍ D. Layer 7

Find the Answer p. 284

63. What device is able to divide collision domains and divide broadcast domains?Select the best answer.

- ❍ A. Switch
- ❍ B. Router
- ❍ C. Bridge
- ❍ D. Hub

Find the Answer p. 284

64. Which of the following is NOT a form of denial of service attack?Select the best answer.

- ❍ A. Sending a victim large e-mail attachments
- ❍ B. Tasking all TCP ports for illegitimate traffic
- ❍ C. Submitting a large stream of fragmented IP packets to a system
- ❍ D. Attempting to break a logon using a brute force password attack

Find the Answer p. 284

65. What protocol is a replacement for PPTP (Point to Point Tunneling Protocol) as used in VPNs (Virtual Private Networks)?Select the best answer.

- ❍ A. CHAP
- ❍ B. L2TP
- ❍ C. PPP
- ❍ D. HDLC

Find the Answer p. 284

66. What network device can be used as a boundary protection and security mechanism?Select the best answer.

- ❍ A. Bridge
- ❍ B. Router
- ❍ C. Firewall
- ❍ D. Switch

Find the Answer p. 284

67. Which of the following is a technology that functions at Layer 1 of the OSI model?Select the best answer.

- ❍ A. SMTP
- ❍ B. UDP
- ❍ C. ARP
- ❍ D. DSSS

Find the Answer p. 284

68. What protocol is used in a diskless workstation environment to initiate the startup process of terminals?Select the best answer.

- ❍ A. BootP
- ❍ B. X Windows
- ❍ C. LPD
- ❍ D. FTP

Find the Answer p. 284

69. ThinNet cabling is also known as?Select the best answer.

- ❍ A. CAT 5
- ❍ B. RG-58
- ❍ C. Twisted pair
- ❍ D. Plenum

Find the Answer p. 284

70. Firewalls offer the best control over security and traffic when combined with?Select the best answer.

- ❍ A. Routers
- ❍ B. Bridges
- ❍ C. Hubs
- ❍ D. Repeaters

Find the Answer p. 284

71. Which of the following is unaffected by RFI and EMI?Select the best answer.

- ❍ A. Coax
- ❍ B. Fiber optic
- ❍ C. Twisted pair
- ❍ D. Shielded twisted pair

Find the Answer p. 284

72. The TCP/IP protocol stack or protocol model, unlike the OSI model, contains _____ layers.Select the best answer.

- ❍ A. 8
- ❍ B. 5
- ❍ C. 4
- ❍ D. 7

Find the Answer p. 284

73. What networking device prevents broadcast storms?Select the best answer.

- ❍ A. Repeater
- ❍ B. Hub
- ❍ C. Bridge
- ❍ D. Routers

Find the Answer p. 284

74. What networking device is primarily software and can be used to connect networks that use different protocols?Select the best answer.

- ❍ A. Gateway
- ❍ B. Switch
- ❍ C. Router
- ❍ D. Bridge

Find the Answer p. 285

75. What layer of the OSI model provides end-to-end conveyance services and establishes a logical connection between server and client?Select the best answer.

- ❍ A. Presentation
- ❍ B. Transport
- ❍ C. Network
- ❍ D. Data link

Find the Answer p. 285

76. The most common cause of network hardware failures is what?Select the best answer.

- ❍ A. Power loss
- ❍ B. Router tables
- ❍ C. Cabling
- ❍ D. Protocol configuration

Find the Answer p. 285

77. The total number of ports available within TCP/IP for communication sessions is?Select the best answer.

- ❍ A. 2
- ❍ B. 1024
- ❍ C. 65536
- ❍ D. 130072

Find the Answer p. 285

Answers: Chapter 1

1. **A**	Review Question p. 2	Detailed Explanation p. 287
2. **B**	Review Question p. 2	Detailed Explanation p. 287
3. **D**	Review Question p. 2	Detailed Explanation p. 287
4. **A**	Review Question p. 3	Detailed Explanation p. 288
5. **C**	Review Question p. 3	Detailed Explanation p. 288
6. **D**	Review Question p. 3	Detailed Explanation p. 288
7. **A**	Review Question p. 4	Detailed Explanation p. 289
8. **B**	Review Question p. 4	Detailed Explanation p. 289
9. **A**	Review Question p. 4	Detailed Explanation p. 290
10. **B**	Review Question p. 5	Detailed Explanation p. 290
11. **C**	Review Question p. 5	Detailed Explanation p. 290
12. **D**	Review Question p. 5	Detailed Explanation p. 291
13. **A**	Review Question p. 6	Detailed Explanation p. 291
14. **B**	Review Question p. 6	Detailed Explanation p. 292
15. **C**	Review Question p. 6	Detailed Explanation p. 292
16. **D**	Review Question p. 7	Detailed Explanation p. 292
17. **A**	Review Question p. 7	Detailed Explanation p. 292
18. **B**	Review Question p. 7	Detailed Explanation p. 293
19. **C**	Review Question p. 8	Detailed Explanation p. 293
20. **C**	Review Question p. 8	Detailed Explanation p. 293
21. **C**	Review Question p. 8	Detailed Explanation p. 294
22. **D**	Review Question p. 9	Detailed Explanation p. 294
23. **A**	Review Question p. 9	Detailed Explanation p. 295

24. **B**	Review Question p. 9	Detailed Explanation p. 295
25. **A**	Review Question p. 10	Detailed Explanation p. 295
26. **B**	Review Question p. 10	Detailed Explanation p. 296
27. **C**	Review Question p. 10	Detailed Explanation p. 296
28. **D**	Review Question p. 11	Detailed Explanation p. 296
29. **A**	Review Question p. 11	Detailed Explanation p. 297
30. **B**	Review Question p. 11	Detailed Explanation p. 297
31. **C**	Review Question p. 12	Detailed Explanation p. 298
32. **D**	Review Question p. 12	Detailed Explanation p. 298
33. **A**	Review Question p. 12	Detailed Explanation p. 298
34. **B**	Review Question p. 12	Detailed Explanation p. 299
35. **C**	Review Question p. 13	Detailed Explanation p. 299
36. **D**	Review Question p. 13	Detailed Explanation p. 299
37. **A**	Review Question p. 13	Detailed Explanation p. 300
38. **B**	Review Question p. 14	Detailed Explanation p. 300
39. **C**	Review Question p. 14	Detailed Explanation p. 301
40. **D**	Review Question p. 14	Detailed Explanation p. 301
41. **B**	Review Question p. 15	Detailed Explanation p. 302
42. **D**	Review Question p. 15	Detailed Explanation p. 302
43. **A**	Review Question p. 15	Detailed Explanation p. 302
44. **C**	Review Question p. 15	Detailed Explanation p. 303
45. **D**	Review Question p. 16	Detailed Explanation p. 303
46. **B**	Review Question p. 16	Detailed Explanation p. 304
47. **C**	Review Question p. 16	Detailed Explanation p. 304
48. **D**	Review Question p. 17	Detailed Explanation p. 304

49. **B**	Review Question p. 17	Detailed Explanation p. 305
50. **C**	Review Question p. 17	Detailed Explanation p. 305
51. **D**	Review Question p. 18	Detailed Explanation p. 305
52. **A**	Review Question p. 18	Detailed Explanation p. 306
53. **A**	Review Question p. 18	Detailed Explanation p. 306
54. **B**	Review Question p. 19	Detailed Explanation p. 306
55. **C**	Review Question p. 19	Detailed Explanation p. 307
56. **B**	Review Question p. 19	Detailed Explanation p. 307
57. **C**	Review Question p. 20	Detailed Explanation p. 307
58. **D**	Review Question p. 20	Detailed Explanation p. 308
59. **A**	Review Question p. 20	Detailed Explanation p. 308
60. **B**	Review Question p. 21	Detailed Explanation p. 309
61. **C**	Review Question p. 21	Detailed Explanation p. 309
62. **B**	Review Question p. 21	Detailed Explanation p. 309
63. **D**	Review Question p. 22	Detailed Explanation p. 310
64. **C**	Review Question p. 22	Detailed Explanation p. 310
65. **B**	Review Question p. 22	Detailed Explanation p. 310
66. **B**	Review Question p. 23	Detailed Explanation p. 311

Answers: Chapter 2

1. **D**	Review Question p. 24	Detailed Explanation p. 312
2. **B**	Review Question p. 24	Detailed Explanation p. 312
3. **D**	Review Question p. 24	Detailed Explanation p. 312
4. **D**	Review Question p. 25	Detailed Explanation p. 313
5. **A**	Review Question p. 25	Detailed Explanation p. 313
6. **A**	Review Question p. 25	Detailed Explanation p. 313
7. **C**	Review Question p. 26	Detailed Explanation p. 314
8. **A**	Review Question p. 26	Detailed Explanation p. 314
9. **B**	Review Question p. 26	Detailed Explanation p. 315
10. **C**	Review Question p. 27	Detailed Explanation p. 315
11. **C**	Review Question p. 27	Detailed Explanation p. 315
12. **B**	Review Question p. 27	Detailed Explanation p. 316
13. **D**	Review Question p. 28	Detailed Explanation p. 316
14. **A**	Review Question p. 28	Detailed Explanation p. 317
15. **B**	Review Question p. 28	Detailed Explanation p. 317
16. **C**	Review Question p. 29	Detailed Explanation p. 317
17. **D**	Review Question p. 29	Detailed Explanation p. 318
18. **A**	Review Question p. 29	Detailed Explanation p. 318
19. **B**	Review Question p. 30	Detailed Explanation p. 318
20. **C**	Review Question p. 30	Detailed Explanation p. 319
21. **D**	Review Question p. 30	Detailed Explanation p. 319
22. **A**	Review Question p. 31	Detailed Explanation p. 319
23. **B**	Review Question p. 31	Detailed Explanation p. 320

24. **D**	Review Question p. 31	Detailed Explanation p. 320
25. **A**	Review Question p. 31	Detailed Explanation p. 320
26. **B**	Review Question p. 32	Detailed Explanation p. 321
27. **C**	Review Question p. 32	Detailed Explanation p. 321
28. **D**	Review Question p. 32	Detailed Explanation p. 321
29. **A**	Review Question p. 33	Detailed Explanation p. 322
30. **A**	Review Question p. 33	Detailed Explanation p. 322
31. **B**	Review Question p. 33	Detailed Explanation p. 322
32. **C**	Review Question p. 34	Detailed Explanation p. 323
33. **D**	Review Question p. 34	Detailed Explanation p. 323
34. **A**	Review Question p. 34	Detailed Explanation p. 324
35. **B**	Review Question p. 35	Detailed Explanation p. 324
36. **C**	Review Question p. 35	Detailed Explanation p. 324
37. **D**	Review Question p. 35	Detailed Explanation p. 325
38. **A**	Review Question p. 36	Detailed Explanation p. 325
39. **B**	Review Question p. 36	Detailed Explanation p. 326
40. **C**	Review Question p. 36	Detailed Explanation p. 326
41. **D**	Review Question p. 37	Detailed Explanation p. 326
42. **A**	Review Question p. 37	Detailed Explanation p. 327
43. **B**	Review Question p. 37	Detailed Explanation p. 327
44. **C**	Review Question p. 38	Detailed Explanation p. 327
45. **D**	Review Question p. 38	Detailed Explanation p. 328
46. **A**	Review Question p. 38	Detailed Explanation p. 328
47. **B**	Review Question p. 39	Detailed Explanation p. 329
48. **C**	Review Question p. 39	Detailed Explanation p. 329

49. **D**	Review Question p. 39	Detailed Explanation p. 330
50. **C**	Review Question p. 40	Detailed Explanation p. 330
51. **D**	Review Question p. 40	Detailed Explanation p. 330
52. **A**	Review Question p. 40	Detailed Explanation p. 330
53. **B**	Review Question p. 40	Detailed Explanation p. 331
54. **C**	Review Question p. 41	Detailed Explanation p. 331
55. **D**	Review Question p. 41	Detailed Explanation p. 331
56. **B**	Review Question p. 41	Detailed Explanation p. 332
57. **A**	Review Question p. 42	Detailed Explanation p. 332
58. **B**	Review Question p. 42	Detailed Explanation p. 332
59. **C**	Review Question p. 42	Detailed Explanation p. 333
60. **D**	Review Question p. 43	Detailed Explanation p. 333
61. **A**	Review Question p. 43	Detailed Explanation p. 333
62. **B**	Review Question p. 43	Detailed Explanation p. 334
63. **C**	Review Question p. 44	Detailed Explanation p. 334
64. **D**	Review Question p. 44	Detailed Explanation p. 334
65. **A**	Review Question p. 44	Detailed Explanation p. 335
66. **B**	Review Question p. 45	Detailed Explanation p. 335
67. **D**	Review Question p. 45	Detailed Explanation p. 336
68. **A**	Review Question p. 45	Detailed Explanation p. 336
69. **B**	Review Question p. 46	Detailed Explanation p. 336
70. **C**	Review Question p. 46	Detailed Explanation p. 337
71. **D**	Review Question p. 46	Detailed Explanation p. 337
72. **A**	Review Question p. 47	Detailed Explanation p. 337
73. **B**	Review Question p. 47	Detailed Explanation p. 338

74. **D** Review Question p. 47 Detailed Explanation p. 338

75. **C** Review Question p. 47 Detailed Explanation p. 338

76. **B** Review Question p. 48 Detailed Explanation p. 339

77. **D** Review Question p. 48 Detailed Explanation p. 339

Answers: Chapter 3

1. **A**	Review Question p. 49	Detailed Explanation p. 340
2. **A**	Review Question p. 49	Detailed Explanation p. 340
3. **B**	Review Question p. 49	Detailed Explanation p. 340
4. **C**	Review Question p. 50	Detailed Explanation p. 341
5. **D**	Review Question p. 50	Detailed Explanation p. 341
6. **A**	Review Question p. 50	Detailed Explanation p. 342
7. **B**	Review Question p. 51	Detailed Explanation p. 342
8. **C**	Review Question p. 51	Detailed Explanation p. 343
9. **D**	Review Question p. 51	Detailed Explanation p. 343
10. **A**	Review Question p. 52	Detailed Explanation p. 343
11. **B**	Review Question p. 52	Detailed Explanation p. 344
12. **C**	Review Question p. 52	Detailed Explanation p. 344
13. **D**	Review Question p. 53	Detailed Explanation p. 344
14. **A**	Review Question p. 53	Detailed Explanation p. 345
15. **B**	Review Question p. 53	Detailed Explanation p. 345
16. **C**	Review Question p. 54	Detailed Explanation p. 346
17. **D**	Review Question p. 54	Detailed Explanation p. 346
18. **A**	Review Question p. 54	Detailed Explanation p. 346
19. **C**	Review Question p. 55	Detailed Explanation p. 347
20. **B**	Review Question p. 55	Detailed Explanation p. 347
21. **C**	Review Question p. 55	Detailed Explanation p. 347
22. **D**	Review Question p. 56	Detailed Explanation p. 348
23. **A**	Review Question p. 56	Detailed Explanation p. 348

24. **B**	Review Question p. 56	Detailed Explanation p. 349
25. **D**	Review Question p. 57	Detailed Explanation p. 349
26. **A**	Review Question p. 57	Detailed Explanation p. 349
27. **C**	Review Question p. 57	Detailed Explanation p. 350
28. **D**	Review Question p. 58	Detailed Explanation p. 350
29. **A**	Review Question p. 58	Detailed Explanation p. 350
30. **B**	Review Question p. 58	Detailed Explanation p. 351
31. **C**	Review Question p. 59	Detailed Explanation p. 351
32. **A**	Review Question p. 59	Detailed Explanation p. 352
33. **B**	Review Question p. 59	Detailed Explanation p. 352
34. **C**	Review Question p. 60	Detailed Explanation p. 352
35. **D**	Review Question p. 60	Detailed Explanation p. 353
36. **A**	Review Question p. 60	Detailed Explanation p. 353
37. **C**	Review Question p. 61	Detailed Explanation p. 354
38. **D**	Review Question p. 61	Detailed Explanation p. 354
39. **C**	Review Question p. 61	Detailed Explanation p. 354
40. **A**	Review Question p. 62	Detailed Explanation p. 355
41. **B**	Review Question p. 62	Detailed Explanation p. 355
42. **D**	Review Question p. 62	Detailed Explanation p. 356
43. **A**	Review Question p. 63	Detailed Explanation p. 356
44. **B**	Review Question p. 63	Detailed Explanation p. 356
45. **C**	Review Question p. 63	Detailed Explanation p. 357
46. **A**	Review Question p. 64	Detailed Explanation p. 357
47. **B**	Review Question p. 64	Detailed Explanation p. 358
48. **D**	Review Question p. 64	Detailed Explanation p. 358

49. **B**	Review Question p. 65	Detailed Explanation p. 358
50. **C**	Review Question p. 65	Detailed Explanation p. 359
51. **D**	Review Question p. 65	Detailed Explanation p. 359
52. **B**	Review Question p. 66	Detailed Explanation p. 359
53. **C**	Review Question p. 66	Detailed Explanation p. 360
54. **D**	Review Question p. 66	Detailed Explanation p. 360
55. **A**	Review Question p. 67	Detailed Explanation p. 360
56. **C**	Review Question p. 67	Detailed Explanation p. 361
57. **D**	Review Question p. 67	Detailed Explanation p. 361
58. **C**	Review Question p. 68	Detailed Explanation p. 362
59. **B**	Review Question p. 68	Detailed Explanation p. 362
60. **C**	Review Question p. 68	Detailed Explanation p. 362
61. **D**	Review Question p. 69	Detailed Explanation p. 363
62. **A**	Review Question p. 69	Detailed Explanation p. 363
63. **B**	Review Question p. 69	Detailed Explanation p. 363
64. **A**	Review Question p. 70	Detailed Explanation p. 364
65. **B**	Review Question p. 70	Detailed Explanation p. 364
66. **D**	Review Question p. 70	Detailed Explanation p. 364
67. **A**	Review Question p. 71	Detailed Explanation p. 365
68. **B**	Review Question p. 71	Detailed Explanation p. 365
69. **C**	Review Question p. 71	Detailed Explanation p. 366
70. **D**	Review Question p. 72	Detailed Explanation p. 366
71. **A**	Review Question p. 72	Detailed Explanation p. 367
72. **B**	Review Question p. 72	Detailed Explanation p. 367
73. **C**	Review Question p. 73	Detailed Explanation p. 367

74. **D** Review Question p. 73 Detailed Explanation p. 368

75. **B** Review Question p. 73 Detailed Explanation p. 368

76. **A** Review Question p. 74 Detailed Explanation p. 369

77. **C** Review Question p. 74 Detailed Explanation p. 369

78. **C** Review Question p. 74 Detailed Explanation p. 369

79. **D** Review Question p. 75 Detailed Explanation p. 370

80. **A** Review Question p. 75 Detailed Explanation p. 370

Answers: Chapter 4

1. **B**	Review Question p. 76	Detailed Explanation p. 372
2. **C**	Review Question p. 76	Detailed Explanation p. 372
3. **D**	Review Question p. 76	Detailed Explanation p. 372
4. **A**	Review Question p. 77	Detailed Explanation p. 373
5. **B**	Review Question p. 77	Detailed Explanation p. 373
6. **C**	Review Question p. 77	Detailed Explanation p. 373
7. **D**	Review Question p. 78	Detailed Explanation p. 374
8. **A**	Review Question p. 78	Detailed Explanation p. 374
9. **B**	Review Question p. 78	Detailed Explanation p. 374
10. **C**	Review Question p. 79	Detailed Explanation p. 375
11. **D**	Review Question p. 79	Detailed Explanation p. 375
12. **A**	Review Question p. 79	Detailed Explanation p. 375
13. **B**	Review Question p. 80	Detailed Explanation p. 376
14. **C**	Review Question p. 80	Detailed Explanation p. 376
15. **D**	Review Question p. 80	Detailed Explanation p. 376
16. **A**	Review Question p. 80	Detailed Explanation p. 377
17. **B**	Review Question p. 81	Detailed Explanation p. 377
18. **C**	Review Question p. 81	Detailed Explanation p. 377
19. **D**	Review Question p. 81	Detailed Explanation p. 378
20. **A**	Review Question p. 82	Detailed Explanation p. 378
21. **B**	Review Question p. 82	Detailed Explanation p. 379
22. **C**	Review Question p. 82	Detailed Explanation p. 379
23. **D**	Review Question p. 83	Detailed Explanation p. 379

24. **A**	Review Question p. 83	Detailed Explanation p. 380
25. **B**	Review Question p. 83	Detailed Explanation p. 380
26. **C**	Review Question p. 84	Detailed Explanation p. 380
27. **B**	Review Question p. 84	Detailed Explanation p. 381
28. **C**	Review Question p. 84	Detailed Explanation p. 381
29. **D**	Review Question p. 85	Detailed Explanation p. 381
30. **A**	Review Question p. 85	Detailed Explanation p. 382
31. **B**	Review Question p. 85	Detailed Explanation p. 382
32. **D**	Review Question p. 86	Detailed Explanation p. 382
33. **A**	Review Question p. 86	Detailed Explanation p. 383
34. **B**	Review Question p. 86	Detailed Explanation p. 383
35. **C**	Review Question p. 87	Detailed Explanation p. 384
36. **D**	Review Question p. 87	Detailed Explanation p. 384
37. **A**	Review Question p. 87	Detailed Explanation p. 385
38. **B**	Review Question p. 88	Detailed Explanation p. 385
39. **C**	Review Question p. 88	Detailed Explanation p. 386
40. **D**	Review Question p. 88	Detailed Explanation p. 386
41. **A**	Review Question p. 89	Detailed Explanation p. 386
42. **B**	Review Question p. 89	Detailed Explanation p. 387
43. **C**	Review Question p. 89	Detailed Explanation p. 387
44. **D**	Review Question p. 90	Detailed Explanation p. 387
45. **A**	Review Question p. 90	Detailed Explanation p. 388
46. **B**	Review Question p. 90	Detailed Explanation p. 388
47. **C**	Review Question p. 91	Detailed Explanation p. 388
48. **D**	Review Question p. 91	Detailed Explanation p. 389

49. **A**	Review Question p. 91	Detailed Explanation p. 389
50. **B**	Review Question p. 92	Detailed Explanation p. 390
51. **C**	Review Question p. 92	Detailed Explanation p. 390
52. **D**	Review Question p. 92	Detailed Explanation p. 390
53. **A**	Review Question p. 93	Detailed Explanation p. 391
54. **A**	Review Question p. 93	Detailed Explanation p. 391
55. **B**	Review Question p. 93	Detailed Explanation p. 391
56. **C**	Review Question p. 94	Detailed Explanation p. 392
57. **D**	Review Question p. 94	Detailed Explanation p. 392
58. **A**	Review Question p. 94	Detailed Explanation p. 392
59. **B**	Review Question p. 95	Detailed Explanation p. 393
60. **C**	Review Question p. 95	Detailed Explanation p. 393
61. **D**	Review Question p. 95	Detailed Explanation p. 393
62. **A**	Review Question p. 96	Detailed Explanation p. 394
63. **B**	Review Question p. 96	Detailed Explanation p. 394
64. **C**	Review Question p. 96	Detailed Explanation p. 394
65. **D**	Review Question p. 97	Detailed Explanation p. 395
66. **C**	Review Question p. 97	Detailed Explanation p. 395
67. **D**	Review Question p. 97	Detailed Explanation p. 396
68. **A**	Review Question p. 98	Detailed Explanation p. 396
69. **B**	Review Question p. 98	Detailed Explanation p. 396
70. **D**	Review Question p. 98	Detailed Explanation p. 397

Answers: Chapter 5

1. **C**	Review Question p. 99	Detailed Explanation p. 398
2. **B**	Review Question p. 99	Detailed Explanation p. 398
3. **B**	Review Question p. 99	Detailed Explanation p. 398
4. **A**	Review Question p. 100	Detailed Explanation p. 399
5. **C**	Review Question p. 100	Detailed Explanation p. 399
6. **A**	Review Question p. 100	Detailed Explanation p. 399
7. **B**	Review Question p. 101	Detailed Explanation p. 400
8. **D**	Review Question p. 101	Detailed Explanation p. 400
9. **B**	Review Question p. 101	Detailed Explanation p. 401
10. **C**	Review Question p. 102	Detailed Explanation p. 401
11. **D**	Review Question p. 102	Detailed Explanation p. 401
12. **A**	Review Question p. 102	Detailed Explanation p. 402
13. **A**	Review Question p. 103	Detailed Explanation p. 402
14. **B**	Review Question p. 103	Detailed Explanation p. 402
15. **C**	Review Question p. 103	Detailed Explanation p. 403
16. **D**	Review Question p. 104	Detailed Explanation p. 403
17. **D**	Review Question p. 104	Detailed Explanation p. 404
18. **B**	Review Question p. 104	Detailed Explanation p. 404
19. **D**	Review Question p. 104	Detailed Explanation p. 404
20. **A**	Review Question p. 105	Detailed Explanation p. 405
21. **C**	Review Question p. 105	Detailed Explanation p. 405
22. **A**	Review Question p. 105	Detailed Explanation p. 405
23. **B**	Review Question p. 105	Detailed Explanation p. 406

24. **C**	Review Question p. 106	Detailed Explanation p. 406
25. **C**	Review Question p. 106	Detailed Explanation p. 407
26. **D**	Review Question p. 106	Detailed Explanation p. 407
27. **D**	Review Question p. 106	Detailed Explanation p. 408
28. **B**	Review Question p. 107	Detailed Explanation p. 408
29. **B**	Review Question p. 107	Detailed Explanation p. 408
30. **C**	Review Question p. 107	Detailed Explanation p. 409
31. **C**	Review Question p. 107	Detailed Explanation p. 409
32. **D**	Review Question p. 108	Detailed Explanation p. 409
33. **A**	Review Question p. 108	Detailed Explanation p. 410
34. **A**	Review Question p. 108	Detailed Explanation p. 410
35. **B**	Review Question p. 109	Detailed Explanation p. 410
36. **C**	Review Question p. 109	Detailed Explanation p. 411
37. **D**	Review Question p. 109	Detailed Explanation p. 411
38. **A**	Review Question p. 110	Detailed Explanation p. 411
39. **B**	Review Question p. 110	Detailed Explanation p. 412
40. **D**	Review Question p. 110	Detailed Explanation p. 412
41. **C**	Review Question p. 111	Detailed Explanation p. 412
42. **B**	Review Question p. 111	Detailed Explanation p. 413
43. **C**	Review Question p. 111	Detailed Explanation p. 413
44. **A**	Review Question p. 112	Detailed Explanation p. 414
45. **C**	Review Question p. 112	Detailed Explanation p. 414
46. **D**	Review Question p. 112	Detailed Explanation p. 414
47. **A**	Review Question p. 112	Detailed Explanation p. 415
48. **C**	Review Question p. 113	Detailed Explanation p. 415

49. **A**	Review Question p. 113	Detailed Explanation p. 415
50. **B**	Review Question p. 113	Detailed Explanation p. 416
51. **A**	Review Question p. 114	Detailed Explanation p. 416
52. **C**	Review Question p. 114	Detailed Explanation p. 417
53. **D**	Review Question p. 114	Detailed Explanation p. 417
54. **A**	Review Question p. 115	Detailed Explanation p. 418
55. **C**	Review Question p. 115	Detailed Explanation p. 418
56. **D**	Review Question p. 115	Detailed Explanation p. 418
57. **A**	Review Question p. 116	Detailed Explanation p. 419
58. **B**	Review Question p. 116	Detailed Explanation p. 419
59. **C**	Review Question p. 116	Detailed Explanation p. 419
60. **D**	Review Question p. 117	Detailed Explanation p. 420
61. **A**	Review Question p. 117	Detailed Explanation p. 420
62. **D**	Review Question p. 117	Detailed Explanation p. 420
63. **A**	Review Question p. 118	Detailed Explanation p. 421
64. **B**	Review Question p. 118	Detailed Explanation p. 421
65. **C**	Review Question p. 118	Detailed Explanation p. 422
66. **D**	Review Question p. 119	Detailed Explanation p. 422
67. **A**	Review Question p. 119	Detailed Explanation p. 423
68. **B**	Review Question p. 119	Detailed Explanation p. 423
69. **C**	Review Question p. 120	Detailed Explanation p. 423
70. **D**	Review Question p. 120	Detailed Explanation p. 424
71. **A**	Review Question p. 120	Detailed Explanation p. 424
72. **B**	Review Question p. 120	Detailed Explanation p. 424
73. **A**	Review Question p. 121	Detailed Explanation p. 425

74. **B**	Review Question p. 121	Detailed Explanation p. 425
75. **C**	Review Question p. 121	Detailed Explanation p. 425
76. **D**	Review Question p. 122	Detailed Explanation p. 426
77. **A**	Review Question p. 122	Detailed Explanation p. 426
78. **B**	Review Question p. 122	Detailed Explanation p. 426
79. **C**	Review Question p. 123	Detailed Explanation p. 427
80. **D**	Review Question p. 123	Detailed Explanation p. 427
81. **B**	Review Question p. 123	Detailed Explanation p. 428
82. **D**	Review Question p. 124	Detailed Explanation p. 428
83. **B**	Review Question p. 124	Detailed Explanation p. 428
84. **C**	Review Question p. 124	Detailed Explanation p. 429
85. **D**	Review Question p. 125	Detailed Explanation p. 429
86. **A**	Review Question p. 125	Detailed Explanation p. 429
87. **B**	Review Question p. 125	Detailed Explanation p. 430
88. **D**	Review Question p. 125	Detailed Explanation p. 430
89. **A**	Review Question p. 126	Detailed Explanation p. 430
90. **C**	Review Question p. 126	Detailed Explanation p. 431
91. **D**	Review Question p. 126	Detailed Explanation p. 431
92. **A**	Review Question p. 127	Detailed Explanation p. 432
93. **D**	Review Question p. 127	Detailed Explanation p. 432
94. **A**	Review Question p. 127	Detailed Explanation p. 432
95. **B**	Review Question p. 128	Detailed Explanation p. 433
96. **C**	Review Question p. 128	Detailed Explanation p. 433

Answers: Chapter 6

1. **C**	Review Question p. 129	Detailed Explanation p. 435
2. **D**	Review Question p. 129	Detailed Explanation p. 435
3. **A**	Review Question p. 129	Detailed Explanation p. 435
4. **C**	Review Question p. 130	Detailed Explanation p. 436
5. **A**	Review Question p. 130	Detailed Explanation p. 436
6. **B**	Review Question p. 130	Detailed Explanation p. 437
7. **D**	Review Question p. 131	Detailed Explanation p. 437
8. **B**	Review Question p. 131	Detailed Explanation p. 438
9. **C**	Review Question p. 131	Detailed Explanation p. 438
10. **D**	Review Question p. 132	Detailed Explanation p. 439
11. **A**	Review Question p. 132	Detailed Explanation p. 439
12. **B**	Review Question p. 132	Detailed Explanation p. 439
13. **C**	Review Question p. 133	Detailed Explanation p. 440
14. **D**	Review Question p. 133	Detailed Explanation p. 440
15. **A**	Review Question p. 133	Detailed Explanation p. 441
16. **B**	Review Question p. 134	Detailed Explanation p. 441
17. **C**	Review Question p. 134	Detailed Explanation p. 441
18. **D**	Review Question p. 134	Detailed Explanation p. 442
19. **B**	Review Question p. 135	Detailed Explanation p. 442
20. **C**	Review Question p. 135	Detailed Explanation p. 443
21. **D**	Review Question p. 135	Detailed Explanation p. 443
22. **A**	Review Question p. 136	Detailed Explanation p. 444
23. **A**	Review Question p. 136	Detailed Explanation p. 444

24. **B**	Review Question p. 136	Detailed Explanation p. 444
25. **D**	Review Question p. 137	Detailed Explanation p. 445
26. **B**	Review Question p. 137	Detailed Explanation p. 445
27. **C**	Review Question p. 137	Detailed Explanation p. 445
28. **D**	Review Question p. 138	Detailed Explanation p. 446
29. **C**	Review Question p. 138	Detailed Explanation p. 446
30. **D**	Review Question p. 138	Detailed Explanation p. 446
31. **A**	Review Question p. 139	Detailed Explanation p. 447
32. **B**	Review Question p. 139	Detailed Explanation p. 447
33. **A**	Review Question p. 139	Detailed Explanation p. 448
34. **B**	Review Question p. 140	Detailed Explanation p. 448
35. **D**	Review Question p. 140	Detailed Explanation p. 449
36. **A**	Review Question p. 140	Detailed Explanation p. 449
37. **B**	Review Question p. 141	Detailed Explanation p. 449
38. **C**	Review Question p. 141	Detailed Explanation p. 450
39. **D**	Review Question p. 141	Detailed Explanation p. 450
40. **B**	Review Question p. 141	Detailed Explanation p. 451
41. **C**	Review Question p. 142	Detailed Explanation p. 451
42. **D**	Review Question p. 142	Detailed Explanation p. 451
43. **A**	Review Question p. 142	Detailed Explanation p. 452
44. **B**	Review Question p. 143	Detailed Explanation p. 452
45. **C**	Review Question p. 143	Detailed Explanation p. 452
46. **D**	Review Question p. 143	Detailed Explanation p. 453
47. **A**	Review Question p. 144	Detailed Explanation p. 453
48. **C**	Review Question p. 144	Detailed Explanation p. 454

49. **D**	Review Question p. 144	Detailed Explanation p. 454
50. **C**	Review Question p. 145	Detailed Explanation p. 455
51. **D**	Review Question p. 145	Detailed Explanation p. 455
52. **D**	Review Question p. 145	Detailed Explanation p. 455
53. **A**	Review Question p. 146	Detailed Explanation p. 456
54. **C**	Review Question p. 146	Detailed Explanation p. 456
55. **D**	Review Question p. 146	Detailed Explanation p. 456
56. **A**	Review Question p. 147	Detailed Explanation p. 457
57. **D**	Review Question p. 147	Detailed Explanation p. 457
58. **B**	Review Question p. 147	Detailed Explanation p. 458
59. **C**	Review Question p. 148	Detailed Explanation p. 458
60. **B**	Review Question p. 148	Detailed Explanation p. 458
61. **C**	Review Question p. 148	Detailed Explanation p. 459
62. **D**	Review Question p. 149	Detailed Explanation p. 459
63. **A**	Review Question p. 149	Detailed Explanation p. 459
64. **A**	Review Question p. 149	Detailed Explanation p. 460
65. **B**	Review Question p. 150	Detailed Explanation p. 460
66. **C**	Review Question p. 150	Detailed Explanation p. 460
67. **B**	Review Question p. 150	Detailed Explanation p. 461
68. **B**	Review Question p. 151	Detailed Explanation p. 461

Answers: Chapter 7

1. **D**	Review Question p. 152	Detailed Explanation p. 462
2. **B**	Review Question p. 152	Detailed Explanation p. 462
3. **C**	Review Question p. 152	Detailed Explanation p. 462
4. **D**	Review Question p. 153	Detailed Explanation p. 463
5. **A**	Review Question p. 153	Detailed Explanation p. 463
6. **B**	Review Question p. 153	Detailed Explanation p. 463
7. **D**	Review Question p. 154	Detailed Explanation p. 464
8. **A**	Review Question p. 154	Detailed Explanation p. 464
9. **C**	Review Question p. 154	Detailed Explanation p. 465
10. **C**	Review Question p. 155	Detailed Explanation p. 465
11. **D**	Review Question p. 155	Detailed Explanation p. 465
12. **A**	Review Question p. 155	Detailed Explanation p. 466
13. **B**	Review Question p. 156	Detailed Explanation p. 466
14. **B**	Review Question p. 156	Detailed Explanation p. 466
15. **C**	Review Question p. 156	Detailed Explanation p. 467
16. **D**	Review Question p. 157	Detailed Explanation p. 467
17. **A**	Review Question p. 157	Detailed Explanation p. 468
18. **B**	Review Question p. 157	Detailed Explanation p. 468
19. **C**	Review Question p. 158	Detailed Explanation p. 468
20. **D**	Review Question p. 158	Detailed Explanation p. 469
21. **B**	Review Question p. 158	Detailed Explanation p. 469
22. **C**	Review Question p. 159	Detailed Explanation p. 470
23. **D**	Review Question p. 159	Detailed Explanation p. 470

24. **A**	Review Question p. 159	Detailed Explanation p. 470
25. **D**	Review Question p. 160	Detailed Explanation p. 471
26. **A**	Review Question p. 160	Detailed Explanation p. 471
27. **C**	Review Question p. 160	Detailed Explanation p. 471
28. **D**	Review Question p. 161	Detailed Explanation p. 472
29. **A**	Review Question p. 161	Detailed Explanation p. 472
30. **B**	Review Question p. 161	Detailed Explanation p. 473
31. **B**	Review Question p. 162	Detailed Explanation p. 473
32. **C**	Review Question p. 162	Detailed Explanation p. 473
33. **C**	Review Question p. 162	Detailed Explanation p. 474
34. **A**	Review Question p. 162	Detailed Explanation p. 474
35. **B**	Review Question p. 163	Detailed Explanation p. 475
36. **C**	Review Question p. 163	Detailed Explanation p. 475
37. **D**	Review Question p. 163	Detailed Explanation p. 475
38. **A**	Review Question p. 164	Detailed Explanation p. 476
39. **B**	Review Question p. 164	Detailed Explanation p. 476
40. **D**	Review Question p. 164	Detailed Explanation p. 477
41. **A**	Review Question p. 165	Detailed Explanation p. 477
42. **B**	Review Question p. 165	Detailed Explanation p. 477
43. **D**	Review Question p. 165	Detailed Explanation p. 478
44. **A**	Review Question p. 166	Detailed Explanation p. 478
45. **B**	Review Question p. 166	Detailed Explanation p. 479
46. **C**	Review Question p. 166	Detailed Explanation p. 479
47. **A**	Review Question p. 167	Detailed Explanation p. 479
48. **B**	Review Question p. 167	Detailed Explanation p. 480

49. **D**	Review Question p. 167	Detailed Explanation p. 480
50. **D**	Review Question p. 168	Detailed Explanation p. 480
51. **A**	Review Question p. 168	Detailed Explanation p. 481
52. **B**	Review Question p. 168	Detailed Explanation p. 481
53. **D**	Review Question p. 169	Detailed Explanation p. 481
54. **A**	Review Question p. 169	Detailed Explanation p. 482
55. **D**	Review Question p. 169	Detailed Explanation p. 482
56. **C**	Review Question p. 170	Detailed Explanation p. 483
57. **D**	Review Question p. 170	Detailed Explanation p. 483
58. **B**	Review Question p. 170	Detailed Explanation p. 483
59. **C**	Review Question p. 171	Detailed Explanation p. 484
60. **D**	Review Question p. 171	Detailed Explanation p. 484
61. **A**	Review Question p. 171	Detailed Explanation p. 485

Answers: Chapter 8

1. **A**	Review Question p. 172	Detailed Explanation p. 486
2. **A**	Review Question p. 172	Detailed Explanation p. 486
3. **A**	Review Question p. 172	Detailed Explanation p. 486
4. **C**	Review Question p. 173	Detailed Explanation p. 487
5. **B**	Review Question p. 173	Detailed Explanation p. 487
6. **C**	Review Question p. 173	Detailed Explanation p. 487
7. **A**	Review Question p. 173	Detailed Explanation p. 488
8. **B**	Review Question p. 174	Detailed Explanation p. 488
9. **C**	Review Question p. 174	Detailed Explanation p. 488
10. **D**	Review Question p. 174	Detailed Explanation p. 489
11. **A**	Review Question p. 175	Detailed Explanation p. 489
12. **B**	Review Question p. 175	Detailed Explanation p. 490
13. **C**	Review Question p. 175	Detailed Explanation p. 490
14. **D**	Review Question p. 175	Detailed Explanation p. 490
15. **A**	Review Question p. 176	Detailed Explanation p. 491
16. **B**	Review Question p. 176	Detailed Explanation p. 491
17. **C**	Review Question p. 176	Detailed Explanation p. 491
18. **D**	Review Question p. 177	Detailed Explanation p. 492
19. **A**	Review Question p. 177	Detailed Explanation p. 492
20. **B**	Review Question p. 177	Detailed Explanation p. 492
21. **C**	Review Question p. 178	Detailed Explanation p. 493
22. **C**	Review Question p. 178	Detailed Explanation p. 493
23. **D**	Review Question p. 178	Detailed Explanation p. 494

24. **A**	Review Question p. 179	Detailed Explanation p. 494
25. **B**	Review Question p. 179	Detailed Explanation p. 495
26. **D**	Review Question p. 179	Detailed Explanation p. 495
27. **A**	Review Question p. 180	Detailed Explanation p. 495
28. **B**	Review Question p. 180	Detailed Explanation p. 496
29. **C**	Review Question p. 180	Detailed Explanation p. 496
30. **C**	Review Question p. 181	Detailed Explanation p. 496
31. **D**	Review Question p. 181	Detailed Explanation p. 497
32. **A**	Review Question p. 181	Detailed Explanation p. 497
33. **A**	Review Question p. 182	Detailed Explanation p. 497
34. **B**	Review Question p. 182	Detailed Explanation p. 498
35. **C**	Review Question p. 182	Detailed Explanation p. 498
36. **D**	Review Question p. 183	Detailed Explanation p. 499
37. **A**	Review Question p. 183	Detailed Explanation p. 499
38. **B**	Review Question p. 183	Detailed Explanation p. 500
39. **C**	Review Question p. 184	Detailed Explanation p. 500
40. **D**	Review Question p. 184	Detailed Explanation p. 500
41. **D**	Review Question p. 184	Detailed Explanation p. 501
42. **B**	Review Question p. 185	Detailed Explanation p. 501
43. **C**	Review Question p. 185	Detailed Explanation p. 501
44. **D**	Review Question p. 185	Detailed Explanation p. 502
45. **A**	Review Question p. 186	Detailed Explanation p. 502
46. **B**	Review Question p. 186	Detailed Explanation p. 503
47. **C**	Review Question p. 186	Detailed Explanation p. 503
48. **A**	Review Question p. 187	Detailed Explanation p. 503

49. **C**	Review Question p. 187	Detailed Explanation p. 504
50. **B**	Review Question p. 187	Detailed Explanation p. 504
51. **A**	Review Question p. 188	Detailed Explanation p. 505
52. **D**	Review Question p. 188	Detailed Explanation p. 505
53. **B**	Review Question p. 188	Detailed Explanation p. 505
54. **C**	Review Question p. 189	Detailed Explanation p. 506
55. **D**	Review Question p. 189	Detailed Explanation p. 506
56. **A**	Review Question p. 189	Detailed Explanation p. 506
57. **B**	Review Question p. 190	Detailed Explanation p. 507
58. **C**	Review Question p. 190	Detailed Explanation p. 508
59. **D**	Review Question p. 190	Detailed Explanation p. 508
60. **A**	Review Question p. 191	Detailed Explanation p. 508
61. **B**	Review Question p. 191	Detailed Explanation p. 509
62. **C**	Review Question p. 191	Detailed Explanation p. 509
63. **D**	Review Question p. 192	Detailed Explanation p. 509
64. **A**	Review Question p. 192	Detailed Explanation p. 510
65. **B**	Review Question p. 192	Detailed Explanation p. 510
66. **C**	Review Question p. 193	Detailed Explanation p. 511
67. **D**	Review Question p. 193	Detailed Explanation p. 511
68. **A**	Review Question p. 193	Detailed Explanation p. 511
69. **B**	Review Question p. 194	Detailed Explanation p. 512
70. **C**	Review Question p. 194	Detailed Explanation p. 512
71. **A**	Review Question p. 194	Detailed Explanation p. 513
72. **D**	Review Question p. 195	Detailed Explanation p. 513
73. **B**	Review Question p. 195	Detailed Explanation p. 514

74. **C** Review Question p. 195 Detailed Explanation p. 514

75. **B** Review Question p. 196 Detailed Explanation p. 514

Answers: Chapter 9

1. **C**	Review Question p. 197	Detailed Explanation p. 516
2. **C**	Review Question p. 197	Detailed Explanation p. 516
3. **A**	Review Question p. 197	Detailed Explanation p. 516
4. **B**	Review Question p. 198	Detailed Explanation p. 517
5. **C**	Review Question p. 198	Detailed Explanation p. 517
6. **D**	Review Question p. 198	Detailed Explanation p. 517
7. **C**	Review Question p. 199	Detailed Explanation p. 518
8. **A**	Review Question p. 199	Detailed Explanation p. 518
9. **B**	Review Question p. 199	Detailed Explanation p. 519
10. **D**	Review Question p. 200	Detailed Explanation p. 519
11. **A**	Review Question p. 200	Detailed Explanation p. 520
12. **B**	Review Question p. 200	Detailed Explanation p. 520
13. **C**	Review Question p. 201	Detailed Explanation p. 520
14. **D**	Review Question p. 201	Detailed Explanation p. 521
15. **A**	Review Question p. 201	Detailed Explanation p. 521
16. **B**	Review Question p. 202	Detailed Explanation p. 521
17. **C**	Review Question p. 202	Detailed Explanation p. 522
18. **D**	Review Question p. 202	Detailed Explanation p. 522
19. **A**	Review Question p. 203	Detailed Explanation p. 522
20. **B**	Review Question p. 203	Detailed Explanation p. 523
21. **C**	Review Question p. 203	Detailed Explanation p. 523
22. **D**	Review Question p. 204	Detailed Explanation p. 524
23. **A**	Review Question p. 204	Detailed Explanation p. 524

24. **B**	Review Question p. 204	Detailed Explanation p. 524
25. **C**	Review Question p. 205	Detailed Explanation p. 525
26. **D**	Review Question p. 205	Detailed Explanation p. 525
27. **A**	Review Question p. 205	Detailed Explanation p. 526
28. **B**	Review Question p. 206	Detailed Explanation p. 526
29. **C**	Review Question p. 206	Detailed Explanation p. 526
30. **D**	Review Question p. 206	Detailed Explanation p. 527
31. **A**	Review Question p. 207	Detailed Explanation p. 527
32. **C**	Review Question p. 207	Detailed Explanation p. 528
33. **D**	Review Question p. 207	Detailed Explanation p. 528
34. **A**	Review Question p. 208	Detailed Explanation p. 528
35. **B**	Review Question p. 208	Detailed Explanation p. 529
36. **C**	Review Question p. 208	Detailed Explanation p. 529
37. **A**	Review Question p. 209	Detailed Explanation p. 530
38. **B**	Review Question p. 209	Detailed Explanation p. 530
39. **C**	Review Question p. 209	Detailed Explanation p. 530
40. **A**	Review Question p. 210	Detailed Explanation p. 531
41. **B**	Review Question p. 210	Detailed Explanation p. 531
42. **D**	Review Question p. 210	Detailed Explanation p. 531
43. **C**	Review Question p. 211	Detailed Explanation p. 532
44. **D**	Review Question p. 211	Detailed Explanation p. 532
45. **A**	Review Question p. 211	Detailed Explanation p. 533
46. **B**	Review Question p. 212	Detailed Explanation p. 533
47. **C**	Review Question p. 212	Detailed Explanation p. 533
48. **D**	Review Question p. 212	Detailed Explanation p. 534

49. **A**	Review Question p. 213	Detailed Explanation p. 534
50. **B**	Review Question p. 213	Detailed Explanation p. 534
51. **C**	Review Question p. 213	Detailed Explanation p. 535
52. **A**	Review Question p. 214	Detailed Explanation p. 535
53. **B**	Review Question p. 214	Detailed Explanation p. 535
54. **C**	Review Question p. 214	Detailed Explanation p. 536
55. **D**	Review Question p. 215	Detailed Explanation p. 536
56. **B**	Review Question p. 215	Detailed Explanation p. 537
57. **C**	Review Question p. 215	Detailed Explanation p. 537
58. **D**	Review Question p. 216	Detailed Explanation p. 538
59. **A**	Review Question p. 216	Detailed Explanation p. 538
60. **B**	Review Question p. 216	Detailed Explanation p. 538
61. **C**	Review Question p. 217	Detailed Explanation p. 539
62. **A**	Review Question p. 217	Detailed Explanation p. 539
63. **B**	Review Question p. 217	Detailed Explanation p. 539
64. **D**	Review Question p. 218	Detailed Explanation p. 540
65. **A**	Review Question p. 218	Detailed Explanation p. 540
66. **C**	Review Question p. 218	Detailed Explanation p. 541
67. **A**	Review Question p. 219	Detailed Explanation p. 541
68. **B**	Review Question p. 219	Detailed Explanation p. 541
69. **D**	Review Question p. 219	Detailed Explanation p. 542
70. **A**	Review Question p. 220	Detailed Explanation p. 542
71. **C**	Review Question p. 220	Detailed Explanation p. 542
72. **D**	Review Question p. 220	Detailed Explanation p. 543
73. **B**	Review Question p. 221	Detailed Explanation p. 543

74. **C**	Review Question p. 221	Detailed Explanation p. 544
75. **D**	Review Question p. 221	Detailed Explanation p. 544
76. **A**	Review Question p. 222	Detailed Explanation p. 544
77. **B**	Review Question p. 222	Detailed Explanation p. 545
78. **D**	Review Question p. 222	Detailed Explanation p. 545
79. **B**	Review Question p. 223	Detailed Explanation p. 546
80. **C**	Review Question p. 223	Detailed Explanation p. 546

Answers: Chapter 10

1. **C**	Review Question p. 224	Detailed Explanation p. 547
2. **A**	Review Question p. 224	Detailed Explanation p. 547
3. **B**	Review Question p. 224	Detailed Explanation p. 547
4. **C**	Review Question p. 225	Detailed Explanation p. 547
5. **D**	Review Question p. 225	Detailed Explanation p. 548
6. **A**	Review Question p. 225	Detailed Explanation p. 548
7. **B**	Review Question p. 226	Detailed Explanation p. 549
8. **A**	Review Question p. 226	Detailed Explanation p. 549
9. **B**	Review Question p. 226	Detailed Explanation p. 549
10. **C**	Review Question p. 227	Detailed Explanation p. 550
11. **D**	Review Question p. 227	Detailed Explanation p. 550
12. **A**	Review Question p. 227	Detailed Explanation p. 550
13. **B**	Review Question p. 228	Detailed Explanation p. 551
14. **C**	Review Question p. 228	Detailed Explanation p. 551
15. **D**	Review Question p. 228	Detailed Explanation p. 552
16. **A**	Review Question p. 229	Detailed Explanation p. 552
17. **B**	Review Question p. 229	Detailed Explanation p. 553
18. **C**	Review Question p. 229	Detailed Explanation p. 553
19. **D**	Review Question p. 230	Detailed Explanation p. 553
20. **A**	Review Question p. 230	Detailed Explanation p. 554
21. **B**	Review Question p. 230	Detailed Explanation p. 554
22. **B**	Review Question p. 231	Detailed Explanation p. 555
23. **C**	Review Question p. 231	Detailed Explanation p. 555

24. **D**	Review Question p. 231	Detailed Explanation p. 555
25. **A**	Review Question p. 232	Detailed Explanation p. 556
26. **B**	Review Question p. 232	Detailed Explanation p. 556
27. **C**	Review Question p. 232	Detailed Explanation p. 556
28. **D**	Review Question p. 233	Detailed Explanation p. 557
29. **A**	Review Question p. 233	Detailed Explanation p. 557
30. **C**	Review Question p. 233	Detailed Explanation p. 557
31. **D**	Review Question p. 234	Detailed Explanation p. 558
32. **A**	Review Question p. 234	Detailed Explanation p. 558
33. **B**	Review Question p. 234	Detailed Explanation p. 558
34. **C**	Review Question p. 235	Detailed Explanation p. 559
35. **D**	Review Question p. 235	Detailed Explanation p. 559
36. **A**	Review Question p. 235	Detailed Explanation p. 560
37. **C**	Review Question p. 236	Detailed Explanation p. 560
38. **D**	Review Question p. 236	Detailed Explanation p. 560
39. **A**	Review Question p. 236	Detailed Explanation p. 561
40. **A**	Review Question p. 236	Detailed Explanation p. 561
41. **B**	Review Question p. 237	Detailed Explanation p. 561
42. **C**	Review Question p. 237	Detailed Explanation p. 562
43. **D**	Review Question p. 237	Detailed Explanation p. 562
44. **A**	Review Question p. 238	Detailed Explanation p. 563
45. **B**	Review Question p. 238	Detailed Explanation p. 563
46. **B**	Review Question p. 238	Detailed Explanation p. 563
47. **C**	Review Question p. 239	Detailed Explanation p. 564
48. **D**	Review Question p. 239	Detailed Explanation p. 564

49. **A**	Review Question p. 239	Detailed Explanation p. 564
50. **C**	Review Question p. 240	Detailed Explanation p. 565
51. **D**	Review Question p. 240	Detailed Explanation p. 565
52. **A**	Review Question p. 240	Detailed Explanation p. 565
53. **B**	Review Question p. 241	Detailed Explanation p. 566
54. **C**	Review Question p. 241	Detailed Explanation p. 566
55. **D**	Review Question p. 241	Detailed Explanation p. 567
56. **B**	Review Question p. 242	Detailed Explanation p. 567
57. **B**	Review Question p. 242	Detailed Explanation p. 568
58. **C**	Review Question p. 242	Detailed Explanation p. 568
59. **D**	Review Question p. 243	Detailed Explanation p. 568
60. **C**	Review Question p. 243	Detailed Explanation p. 569
61. **A**	Review Question p. 243	Detailed Explanation p. 569
62. **A**	Review Question p. 244	Detailed Explanation p. 570
63. **B**	Review Question p. 244	Detailed Explanation p. 570
64. **D**	Review Question p. 244	Detailed Explanation p. 570
65. **B**	Review Question p. 245	Detailed Explanation p. 571
66. **C**	Review Question p. 245	Detailed Explanation p. 571
67. **D**	Review Question p. 245	Detailed Explanation p. 572
68. **A**	Review Question p. 246	Detailed Explanation p. 572
69. **B**	Review Question p. 246	Detailed Explanation p. 572
70. **A**	Review Question p. 246	Detailed Explanation p. 573
71. **B**	Review Question p. 246	Detailed Explanation p. 573
72. **C**	Review Question p. 247	Detailed Explanation p. 573
73. **D**	Review Question p. 247	Detailed Explanation p. 574

74. **A** Review Question p. 247 Detailed Explanation p. 574

75. **B** Review Question p. 248 Detailed Explanation p. 574

76. **C** Review Question p. 248 Detailed Explanation p. 575

77. **D** Review Question p. 248 Detailed Explanation p. 575

Explanations: Chapter 1

1. Review Question p. 2

   Answers: A

   Explanation A. Authorization is what allows you to perform requested actions or denies such actions based on access criteria.

   Explanation B. Identification is the "who" that a subject claims to be.

   Explanation C. Authentication is the verification of the subject's identity with one or more authentication factors, such as a password.

   Explanation D. Auditing enables the activities of subjects to be tracked in order to sustain accountability.

   PrepLogic Question: 4293-100

2. Review Question p. 2

   Answers: B

   Explanation A. Group-based access controls are based on collections of similar users.

   Explanation B. Role-based access controls are based on job descriptions.

   Explanation C. Transaction-based access controls are based on the content of a communication exchange.

   Explanation D. Discretionary access controls are based on arbitrary decisions by the data custodians and data owners.

   PrepLogic Question: 4293-101

3. Review Question p. 2

   Answers: D

   Explanation A. Simplified password management and administration is a security advantage of single sign-on.

   Explanation B. Less time required overall to perform logon and authentication is a security advantage of single sign-on.

   Explanation C. Stronger passwords are often used is a security advantage of single

sign-on.

Explanation D. Being able to roam the network without restrictions is a disadvantage of single sign-on, as this makes securing the sign-ons more difficult.

PrepLogic Question: 4293-102

4. Review Question p. 3

Answers: A

Explanation A. TACACS is an example of a centralized remote access authentication technology similar to RADIUS, not single sign-on.

Explanation B. Kerberos is an example of a single sign-on technology.

Explanation C. SESAME is an example of a single sign-on technology.

Explanation D. KryptoKnight is an example of a single sign-on technology.

PrepLogic Question: 4293-103

5. Review Question p. 3

Answers: C

Explanation A. Discretionary access control is based on data custodian/owner discretion, and thus not a valid label for role based access control.

Explanation B. Mandatory access control is based on data classification, and thus not a valid label for role based access control.

Explanation C. Nondiscretionary access control is a category of access controls based on rules rather than discretion. Role based access control is an example of nondiscretionary access controls as are mandatory and task based access control.

Explanation D. Recursive is not a valid type of access control.

PrepLogic Question: 4293-104

6. Review Question p. 3

Answers: D

Explanation A. Role based or nondiscretionary access controls are based on job descriptions and work tasks. Role based access control uses labels on subjects rather than ACLs on objects.

Explanation B. Mandatory access control is based on data classification. Mandatory access control uses labels on subjects rather than ACLs on objects.

Explanation C. Role-based or nondiscretionary access controls are based on job descriptions and work tasks. Nondiscretionary access control uses labels on subjects rather than ACLs on objects.

Explanation D. ACLs on objects are the most common implementation of discretionary access control.

PrepLogic Question: 4293-105

7. Review Question p. 4

Answers: A

Explanation A. Discretionary access control is not centrally managed. Since object owners can exist anywhere in a DAC environment, there is no central control over the access control of resources.

Explanation B. Mandatory access control is centrally managed through a rule system of classifications (i.e., clearances of subjects and sensitivity labels of objects).

Explanation C. Nondiscretionary access control is centrally managed through a rule system.

Explanation D. Role-based access control is centrally managed through a rule system of job descriptions.

PrepLogic Question: 4293-106

8. Review Question p. 4

Answers: B

Explanation A. Interpretive is not a valid form of access control.

Explanation B. Role based access control is the most efficient form of access control for environments with a high rate of personnel turnover.

Explanation C. Mandatory access control is not best suited for environments with a high rate of personnel turnover.

Explanation D. Discretionary access control is not best suited for environments with a high rate of personnel turnover.

PrepLogic Question: 4293-107

9. Review Question p. 4

Answers: A

Explanation A. Encryption is not typically used as an access control technique, rather it is commonly used to prevent disclosure.

Explanation B. Rule-based access is a technique to control access.

Explanation C. A restricted interface is a technique to control access.

Explanation D. A capability table is a technique to control access.

PrepLogic Question: 4293-108

10. Review Question p. 5

Answers: B

Explanation A. Centralized is a form of access control administration.

Explanation B. Delegation is not a form of access control administration. Delegation is used to place, transfer, or assign responsibility for an activity onto another person.

Explanation C. Decentralized is a form of access control administration.

Explanation D. Hybrid is a form of access control administration. It combines features of both centralized and decentralized access control adminsitration. Hybrid is in fact the most common form of access control administration.

PrepLogic Question: 4293-109

11. Review Question p. 5

Answers: C

Explanation A. RADIUS (Remote Authentication Dial-in User Service) is a centralized access control mechanism that provides a centralized server for a single point of authentication on the network.

Explanation B. Extended TACACS (XTACACS - (Terminal Access Controller Access Control System) is a centralized access control mechanism that provides resynchronization of security tokens, audit trails, session accounting, and two-factor authentication service. It is an improvement over the original TACACS.

Explanation C. Security domains are decentralized access control mechanisms. Security domains are based on a realm of trust rather than a centralized or single trusted system.

Explanation D. 802.1x is a centralized access control mechanism. 802.1x is a network access control technique in which users must authenticate to a port or a service before communication across the socket is permitted.

PrepLogic Question: 4293-110

12. Review Question p. 5

Answers: D

Explanation A. TACACS (Terminal Access Controller Access Control System) employs the user ID and a static password, and it does not support two-factor authentication or dynamic passwords.

Explanation B. Dual-TACACS (Dual Terminal Access Controller Access Control System) is a destractor. There is no such mechanism as Dual-TACACS.

Explanation C. XTACACS (Extended Terminal Access Controller Access Control System) separates authentication, authorization, and accounting into separate processes, but does not support two-factor authentication or dynamic passwords.

Explanation D. TACACS+ (Terminal Access Controller Access Control System Plus) uses tokens for two-factor authentication and supports dynamic password authentication.

PrepLogic Question: 4293-111

13. Review Question p. 6

Answers: A

Explanation A. Work area separation is a physical access control method.

Explanation B. Policies and procedures is an administrative access control method.

Explanation C. Personnel controls is an administrative access control method.

Explanation D. Supervisory structure is an administrative access control method.

PrepLogic Question: 4293-112

14. Review Question p. 6

Answers: B

Explanation A. Data backups is considered a physical access control method on this exam. A data backup usually results in a copy of the data in a different physical locaiton, thus providing some physical security.

Explanation B. Security awareness training is an administrative access control method.

Explanation C. Network architecture is a logical/technical access control method.

Explanation D. Auditing is a logical/technical access control method.

PrepLogic Question: 4293-113

15. Review Question p. 6

Answers: C

Explanation A. Network segregation is a physical access control method.

Explanation B. Perimeter security is a physical access control method.

Explanation C. Testing is an administrative access control method.

Explanation D. Cabling is a physical access control method.

PrepLogic Question: 4293-114

16. Review Question p. 7

Answers: D

Explanation A. Restricting computer system and network access is a logical/technical access control method.

Explanation B. Encryption is a logical/technical access control method.

Explanation C. Security awareness training is an administrative access control method.

Explanation D. Computer media inventory is a physical access control method.

PrepLogic Question: 4293-115

17. Review Question p. 7

Answers: A

Explanation A. Security awareness training is an administrative access control method.

Explanation B. Network architecture is a technical/logical access control method.

Explanation C. Encryption is a technical/logical access control method.

Explanation D. Control zones is a technical/logical access control method.

PrepLogic Question: 4293-116

18. Review Question p. 7

Answers: B

Explanation A. Work area separation is a physical access control method.

Explanation B. Auditing is a technical/logical access control method.

Explanation C. Data backups is a physical access control method.

Explanation D. Policies and procedures is an administrative access control method.

PrepLogic Question: 4293-117

19. Review Question p. 8

Answers: C

Explanation A. Detective security controls serve to identify unwanted events.

Explanation B. Corrective security controls serve to rectify or undo unwanted events.

Explanation C. Preventative security controls reduce the likelihood of security violations.

Explanation D. Recovery security controls serve to restore resources.

PrepLogic Question: 4293-122

20. Review Question p. 8

Answers: C

Explanation A. Need to know is a form of least privilege access. Need to know access requires additional management approval before access is granted. Least privilege access is access based on work tasks.

Explanation B. Access based on work tasks can be a description of the Principle of Least Privilege, Role Based Access Control, or Task Based Access Control.

Explanation C. Data classification is different from the others. Access management under data classification controls is based on defined strata of security for both objects (i.e., assets) and subjects.

Explanation D. Least privilege is access control based on work tasks.

PrepLogic Question: 4293-123

21. Review Question p. 8

Answers: C

Explanation A. Static passwords are the least secure type of password.

Explanation B. Dynamic passwords are not the strongest type of password, but they are stronger than static passwords.

Explanation C. A one time password is the most secure type of password, because it is used only once and then becomes invalid. One-time passwords are a form of dynamic passwords. However, not all types of dynamic passwords are as secure as a one-time password.

Explanation D. Cognitive passwords are not the strongest type of password, but they are stronger than static passwords.

PrepLogic Question: 4293-126

22. Review Question p. 9

Answers: D

Explanation A. The rate at which authorized users are not granted access is known as the False Rejection Rate (Type I) error of a biometric device.

Explanation B. Granting authorized users access is not an error.

Explanation C. Preventing unauthorized users from gaining access is not an error.

Explanation D. The rate at which unauthorized users are granted access is known as the False Acceptance Rate (a Type II) error of a biometric device.

PrepLogic Question: 4293-127

23. Review Question p. 9

Answers: A

Explanation A. A fail-secure access control mechanism will default to no access.

Explanation B. A fail-secure access control mechanism will default to no access. Minimal access is usually read access. Any level of access above no access, if not specifically granted, is a violation of security.

Explanation C. A fail-secure access control mechanism will default to no access. Least privilege is the minimal amount of access needed to complete work tasks. Any level of access above no access, if not specifically granted, is a violation of security.

Explanation D. A fail-secure access control mechanism will default to no access. Need to know access is the granting of access based on approval from the data custodians, indicating your work tasks necessitate access to sensitive data. Any level of access above no access, if not specifically granted, is a violation of security.

PrepLogic Question: 4293-128

24. Review Question p. 9

Answers: B

Explanation A. Password management and account administration of single sign-on is minimized. This is actually an advantage.

Explanation B. The primary disadvantage of single sign-on is that users can roam the network without restrictions, thus increasing the security risk.

Explanation C. Single sign-on is not user work task prohibitive. In fact, it is preferred by users since it requires less interaction with restrictive security mechanisms.

Explanation D. Single sign-on reduces the overall time spent logging on to systems. Thus, it is an advantage.

PrepLogic Question: 4293-129

25. Review Question p. 10

Answers: A

Explanation A. Files are usually labeled only as objects. As the idea of a file acting on another object is usually nonsensical.

Explanation B. Databases can be labeled as either subjects or objects depending on the circumstances.

Explanation C. Programs can be labeled as either subjects or objects depending on the circumstances.

Explanation D. Computers can be labeled as either subjects or objects depending on the circumstances.

PrepLogic Question: 4293-130

26. Review Question p. 10

Answers: B

Explanation A. Authorization is the verification of access of a subject to secured objects. This is usually the second step in establishing accountability.

Explanation B. Identification establishes the "who" of a subject, and is the first step in establishing accountability.

Explanation C. Auditing is the recording of activities for the purposes of upholding accountability.

Explanation D. Non-repudiation is ensuring that the sender or originator of a message or command cannot dispute that they sent a message or were the instigator of an action.

PrepLogic Question: 4293-131

27. Review Question p. 10

Answers: C

Explanation A. Authorization is the control of the type and level of access a subject has over secured objects.

Explanation B. Accountability is the act of holding a subject responsible for their actions.

Explanation C. Authentication represents the activity of verifying the claimed identity of a subject.

Explanation D. Availability is a fundamental security principle concerned with making sure resources are available in a timely manner.

PrepLogic Question: 4293-132

28. Review Question p. 11

Answers: D

Explanation A. Need to know is an example of an authorization method.

Explanation B. An access control matrix is an example of an authorization method.

Explanation C. A security label is an example of an authorization method.

Explanation D. A password is an example of an authentication factor, not an authorization method.

PrepLogic Question: 4293-133

29. Review Question p. 11

Answers: A

Explanation A. Perimeter padlocked gates is an example of physical access control.

Explanation B. Restricted database interfaces is an example of a logical access control.

Explanation C. Required authentication before access is an example of a logical access control.

Explanation D. Centralized remote access authentication services is an example of a logical access control.

PrepLogic Question: 4293-134

30. Review Question p. 11

Answers: B

Explanation A. A smart card can be used as either an identification or an authentication factor.

Explanation B. A password is usually considered an authentication factor.

Explanation C. A biometric feature can be used as either an identification or an authentication factor.

Explanation D. An employee identification is typically used only as an identification factor.

PrepLogic Question: 4293-135

31. Review Question p. 12

Answers: C

Explanation A. A static password is always the same at each logon.

Explanation B. A dynamic password will change over time, but not always between each logon attempt.

Explanation C. A cognitive password is a collection of question and answers that only the subject will know. A random selection from the databank of available queries will be employed at each logon.

Explanation D. A passphrase is usually a form of static password. A static password is always the same at each logon.

PrepLogic Question: 4293-136

32. Review Question p. 12

Answers: D

Explanation A. A passphrase rarely changes, thus it is not a dynamic password.

Explanation B. A PIN rarely changes, thus it is not a dynamic password.

Explanation C. A smart card rarely changes, thus it is not a dynamic password.

Explanation D. A one time password is a form of dynamic password.

PrepLogic Question: 4293-137

33. Review Question p. 12

Answers: A

Explanation A. A password is an example of Type 1: something you know authentication factor.

Explanation B. A smart card is an example of Type 2: something you have authentication factor.

Explanation C. A fingerprint is an example of Type 3: something you are authentication factor.

Explanation D. Typing a passphrase is an example of Type 4: something you do authentication factor. Type 4 is likely not addressed on this exam as it is usually seen as a sub-category of Type 3 factors or biometrics.

PrepLogic Question: 4293-138

34. Review Question p. 12

Answers: B

Explanation A. Something you have is a Type 2 authentication factor. An example of a something you have factor is a smart card.

Explanation B. Something you are is a Type 3 authentication factor. An example of a something you are factor is a fingerprint.

Explanation C. Something you know is a Type 1 authentication factor. An example of a something you know factor is a password.

Explanation D. Something you do is a Type 4 authentication factor. An example of a something you do factor is signing your name on a digital pad.

PrepLogic Question: 4293-139

35. Review Question p. 13

Answers: C

Explanation A. A password is an example of a Type 1 authentication factor: something you know .

Explanation B. Signing your name is an example of a Type 4 authentication factor: something you do.

Explanation C. A fingerprint is an example of a Type 3 authentication factor: something you are.

Explanation D. A smart card is an example of a Type 2 authentication factor: something you have.

PrepLogic Question: 4293-140

36. Review Question p. 13

Answers: D

Explanation A. Biometric authentication (Type 3: something you are) is effective, but not the best method. It can be improved by adding a second authentication factor.

Explanation B. Type 2 authentication (something you have, such as a smart card) is good, but not the best method. It can be improved by adding a second authentication

factor.

Explanation C. Something you do authentication (Type 4, such as typing a passphrase) is good, but not the best method. It can be improved by adding a second authentication factor.

Explanation D. Two-factor authentication provides the greatest level of authentication security.

PrepLogic Question: 4293-141

37. Review Question p. 13

Answers: A

Explanation A. A passphrase is converted to a hash value (a.k.a. a virtual password), possibly then encrypted, before being sent to the authentication server for processing.

Explanation B. A smart card swipe is either sent in its current form or encrypted before being sent to the authentication server for processing. The contents of a smart card are rarely hashed as they are usually digital certificates or keys and thus are used directly.

Explanation C. A fingerprint scan, converted to a digital form and usually encrypted, is sent to the authentication server for processing. All biometrics create a digital representation of the scanned body part, but this is usually not hashed when transmitted to the authentications server.

Explanation D. A MAC filtering check does not use hashing instead it uses the plain text version of the MAC address to check it against an allow/deny access control list.

PrepLogic Question: 4293-142

38. Review Question p. 14

Answers: B

Explanation A. A synchronous dynamic password token generates new passwords in fixed time intervals. These generated passwords must be entered into the system within a valid time window.

Explanation B. A static password token requires the subject to authenticate himself to the token, then the token authenticates to the system. This is a logical concept that might not seem obvious. A static password token often protects credentials that are more complex than the credentials used to acces the token itself. Thus, it is the token that is really authenticating to the system, not the user.

Explanation C. An asynchronous dynamic password token generates new passwords on demand without a valid time window.

Explanation D. A challenge-response token is used to craft a response by entering a system generated challenge message along with a PIN into the token. The token then generates a response, which is used to authenticate to the system.

PrepLogic Question: 4293-143

39. Review Question p. 14

Answers: C

Explanation A. Biometrics can be used directly as a means of identification.

Explanation B. Biometrics can be used directly as a means of physical access control. This is basically a form of identification and authentication associated with granting access to a physical, rather than a logical, environment.

Explanation C. Biometrics cannot be used directly to provide for accountability. Biometrics are used indirectly for accountability if they are employed as a means of identification or authentication.

Explanation D. Biometrics can be used directly as a means of authentication.

PrepLogic Question: 4293-144

40. Review Question p. 14

Answers: D

Explanation A. When used as an identification method, biometrics function as a one to many function. The currenlty provided biometric element is the one item compared to all elements currently stored in the account database. Essentially the biometric element is taking the form of a username or an account number.

Explanation B. Biometrics are not used directly as a means to provide authorization.

Explanation C. The use of biometrics makes impersonation difficult.

Explanation D. When used as an authentication method, biometrics function as a one-to-one function. The currenlty provided biometric element is one item compared to the one stored item in the specific user account selected in the identification process.

PrepLogic Question: 4293-145

41. Review Question p. 15

Answers: B

Explanation A. The crossover error rate is not used to adjust a biometric device's sensitivity, it is simply the point at which the graphed lines of Type I and Type II errors intersect on a scale of sensitivity vs. percentage cross.

Explanation B. The primary use of the crossover error rate is to compare similar biometric devices.

Explanation C. The crossover error rate is not used in configuration control of a biometric device, it is simply the point at which the graphed lines of Type I and Type II errors intersect on a scale of sensitivity vs. percentage cross.

Explanation D. The crossover error rate is not used to reduce enrollment time of a biometric device, it is simply the point at which the graphed lines of Type I and Type II errors intersect on a scale of sensitivity vs. percentage cross.

PrepLogic Question: 4293-146

42. Review Question p. 15

Answers: D

Explanation A. Any less than 10 subjects per minute is generally considered unacceptable as a rate of throughput processing. 50 subjects per minute is highly desired.

Explanation B. Any less than 10 subjects per minute is generally considered unacceptable as a rate of throughput processing. 2 subjects per minute is severely unacceptable.

Explanation C. Any less than 10 subjects per minute is generally considered unacceptable as a rate of throughput processing. 5 subjects per minute is unacceptable.

Explanation D. Any less than 10 subjects per minute is generally considered the threshold rate at which a specific device has an unacceptable rate of throughput processing.

PrepLogic Question: 4293-147

43. Review Question p. 15

Answers: A

Explanation A. A False Rejection Rate (Type I) error of a biometric device indicates

the rate at which authorized users are not granted access.

Explanation B. Granting authorized users access is not an error.

Explanation C. Preventing unauthorized users from gaining access is not an error.

Explanation D. A False Acceptance Rate (a Type II) error of a biometric device indicates the rate at which unauthorized users are granted access.

PrepLogic Question: 4293-148

44. Review Question p. 15

Answers: C

Explanation A. A maximum of 2 minutes for enrollment will ensure that the majority of users will accept the use of biometric devices in a secure environment. An enrollment time of 30 seconds will vastly improve acceptance.

Explanation B. A maximum of 2 minutes for enrollment will ensure that the majority of users will accept the use of biometric devices in a secure environment. An enrollment time of 1 minute will moderately improve acceptance.

Explanation C. A maximum of 2 minutes for enrollment will ensure that the majority of users will accept the use of biometric devices in a secure environment.

Explanation D. A maximum of 2 minutes for enrollment will ensure that the majority of users will accept the use of biometric devices in a secure environment. 10 minutes is nearly universally unacceptable.

PrepLogic Question: 4293-149

45. Review Question p. 16

Answers: D

Explanation A. A biometric scanner for facility access is considered a type of preventative access control.

Explanation B. A biometric scanner for facility access is considered a type of detective access control.

Explanation C. A biometric scanner for facility access is considered a type of corrective access control.

Explanation D. A biometric scanner for facility access is not considered a type of

recovery access control.

PrepLogic Question: 4293-150

46. Review Question p. 16

Answers: B

Explanation A. Monitoring is a detective security control.

Explanation B. Separation of duties is not a detective security control, rather it is a preventative and deterrent security control.

Explanation C. Job rotation is a detective security control. Job rotation's primary purpose is as a preventative control, but a secondary aspect is its detective property. When workers switch jobs every few months, they are able to detect violations performed by the previous worker in that position.

Explanation D. Intrusion detection is a detective security control.

PrepLogic Question: 4293-152

47. Review Question p. 16

Answers: C

Explanation A. Intrusion detection is an example of a detective security control.

Explanation B. Encryption is an example of preventative security control.

Explanation C. Anti-virus software is an example of a recovery security control.

Explanation D. Smart cards are an example of preventative security control.

PrepLogic Question: 4293-153

48. Review Question p. 17

Answers: D

Explanation A. Background checks are an example of a preventative administrative access control.

Explanation B. Controlled termination process is an example of a preventative administrative access control.

Explanation C. Data classification is an example of a preventative administrative

access control.

Explanation D. Alarms are an example of a preventative physical access control.

PrepLogic Question: 4293-154

49. Review Question p. 17

Answers: B

Explanation A. Passwords are an example of a preventative technical/logical access control.

Explanation B. Motion detectors are an example of a detective physical access control.

Explanation C. Constrained user interfaces are an example of a preventative technical/logical access control.

Explanation D. Firewalls are an example of a preventative technical/logical access control.

PrepLogic Question: 4293-156

50. Review Question p. 17

Answers: C

Explanation A. Biometrics are preventative physical access controls.

Explanation B. Fences are preventative physical access controls.

Explanation C. Call back systems are preventive technical access controls.

Explanation D. CCTV is a preventative physical access control.

PrepLogic Question: 4293-157

51. Review Question p. 18

Answers: D

Explanation A. Auditing is a required element to support and provide for accountability.

Explanation B. Authentication is a required element to support and provide for accountability.

Explanation C. Identification is a required element to support and provide for accountability.

Explanation D. Accountability is used to ensure that users are held responsible for their actions.

PrepLogic Question: 4293-158

52. Review Question p. 18

Answers: A

Explanation A. Auditing is not related to controlling data classifications. Data classification is assigned by the data owner.

Explanation B. Auditing allows for reconstruction of events.

Explanation C. Auditing provides evidence for legal action.

Explanation D. Auditing can be used to produce problem reports.

PrepLogic Question: 4293-159

53. Review Question p. 18

Answers: A

Explanation A. A malicious code scanning tool, such as anti-virus or anti-trojan software, is not a type of audit analysis tool.

Explanation B. A data reduction tool is an audit analysis tool.

Explanation C. A variance detection tool is an audit analysis tool.

Explanation D. An attack signature detection tool is an audit analysis tool.

PrepLogic Question: 4293-163

54. Review Question p. 19

Answers: B

Explanation A. Data backups provide an assurance of integrity, but does not address accountability.

Explanation B. Keystroke logging is a method by which accountability can be enforced.

Explanation C. Bandwidth throttling is used to control excessive network usage, not enforce accountability.

Explanation D. Trusted recovery ensures that a system always returns to a secure state even after encountering an error. Trusted recovery has nothing to do with accountability.

PrepLogic Question: 4293-164

55. Review Question p. 19

Answers: C

Explanation A. Spoofing is the act of altering the true source and/or destination addresses in TCP/IP packets.

Explanation B. Masquerading is the act of impersonating someone or something else in order to gain unauthorized access.

Explanation C. Scrubbing is the act of cleaning out all traces of activities from audit logs.

Explanation D. While altering any file is technically data diddling, cleaning out audit logs is specifically known as scrubbing.

PrepLogic Question: 4293-165

56. Review Question p. 19

Answers: B

Explanation A. Audit logs can be used as legal evidence.

Explanation B. Audit logs may provide clues, but they cannot accurately predict the source of the next intrusion attempt.

Explanation C. Audit logs can demonstrate the means by which an attack was waged.

Explanation D. Audit logs can be used to corroborate and verify the story of a suspect.

PrepLogic Question: 4293-169

57. Review Question p. 20

Answers: C

Explanation A. Social engineering is a means by which data may be disclosed

unintentionally.

Explanation B. Malicious code is a means by which data may be disclosed unintentionally.

Explanation C. Espionage is the deliberate and intentional act of gathering and disclosing confidential data.

Explanation D. Object/media reuse is a means by which data may be disclosed unintentionally.

PrepLogic Question: 4293-170

58. Review Question p. 20

Answers: D

Explanation A. TEMPEST is not a centralized remote access authentication service, however RADIUS and TACACS are.

Explanation B. TEMPEST is not a security domain authorization system, but Kerberos and SESAME are.

Explanation C. TEMPEST is not a vulnerability scanner, but Tripwire is.

Explanation D. TEMPEST is the study and control of stray electrical signals.

PrepLogic Question: 4293-174

59. Review Question p. 20

Answers: A

Explanation A. Sound dampening insulation is ineffective as a countermeasure against radio frequency and other electromagnetic radiation signals.

Explanation B. TEMPEST equipment is specifically designed to block and control radio frequency and other electromagnetic radiation signals to prevent interception.

Explanation C. White noise generation is used to mask confidential radio frequency and other electromagnetic radiation signals so interception is more difficult.

Explanation D. Control zones are areas within a building designed to block the emanation of radio frequency and other electromagnetic radiation signals.

PrepLogic Question: 4293-441

60. Review Question p. 21

Answers: B

Explanation A. Security can be maintained without removable media usage controls, such as in an environment without removable media.

Explanation B. Without physical access controls there is no security. Physical controls protect against physical attacks. Logicial controls protect against logical attacks. Without both, a compelte security solution is not possible.

Explanation C. Security can be maintained without ACLs, such as in a MAC or non-DAC environment.

Explanation D. Security can be maintained without firewalls, such as in an environment those without external communication connections.

PrepLogic Question: 4293-485

61. Review Question p. 21

Answers: C

Explanation A. Intrusion detection is a monitoring or reconnaisance technique.

Explanation B. Probing is a monitoring or reconnaisance technique.

Explanation C. Proximity detectors are access controls, not monitoring or reconnaisance techniques.

Explanation D. Dumpster diving is a monitoring or reconnaisance technique.

PrepLogic Question: 4293-486

62. Review Question p. 21

Answers: B

Explanation A. The clipping level is the point at which normal activity is distinguished from abnormal.

Explanation B. The clipping level is the point at which normal activity is distinguished from abnormal.

Explanation C. The clipping level is the point at which normal activity is distinguished from abnormal.

Explanation D. The clipping level is the point at which normal activity is distinguished

from abnormal.

PrepLogic Question: 4293-489

63. Review Question p. 22

Answers: D

Explanation A. The audit log will contain time and date information.

Explanation B. The audit log will contain location information.

Explanation C. The audit log will contain details about the event that caused the violation record to be created.

Explanation D. An audit log will not contain the biometric profiles for individuals: those are stored in the security database. Only the user account name or ID number will appear in the audit log.

PrepLogic Question: 4293-533

64. Review Question p. 22

Answers: C

Explanation A. Scavenging is an attack to discover information about a system in order to attack it. It is not the process used to locate significant information within audit trails.

Explanation B. Data diddling is the alteration of data.

Explanation C. Data mining is used to locate significant information within audit trails.

Explanation D. Random access is not the process used to locate significant information within audit trails.

PrepLogic Question: 4293-535

65. Review Question p. 22

Answers: B

Explanation A. Encryption is a technical or logical security control. There are three types of security controls: administrative, physical, and logical or technical.

Explanation B. Personnel screening is an administrative security control. There are three types of security controls: administrative, physical, and logical or technical.

Explanation C. Identification is a technical or logical security control. There are three types of security controls: administrative, physical, and logical or technical.

Explanation D. Access Control Lists is a technical or logical security control. There are three types of security controls: administrative, physical, and logical or technical.

PrepLogic Question: 4293-725

66. Review Question p. 23

Answers: B

Explanation A. Incorrect. Manual encryption is the process of manually picking individual pieces of data to encrypt based on use requirements.

Explanation B. Correct. Transparent Encryption is the process of making sure that all data upon the volume is encrypted at all levels throughout the system.

Explanation C. Incorrect. Semi-Transparent Encryption occurs on the fly during read and write operations. Sometimes, data is encrypted, and sometimes it is not.

Explanation D. Incorrect. There is no such thing as solid state encryption. Solid State refers to a type of data storage that is non-volatile.

PrepLogic Question: 4293-850

Explanations: Chapter 2

1. Review Question p. 24

Answers: D

Explanation A. The issue of optical versus magnet storage media is not usually a signficant factor in protecting the integrity of stored audit logs.

Explanation B. Periodic manual inspection (as well as ongoing automated inspection) is a good security practice, but it does not maintain the integrity of stored audit logs.

Explanation C. Storing audit logs in binary format does not prevent alteration.

Explanation D. Digital signatures provide a means to maintain the integrity of stored audit logs.

PrepLogic Question: 4293-166

2. Review Question p. 24

Answers: B

Explanation A. Processes are informal in the initiating level of the software capability maturity model.

Explanation B. Security requirements are institutionalized in the repeatable level of the software capability maturity model.

Explanation C. Technical practices are integrated with management practices in the defined level of the software capability maturity model.

Explanation D. Product and processes are quality controlled in the managed level of the software capability maturity model.

PrepLogic Question: 4293-175

3. Review Question p. 24

Answers: D

Explanation A. Assembly language is not as vulnerable to insertion of malicious code as is interpreted code, such as CGI scripts.

Explanation B. Compiled language is not as vulnerable to insertion of malicious code as is interpreted code, such as CGI scripts.

Explanation C. Commercial software is not as vulnerable to insertion of malicious code as is interpreted code, such as CGI scripts.

Explanation D. CGI scripts, being interpreted, are most susceptible to insertion of malicious code.

PrepLogic Question: 4293-176

4. Review Question p. 25

Answers: D

Explanation A. The code that defines the actions that an object performs in response to an instruction is known as a method.

Explanation B. The result exhibited by an object upon receipt of an instruction is known as a behavior.

Explanation C. The forwarding of an instruction from one object to another is known as delegation.

Explanation D. The communications sent to an object in order to instruct it to perform some operation is known as a message.

PrepLogic Question: 4293-177

5. Review Question p. 25

Answers: A

Explanation A. The code that defines the actions that an object performs in response to an instruction is known as a method.

Explanation B. The result exhibited by an object upon receipt of an instruction is known as a behavior.

Explanation C. The forwarding of an instruction from one object to another is known as delegation.

Explanation D. The communications sent to an object in order to instruct it to perform some operation is known as a message.

PrepLogic Question: 4293-178

6. Review Question p. 25

Answers: A

Explanation A. Risk control is not one of the elements of the software maintenance phase and change control process. Risk control is a concept from the software development life cycle's initalization phase.

Explanation B. The elements of the software maintenance phase and change control process are: request control, change control, and release control.

Explanation C. The elements of the software maintenance phase and change control process are: request control, change control, and release control.

Explanation D. The elements of the software maintenance phase and change control process are: request control, change control, and release control.

PrepLogic Question: 4293-179

7. Review Question p. 26

Answers: C

Explanation A. Assembly language must be assembled into machine language before it can be used directly by a computer.

Explanation B. AI language must be compiled into machine language before it can be used directly by a computer.

Explanation C. A computer can only use machine language directly.

Explanation D. Interpreted languages must be compiled (one command at a time) into machine language before it can be used directly by a computer.

PrepLogic Question: 4293-180

8. Review Question p. 26

Answers: A

Explanation A. These are objects created on-the-fly, by software, as it executes.

Explanation B. Transient elements are created by the programmer---not the program---and are used as agents to pass information between persistent objects.

Explanation C. Volatile agents are those that work directly with volatile storage, similar to transient elements. They are, likewise, not created by the program, on-the-fly.

Explanation D. Applications that rely on distributed computing use several autonomous

computational entities, each with their own memory, to perform calculations and communicate with each other via message passing. This term is outside the scope of our question.

PrepLogic Question: 4293-181

9. Review Question p. 26

Answers: B

Explanation A. Objects producing multiple outputs from a single input describes the characteristic of polymorphism.

Explanation B. Encapsulation means that objects are self-contained.

Explanation C. Objects are not necessarily more secure than compiled programs; however, object-oriented programming systems typically have fewer propagated errors than compiled programs.

Explanation D. Objects can be considered transient if they are dynamic lifetime objects, but that is not related to encapsulation.

PrepLogic Question: 4293-182

10. Review Question p. 27

Answers: C

Explanation A. Polymorphism is the ability for a virus to alter itself in order to attempt to avoid detection by an anti-virus scanner.

Explanation B. Data diddling is the alteration of data.

Explanation C. The ability for one object to be removed from a system and be replaced with another object is known as the substitution property.

Explanation D. Normalization is a process used in database management to correct errors in a database.

PrepLogic Question: 4293-183

11. Review Question p. 27

Answers: C

Explanation A. The code that defines the actions that an object performs in response to an instruction is known as a method.

Explanation B. The result exhibited by an object upon receipt of an instruction is known as a behavior.

Explanation C. The forwarding of an instruction from one object to another is known as delegation.

Explanation D. The communications sent to an object in order to instruct it to perform some operation is known as a message.

PrepLogic Question: 4293-184

12. Review Question p. 27

Answers: B

Explanation A. The code that defines the actions that an object performs in response to an instruction is known as a method.

Explanation B. The result exhibited by an object upon receipt of an instruction is known as a behavior.

Explanation C. The forwarding of an instruction from one object to another is known as delegation.

Explanation D. The communications sent to an object in order to instruct it to perform some operation is known as a message.

PrepLogic Question: 4293-185

13. Review Question p. 28

Answers: D

Explanation A. The code that defines the actions that an object performs in response to an instruction is known as a method.

Explanation B. Data diddling is the alteration of data.

Explanation C. Electronic vaulting is a form of batch or bulk processing used to provide redundancy of transactions.

Explanation D. The ability for an object to produce different behaviors from the same message is known as polymorphism.

PrepLogic Question: 4293-186

14. Review Question p. 28

Answers: A

Explanation A. An expert system is a computer system that exhibits the same reasoning capabilities as those of a human.

Explanation B. A neural network is a computer system that mimics the functioning of biological neurons.

Explanation C. Object-oriented systems are not necessarily related to AI systems.

Explanation D. Not all AI systems are expert systems; some are neural networks.

PrepLogic Question: 4293-187

15. Review Question p. 28

Answers: B

Explanation A. An expert system is a computer system that exhibits the same reasoning capabilities as those of a human.

Explanation B. A neural network is a computer system that mimics the functioning of biological neurons.

Explanation C. Object-oriented systems are not necessarily related to AI systems.

Explanation D. Not all AI systems are expert systems; some are neural networks.

PrepLogic Question: 4293-188

16. Review Question p. 29

Answers: C

Explanation A. Expert systems function using an if-then statement rule database, fuzzy logic, and inference engines.

Explanation B. Expert systems function using an if-then statement rule database, fuzzy logic, and inference engines.

Explanation C. Expert systems do not use the delta rule. Neural networks use the delta rule.

Explanation D. Expert systems function using an if-then statement rule database, fuzzy logic, and inference engines.

PrepLogic Question: 4293-189

17. Review Question p. 29

Answers: D

Explanation A. The steps in fuzzy logic operations are: fuzzification, inference, composition, and then defuzzification.

Explanation B. The steps in fuzzy logic operations are: fuzzification, inference, composition, and then defuzzification.

Explanation C. The steps in fuzzy logic operations are: fuzzification, inference, composition, and then defuzzification.

Explanation D. Normalization is not one of the steps used in fuzzy logic operations. Normalization is the removal of errors from a database.

PrepLogic Question: 4293-190

18. Review Question p. 29

Answers: A

Explanation A. A client/server system is the most common example of a DCE.

Explanation B. Terminal/host is not a DCE. It is a centralized computing environment.

Explanation C. A stand alone system is not a DCE. It is a centralized computing environment.

Explanation D. A portable computer, if it is not connected to anything, is not a DCE. It is a centralized computing environment.

PrepLogic Question: 4293-191

19. Review Question p. 30

Answers: B

Explanation A. ActiveX, Java, and Macromedia Flash are all examples of mobile code languages used in DCE.

Explanation B. Fortran is a 3rd generation programming language, but it is not a mobile code language used in DCE.

Explanation C. ActiveX, Java, and Macromedia Flash are all examples of mobile code

languages used in DCE.

Explanation D. ActiveX, Java, and Macromedia Flash are all examples of mobile code languages used in DCE.

PrepLogic Question: 4293-192

20. Review Question p. 30

Answers: C

Explanation A. ActiveX is platform dependent (Windows only) and language independent.

Explanation B. ActiveX is platform dependent (Windows only) and language independent.

Explanation C. ActiveX is platform dependent (Windows only) and language independent.

Explanation D. ActiveX is platform dependent (Windows only) and language independent.

PrepLogic Question: 4293-193

21. Review Question p. 30

Answers: D

Explanation A. Java is platform independent and language dependent.

Explanation B. Java is platform independent and language dependent.

Explanation C. Java is platform independent and language dependent.

Explanation D. Java is platform independent and language dependent.

PrepLogic Question: 4293-194

22. Review Question p. 31

Answers: A

Explanation A. The primary security flaw of ActiveX is that it stores controls to the hard drive.

Explanation B. ActiveX does not use a sandbox, Java does.

Explanation C. Being Windows OS specific is not a security flaw.

Explanation D. Being language independent is not a security flaw.

PrepLogic Question: 4293-195

23. Review Question p. 31

Answers: B

Explanation A. Java is constrained by a sandbox.

Explanation B. Java is not stored to the hard drive. ActiveX is stored to the hard drive.

Explanation C. Java is multithreaded.

Explanation D. Java is temporarily stored in memory.

PrepLogic Question: 4293-196

24. Review Question p. 31

Answers: D

Explanation A. The three primary models of databases are: relational, hierarchical, and distributed.

Explanation B. The three primary models of databases are: relational, hierarchical, and distributed.

Explanation C. The three primary models of databases are: relational, hierarchical, and distributed.

Explanation D. There is no such database model as the dynamic model.

PrepLogic Question: 4293-197

25. Review Question p. 31

Answers: A

Explanation A. A relational database provides for one-to-one relationships.

Explanation B. A hierarchical database provides for one-to-many relationships.

Explanation C. A distributed database provides for many-to-many relationships.

Explanation D. None of the three primary database models provide for many-to-one relationships.

PrepLogic Question: 4293-198

26. Review Question p. 32

Answers: B

Explanation A. Saving a memory dump may be useful, but reverting to a secure state is more important.

Explanation B. After a failure state, the program or system should revert to a secure state.

Explanation C. Restarting into a privilege mode is exactly the opposite of what is needed when a failure state is experienced.

Explanation D. Automatically rebooting may be involved after a failure state, but the key is reverting into a secure state.

PrepLogic Question: 4293-200

27. Review Question p. 32

Answers: C

Explanation A. A relation is a table stored in a database.

Explanation B. A primary key is a column that has a unique value in each row.

Explanation C. An attribute is a column in a database.

Explanation D. A schema is the data that describes the database.

PrepLogic Question: 4293-201

28. Review Question p. 32

Answers: D

Explanation A. A relational data model only offers one-to-one relationships.

Explanation B. A hierarchical data model offers one-to-many relationships.

Explanation C. A networked data model database is the storage of a relational, heirarchical, or distributed database across numerous networked computers.

Explanation D. A distributed data model offers many-to-many relationships.

PrepLogic Question: 4293-202

29. Review Question p. 33

Answers: A

Explanation A. If the primary key contains a null value, then integrity has been violated.

Explanation B. A cell, as long as it is not within the primary key, can have a null value without violating integrity.

Explanation C. A tuple, as long as it is not the primary key, can have a null value without violating integrity.

Explanation D. A relation, as long as it is not within the primary key, can have a null value without violating integrity.

PrepLogic Question: 4293-203

30. Review Question p. 33

Answers: A

Explanation A. Environmental controls and hardware devices cannot prevent problems created by bad program coding.

Explanation B. Hardware devices can be used to prevent problems created by unrestricted physical access via proving boundary protection mechanisms.

Explanation C. Hardware devices can be used to prevent problems created by a lack of boundary controls by implementing a physical security perimeter.

Explanation D. Environmental controls can prevent problems caused by poor air quality by cleaning the air and reducing the levels of smoke, dust, and debris.

PrepLogic Question: 4293-204

31. Review Question p. 33

Answers: B

Explanation A. A reliable and controlled software development, design, and coding process does not ensure marketability.

Explanation B. A reliable and controlled software development, design, and coding process is necessary to ensure security.

Explanation C. A reliable and controlled software development, design, and coding process does not ensure interoperability.

Explanation D. A reliable and controlled software development, design, and coding process does not ensure compatibility.

PrepLogic Question: 4293-205

32. Review Question p. 34

Answers: C

Explanation A. Buffer overflows are caused by programmers failing to compensate for invalid input data, such as block sizes that are too large.

Explanation B. Buffer overflows are caused by programmers failing to compensate for invalid input data, such as ASCII vs. Binary input.

Explanation C. Buffer overflows are usually not caused by differences in languages.

Explanation D. Buffer overflows are caused by programmers failing to compensate for invalid input data, such as alpha vs. numeric input.

PrepLogic Question: 4293-206

33. Review Question p. 34

Answers: D

Explanation A. Failing to compensate for invalid or extensive values of data types, formats, or lengths in input to programs will not cause TOC/TOU attacks. A TOC/TOU attack is an asynchronous attack where an attack is performed between the time of authorization and resource access.

Explanation B. Failing to compensate for invalid or extensive values of data types, formats, or lengths in input to programs will not cause aggregation. Aggregation is the creation of sensitive data by combining information from a lower sensitivity level.

Explanation C. Failing to compensate for invalid or extensive values of data types, formats, or lengths in input to programs will not cause unauthorized alterations of a configuration item. A configuration item is the benchmark element used in software configuration management.

Explanation D. Failing to compensate for invalid or extensive values of data types, formats, or lengths in input to programs can cause a buffer overflow.

PrepLogic Question: 4293-207

34. Review Question p. 34

Answers: A

Explanation A. Security and functionality are usually inversely proportional; the greater the security, the less functionality a system offers.

Explanation B. Security is usually disabled for installation.

Explanation C. Security must be configured for the environment.

Explanation D. Security is often a tradeoff for ease of use. As security increases, the user friendliness of the system decreases.

PrepLogic Question: 4293-208

35. Review Question p. 35

Answers: B

Explanation A. Platform dependence is not generally considered a security failure or downfall.

Explanation B. A wide range of features or functionality is considered a security failure or downfall. The more capabilities a system has, the greater the range of its vulnerabilities and risks.

Explanation C. Whether software uses interpreted or compiled languages is not a definitive designation of whether the software has poor security.

Explanation D. The implementation of software within a DCE is not a definitive designation of whether the software has poor security.

PrepLogic Question: 4293-209

36. Review Question p. 35

Answers: C

Explanation A. The use of an interpreted language does not directly lead to software's inability to securely handle failures.

Explanation B. Whether or not software is designed to be used in a DCE does not directly lead to software's inability to securely handle failures.

Explanation C. The primary reason software is unable to handle failures in a secure fashion is that circumstances of use are difficult to predict and plan for.

Explanation D. The lack of software change management does not directly relate to software's inability to securely handle failures.

PrepLogic Question: 4293-210

37. Review Question p. 35

Answers: D

Explanation A. Avoiding the production of software does not address the issue.

Explanation B. Using fifth generation programming languages will not provide a means by which failures will be securely handled.

Explanation C. Avoiding CGI scripts does not address the issue.

Explanation D. Since all circumstances of use are difficult to predict and plan for, programmers should design into their software a general method for handling unexpected failures.

PrepLogic Question: 4293-211

38. Review Question p. 36

Answers: A

Explanation A. If a system should fail for any reason, it should always perform a fail safe operation.

Explanation B. Performing a self-diagnostic will not address the issue of needing to prevent the system from reverting to an insecure state.

Explanation C. Using a fail over maneuver may enable a secondary or backup solution to take over supporting processing; however, the failed system still needs to have a mechanism in place to prevent it from reverting to an insecure state.

Explanation D. Under no circumstances should a system failure result in a privileged restart function; instead the system should revert to a secure state.

PrepLogic Question: 4293-212

39. Review Question p. 36

Answers: B

Explanation A. Preventing a system from rebooting after a failure does not protect against a DoS, but often causes or prolongs a DoS.

Explanation B. If a system encounters a failure and it is prevented from rebooting, this will help avoid IPL vulnerabilities.

Explanation C. Preventing a system from rebooting after a failure does not protect against or allow a TOC/TOU attacks since they are unrelated and require a functioning system to be perpetrated.

Explanation D. Preventing a system from rebooting after a failure does not relate at all to inference. Inference is the ability to infer or deduce data at a higher sensitivity or clearance level than you have access for.

PrepLogic Question: 4293-213

40. Review Question p. 36

Answers: C

Explanation A. Security is most effective if it is planned and managed throughout the lifecycle of a system or application.

Explanation B. Security is most effective if it is planned and managed throughout the lifecycle of a system or application.

Explanation C. Security is most effective if it is planned and managed throughout the lifecycle of a system or application.

Explanation D. Security is most effective if it is planned and managed throughout the lifecycle of a system or application.

PrepLogic Question: 4293-214

41. Review Question p. 37

Answers: D

Explanation A. Business continuity planning keeps an organization functioning in spite of minor disruptive events. BCP is not related to project development.

Explanation B. Change control management ensures that changes do not negatively affect security.

Explanation C. Facility design and construction ensures the physical location of an organization is secure from a physical perspective.

Explanation D. Project management keeps the development project on target and moving toward the goal of a completed product.

PrepLogic Question: 4293-216

42. Review Question p. 37

Answers: A

Explanation A. Penetration testing is not one of the phases in the system life cycle.

Explanation B. Project initiation is one of the phases in the system life cycle.

Explanation C. System design specifications is one of the phases in the system life cycle.

Explanation D. Maintenance is one of the phases in the system life cycle.

PrepLogic Question: 4293-217

43. Review Question p. 37

Answers: B

Explanation A. Functional design analysis and planning is one of the phases in the system life cycle.

Explanation B. Risk assessment is not one of the phases in the system life cycle.

Explanation C. Software development is one of the phases in the system life cycle.

Explanation D. Installation is one of the phases in the system life cycle.

PrepLogic Question: 4293-218

44. Review Question p. 38

Answers: C

Explanation A. Disaster recovery planning has nothing to do with software/system development, instead it is useful for restoring an organization to a functional state after a significant disruptive event.

Explanation B. The software capability maturity model is not a means by which to

incorporate improvements in the software/system development process, instead it is used to ensure quality in the post-development lifetime of a system or software.

Explanation C. The waterfall model is a means by which to incorporate improvements in the software/system development process.

Explanation D. Change and control management is not a means by which to incorporate improvements in the software/system development process, instead it is used to ensure that changes do not result in a less-secure environment.

PrepLogic Question: 4293-219

45. Review Question p. 38

Answers: D

Explanation A. The waterfall model does not improve management. In fact, even with the waterfall model the life cycle process is still difficult to manage.

Explanation B. The waterfall model does not allow for greater control over project progress toward objective completion. In fact, even with the waterfall model, there is a lack of overall project control.

Explanation C. The waterfall model does not support the creation of multiple prototypes, that is the function of the spiral model.

Explanation D. The waterfall model of the life cycle development process allows for modifications only to the immediately previous stage of the life cycle process.

PrepLogic Question: 4293-220

46. Review Question p. 38

Answers: A

Explanation A. The spiral model allows the initial phases of the life cycle process to be repeated as necessary.

Explanation B. The waterfall model allows for modifications only to the immediately previous stage of the life cycle process; it does not allow for repeating of initial phases of the life cycle model.

Explanation C. The modified waterfall model allows for modifications only to the immediately previous stage of the life cycle process, and thus it does not allow for repeating of initial phases of the life cycle model. The modified waterfall model does include an additional element to provide validation and verification of the completion of

each phase.

Explanation D. The information security and life cycle model simply stresses that security should be introduced early and managed throughout the life cycle process. It has nothing to do with repeating the initial phases of the life cycle process.

PrepLogic Question: 4293-221

47. Review Question p. 39

Answers: B

Explanation A. The spiral model does not include back verification and validation mechanisms. The spiral model allows the phases of the life cycle process to be repeated as necessary.

Explanation B. The modified waterfall model provides mechanisms for back verification and validation against defined baselines.

Explanation C. The Clark Wilson model is a security model that focuses on protecting integrity. It is not related to the life cycle process.

Explanation D. The information security and life cycle model simply stresses that security should be introduced early and managed throughout the life cycle process. It does not include back verification and validation mechanisms.

PrepLogic Question: 4293-222

48. Review Question p. 39

Answers: C

Explanation A. The Information security life cycle model states that introducing security early in the life cycle process results in a greater chance for success, lower costs, and reduced work.

Explanation B. The Information security life cycle model states that introducing security early in the life cycle process results in a greater chance for success, lower costs, and reduced work.

Explanation C. The Information security life cycle model does not indicate whether introducing security early in the life cycle process results in greater granularity.

Explanation D. The Information security life cycle model states that introducing security early in the life cycle process results in a greater chance for success, lower costs, and reduced work.

PrepLogic Question: 4293-223

49. Review Question p. 39

Answers: D

Explanation A. All aspects of the system should be testable.

Explanation B. Testing should examine how incorrect values are handled.

Explanation C. Testing should probe boundary conditions.

Explanation D. Testing should never use real or live data. Testing using real data can result in disclosure or alteration of sensitive information.

PrepLogic Question: 4293-224

50. Review Question p. 40

Answers: C

Explanation A. A file is a collection of records of the same type.

Explanation B. A tuple is a row of a relational database table.

Explanation C. A cell is the intersection of a row and a column.

Explanation D. An attribute is a column in a relational database table.

PrepLogic Question: 4293-225

51. Review Question p. 40

Answers: D

Explanation A. A file is a collection of records of the same type.

Explanation B. A tuple is a row of a relational database table.

Explanation C. A cell is the intersection of a row and a column.

Explanation D. An attribute is a column in a relational database table.

PrepLogic Question: 4293-226

52. Review Question p. 40

Answers: A

Explanation A. A file is a collection of records of the same type.

Explanation B. A tuple is a row of a relational database table.

Explanation C. A cell is the intersection of a row and a column.

Explanation D. An attribute is a column in a relational database table.

PrepLogic Question: 4293-227

53. Review Question p. 40

Answers: B

Explanation A. A file is a collection of records of the same type.

Explanation B. A tuple is a row of a relational database table.

Explanation C. A cell is the intersection of a row and a column.

Explanation D. An attribute is a column in a relational database table.

PrepLogic Question: 4293-228

54. Review Question p. 41

Answers: C

Explanation A. The domain is the range of allowable or valid values for attributes.

Explanation B. A candidate key is any attribute in a relational database that provides a unique identifier for tuples.

Explanation C. The primary key is the attribute that makes each tuple unique in relational database.

Explanation D. A foreign key is a unique attribute from another relational database table.

PrepLogic Question: 4293-229

55. Review Question p. 41

Answers: D

Explanation A. The domain is the range of allowable or valid values for attributes.

Explanation B. A candidate key is any attribute in a relational database that provides a unique identifier for tuples.

Explanation C. The primary key is the attribute that makes each tuple unique in relational database.

Explanation D. A foreign key is a unique attribute from a second relational database table used in a primary table in order to link the contents of the two tables.

PrepLogic Question: 4293-230

56. Review Question p. 41

Answers: B

Explanation A. A relational database provides for one-to-one relationships.

Explanation B. A hierarchical database provides for one-to-many relationships.

Explanation C. A distributed database provides for many-to-may relationships.

Explanation D. None of the three primary database models provides for many-to-one.

PrepLogic Question: 4293-231

57. Review Question p. 42

Answers: A

Explanation A. The domain is the range of allowable or valid values for attributes.

Explanation B. A candidate key is any attribute in a relational database that provides a unique identifier for tuples.

Explanation C. The primary key is the attribute that makes each tuple unique in relational database.

Explanation D. A foreign key is a unique attribute from another relational database table.

PrepLogic Question: 4293-232

58. Review Question p. 42

Answers: B

Explanation A. The domain is the range of allowable or valid values for attributes.

Explanation B. A candidate key is an attribute in a relational database that provides an additional unique identifier for tuples. In other words, a candidate key has the same uniqueness properties of the primary key.

Explanation C. The primary key is the attribute that makes each tuple unique in relational database.

Explanation D. A foreign key is a unique attribute from another relational database table.

PrepLogic Question: 4293-233

59. Review Question p. 42

Answers: C

Explanation A. The schema is the data that defines the structure of the database.

Explanation B. The data dictionary is the central repository for the data elements and their relationships.

Explanation C. The cardinality is the number of rows in a relational database.

Explanation D. The degree is the number of columns in a relational database.

PrepLogic Question: 4293-234

60. Review Question p. 43

Answers: D

Explanation A. The schema is the data that defines the structure of the database.

Explanation B. The data dictionary is the central repository for the data elements and their relationships.

Explanation C. The cardinality is the number of rows in a relational database.

Explanation D. The degree is the number of columns in a relational database.

PrepLogic Question: 4293-235

61. Review Question p. 43

Answers: A

Explanation A. The schema is the data that defines the structure of the database.

Explanation B. The data dictionary is the central repository for the data elements and their relationships.

Explanation C. The cardinality is the number of rows in a relational database.

Explanation D. The degree is the number of columns in a relational database.

PrepLogic Question: 4293-236

62. Review Question p. 43

Answers: B

Explanation A. The schema is the data that defines the structure of the database.

Explanation B. The data dictionary is the central repository for the data elements and their relationships.

Explanation C. The cardinality is the number of rows in a relational database.

Explanation D. The degree is the number of columns in a relational database.

PrepLogic Question: 4293-237

63. Review Question p. 44

Answers: C

Explanation A. Eliminating repeating groups is an element of normalization.

Explanation B. Eliminating redundant data is an element of normalization.

Explanation C. Locking cells is an aspect of concurrency protection, not normalization.

Explanation D. Eliminating attributes that are not dependant on the primary key is an element of normalization.

PrepLogic Question: 4293-238

64. Review Question p. 44

Answers: D

Explanation A. The semantic integrity rules would address or examine data type, logical value, and uniqueness constraints.

Explanation B. The semantic integrity rules would address or examine data type,

logical value, and uniqueness constraints.

Explanation C. The semantic integrity rules would address or examine data type, logical value, and uniqueness constraints.

Explanation D. The semantic integrity rules would not address or examine the relevance of the data.

PrepLogic Question: 4293-239

65. Review Question p. 44

Answers: A

Explanation A. The mechanism that ensures that every tuple has a primary key and that that primary key is related to an existing record is the referential integrity mechanism.

Explanation B. Concurrency ensures that the database information is always correct and it uses a lock feature to protect cells during editing.

Explanation C. Semantic integrity rules ensure that all structural and semantic rules of the database are not violated.

Explanation D. Transaction management ensures that concurrent transactions can be processed without encountering problems.

PrepLogic Question: 4293-240

66. Review Question p. 45

Answers: B

Explanation A. Rollback statements, commit statements, and checkpoints are all elements of database transaction management.

Explanation B. Normalization is a process used on databases to ensure that the attributes of a table depend upon the primary key. However, normalization is not part of transaction management.

Explanation C. Rollback statements, commit statements, and checkpoints are all elements of database transaction management.

Explanation D. Rollback statements, commit statements, and checkpoints are all elements of database transaction management.

PrepLogic Question: 4293-241

67. Review Question p. 45

Answers: D

Explanation A. SQL is vulnerable to aggregation attacks.

Explanation B. SQL is vulnerable to inference attacks.

Explanation C. SQL is vulnerable to salami technique attacks, a form of aggregation attack.

Explanation D. SQL is not vulnerable to dead locks since it supports concurrent transaction through transaction management.

PrepLogic Question: 4293-243

68. Review Question p. 45

Answers: A

Explanation A. Databases may be still vulnerable to inferencing even with transaction management.

Explanation B. Databases with transaction management are invulnerable to deadlocks, denial of service, and data integrity loss to user access to data cells.

Explanation C. Databases with transaction management are invulnerable to deadlocks, denial of service, and data integrity loss to user access to data cells.

Explanation D. Databases with transaction management are invulnerable to deadlocks, denial of service, and data integrity loss to user access to data cells.

PrepLogic Question: 4293-244

69. Review Question p. 46

Answers: B

Explanation A. Database views and client interfaces support confidentiality, protect against disclosure, and maintain integrity.

Explanation B. Database views and client interfaces do not provide availability as they control client access to the database but do not support the uptime or availability of the database itself.

Explanation C. Database views and client interfaces support confidentiality, protect against disclosure, and maintain integrity.

Explanation D. Database views and client interfaces support confidentiality, protect against disclosure, and maintain integrity.

PrepLogic Question: 4293-245

70. Review Question p. 46

Answers: C

Explanation A. Polyinstantiation is the ability for a database to hold duplicate objects at different clearance levels to prevent inferencing.

Explanation B. Database partitioning is the logical separation of a database into multiple parts to prevent inferencing.

Explanation C. Cell suppression is the technique of hiding specific cells in a database to prevent against inference attacks.

Explanation D. Perturbation is the insertion of false or misleading information in a database to prevent inferencing.

PrepLogic Question: 4293-246

71. Review Question p. 46

Answers: D

Explanation A. Data mining is a technique used against a data warehouse to discover or extract information about the data stored there.

Explanation B. Data mart is a highly-secured area where data created through data mining is stored.

Explanation C. A data dictionary is the collection of data elements and relationships for a specific single database.

Explanation D. A data warehouse is a centralized repository of normalized information from various databases that is made available to users to perform queries against.

PrepLogic Question: 4293-247

72. Review Question p. 47

Answers: A

Explanation A. A common virus, also known as a file virus, needs only a host program to replicate and distribute itself.

Explanation B. A boot virus needs the boot partition of a hard drive.

Explanation C. A multi-part virus needs both a host program and a hard drive.

Explanation D. A macro virus needs a specific document type to replicate and function.

PrepLogic Question: 4293-248

73. Review Question p. 47

Answers: B

Explanation A. Hash signature file verification is a valid virus safeguard.

Explanation B. Biometric authentication has no bearing on virus protection.

Explanation C. Strong DAC access controls are a valid virus safeguard.

Explanation D. Scanning for e-mail born viruses on e-mail gateway systems is a valid virus safeguard.

PrepLogic Question: 4293-249

74. Review Question p. 47

Answers: D

Explanation A. The purpose of audit trails is to recreate events. Audit trails will include records focusing on both normal and abnormal activity.

Explanation B. The purpose of audit trails is to recreate events. Penetration testing is used to test system security.

Explanation C. The purpose of audit trails is to recreate events. Validating trust is the process of reviewing trust relationships and determining whether or not violations of that trust have occurred.

Explanation D. The purpose of audit trails is to recreate events and to maintain a record of historical events.

PrepLogic Question: 4293-495

75. Review Question p. 47

Answers: C

Explanation A. Superzap can bypass system security mechanisms.

Explanation B. Superzap is not easily detected.

Explanation C. Superzap is usually not logged by the system because it bypasses the auditing capabilities, as well as the access controls of the system.

Explanation D. Superzap is used to recover from system freezes. However, superzap is limited in that it only operates on mainframe systems.

PrepLogic Question: 4293-531

76. Review Question p. 48

Answers: B

Explanation A. Booting from a CD is an IPL vulnerability.

Explanation B. IPL vulnerabilities do not include removing power from a system.

Explanation C. Using an alternate boot menu is an IPL vulnerability.

Explanation D. Accessing CMOS is an IPL vulnerability.

PrepLogic Question: 4293-548

77. Review Question p. 48

Answers: D

Explanation A. Elevation of privileges can be an end result of a buffer overflow, but this requires that malicious code be executed in privileged mode.

Explanation B. If the system was properly programmed with boundaries for input, the extra data would be dropped. But if a buffer overflow occurs, the extra data is not dropped, instead it is sent to the CPU where it is usually executed in privileged mode.

Explanation C. If the system has been programmed to record an error event log when a buffer overflow is attempted, then it is most likely configured to prevent buffer overflows by validating input. Thus no buffer overflows occur and data is not sent to the CPU and executed in privileged mode.

Explanation D. Buffer overflows often result in the execution of malicious code in privileged mode.

PrepLogic Question: 4293-657

Explanations: Chapter 3

1. Review Question p. 49

Answers: A

Explanation A. Failing to limit or restrict the data input block size can result in buffer overflows.

Explanation B. Failing to address ASCI vs. binary input will not lead directly to buffer overflows. However, failing to address ASCI vs. binary input may lead to invalid operations or failed processing.

Explanation C. Failing to address alpha vs. numeric input will not lead directly to buffer overflows. However, failing to address alpha vs. numeric input may lead to invalid operations or failed processing.

Explanation D. Failing to address data input length of numerals will not lead directly to buffer overflows. However, failing to address data input length of numerals may lead to invalid operations or failed processing.

PrepLogic Question: 4293-215

2. Review Question p. 49

Answers: A

Explanation A. Maintaining critical functions through a minor disruptive event is business continuity planning, not disaster recovery planning.

Explanation B. Protecting an organization from major IT failure is a goal of disaster recovery planning.

Explanation C. Minimizing the risk to an organization from the interruption of mission critical processes is a goal of disaster recovery planning.

Explanation D. Maintaining reliable backup and restoration solutions through testing and simulation is a goal of disaster recovery planning.

PrepLogic Question: 4293-250

3. Review Question p. 49

Answers: B

Explanation A. A committee leadership is a decision making body and thus not suitable

for implementing a disaster recovery plan.

Explanation B. A disaster recovery plan should minimize the need for personnel to make decisions during and after a disaster. Thus a procedural leadership would simply follow the directions as outlined in the disaster recovery plan.

Explanation C. An interactive leadership is a decision making body and thus not suitable for implementing a disaster recovery plan.

Explanation D. A democratic leadership allows for decisions to be made by a majority and thus not suitable for implementing a disaster recovery plan.

PrepLogic Question: 4293-251

4. Review Question p. 50

Answers: C

Explanation A. Maintaining data integrity throughout the disaster is important, but it is not the primary goal of the data processing continuity aspect of disaster recovery planning.

Explanation B. Maintaining functional networking access throughout the disaster is important, and may be required to ensure that workers can complete their work tasks, but it is not the primary goal of the data processing continuity aspect of disaster recovery planning.

Explanation C. The primary goal of the data processing continuity aspect of disaster recovery planning is to ensure workers can complete their work tasks.

Explanation D. Moving the entire IT infrastructure over to a secondary location is not the primary goal of the data processing continuity aspect of disaster recovery planning. In fact, migration to a secondary location does not always occur when the disaster recovery plan is triggered.

PrepLogic Question: 4293-252

5. Review Question p. 50

Answers: D

Explanation A. A mutual aid agreement is an option for alternate site selection within disaster recovery planning.

Explanation B. Subscription services are an option for alternate site selection within disaster recovery planning.

Explanation C. Service bureaus are an option for alternate site selection within disaster recovery planning.

Explanation D. Adjacent building rental is the poorest choice for an alternate site since it is so close to the original site that it is susceptible to the same disasters that could destroy the primary site.

PrepLogic Question: 4293-253

6. Review Question p. 50

Answers: A

Explanation A. A mutual aid agreement is when two parties agree to support each other's critical business functions in the event of a disaster.

Explanation B. A mutual aid agreement is where two parties agree to support each other's critical business functions in the event of a disaster. A mutual aid agreement implies that alternate sites are not in use.

Explanation C. A mutual aid agreement is where two parties agree to support the other's critical business functions in the event of a disaster. A mutual aid agreement implies that secondary locations are not in use.

Explanation D. A mutual aid agreement is where two parties agree to support the other's critical business functions in the event of a disaster. A mutual aid agreement implies that relocation services are not in use.

PrepLogic Question: 4293-254

7. Review Question p. 51

Answers: B

Explanation A. A hot site is the most costly alternate site location, but it is also the most reliable.

Explanation B. A mutual aid agreement is the cheapest form of alternate site location. Unfortunately, since most companies barely have the capacity to practically support their own mission critical processes, when needed in a disaster, these agreements are usually worthless.

Explanation C. A portable warm site is not as costly as a hot site, but it is fairly reliable.

Explanation D. A service bureau contract can be costly, but as long as the service

bureau doesn't oversell its capacity, it can be effective.

PrepLogic Question: 4293-255

8. Review Question p. 51

Answers: C

Explanation A. Having a duplicate copy of sensitive data is a disadvantage since it requires strong security at two locations to protect the same data.

Explanation B. Cost is a disadvantage of a hot site.

Explanation C. The fact that a hot site has fully configured systems with all supporting utilities and infrastructure is an advantage of a hot site.

Explanation D. The level of constant maintenance is a disadvantage of a hot site.

PrepLogic Question: 4293-256

9. Review Question p. 51

Answers: D

Explanation A. The fact that applications are not fully installed at a warm site is a disadvantage.

Explanation B. The fact that systems may not be fully configured at a warm site is a disadvantage.

Explanation C. A warm site usually has hard-to-obtain communication links, while a cold site is without communication links.

Explanation D. A warm site has considerably less administrative and maintenance costs than a hot site, since it is not a duplicate production environment.

PrepLogic Question: 4293-257

10. Review Question p. 52

Answers: A

Explanation A. A cold site can make adequate recovery impossible because installing and configuring the infrastructure can take longer than the maximum time to recovery an organization can withstand.

Explanation B. Service bureaus are usually well suited to supporting adequate

recovery.

Explanation C. Multiple production centers makes disaster recovery less critical since functions can be moved to other existing locations.

Explanation D. A mobile hot backup site often enables adequate recovery.

PrepLogic Question: 4293-258

11. Review Question p. 52

Answers: B

Explanation A. The use of a service bureau as an alternate site is common, but it is a fairly effective solution.

Explanation B. A cold site is the most common form of alternate backup site, but is also the least effective solution since most companies cannot withstand the down time required to bring a cold site up and running.

Explanation C. The use of a mobile backup as an alternate site is not very common, yet it is a fairly effective solution.

Explanation D. The use of multiple processing centers as an alternate site is common and is a fairly effective solution.

PrepLogic Question: 4293-259

12. Review Question p. 52

Answers: C

Explanation A. A cold site will need to have equipment brought it.

Explanation B. A cold site may not have communication lines installed.

Explanation C. A cold site has no means to support a duplicate copy of critical data.

Explanation D. A cold site probably has HVAC installed.

PrepLogic Question: 4293-260

13. Review Question p. 53

Answers: D

Explanation A. Often all of the locations of an organization using multiple processing

centers are owned and managed by that company, not different entities.

Explanation B. A benefit of multiple processing centers exists when the locations are distant enough not to be effected by the same disasters.

Explanation C. A disadvantage of many multiple processing center implementations is the failure to build in sufficient capacity that the compromise of a single location will not cause the entire organization to fail.

Explanation D. The primary benefit of using multiple processing centers is that mission critical applications of an organization are spread among numerous physical locations.

PrepLogic Question: 4293-261

14. Review Question p. 53

Answers: A

Explanation A. Service bureau contracts for alternate processing sites becomes a disadvantage when the resources are over allocated and are insufficient to handle all clients during a large emergency.

Explanation B. Service bureau contracts for alternate processing sites have the benefit of supporting testing.

Explanation C. Service bureau contracts for alternate processing sites have the benefit of being cost effective, especially when compared to a hot site.

Explanation D. Service bureau contracts for alternate processing sites have the benefit of offering quick response and reasonable availability.

PrepLogic Question: 4293-262

15. Review Question p. 53

Answers: B

Explanation A. Vendor re-supply of hardware is an acceptable practice for rolling mobile backup sites.

Explanation B. Vendor re-supply of hardware is an acceptable practice for all forms of alternate site locations except for hot sites. A hot site should have all necessary hardware installed and in active use.

Explanation C. Vendor re-supply of hardware is an acceptable practice for multiple processing centers.

Explanation D. Vendor re-supply of hardware is an acceptable practice for service bureau contracts.

PrepLogic Question: 4293-263

16. Review Question p. 54

Answers: C

Explanation A. While locating the alternate site is should have sufficient capacity to support all critical business functions.

Explanation B. The alternate site should be far enough away from the primary site as not to be affected by the same disaster.

Explanation C. The alternate site should not be very close to the primary site, otherwise it could be susceptible to the same disaster that affects the primary site.

Explanation D. The alternate site should support the mission critical processes of the organization.

PrepLogic Question: 4293-264

17. Review Question p. 54

Answers: D

Explanation A. Remote journaling is the same thing as parallel processing, not batch processing or electronic vaulting.

Explanation B. Parallel processing is the same thing as remote journaling, not batch processing or electronic vaulting.

Explanation C. Database shadowing is the redundant procedure by which modifications to a server, such as a database, are simultaneously duplicated to several other backup servers.

Explanation D. Batch processing is another name for electronic vaulting.

PrepLogic Question: 4293-265

18. Review Question p. 54

Answers: A

Explanation A. Remote journaling is the act of parallel processing of transactions.

Explanation B. Electronic vaulting is a batch dump process, not a parallel processing of transactions.

Explanation C. Batch processing is not a parallel processing of transactions.

Explanation D. Database shadowing is the redundant procedure by which modifications to a server, such as a database, are simultaneously duplicated to several other backup servers.

PrepLogic Question: 4293-266

19. Review Question p. 55

Answers: C

Explanation A. A full interruption test performs all activities of the plan up to point of terminating processing at the primary site.

Explanation B. A structured walk through test is an on-paper only walk through of the plan in a group meeting.

Explanation C. A simulation test performs all activities of the plan up to but not including the point of starting processing at the alternate site.

Explanation D. A parallel test performs all activities of the plan while processing at the primary facility continues.

PrepLogic Question: 4293-267

20. Review Question p. 55

Answers: B

Explanation A. Testing verifies the accuracy of the procedures.

Explanation B. Testing alone does not minimize legal liability, rather the overall act of designing and implementing a plan minimizes legal liability.

Explanation C. Testing trains personnel.

Explanation D. Testing verifies the processing capability of the alternate site.

PrepLogic Question: 4293-268

21. Review Question p. 55

Answers: C

Explanation A. The length of the test should be defined in the test document.

Explanation B. The participants of the test should be defined in the test document.

Explanation C. The productivity loss due to the test is not an element of the test document. Rather it is a side effect of performing a test that must be absorbed by the organization in order to gain a better disaster recovery plan.

Explanation D. The resources and services to be included in the test should be defined in the test document.

PrepLogic Question: 4293-269

22. Review Question p. 56

Answers: D

Explanation A. A structured walk through test is considered a valid test, not just a preliminary step to a real test.

Explanation B. A simulation test is considered a valid test, not just a preliminary step to a real test.

Explanation C. A parallel test is considered a valid test, not just a preliminary step to a real test.

Explanation D. A checklist test allows for department heads or functional managers to review the plan and indicate if anything has been omitted or needs to be modified. The planning team can then implement those changes to the plan.

PrepLogic Question: 4293-270

23. Review Question p. 56

Answers: A

Explanation A. A checklist test is performed by individuals separately rather than by a group of personnel working together as a team.

Explanation B. A simulation test is performed by a group of personnel working together as a team.

Explanation C. A structured walk through test is performed by a group of personnel working together as a team.

Explanation D. A parallel test is performed by a group of personnel working together as a team.

PrepLogic Question: 4293-271

24. Review Question p. 56

Answers: B

Explanation A. A simulation test can only be performed simultaneously with a checklist or a structured walk through test.

Explanation B. A structured walk through test can be performed simultaneously with any of the other tests. A checklist test can also be performed simultaneously with any other test to keep the plan current. The checklist is usually the first test to be performed.

Explanation C. A parallel test can only be performed simultaneously with a checklist or a structured walk through test.

Explanation D. A full interruption test can only be performed simultaneously with a checklist or a structured walk through test.

PrepLogic Question: 4293-272

25. Review Question p. 57

Answers: D

Explanation A. A full interruption test performs all activities of the plan up to point of terminating processing at the primary site.

Explanation B. A structured walk through test is an on-paper only walk through of the plan in a group meeting.

Explanation C. A simulation test performs all activities of the plan up to but not including point of starting processing at the alternate site.

Explanation D. A parallel test performs all activities of the plan while processing at the primary facility continues.

PrepLogic Question: 4293-273

26. Review Question p. 57

Answers: A

Explanation A. A full interruption test performs all activities of the plan, including

terminating processing at the primary site.

Explanation B. A structured walk through test is an on-paper only walk through of the plan in a group meeting.

Explanation C. A simulation test performs all activities of the plan up to, but not including, the point where processing begins at the alternate site.

Explanation D. A parallel test performs all activities of the plan while processing at the primary facility continues.

PrepLogic Question: 4293-274

27. Review Question p. 57

Answers: C

Explanation A. Criticality Prioritization is one of the three primary goals of BIA.

Explanation B. Downtime Estimation is one of the three primary goals of BIA.

Explanation C. Risk Mitigation is not one of the three primary goals of BIA. It is, however, a factor in Risk Analysis.

Explanation D. Resource Requirements is one of the three primary goals of BIA.

PrepLogic Question: 4293-275

28. Review Question p. 58

Answers: D

Explanation A. Prefabricated buildings are more expensive that mutual aid agreements.

Explanation B. Warm sites are more expensive that mutual aid agreements.

Explanation C. Rolling backup sites are more expensive that mutual aid agreements.

Explanation D. A mutual aid agreement is the least expensive facility continuation plan, however it is also the least likely to succeed.

PrepLogic Question: 4293-276

29. Review Question p. 58

Answers: A

Explanation A. Database shadowing is a transaction redundancy implementation that duplicates data on multiple servers.

Explanation B. Remote journaling performs parallel processing at an alternate site.

Explanation C. Electronic vaulting performs batched transfer of data to an off-site storage facility.

Explanation D. Backups simply create backup copies of the data, they do not provide for processing redundancy.

PrepLogic Question: 4293-277

30. Review Question p. 58

Answers: B

Explanation A. A checklist test is a paper-only test. Also, no walk through occurs.

Explanation B. A simulation test is a disaster recovery plan test that walks through the entire plan but does not implement alternate processing.

Explanation C. A parallel test involves alternate processing.

Explanation D. A full interruption test involves alternate processing and interruption of processing at the primary facility.

PrepLogic Question: 4293-278

31. Review Question p. 59

Answers: C

Explanation A. Just because alternate processing is initiated does not mean the primary site is safe.

Explanation B. A disaster is only over when the entire organization can return to the primary site. This is long after the salvage team would return to the primary site.

Explanation C. The salvage team should only return to the primary site once personnel safety is assured.

Explanation D. All data needed for business continuity should be stored offsite before a disaster occurs. Continued operation is secondary to the safety of personnel, even if a return to the primary site is needed.

PrepLogic Question: 4293-279

32. Review Question p. 59

Answers: A

Explanation A. Business continuity planning is the security issue that addresses ongoing processing activity in the face of minor disruptive events.

Explanation B. Disaster recovery planning is the security issue that addresses ongoing processing activity in the face of major disruptive events.

Explanation C. Mission critical relocation planning is an aspect of disaster recovery planning.

Explanation D. Redundancy development planning is a form of fault tolerant systems design outside of business continuity planning.

PrepLogic Question: 4293-280

33. Review Question p. 59

Answers: B

Explanation A. Business continuity planning has a goal of reducing the risks associated with a disruptive event.

Explanation B. Business continuity planning does not deal with recovering from disruptive events, rather maintaining business activity during a disruptive event. Disaster recovery planning deals with recovery.

Explanation C. Business continuity planning has a goal of maintaining business capability during a disruptive event.

Explanation D. Business continuity planning has a goal of providing a procedural guide so no decisions are necessary during a disruptive event.

PrepLogic Question: 4293-281

34. Review Question p. 60

Answers: C

Explanation A. Restoring critical functions to the alternate site is the second priority in disaster recovery. The priority for both disaster recovery and business continuity is always to maintain personnel safety.

Explanation B. Restoring non-critical functions is lower in priority than ensuring personnel safety.

Explanation C. Maintaining personnel safety is always the first and top priority.

Explanation D. Locating an alternate site is an aspect of disaster recovery planning, not business continuity planning. Also, locating the site should occur before the plan has to be used.

PrepLogic Question: 4293-282

35. Review Question p. 60

Answers: D

Explanation A. The severity of damage to the area is not the key or differential factor between business continuity and disaster recovery.

Explanation B. Both business continuity and disaster recovery can make use of a secondary site.

Explanation C. Both business continuity and disaster recovery plans can be expensive to maintain over time. However, the differences in the costs are not significant enough in all cases to be used as an identification factor.

Explanation D. The primary difference is whether mission critical processes are interrupted. If they are, then disaster recovery is used, if not, then business continuity is used.

PrepLogic Question: 4293-283

36. Review Question p. 60

Answers: A

Explanation A. Senior management is always ultimately responsible for all aspects of security and maintaining productivity in their organization, even though the actual tasks to accomplish this may be delegated.

Explanation B. InfoSec teams are often the people to whom the activities are delegated, but ultimate responsibility lies with senior management.

Explanation C. System auditors may inspect and verify that the business continuity plan is sufficient, but ultimate responsibility lies with senior management.

Explanation D. Department managers may be the people to whom the activities are

delegated, but ultimate responsibility lies with senior management.

PrepLogic Question: 4293-284

37. Review Question p. 61

Answers: C

Explanation A. Local area network components should be addressed in business continuity planning.

Explanation B. Telecommunications should be addressed in business continuity planning.

Explanation C. Employee personal possessions are the responsibility of the employees, not the organization and its business continuity planning.

Explanation D. Applications and software should be addressed in business continuity planning.

PrepLogic Question: 4293-285

38. Review Question p. 61

Answers: D

Explanation A. The four elements of business continuity planning are scope and plan initiation, business impact assessment, business continuity plan development, and plan approval and implementation.

Explanation B. The four elements of business continuity planning are scope and plan initiation, business impact assessment, business continuity plan development, and plan approval and implementation.

Explanation C. The four elements of business continuity planning are scope and plan initiation, business impact assessment, business continuity plan development, and plan approval and implementation.

Explanation D. Alternate site location only applies to disaster recovery planning, not business continuity planing.

PrepLogic Question: 4293-286

39. Review Question p. 61

Answers: C

Explanation A. Criticality prioritization is a goal of business impact assessment.

Explanation B. Establishing resource requirements is a goal of business impact assessment.

Explanation C. OS migration is not a task that should be performed while implementing a business continuity plan or a disaster recovery plan. Thus, it is not a factor or goal of a business impact assessment.

Explanation D. Downtime estimation is a goal of business impact assessment.

PrepLogic Question: 4293-287

40. Review Question p. 62

Answers: A

Explanation A. Criticality prioritization is the business continuity planning task of identifying key (critical) business processes, ordering (prioritizing) those processes, and evaluating event impact.

Explanation B. Business impact assessment is an activity that includes criticality prioritization. So this is not the best answer.

Explanation C. Vulnerability assessment is a form of risk assessment performed within business impact assessment. It does not include prioritizing processes.

Explanation D. Quantitative analysis is a task within vulnerability assessment and thus does not include prioritizing processes.

PrepLogic Question: 4293-288

41. Review Question p. 62

Answers: B

Explanation A. Creation of InfoSec teams may help implement business continuity and disaster recovery plans, but the creation of implementation teams is not an essential aspect of due care and due diligence.

Explanation B. Business continuity and disaster recovery planning are considered essential elements of due care and due diligence.

Explanation C. Delegating implementation tasks to subordinates may facilitate the implementation of business continuity and disaster recovery plans, but the delegation action itself is not an essential aspect of due care and due diligence.

Explanation D. Senior management must sign off on all security planning, but their participation in the planning activities themselves is not an essential aspect of due care and due diligence.

PrepLogic Question: 4293-289

42. Review Question p. 62

Answers: D

Explanation A. A fire can trigger the business continuity plan.

Explanation B. An earthquake can trigger the business continuity plan.

Explanation C. A flood of any significance can trigger the business continuity plan.

Explanation D. Intrusion attacks are not events that trigger the business continuity plan. Instead, intrusion attacks trigger normal InfoSec or CIRT (Computer Incident Response Team) teams.

PrepLogic Question: 4293-290

43. Review Question p. 63

Answers: A

Explanation A. Destruction of a primary site would trigger the disaster recovery plan, not the business continuity plan.

Explanation B. A wind storm can trigger the business continuity plan.

Explanation C. A hurricane can trigger the business continuity plan.

Explanation D. A pipe rupture can trigger the business continuity plan.

PrepLogic Question: 4293-291

44. Review Question p. 63

Answers: B

Explanation A. Destruction of the primary site triggers the disaster recovery plan.

Explanation B. Internet communication interruptions that are not related to your mission critical processes will not trigger the disaster recovery plan.

Explanation C. Any event, such as fire, that interrupts mission critical processes

triggers the disaster recovery plan.

Explanation D. Any event, such as robbery of key IT equipment, that interrupts mission critical processes triggers the disaster recovery plan.

PrepLogic Question: 4293-292

45. Review Question p. 63

Answers: C

Explanation A. This scope is incomplete because it does not include facilities.

Explanation B. This scope is incomplete because it does not include infrastructure. Also, media relations and human resources are usually aspects of disaster recovery planning more than business continuity planning.

Explanation C. The scope of the business continuity plan should include everything necessary to support your mission critical services, such as office supplies, people, infrastructure, and facilities.

Explanation D. This scope is incomplete because it does not include people.

PrepLogic Question: 4293-293

46. Review Question p. 64

Answers: A

Explanation A. To avoid confusion or using an outdated version of the plan, only a single copy of the business continuity plan should exist throughout the organization.

Explanation B. Each department should not maintain independent and separate business continuity plans, a single overarching plan for the entire organization is needed.

Explanation C. It is possible for the process of developing and maintaining a business continuity plan to reveal weaknesses in the overall security policy. It is not uncommon to revise a security policy in light of the findings of a business continuity plan.

Explanation D. The most important part of a business continuity plan is to keep mission critical processes functioning, not how much it costs to do so.

PrepLogic Question: 4293-294

47. Review Question p. 64

Answers: B

Explanation A. The business impact assessment is used to determine threats, risks, and costs upon which to base a business continuity plan.

Explanation B. Staff awareness is an aspect of the plan approval and implementation element of the business continuity plan development process.

Explanation C. The business continuity plan development element is the stage where the plan is actually developed.

Explanation D. The scope and plan initiation element is the stage where the needs of business continuity planning are first outlined.

PrepLogic Question: 4293-295

48. Review Question p. 64

Answers: D

Explanation A. The Maximum Tolerable Downtime estimation is an indication of how long mission critical processes can be down and still allow the organization to recover.

Explanation B. The Maximum Tolerable Downtime estimation is an indication of how long mission critical processes can be down and still allow the organization to recover.

Explanation C. The Maximum Tolerable Downtime estimation is an indication of how long mission critical processes can be down and still allow the organization to recover.

Explanation D. The Maximum Tolerable Downtime estimation is an indication of how long mission critical processes can be down and still allow the organization to recover.

PrepLogic Question: 4293-296

49. Review Question p. 65

Answers: B

Explanation A. An org chart is a common assessment material item to be gathered when performing a business impact analysis.

Explanation B. The mission statement is inconsequential and useless to the act of business impact analysis.

Explanation C. A definition of the business units is a common assessment material item to be gathered when performing a business impact analysis.

Explanation D. An outline of relationships within the organization is a common assessment material item to be gathered when performing a business impact analysis.

PrepLogic Question: 4293-297

50. Review Question p. 65

Answers: C

Explanation A. A risk analysis report is the result of a risk assessment.

Explanation B. An auditor's final report is the result of an audit.

Explanation C. The result of business impact analysis is a business continuity plan.

Explanation D. An organizational security policy is the result of a directed effort by senior management to create such an infrastructure document.

PrepLogic Question: 4293-298

51. Review Question p. 65

Answers: D

Explanation A. Quantitative analysis is an element of the vulnerability assessment process of business impact analysis.

Explanation B. Qualitative analysis is an element of the vulnerability assessment process of business impact analysis.

Explanation C. Defining critical areas and dependencies is an element of the vulnerability assessment process of business impact analysis.

Explanation D. Countermeasure selection is associated with risk analysis, not business impact analysis vulnerability assessment.

PrepLogic Question: 4293-299

52. Review Question p. 66

Answers: B

Explanation A. A full interruption test performs all activities of the plan up to the point of terminating processing at the primary site.

Explanation B. A structured walk through test is an on-paper only walk through of the plan in a group meeting.

Explanation C. A simulation test performs all activities of the plan up to but not including point of starting processing at the alternate site.

Explanation D. A parallel test performs all activities of the plan but processing at the primary facility continues.

PrepLogic Question: 4293-300

53. Review Question p. 66

Answers: C

Explanation A. A simulation test is not the best method to test a disaster recovery plan.

Explanation B. A structured walk through test is not the best method to test a disaster recovery plan.

Explanation C. A full interruption test is the best method to test that a disaster recovery plan is fully capable of handling a serious disaster. However, doing so can cause a disaster of its own.

Explanation D. A parallel test is not the best method to test a disaster recovery plan.

PrepLogic Question: 4293-301

54. Review Question p. 66

Answers: D

Explanation A. Returning to the primary site is the responsibility of the salvage team.

Explanation B. Getting non-critical processing operations up at the primary site is the responsibility of the salvage team.

Explanation C. Ensuring that threat to personnel at the primary site has been eliminated is the responsibility of the recovery team.

Explanation D. Implementing the disaster recovery plan is the responsibility of the recovery team.

PrepLogic Question: 4293-302

55. Review Question p. 67

Answers: A

Explanation A. The primary responsibility of the salvage team is to return the primary

site back to normal operating conditions.

Explanation B. Implementing the disaster recovery plan to get business functions operational at the alternate site is the responsibility of the recovery team.

Explanation C. Ensuring personnel safety at the alternate site is the responsibility of the recovery team.

Explanation D. Minimizing the risk of disaster effect at the primary site is the responsibility of the recovery team.

PrepLogic Question: 4293-303

56. Review Question p. 67

Answers: C

Explanation A. The scope of threats are man-made, natural, and technical.

Explanation B. The scope of threats are man-made, natural, and technical.

Explanation C. The scope of threats are man-made, natural, and technical.

Explanation D. The scope of threats are man-made, natural, and technical.

PrepLogic Question: 4293-304

57. Review Question p. 67

Answers: D

Explanation A. A vulnerability assessment is often used during the initial creation process of a disaster recovery plan, but it is not essential to maintaining the viability of the plan.

Explanation B. Project initiation is important, but the maintenance portion of plan's development process is key to sustaining its viability.

Explanation C. Senior management signoff is required throughout the life of a disaster recovery plan, but it is the ongoing maintenance that ensures that the plan remains viable.

Explanation D. Ongoing maintenance ensures that a disaster recovery plan remains viable.

PrepLogic Question: 4293-305

58. Review Question p. 68

Answers: C

Explanation A. Testing will effectively train personnel in the use of the plan.

Explanation B. Testing will effectively make personnel aware of the plan.

Explanation C. The results of a test may indicate that the plan needs to be improved, but actual design improvements are not the result of the testing process itself.

Explanation D. Testing will effectively validate the viability of the plan.

PrepLogic Question: 4293-306

59. Review Question p. 68

Answers: B

Explanation A. Returning to the primary site is not determined by what occurs at the alternate site.

Explanation B. The salvage team should return to the primary site only after threat to personal safety is eliminated.

Explanation C. The backup media should not be stored at the primary site, but should be stored off-site in a secure facility. This should thus not be a reason to return to the primary site.

Explanation D. The time since a disaster is not the determining factor for when the salvage team can return to the primary site.

PrepLogic Question: 4293-307

60. Review Question p. 68

Answers: C

Explanation A. The emergency still exists as long as the organization is not fully back at its primary site.

Explanation B. The threat of human safety is not the determining factor when a disaster emergency is over.

Explanation C. The emergency is over when all operations are back at the primary site.

Explanation D. The length of time the organization remains at the alternate site does not determine when the emergency is over.

PrepLogic Question: 4293-308

61. Review Question p. 69

Answers: D

Explanation A. Human safety must be protected at all points of a disaster recovery plan. The presence of a safety threat does not affect when an emergency is declared over.

Explanation B. There are no legal, insurance-related requirements that define when an emergency is over.

Explanation C. The alternate site should be able to support all of the operations of the organization.

Explanation D. An emergency is not over until the organization fully returns to the primary site, because a vulnerability exists when shifting mission critical applications from the alternate back to the primary site.

PrepLogic Question: 4293-309

62. Review Question p. 69

Answers: A

Explanation A. The first step in returning to the primary site is to get non-mission critical functions operating. This will ensure that the restored IT infrastructure will be able to support the full load of the mission critical operations.

Explanation B. The operations at the alternate site should not be terminated until the primary site is running all operations.

Explanation C. Mission critical functions should only be returned to the primary site after non-mission critical functions are used to test the restored IT infrastructure.

Explanation D. The safety of the alternate site should be maintained at all times. It is not a determining factor or a step in returning to the primary site.

PrepLogic Question: 4293-310

63. Review Question p. 69

Answers: B

Explanation A. Establishing an alternate or backup site is essential to complete before a disaster to ensure that the company can recover.

Explanation B. There is no need to establish media contacts before a disaster.

Explanation C. Employees need to be paid even if the company is unable to fully return to normal operations. Without paid employees, an organization will not recover.

Explanation D. Watching out for human safety is always a priority. Establishing a rendezvous point to verify the safety of employees after a disaster is one way to help accomplish this.

PrepLogic Question: 4293-311

64. Review Question p. 70

Answers: A

Explanation A. The disaster recovery plan is not information that should be shared with the general public.

Explanation B. The plan should be tested for viability.

Explanation C. Staff should be trained in using the plan.

Explanation D. There should be only one version of the plan in existence.

PrepLogic Question: 4293-312

65. Review Question p. 70

Answers: B

Explanation A. If the plan is not sufficient for the organization, senior management should not give its final approval of it.

Explanation B. The details of plans from other organizations is the least important factor when obtaining final senior management signoff of a disaster recovery plan.

Explanation C. If the plan has not been tested for viability, senior management should not give its final approval of it.

Explanation D. If the plan does not have sufficient procedural details, senior management should not give its final approval of it.

PrepLogic Question: 4293-313

66. Review Question p. 70

Answers: D

Explanation A. Vulnerability assessment is a key element in developing these plans, but management support is crucial.

Explanation B. Criticality prioritization is a key element in developing these plans, but management support is crucial.

Explanation C. Maintaining critical processes across any disruptive event are the goals of business continuity planning or disaster recovery planning, but the most important aspect is management support.

Explanation D. The most important element is management support. Without management support, the chances of coming up with a business continuity plan or a disaster recover plan that will maintain critical processes across any disruptive event is greatly diminished.

PrepLogic Question: 4293-314

67. Review Question p. 71

Answers: A

Explanation A. Initiating the business continuity plan is the activity that should take place after a minor disaster to restore systems and recover data files.

Explanation B. Restoring files from backup may be an element in the recovery process, but it should be guided by the business continuity plan.

Explanation C. A full interruption test is a test for disaster recovery plans, not business continuity plans. Plus, once a disaster of any type occurs, the plan it activated, not tested.

Explanation D. Performing a vulnerability analysis is an element of developing a business continuity plan, not activating it in the event of a minor disaster.

PrepLogic Question: 4293-315

68. Review Question p. 71

Answers: B

Explanation A. Senior management approval does not include qualitative and quantitative elements.

Explanation B. Business impact analysis includes qualitative and quantitative elements.

Explanation C. Simulation testing does not include qualitative and quantitative elements.

Explanation D. Criticality prioritization does not include qualitative and quantitative elements.

PrepLogic Question: 4293-316

69. Review Question p. 71

Answers: C

Explanation A. RAID alone is not sufficient to eliminate single points of failure throughout an organization, but it can be one of the many implementation points used to accomplish this goal.

Explanation B. Testing backups is important to ensure that backups are reliable, but prevention of single points of failure requires redundant systems.

Explanation C. Prevention of single points of failure involves implementation of redundancy throughout the IT infrastructure.

Explanation D. Installing surge protectors is a good idea, but prevention of single points of failure requires redundant systems.

PrepLogic Question: 4293-317

70. Review Question p. 72

Answers: D

Explanation A. The CIRT is usually labeled as the recovery team for implementing these plans in the event of a disaster, however they do not own them for the organization.

Explanation B. An internal auditor may review these plans and even been a key element in the testing and evaluation of the plans, but they do not own them for the organization.

Explanation C. Departmental network administrators may be involved in developing and testing these plans, but they do not own them for the organization.

Explanation D. The senior manager is the owner of the business continuity and disaster recovery plans for an organization.

PrepLogic Question: 4293-318

71. Review Question p. 72

Answers: A

Explanation A. Business impact analysis includes defining or outlining the dependencies of critical business operations.

Explanation B. Business impact analysis does not include contracting with service bureaus. This activity takes place at a later stage in plan development.

Explanation C. Business impact analysis does not include countermeasure selection. Countermeasure selection is an aspect of risk analysis, not disaster or continuity planning.

Explanation D. Business impact analysis does not include defining staff responsibilities. This activity takes place at a later stage in plan development.

PrepLogic Question: 4293-319

72. Review Question p. 72

Answers: B

Explanation A. Testing a disaster recovery plan and learning whether it passed or failed overall, does not offer detailed or useful data on why the plan failed or succeeded in each area.

Explanation B. Testing a disaster recovery plan and learning what aspects failed offers the most useful and meaningful information from this list of selections.

Explanation C. Testing a business continuity plan and learning which staff members failed to follow procedure, does not offer broad enough information about the plan itself.

Explanation D. Testing a business continuity plan and restoring files from the most recent full backup, doesn't indicate whether the plan worked or not and it limits the test to a full backup. The most recent full backup may not be the most recent backup available (such as an incremental backup).

PrepLogic Question: 4293-320

73. Review Question p. 73

Answers: C

Explanation A. Intrusion attacks should be addressed by the overall security policy, not the business continuity plan.

Explanation B. Hardware failures should be addressed by the overall security policy, not the business continuity plan.

Explanation C. A business continuity plan should address the threats of natural and man-made disasters.

Explanation D. Technical failures and human error should be addressed by the overall security policy, not the business continuity plan.

PrepLogic Question: 4293-321

74. Review Question p. 73

Answers: D

Explanation A. Location is not the most important aspect of alternate site selection. As long as the site is far enough away from the primary site to not be affected by the same disaster, and the site is not too far away, location is not important.

Explanation B. Size is not the most important aspect of alternate site selection. The physical size of the site is irrelevant as long as it is large enough to support business processing.

Explanation C. Cost, while important, is not the most important aspect of alternate site selection. Cost is often an important factor to budgets, but in actual site selection, it is a secondary concern.

Explanation D. The ability for an alternate site to support business processing is the most important aspect when selecting an alternate site.

PrepLogic Question: 4293-322

75. Review Question p. 73

Answers: B

Explanation A. The ground floor is not the best choice for a data center for any type of site since it makes physical intrusion easiest.

Explanation B. The center of the building is always the best choice for a data center in any type of site.

Explanation C. The sub-basement is not the best choice for a data center for any type of site since it is vulnerable to flooding.

Explanation D. The penthouse is not the best choice for a data center for any type of

site since it is vulnerable to numerous severe weather threats.

PrepLogic Question: 4293-323

76. Review Question p. 74

Answers: A

Explanation A. The most often overlooked aspect of disaster recovery is maintaining a mechanism by which to continue issuing employee paychecks.

Explanation B. Human safety is well-known to be the most important factor and is rarely overlooked in disaster recovery planning.

Explanation C. Restoring and maintaining critical business functions is the key purpose of disaster recovery planning and is rarely overlooked.

Explanation D. Selecting an alternate site is a key factor of restoring and maintaining critical business functions, thus it is rarely overlooked.

PrepLogic Question: 4293-324

77. Review Question p. 74

Answers: C

Explanation A. Knowing the locations of hardware vendors is a poor substitute for a service level agreement. Such a situation does not provide a reasonable level of protection against the failure of hardware.

Explanation B. Maintaining a hot site duplicate facility is cost prohibitive, but it does offer solution protection against hardware failure.

Explanation C. Obtaining a service level agreement with a hardware vendor provides a reasonable level of protection against the failure of hardware.

Explanation D. Storing replacement parts on site does provide a reasonable level of protection against the failure of hardware, but it can be cost prohibitive.

PrepLogic Question: 4293-549

78. Review Question p. 74

Answers: C

Explanation A. Grandfather, father, son is a commonly used backup tape management scheme.

Explanation B. Six-cartridge weekly backup principle is a commonly used backup tape management scheme.

Explanation C. Pillar of Absolom is not a commonly used backup tape management scheme. It is a fake distracter.

Explanation D. Tower of Hanoi is a commonly used backup tape management scheme.

PrepLogic Question: 4293-825

79. Review Question p. 75

Answers: D

Explanation A. A full backup resets the archive bit.

Explanation B. A daily backup does not reset the archive bit, but it only backs up data that has been modified on the day the daily backup process is performed. It does not backup all data that has changed since the last full or incremental backup.

Explanation C. An incremental backup resets the archive bit. An incremental backup is used to backup all new data since the last full, daily, or incremental backup.

Explanation D. A differential backup does not reset the archive bit. A differential backup is used to backup all new data since the last full, daily, or incremental backup.

PrepLogic Question: 4293-826

80. Review Question p. 75

Answers: A

Explanation A. Some data lost always occurs when the primary source fails because there is always a time lag between the last backup and the failure, especially when a periodic backup rather than a real-time backup method is used. This time lag provides a windows for data changes that are not stored on the backup media.

Explanation B. Transfer rates vary from very slow to very fast; however, in most cases, the transfer rate is less than that of the network's capacity.

Explanation C. The time required to perform backup increases as the amount of data increases.

Explanation D. The number of backup medias needed to perform backup increases as the amount of data increases.

PrepLogic Question: 4293-827

Explanations: Chapter 4

1. Review Question p. 76

Answers: B

Explanation A. Scripting does not employ symmetric key cryptography and DES encryption to provide end-to-end security. Moreover, it stores authentication credentials in the plain text form of the scripting language.

Explanation B. Kerberos employs symmetric key cryptography and DES encryption to provide end-to-end security.

Explanation C. SESAME employs the Needham-Schroeder protocol (which is a trusted authentication server based solution), MD5, and crc32.

Explanation D. KryptoKnight employs a nonce (random one time authenticator) and the user's password for the initial exchange from the party to the Key Distribution Center.

PrepLogic Question: 4293-124

2. Review Question p. 76

Answers: C

Explanation A. The algorithm is the publicly known mathematical transformation that is the core of a cryptographic system.

Explanation B. The key length often determines the strength of a cryptographic system, but it does not address the effort involved in breaking a cryptographic system.

Explanation C. The work function is the time, effort, and/or cost involved in breaking a cryptographic system.

Explanation D. The key space is the range of valid keys for a specific algorithm. It is not a direct determination of the effort involved in breaking a cryptographic system.

PrepLogic Question: 4293-325

3. Review Question p. 76

Answers: D

Explanation A. The strength of a cryptosystem is dependant upon the algorithm, length of the key, secrecy of the key, and the initialization vector.

Explanation B. The strength of a cryptosystem is dependant upon the algorithm, length of the key, secrecy of the key, and the initialization vector.

Explanation C. The strength of a cryptosystem is dependant upon the algorithm, length of the key, secrecy of the key, and the initialization vector.

Explanation D. The strength of a cryptosystem is not usually dependant upon the length of the ciphertext; i.e., the output of the system.

PrepLogic Question: 4293-326

4. Review Question p. 77

Answers: A

Explanation A. Availability is not a benefit of a cryptosystem.

Explanation B. The protection of confidentiality is a benefit of a cryptosystem.

Explanation C. The protection of integrity is a benefit of a cryptosystem.

Explanation D. The protection of non-repudiation is a benefit of a cryptosystem.

PrepLogic Question: 4293-327

5. Review Question p. 77

Answers: B

Explanation A. A birthday attack is aimed against hash functions or cryptogaphic keys, not polyalphabetic substitution ciphers.

Explanation B. A polyalphabetic cipher is vulnerable to frequency analysis.

Explanation C. A monoalphabetic cipher is vulnerable to a period analysis, not a polyalphabetic cipher.

Explanation D. A collision occurs when the same hash value is generated by two different plaintexts.

PrepLogic Question: 4293-328

6. Review Question p. 77

Answers: C

Explanation A. Vernam ciphers are not vulnerable to simple frequency analysis.

Explanation B. Running key ciphers are not vulnerable to simple frequency analysis, but its redundancy can be a weakness.

Explanation C. Substitution ciphers are vulnerable to frequency analysis.

Explanation D. Code ciphers are not vulnerable to frequency analysis.

PrepLogic Question: 4293-329

7. Review Question p. 78

Answers: D

Explanation A. Vernam cipher is not a transposition cipher.

Explanation B. Vernam cipher is not a running key cipher.

Explanation C. Vernam cipher is not a polyalphabetic substitution cipher.

Explanation D. Vernam cipher is an example of a one-time pad.

PrepLogic Question: 4293-330

8. Review Question p. 78

Answers: A

Explanation A. The Escrowed Encryption Standard (EES) is embodied in the clipper chip.

Explanation B. The Escrowed Encryption Standard (EES) is not embodied in Data Encryption Standard (DES). DES is a symmetric 56-bit key cryptographic system.

Explanation C. The Escrowed Encryption Standard (EES) is not a symmetric cryptographic system, it is an asymmetric cryptographic system.

Explanation D. The Escrowed Encryption Standard (EES) is not embodied in Digital Signature Standard (DSS). DSS is the formalized collection of hashing mechanisms.

PrepLogic Question: 4293-331

9. Review Question p. 78

Answers: B

Explanation A. DES uses a 56-bit key, not Skipjack.

Explanation B. Skipjack uses an 80-bit key.

Explanation C. AES (amongst others) can use a 128-bit key, not Skipjack.

Explanation D. AES (amongst others) can use a 256-bit key, not Skipjack.

PrepLogic Question: 4293-332

10. Review Question p. 79

Answers: C

Explanation A. Symmetric key cryptography uses secret shared common keys.

Explanation B. Symmetric key cryptography uses secret shared common keys.

Explanation C. Public key is only found in asymmetric cryptographic systems, specifically public key cryptographic systems.

Explanation D. Symmetric key cryptography uses secret shared common keys.

PrepLogic Question: 4293-333

11. Review Question p. 79

Answers: D

Explanation A. Asymmetric cryptography uses key pairs and is often used to implement public key infrastructure (PKI) solutions.

Explanation B. Asymmetric cryptography uses key pairs and is often used to implement public key infrastructure (PKI) solutions.

Explanation C. Asymmetric cryptography uses key pairs and is often used to implement public key infrastructure (PKI) solutions.

Explanation D. Symmetric cryptography is better suited for bulk encryption than asymmetric cryptography.

PrepLogic Question: 4293-334

12. Review Question p. 79

Answers: A

Explanation A. 3DES uses three DES's 56 bit keys, thus it is often said to offer the strength of a 168 bit key.

Explanation B. DES uses a 56-bit key.

Explanation C. No common encryption system uses 124-bit keys.

Explanation D. AES can use a 256-bit key.

PrepLogic Question: 4293-335

13. Review Question p. 80

Answers: B

Explanation A. TwoFish was the runner up behind Rijndael for the cipher to be used in AES.

Explanation B. Advanced Encryption System (AES), using the Rijndael cipher, is the replacement for 3DES.

Explanation C. IDEA is not the replacement for 3DES.

Explanation D. RC5 is not the replacement for 3DES.

PrepLogic Question: 4293-336

14. Review Question p. 80

Answers: C

Explanation A. MD5 is a hashing algorithm, not a symmetric block cipher.

Explanation B. Haval is a hashing algorithm, not a symmetric block cipher.

Explanation C. TwoFish is a symmetric block cipher.

Explanation D. El Gamal is an asymmetric algorithm, not a symmetric block cipher.

PrepLogic Question: 4293-337

15. Review Question p. 80

Answers: D

Explanation A. AES uses a variable key length with valid values of 128, 192, or 256.

Explanation B. AES uses a variable key length with valid values of 128, 192, or 256.

Explanation C. AES uses a variable key length with valid values of 128, 192, or 256.

Explanation D. AES does not support the use of a 64-bit key.

PrepLogic Question: 4293-338

16. Review Question p. 80

Answers: A

Explanation A. IDEA uses a 128-bit key length.

Explanation B. No common cryptographic algorithm uses a 108-bit key.

Explanation C. Few cryptographic algorithms uses a 64-bit key.

Explanation D. DES uses a 56-bit key length.

PrepLogic Question: 4293-339

17. Review Question p. 81

Answers: B

Explanation A. A symmetric cryptosystem is one that uses shared common secret keys.

Explanation B. An asymmetric cryptosystem is one that uses key pairs, where one key is kept secret and one is freely and publicly distributed. Technically, a sub-set of assymetric known as public key cryptography is a more specific answer.

Explanation C. The term digital signature can refer to either an asymmetric system or a message hash/digest system.

Explanation D. A message digest cryptosystem is not an asymmetric cryptographic system. A single hash function is used to create a hash value.

PrepLogic Question: 4293-340

18. Review Question p. 81

Answers: C

Explanation A. Public key cryptographic systems offer the benefit of not needing to exchange secret keys.

Explanation B. Public key cryptographic systems offer the benefit that the private key cannot be derived from the public key.

Explanation C. Public key cryptographic systems still require some form of key

distribution in order to get the public keys out in the public so recipients of messages can use them to decrypt messages encrypted with a communication partner's private key.

Explanation D. Public key cryptographic systems offer the benefit that when one of the keys in a key pair is used to encrypt a message, only the key's partner can be used to decrypt that message.

PrepLogic Question: 4293-341

19. Review Question p. 81

Answers: D

Explanation A. Symmetric key cryptographic systems are not dependant on trapdoor one-way functions. Instead, they rely upon the sharing of a common secret key.

Explanation B. Message digest algorithms depend upon a known hash function and the improbability that two different plaintexts will produce the same hash value.

Explanation C. Cryptosystems relying upon key exchange are symmetric cryptographic systems. Symmetric key cryptographic systems are not dependant on trapdoor one-way functions. Instead, they rely upon the sharing of a common secret key.

Explanation D. Asymmetric key cryptography (public key cryptography) is dependant upon the use of a trapdoor one-way function.

PrepLogic Question: 4293-342

20. Review Question p. 82

Answers: A

Explanation A. RSA is based upon the product of two very large prime numbers.

Explanation B. Diffie-Hellman is based on a discrete logarithm using a random length secret.

Explanation C. Merkle-Hellman Knapsack is based on a shared collection of superincreasing weights.

Explanation D. El Gamal is based on a discrete logarithm.

PrepLogic Question: 4293-343

21. Review Question p. 82

Answers: B

Explanation A. Haval is a hash function, not an asymmetric cryptographic system that requires key exchange.

Explanation B. Diffie-Hellman is an asymmetric cryptographic system that includes a method by which secret keys can be exchanged securely over an insecure medium.

Explanation C. Rijndael is a symmetric key cryptographic block cipher that is used in AES.

Explanation D. El Gamal is a asymmetric key cryptographic system that uses a discrete algorithm, it does not offer or define a means of key exchange.

PrepLogic Question: 4293-344

22. Review Question p. 82

Answers: C

Explanation A. ECC can be used to implement Diffie-Hellman, El Gamal, or Schnorr public key algorithms.

Explanation B. ECC offers stronger encryption, even using smaller keys.

Explanation C. ECC is suitable for hardware applications.

Explanation D. ECC can be used for digital signatures, encryption, and key management.

PrepLogic Question: 4293-345

23. Review Question p. 83

Answers: D

Explanation A. A certificate issued by a publicly trusted CA will usually contain a serial number, identity information, and the signature of the issuing authority. These are some of the elements mandated by the x.509 v3 certificate standard.

Explanation B. A certificate issued by a publicly trusted CA will usually contain a serial number, identity information, and the signature of the issuing authority. These are some of the elements mandated by the x.509 v3 certificate standard.

Explanation C. A certificate issued by a publicly trusted CA will usually contain a serial number, identity information, and the signature of the issuing authority. These are

some of the elements mandated by the x.509 v3 certificate standard.

Explanation D. A certificate issued by a publicly trusted CA will not contain IP address information. The IP address is not an element mandated by the x.509 v3 certificate standard.

PrepLogic Question: 4293-346

24. Review Question p. 83

Answers: A

Explanation A. An RA does not issue new certificates.

Explanation B. An RA confirms the identity of subjects.

Explanation C. An RA distributes the CRL.

Explanation D. An RA shares the workload with the CA.

PrepLogic Question: 4293-347

25. Review Question p. 83

Answers: B

Explanation A. A message digest (i.e., a hash function) does not provide for confidentiality.

Explanation B. A message digest (i.e., a hash function) provides for integrity.

Explanation C. A message digest (i.e., a hash function) does not provide for authentication.

Explanation D. A message digest (i.e., a hash function) does not provide for non-repudiation.

PrepLogic Question: 4293-348

26. Review Question p. 84

Answers: C

Explanation A. The secrecy and security of hash function is based on its one-way-ness.

Explanation B. The hash function algorithm is publicly known.

Explanation C. The original plaintext cannot be reconstructed from the hash value or message digest.

Explanation D. Hash functions produce a fixed length hash value no matter what the length of the inputted plaintext.

PrepLogic Question: 4293-349

27. Review Question p. 84

Answers: B

Explanation A. The algorithm is a determining factor in the strength of a crypto system.

Explanation B. The size of the keyspace does not have a direct correlation to the strength of the crypto system. The keyspace is simply the range of values defined by the algorithm that can be used to construct keys.

Explanation C. The initialization value is a determining factor in the strength of a crypto system.

Explanation D. The length of key is a determining factor in the strength of a crypto system.

PrepLogic Question: 4293-350

28. Review Question p. 84

Answers: C

Explanation A. Confidentiality is a goal of cryptography.

Explanation B. Non-repudiation is a goal of cryptography.

Explanation C. Availability is not a goal of cryptography.

Explanation D. Integrity is a goal of cryptography.

PrepLogic Question: 4293-351

29. Review Question p. 85

Answers: D

Explanation A. A transposition cipher is not subject to cracking by means of period analysis, but is subject to cracking by frequency analysis.

Explanation B. A Vernam cipher is not subject to cracking by means of period analysis. A Vernam cipher is a form of one time pad and thus very difficult to crack.

Explanation C. A running key cipher is not subject to cracking by means of period analysis. A running key cipher can be cracked if you can discover the source of the running key, such as a book or other readily available text sent to the intended recipient.

Explanation D. A polyalphabetic cipher is subject to cracking by means of period analysis.

PrepLogic Question: 4293-352

30. Review Question p. 85

Answers: A

Explanation A. Steganography is the cryptography mechanism which hides information within images.

Explanation B. Coding is pre-arranging the meaning of otherwise meaningless words or phrases to broadcast a directed secret message via a public means.

Explanation C. Substitution is a form of cipher that replaces one letter for another.

Explanation D. A tuple is a row of a database.

PrepLogic Question: 4293-353

31. Review Question p. 85

Answers: B

Explanation A. Twofish was a finalist in the selection process for 3DES, but it is not the selected replacement.

Explanation B. AES is the replacement for 3DES.

Explanation C. IDEA is not the replacement for 3DES. IDEA is used by the PGP e-mail encrypting system.

Explanation D. RC5 is not the replacement for 3DES.

PrepLogic Question: 4293-354

32. Review Question p. 86

Answers: D

Explanation A. A key or the crypto-variable is the information or the sequence of activities that must be kept secret in order to provide strength to the encryption.

Explanation B. Ciphertext is the resultant hidden or encrypted text that is created when cryptography is performed on plaintext.

Explanation C. Code is a cryptographic transformation that operates at the word or phrase level. A code can be used to communicate information to the intended recipient by pre-determining the meaning of a specific code. All other parties who may intercept the code will be unaware of the actual meaning of the code.

Explanation D. The set of mathematical rules that dictate how enciphering and deciphering take place is known as the algorithm.

PrepLogic Question: 4293-355

33. Review Question p. 86

Answers: A

Explanation A. The key of a cryptosystem must be kept secret in order to protect the security provided by encryption.

Explanation B. The algorithm of a cryptosystem is usually known by the public. The publication of the algorithm so it can be tested is the only way for a cryptosystem to be trusted as a secure means of hiding data.

Explanation C. The keyspace of a cryptosystem is usually known by the public. The algorithm, which is also known, defines the valid range of values for its keys (i.e., its keyspace).

Explanation D. The block size of a cryptosystem is usually known by the public. The algorithm defines the block sizes it uses when performing the encryption process.

PrepLogic Question: 4293-356

34. Review Question p. 86

Answers: B

Explanation A. The strength of a cryptosystem is based on the algorithm, the secrecy of the keys, the length of the key, the initialization vectors, and how all of these items are used together.

Explanation B. The strength of a cryptosystem is not based on the length of the

plaintext or even the content of the plaintext. The message to be encrypted is not a determining factor in the strength of a cryptosystem.

Explanation C. The strength of a cryptosystem is based on the algorithm, the secrecy of the keys, the length of the key, the initialization vectors, and how all of these items are used together.

Explanation D. The strength of a cryptosystem is based on the algorithm, the secrecy of the keys, the length of the key, the initialization vectors, and how all of these items are used together.

PrepLogic Question: 4293-357

35. Review Question p. 87

Answers: C

Explanation A. The goals of cryptosystems is to provide for confidentiality, non-repudiation, integrity, and authenticity.

Explanation B. The goals of cryptosystems is to provide for confidentiality, non-repudiation, integrity, and authenticity.

Explanation C. Availability is not a goal of cryptosystems. Cryptosystems do not address the need to make resources available, accessible, or delivered in a timely manner. The goals of cryptosystems is to provide for confidentiality, non-repudiation, integrity, and authenticity.

Explanation D. The goals of cryptosystems is to provide for confidentiality, non-repudiation, integrity, and authenticity.

PrepLogic Question: 4293-358

36. Review Question p. 87

Answers: D

Explanation A. Clustering is the condition where a single plaintext message, using the same algorithm but with two different keys, produces the same ciphertext.

Explanation B. End-to-end encryption is the process of encrypting a message and maintaining that encryption from its source or origin to its recipient or destination.

Explanation C. Encryption streaming is a process by which a continuous flow of data is encrypted on the fly as it is transmitted.

Explanation D. Block ciphering is the action of dividing a plaintext message into fixed length segments and applying the same algorithm to each segment to hide the message.

PrepLogic Question: 4293-359

37. Review Question p. 87

Answers: A

Explanation A. A cryptogram or ciphertext is an unintelligible message - it is a plaintext that has been transformed into a protected message through the application of cryptography.

Explanation B. Cipher is a cryptographic transformation that operates on characters or bits. A cipher is used to hide the meaning of a message by transforming it one letter at a time.

Explanation C. Code is a cryptographic transformation that operates at the word or phrase level. A code can be used to communicate information to the intended recipient by pre-determining the meaning of a specific code. All other parties who may intercept the code will be unaware of the actual meaning of the code.

Explanation D. The set of mathematical rules that dictate how enciphering and deciphering take place is known as the algorithm.

PrepLogic Question: 4293-360

38. Review Question p. 88

Answers: B

Explanation A. Collusion is when two or more people work together to commit a crime.

Explanation B. Clustering occurs when the same ciphertext is produced when a single plaintext is encrypted using two different keys.

Explanation C. Polyinstantiation is a protection mechanism used in databases that allows the creation of duplicate objects at different sensitivity levels to prevent a lower level subject from learning about the existence of the higher level object.

Explanation D. Scavenging is the act of gathering information from data left over from a business activity or left on discarded systems or media.

PrepLogic Question: 4293-361

39. Review Question p. 88

Answers: C

Explanation A. A cipher is a cryptographic transformation that operates at the character or bit level.

Explanation B. A block cipher is a cryptographic transformation that operates by dividing plaintext into standard length segments or blocks for the encryption process.

Explanation C. A code cipher, or just a code, is a cryptographic transformation that operates as the word or phrase level.

Explanation D. A streaming cipher is a cryptographic transformation that operates at the character or bit level as the data is created or transmitted.

PrepLogic Question: 4293-362

40. Review Question p. 88

Answers: D

Explanation A. A work factor is the amount of effort required to break a cryptographic system. There is no such encryption method actually called a work factor encryption.

Explanation B. Link encryption is a form of communication encryption where only segment connected partners share encryption keys. Therefore, the data is decrypted at each hop, then re-encrypted for the trip across the next segment.

Explanation C. Streaming encryption is an encryption system that encrypts each character or bit as it is created or transmitted.

Explanation D. End-to-end encryption is a form of communication encryption where the data is encrypted for the entire trip across an untrusted network from source to destination.

PrepLogic Question: 4293-363

41. Review Question p. 89

Answers: A

Explanation A. Link encryption encrypts the entire packet.

Explanation B. End-to-end encryption does not encrypt the packet header.

Explanation C. IPSec in transport mode does not encrypt the packet header.

Explanation D. PPTP tunnels with CHAP does not provide any form of encryption for data transmission.

PrepLogic Question: 4293-364

42. Review Question p. 89

Answers: B

Explanation A. End-to-end encryption performs its encryption at the application layer.

Explanation B. End-to-end encryption performs its encryption at the application layer.

Explanation C. End-to-end encryption performs its encryption at the application layer.

Explanation D. End-to-end encryption performs its encryption at the application layer.

PrepLogic Question: 4293-365

43. Review Question p. 89

Answers: C

Explanation A. Link encryption performs its encryption at the physical layer.

Explanation B. Link encryption performs its encryption at the physical layer.

Explanation C. Link encryption performs its encryption at the physical layer.

Explanation D. Link encryption performs its encryption at the physical layer.

PrepLogic Question: 4293-366

44. Review Question p. 90

Answers: D

Explanation A. Elliptical curve is a cryptosystem, but it is not a Boolean operation commonly used throughout most cryptographic systems.

Explanation B. A discrete algorithm is used prominently in symmetric cryptosystems; however, it is not a Boolean operation commonly used throughout most cryptographic systems.

Explanation C. ANDing is a Boolean operation, but it is not the operation most commonly used by cryptographic systems.

Explanation D. Exclusive OR is the most common mathematical Boolean operation performed by cryptographic systems.

PrepLogic Question: 4293-367

45. Review Question p. 90

Answers: A

Explanation A. One-time pads are not suitable for modern applications, primarily due to the inability for a computer to create truly non-repeating random codes and the problem of securely exchanging the pad with communication partners.

Explanation B. One-time pads are often used as a stream cipher.

Explanation C. One-time pads are unbreakable if the codes are truly random.

Explanation D. One-time pads use a key length that is the same length as the original message.

PrepLogic Question: 4293-368

46. Review Question p. 90

Answers: B

Explanation A. Microdots are examples of steganography.

Explanation B. Hiding data in a bad sector on a hard drive is an example of the use of a covert storage channel, not steganography.

Explanation C. Watermarks are examples of steganography.

Explanation D. Hiding a text message in a visual image is an example of steganography.

PrepLogic Question: 4293-369

47. Review Question p. 91

Answers: C

Explanation A. Cryptanalysis is the art of obtaining the plaintext (i.e., the original message) or the key from ciphertext.

Explanation B. Stenanography is a form of secret communications where the message is hidden inside another communication, such as an image, a program, or an audio file.

Explanation C. Cryptography is the art and science of hiding the meaning of communications from unintended recipients.

Explanation D. Ciphering is the use of ciphers to hide or reveal messages. However, this is an incomplete answer for this question since there are additional ways to perform this activity other than using ciphers.

PrepLogic Question: 4293-370

48. Review Question p. 91

Answers: D

Explanation A. Stenanography is a form of secret communications where the message is hidden inside another communication, such as an image, a program, or an audio file.

Explanation B. Cryptography is art and science of hiding the meaning of communications from unintended recipients.

Explanation C. Ciphering is the use of ciphers to hide or reveal messages.

Explanation D. Cryptanalysis is the art of obtaining the plaintext (i.e., the original message) or the key from ciphertext.

PrepLogic Question: 4293-371

49. Review Question p. 91

Answers: A

Explanation A. Cryptology is the one item from this list different from the others since it is the parent concept that contains the others. Cryptology is a method of storing and transmitting data in a form that can be read and processed only by the intended recipient.

Explanation B. Cryptography is a subset of cryptology. Cryptography is the art and science of hiding the meaning of communications from unintended recipients.

Explanation C. Cryptanalysis is a subset of cryptology. Cryptanalysis Cryptanalysis is the art of obtaining the plaintext (i.e., the original message) or the key from ciphertext.

Explanation D. Cryptographic algorithm is a subset of cryptology. Cryptographic algorithm is the step-by-step procedure used to encrypt or decrypt ciphertext.

PrepLogic Question: 4293-372

50. Review Question p. 92

Answers: B

Explanation A. A polyalphabetic cipher uses several alphabets in a substitution cipher. The use of multiple alphabets counters frequency analysis attacks.

Explanation B. The process of hiding the meaning of a message by using a mechanism which shifts each letter of the alphabet by three letters is known as a monoalphabetic substitution cipher.

Explanation C. A transposition cipher transforms a message by writing it in a fixed width column, then transpositioning the message by generating the output from each vertical column of letters.

Explanation D. A running key cipher uses a source text, such as a book, as the key. The plaintext to be encrypted is matched with material from the key using a pre-determined mechanism, such as Modulo 26 to effect the encryption.

PrepLogic Question: 4293-373

51. Review Question p. 92

Answers: C

Explanation A. A cryptosystem is comprised of plaintext, keys, algorithms, and ciphertext.

Explanation B. A cryptosystem is comprised of plaintext, keys, algorithms, and ciphertext.

Explanation C. A cryptosystem may use a one way mathematical function as its algorithm, but not all algorithms are one way.

Explanation D. A cryptosystem is comprised of plaintext, keys, algorithms, and ciphertext.

PrepLogic Question: 4293-374

52. Review Question p. 92

Answers: D

Explanation A. A message can be encrypted for confidentiality.

Explanation B. A message can be digitally signed for authentication and integrity.

Explanation C. A message can be encrypted and digitally signed for confidentiality,

integrity, and authentication.

Explanation D. A message can be hashed for integrity, not confidentiality.

PrepLogic Question: 4293-375

53. Review Question p. 93

Answers: A

Explanation A. SHA-1 produces a 160-bit hash value.

Explanation B. HAVAL can produce hashes in lengths of 128 bits, 160 bits, 192 bits, 224 bits, and 256 bits.

Explanation C. MD5 produces a 128-bit hash value.

Explanation D. MD2 produces a 128-bit hash value.

PrepLogic Question: 4293-376

54. Review Question p. 93

Answers: A

Explanation A. HAVAL supports a variable hash value length output.

Explanation B. SHA has a 160-bit hash value output.

Explanation C. HMAC has a 128-bit hash value output.

Explanation D. MD4 has a 128-bit hash value output.

PrepLogic Question: 4293-378

55. Review Question p. 93

Answers: B

Explanation A. Key length should be long enough to provide the necessary level of protection for the encrypted data.

Explanation B. Keys need to be stored and transmitted securely, otherwise the system offers no assurance of security.

Explanation C. Keys should be truly random and use the full spectrum of the key space.

Explanation D. The more often a key is used, the shorter its lifetime should be.

PrepLogic Question: 4293-379

56. Review Question p. 94

Answers: C

Explanation A. E-mail security based on encryption can provide non-repudiation.

Explanation B. E-mail security based on encryption can provide authentication of the message source.

Explanation C. Encryption in any form, including that developed for e-mail systems, is not capable of providing availability.

Explanation D. E-mail security based on encryption can provide delivery verification.

PrepLogic Question: 4293-380

57. Review Question p. 94

Answers: D

Explanation A. PEM is an e-mail encryption system.

Explanation B. MOSS is an e-mail encryption system.

Explanation C. PGP is an e-mail encryption system.

Explanation D. SET is an e-commerce encryption protocol for used in Web transactions, not e-mail.

PrepLogic Question: 4293-381

58. Review Question p. 94

Answers: A

Explanation A. PGP uses IDEA for encryption.

Explanation B. MIME does not use IDEA.

Explanation C. PEM uses RSA for encryption, 3DES for key exchange, and MD5 and MD2 for message digests.

Explanation D. SET uses DES for encryption and RSA for key exchange and digital

signatures.

PrepLogic Question: 4293-382

59. Review Question p. 95

Answers: B

Explanation A. SET is an e-commerce tool to keep transactions confidential.

Explanation B. FIMAS is similar to a cyclic redundancy check (CRC) that is appended to a message prior to transmission to ensure integrity.

Explanation C. MOSS is an e-mail encryption tool, not a CRC check, hash value, or message digest.

Explanation D. TLS is a protocol to secure client to server Internet communications above the Transport layer on a document by document basis.

PrepLogic Question: 4293-383

60. Review Question p. 95

Answers: C

Explanation A. MONDEX is a proprietary payment transaction system used to manage cash on smart cards.

Explanation B. MAC is a message digest or hash function.

Explanation C. SSL (and TLS) authenticates the server to the client using RSA public key cryptography and digital certificates, uses 3DES and MD5 hash functions, and can be used to provide security communications for Telnet, FTP, HTTP, and e-mail.

Explanation D. S/MIME is limited to e-mail.

PrepLogic Question: 4293-384

61. Review Question p. 95

Answers: D

Explanation A. RARP (Reverse ARP) and ARP (Address Resolution Protocol) are not the components of IPSec. They are used in the Network layer of the TCP/IP stack to provide address resolution services.

Explanation B. IGMP (Internet Group Management Protocol) and RIP (Routing

Information Protocol) are not the components of IPSec. IGMP is used to manage multicast groups. RIP is used to manage routing tables.

Explanation C. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are the two Transport layer protocols of the TCP/IP stack, not the components of IPSec.

Explanation D. AH (Authentication Header) and ESP (Encapsulated Security Payload) are the two components of IPSec.

PrepLogic Question: 4293-385

62. Review Question p. 96

Answers: A

Explanation A. IPSec does not provide for availability.

Explanation B. IPSec provides for encryption, access control, non-repudiation, and authentication.

Explanation C. IPSec provides for encryption, access control, non-repudiation, and authentication.

Explanation D. IPSec provides for encryption, access control, non-repudiation, and authentication.

PrepLogic Question: 4293-386

63. Review Question p. 96

Answers: B

Explanation A. In IPSec tunnel mode, the entire IP packet is encrypted.

Explanation B. In IPSec transport mode, the data of the IP packet is encrypted, but the original header is not.

Explanation C. IPSec has two VPN modes: tunnel mode and transport mode.

Explanation D. IPSec does not have a mode named link mode.

PrepLogic Question: 4293-387

64. Review Question p. 96

Answers: C

Explanation A. ISAKMP, SKEME, and Oakley KDP are protocols found in the Internet Key Exchange (IKE) of IPSec.

Explanation B. ISAKMP, SKEME, and Oakley KDP are protocols found in the Internet Key Exchange (IKE) of IPSec.

Explanation C. Merkle-Hellman Knapsack is not a public key algorithm found in the Internet Key Exchange (IKE) of IPSec.

Explanation D. ISAKMP, SKEME, and Oakley KDP are protocols found in the Internet Key Exchange (IKE) of IPSec.

PrepLogic Question: 4293-388

65. Review Question p. 97

Answers: D

Explanation A. IKE is the key management suite of IPSec.

Explanation B. IOTP is a commerce transaction protection protocol.

Explanation C. FIMAS is a message hash solution.

Explanation D. S-HTTP is an alterative to SSL to provide secure Web transactions. However, S-HTTP is no longer a widely supported technology.

PrepLogic Question: 4293-389

66. Review Question p. 97

Answers: C

Explanation A. Asymmetric keys are not vulnerable to birthday attacks.

Explanation B. Symmetric keys are not vulnerable to birthday attacks.

Explanation C. The birthday attack is primarily used against hash values, message digests, and hash functions.

Explanation D. Digital signatures (a form of asymmetric keys) are not vulnerable to birthday attacks.

PrepLogic Question: 4293-395

67. Review Question p. 97

Answers: D

Explanation A. A known key attack is an attack where the encryption key is already known.

Explanation B. A key space attack is another name for a brute force attack. However, key space attack is not a commonly used attack term.

Explanation C. There is no such attack named sequential referenced attack.

Explanation D. A brute force attack attempts to break a cryptosystem by trying every possible key pattern.

PrepLogic Question: 4293-396

68. Review Question p. 98

Answers: A

Explanation A. A meet-in-the-middle attack attempts to break double encryption schemes by comparing the results of a single encrypting a known plaintext with a single decryption of a ciphertext.

Explanation B. A known plaintext attack is not used against double encryption schemes. In a known plaintext attack, a known plaintext is compared with its ciphertext to discover the encryption key.

Explanation C. Linear cryptanalysis is a mathematical attack that attempts to approximate keys by comparing plaintext and ciphertext.

Explanation D. A chosen ciphertext attack decrypts selected portions of the ciphertext and compares it to the known plaintext to discover the key.

PrepLogic Question: 4293-397

69. Review Question p. 98

Answers: B

Explanation A. A cryptographic attack does not have a goal of exploring the key space since it is a known entity.

Explanation B. The primary goals of cryptographic attacks are to discover the key used or to extract the original plaintext.

Explanation C. A cryptographic attack does not have a goal of discovering the

algorithm since this is a known entity.

Explanation D. Once a cryptographic attack is successful and the key is discovered, it can be used to transmit faked encrypted messages. But this is not the primary goal of cryptographic attacks.

PrepLogic Question: 4293-398

70. Review Question p. 98

Answers: D

Explanation A. SEASAME uses Needham-Schroeder, MD5, and crc32.

Explanation B. KryptoKnight does not use DES.

Explanation C. NetSP does not use DES.

Explanation D. Kerberos uses DES. Or at least the initial implementations of Kerberos used DES, modern implementations often use 3DES or AES.

PrepLogic Question: 4293-399

Explanations: Chapter 5

1. Review Question p. 99

Answers: C

Explanation A. Separation of duties is an element of personnel controls.

Explanation B. Handling non-compliance is an element of personnel controls.

Explanation C. Stipulating laws and regulations is an element of policies and procedures, not personnel controls.

Explanation D. Rotation of duties is an element of personnel controls.

PrepLogic Question: 4293-118

2. Review Question p. 99

Answers: B

Explanation A. Network access control is used to protect against outside intruders through the use of routers and firewalls. Network access control addresses confidentiality, but not integrity.

Explanation B. Encryption is used to ensure confidentiality and integrity.

Explanation C. Data backups provide a physical protection of data through a means of physical duplication. Data backups address integrity, but not confidentiality.

Explanation D. Perimeter security prevents unauthorized access into a facility. Perimeter security addresses confidentiality, but not integrity.

PrepLogic Question: 4293-121

3. Review Question p. 99

Answers: B

Explanation A. Auditing is dependant upon identification.

Explanation B. Auditing is not dependant upon accountability. In fact, accountability is dependant upon auditing. Accountability is the result of the mechanisms of identification, authentication, authorization, access control, and auditing, which are used to hold people responsible for their online activities.

Explanation C. Auditing is dependant upon authorization.

Explanation D. Auditing is dependant upon authentication.

PrepLogic Question: 4293-125

4. Review Question p. 100

Answers: A

Explanation A. Privileged operations should be restricted to authorized individuals whose work tasks specifically require greater than normal capabilities.

Explanation B. Backup operations need not be restricted to administrative users, any user should be able to back up their work.

Explanation C. E-mail client use usually does not require greater than normal user capabilities.

Explanation D. Productivity software use usually does not require greater than normal user capabilities.

PrepLogic Question: 4293-480

5. Review Question p. 100

Answers: C

Explanation A. Improvement of the security policy is a secondary benefit of auditing, but auditing is not the primary mechanism to perform this function.

Explanation B. Auditing may be able to detect some networking anomalies, however the primary mechanism or use of auditing is to test for compliance with security policies by recording audit trains.

Explanation C. Auditing is a mechanism to create audit trails.

Explanation D. Auditing is not the testing process to validate the security design of a system, that is penetration testing.

PrepLogic Question: 4293-494

6. Review Question p. 100

Answers: A

Explanation A. The goal of audit trails is to check compliance with security policy.

Explanation B. The goal of audit trails is to check compliance with security policy. Safeguard cost efficiency is evaluated with the cost/benefit equiation.

Explanation C. The goal of audit trails is to check compliance with security policy. Risk analysis is a task of risk management and not directly related to auditing.

Explanation D. The goal of audit trails is to check compliance with security policy. Since security is an ongoing process, there is no need to make up work to keep security administrators busy.

PrepLogic Question: 4293-496

7. Review Question p. 101

Answers: B

Explanation A. Rotation of duties is a safeguard against collusion.

Explanation B. Trusted recovery is not a safeguard against collusion. It is a safeguard against failure states encountered by the OS or software which prevents the system from restarting into an insecure state.

Explanation C. Separation of duties is a safeguard against collusion.

Explanation D. Auditing is a safeguard against collusion.

PrepLogic Question: 4293-499

8. Review Question p. 101

Answers: D

Explanation A. Mandatory vacations are not used to perform job rotation. Job rotation is a security mechanism to limit collusion.

Explanation B. Mandatory vacations are not used to perform background checks. Background checks is a security mechanism to hire only trustworthy and capable personnel.

Explanation C. Mandatory vacations are not used to perform recovery plan testing. Recovery plan testing ensures that a specific recovery plan will function properly when needed.

Explanation D. Mandatory vacations are used to perform auditing.

PrepLogic Question: 4293-501

9. Review Question p. 101

Answers: B

Explanation A. Background checks are one of the administrative controls for personnel security.

Explanation B. Enrollment in biometric authentication systems is a logical or technical control for personnel security.

Explanation C. Mandatory vacations are one of the administrative controls for personnel security.

Explanation D. Job action warnings are one of the administrative controls for personnel security.

PrepLogic Question: 4293-507

10. Review Question p. 102

Answers: C

Explanation A. Security controls should not be obstructive to the authorized user.

Explanation B. Security controls should not be accessible to the authorized user unless they are the specified administrator for the control.

Explanation C. Security controls should be transparent to the authorized user.

Explanation D. Security controls should not be inhibiting to the authorized user.

PrepLogic Question: 4293-508

11. Review Question p. 102

Answers: D

Explanation A. The secrecy of a security control is not a valid measure of the strength of the protection it offers.

Explanation B. Dependancy on the secrecy of a security control should be avoided.

Explanation C. Defense in depth is more important than the secrecy of security controls.

Explanation D. Controls should provide their best security whether they are secret or not. The secrecy of a controls is not a valid measure of their strength.

PrepLogic Question: 4293-509

12. Review Question p. 102

Answers: A

Explanation A. Directive or deterrent controls are used to encourage compliance with other security controls.

Explanation B. Recovery controls are used to restore resources and capabilities after an violation.

Explanation C. Application controls are embedded in software to minimize and detect operational irregularities.

Explanation D. Transaction controls are used to control the input, processing, and output of data by software.

PrepLogic Question: 4293-510

13. Review Question p. 103

Answers: A

Explanation A. Split knowledge is where no single person has total control over a system's security mechanisms.

Explanation B. Rotation of duties is a collusion preventative measure where job tasks are rotated among employees on a regular basis. Rotation of duties provides for peer auditing to discover irregularities, mistakes, or intentional crime.

Explanation C. Mandatory vacations ensures that everyone's work tasks are audited at least once a year, while they are out of the office for a required minimal length of time.

Explanation D. Strong access controls simply prevent someone from overstepping their authority or accessing resources outside of their minimal requirements for their work tasks.

PrepLogic Question: 4293-514

14. Review Question p. 103

Answers: B

Explanation A. Mandatory vacations ensures that everyone's work tasks are audited at least once a year, while they are out of the office for a required minimal length of time. Mandatory vacations are not split knowledge security controls.

Explanation B. Separation of duties is a split-knowledge security control.

Explanation C. Rotation of duties is a collusion preventative measure where job tasks are rotated among employees on a regular basis. Rotation of duties provides for peer auditing to discover irregularities, mistakes, or intentional crime. Rotation of duties is not a split knowledge security control.

Explanation D. Background checks are not split knowledge security controls.

PrepLogic Question: 4293-515

15. Review Question p. 103

Answers: C

Explanation A. Due diligence is the effort senior management must show in the implementation of a sound security policy.

Explanation B. Two-man controls are a form of split-knowledge control that requires two users to work in unison to complete some privileged action.

Explanation C. Principle of Least Privilege is a security mechanism that requires that users have the minimum amount of access that is absolutely required by their job tasks and that they have that access for the shortest amount of time.

Explanation D. Rotation of duties is a collusion preventative measure where job tasks are rotated among employees on a regular basis. Rotation of duties provides for peer auditing to discover irregularities, mistakes, or intentional crime.

PrepLogic Question: 4293-516

16. Review Question p. 104

Answers: D

Explanation A. Mandatory vacations ensures that everyone's work tasks are audited at least once a year, while they are out of the office for a required minimal length of time. Mandatory vacations are not split knowledge security controls.

Explanation B. Auditing is the reviewing of activity on a system for irregularies. Auditing is not a split knowledge security control.

Explanation C. Rotation of duties is a collusion preventative measure where job tasks are rotated among employees on a regular basis. Rotation of duties provides for peer auditing to discover irregularities, mistakes, or intentional crime. Rotation of duties is not a split knowledge security control.

Explanation D. Two-man controls are a form of split-knowledge control that requires two users to work in unison to complete some privileged action.

PrepLogic Question: 4293-517

17. Review Question p. 104

Answers: D

Explanation A. The final report should be issued after the exit conference. Interim reports are used to inform the client of issues that need immediate attention. Interim reports are not the trigger to initiate the final report.

Explanation B. The final report should be issued after the exit conference. The exit conference is held to discuss important items from the audit, but the final report is not given to the client at this time.

Explanation C. The final report should be issued after the exit conference. The final audit report can only be written after the auditng process, not at its beginning.

Explanation D. The final report should be issued after the exit conference.

PrepLogic Question: 4293-528

18. Review Question p. 104

Answers: B

Explanation A. The goals of auditing are problem identification and problem resolution.

Explanation B. The goals of auditing are problem identification and problem resolution.

Explanation C. The goals of auditing are problem identification and problem resolution.

Explanation D. The goals of auditing are problem identification and problem resolution.

PrepLogic Question: 4293-534

19. Review Question p. 104

Answers: D

Explanation A. Senior management, while responsible for the success of a security

solution, is rarely the entity to perform an assessment.

Explanation B. End users are not qualified to perform security audits.

Explanation C. The risk assessment team is not equipped to perform security audits.

Explanation D. External consultants, specifically analysts or auditors, are commonly used to perform reviews and evaluations of the security solutions of an environment.

PrepLogic Question: 4293-536

20. Review Question p. 105

Answers: A

Explanation A. The purposed of interim reports is to communicate regarding items that need immediate attention.

Explanation B. Interim reports should have no effect on the length of the final report.

Explanation C. There is no need for progress reports during an audit.

Explanation D. Interim reports are not used to clarify audit objectives.

PrepLogic Question: 4293-537

21. Review Question p. 105

Answers: C

Explanation A. The exit conference is not used to point fingers and place blame on individuals.

Explanation B. The final report and the exit conference may discuss countermeasures, but that is not their primary purpose. The final report and exit conference should discuss vulnerabilities. The choice of responses is left up to management.

Explanation C. The purpose of the exit conference is to discuss issues with all relevant and effected parties.

Explanation D. Auditing objectives should be discussed and altered at the beginning of the auditing process, not at the end.

PrepLogic Question: 4293-538

22. Review Question p. 105

Answers: A

Explanation A. Senior management is responsible for the selection and delegation of implementation of the changes recommended in the findings report from an external auditor.

Explanation B. End users are not responsible for the implementation of the changes recommended in the findings report from an external auditor.

Explanation C. Internal auditors are not responsible for the implementation of the changes recommended in the findings report from an external auditor. They are only responsible for overseeing that the recommendations are implemented.

Explanation D. System managers are not responsible for the implementation of the changes recommended in the findings report from an external auditor.

PrepLogic Question: 4293-539

23. Review Question p. 105

Answers: B

Explanation A. Problem management may include countermeasure selection.

Explanation B. Once a problem is discovered through auditing, the next step is problem management.

Explanation C. Problem management may include risk analysis.

Explanation D. Problem management may include security policy modification.

PrepLogic Question: 4293-540

24. Review Question p. 106

Answers: C

Explanation A. Reducing failures to a reasonable level is a primary goal of problem management.

Explanation B. Preventing the re-occurrence of discovered problems is a primary goal of problem management.

Explanation C. Maintaining the cost effectiveness of countermeasures is a secondary goal of problem management. In many cases it is an automatic benefit of the risk analysis aspect of problem management.

Explanation D. Mitigating the negative impact of problems is a primary goal of problem management.

PrepLogic Question: 4293-541

25. Review Question p. 106

Answers: C

Explanation A. Need to know is the access restriction that requires both proper subject classification and clearance but also management/supervisor approval to access a restricted resource.

Explanation B. Separation of duties is used to prevent collusion by assigning different tasks and privileges to different personnel.

Explanation C. Least privilege (or the principle of least privilege) means subjects are granted only the minimal amount of access required for them to complete their assigned work tasks.

Explanation D. Privilege elevation is the act of assuming greater than assigned access abilities to perform activities outside of the normal restrictions of a user account. Privilege elevation can be an authorized activity used to perform administrative tasks or an act of abuse or malicious attack.

PrepLogic Question: 4293-626

26. Review Question p. 106

Answers: D

Explanation A. The removal of a threat agent will reduce risk, but that is not accomplished with a safeguard. A safeguard patches the victim (i.e., the IT infrastructure) but it does not act directly on the attacker or threat.

Explanation B. Enhancing an exposure often occurs at the removal of a safeguard, an thus is not the purpose of a safeguard.

Explanation C. Safeguards should not require updating of the security policy in most situations. A security policy should include the application of safeguards as an expected aspect of ongoing security management. A safeguard does not apply directly to a security policy either, rather it is applied to the IT infrastructure.

Explanation D. A safeguard's purpose is to reduce or remove a vulnerability.

PrepLogic Question: 4293-699

27. Review Question p. 106

Answers: D

Explanation A. Removing all risk is not possible.

Explanation B. Performing a qualitative analysis of risk is an element of risk management (i.e., one of the evaluation mechanisms), but it is not the primary goal.

Explanation C. Nothing removes liability from senior management. Senior management is always responsible for the success or failure of a security policy.

Explanation D. The primary goal of risk management is to reduce risk to an acceptable level.

PrepLogic Question: 4293-700

28. Review Question p. 107

Answers: B

Explanation A. Physical damage is an example of a risk.

Explanation B. Blocking ports is a safeguard, not a risk.

Explanation C. Misuse of data is an example of a risk.

Explanation D. Buffer overflow is an example of a risk.

PrepLogic Question: 4293-701

29. Review Question p. 107

Answers: B

Explanation A. Applying a safeguard is a means by which risk is reduced.

Explanation B. Waiting is not a valid response to risk and waiting will not reduce risk.

Explanation C. Removing the vulnerability is a means by which risk is reduced.

Explanation D. Blocking the threat agent is a means by which risk is reduced.

PrepLogic Question: 4293-702

30. Review Question p. 107

Answers: C

Explanation A. A vulnerability is the absence or weakness of a safeguard that could be exploited.

Explanation B. Single loss expectancy is the possible maximum asset loss that would be experienced with a single incident of a security breach.

Explanation C. Exposure is an instance of being exposed to losses from a threat.

Explanation D. Breach is the realization of a threat; i.e., when security is violated or compromised in such a way to allow access to unauthorized intruders.

PrepLogic Question: 4293-703

31. Review Question p. 107

Answers: C

Explanation A. Intruder access through a firewall is an example of a threat.

Explanation B. Activities that violate the security policy is an example of a threat.

Explanation C. A biometric device failing to authenticate a valid user is a False Rejection (Type I) error, but it is not a threat.

Explanation D. A natural disaster that destroys the IT infrastructure is an example of a threat.

PrepLogic Question: 4293-704

32. Review Question p. 108

Answers: D

Explanation A. Blocking all attachments at the e-mail gateway is not a threat but a common security practice.

Explanation B. Scanning for malicious code is not a threat but a common security practice.

Explanation C. Performing penetration testing without senior management approval is not a threat but it is a poor security management activity since senior management should always be consulted before penetration testing is performed. The activities of penetration testing often are the exact same mechanisms used in malicious attacks.

Explanation D. An authorized user destroying confidential data is an example of a threat.

PrepLogic Question: 4293-705

33. Review Question p. 108

Answers: A

Explanation A. Failing to review audit logs is not a risk, but it does show a lack of compliance with a realistic security policy. Audit logs will often reveal when a risk has become an actual intrusion or attack.

Explanation B. Failing to enforce password policy is an example of a risk.

Explanation C. Not updating anti-virus software is an example of a risk.

Explanation D. Not filtering traffic on border communication links is an example of a risk.

PrepLogic Question: 4293-706

34. Review Question p. 108

Answers: A

Explanation A. Relaxing (i.e. reducing) the filters on a firewall is the removal of a safeguard.

Explanation B. Imposing strong password management is an example of a safeguard.

Explanation C. Deploying security guards is an example of a safeguard.

Explanation D. Enabling BIOS passwords is an example of a safeguard.

PrepLogic Question: 4293-707

35. Review Question p. 109

Answers: B

Explanation A. The top down approach to security management does provide for policy initiation, support, and direction from senior management.

Explanation B. The top down approach to security management does not provide for the assignment of responsibility to down-level administrators. Senior management is always ultimately responsible for the success or failure of the security policy and

resulting security solution.

Explanation C. The top down approach to security management does provide for development and implementation of standards, guidelines, and procedures from middle management.

Explanation D. The top down approach to security management does provide for development of security control configurations from operational management.

PrepLogic Question: 4293-708

36. Review Question p. 109

Answers: C

Explanation A. A strategic security plan is useful for 5 years with annual updates.

Explanation B. A strategic security plan defines overall mission, goals, and objectives.

Explanation C. A tactical security plan identifies, schedules, manages and controls the tasks necessary to accomplish resource activities.

Explanation D. A strategic security plan includes risk assessment.

PrepLogic Question: 4293-709

37. Review Question p. 109

Answers: D

Explanation A. A tactical security plan does include maintenance and technical support plans.

Explanation B. Strategic security plans include risk analysis.

Explanation C. Operational security plans define projects and completion milestones.

Explanation D. Tactical security plans include staffing and budgeting plans.

PrepLogic Question: 4293-710

38. Review Question p. 110

Answers: A

Explanation A. A tactical security plan, not an operational one, includes maintenance and technical support plans.

Explanation B. An operational security plan integrates the elements of other plans (i.e., strategic and tactical).

Explanation C. An operational security plan defines short term tasks necessary to the accomplishing of objectives.

Explanation D. An operational security plan prescribes a logical sequence of initiatives.

PrepLogic Question: 4293-711

39. Review Question p. 110

Answers: B

Explanation A. Safeguard evaluation is the goal of risk analysis, which is part of risk management. However, safeguard evaluation is not the goal of risk management.

Explanation B. The purpose of risk management is risk mitigation. However, even in the most successful implementation, there is always some level of risk.

Explanation C. Loss estimation is the goal of risk analysis, which is part of risk management. However, loss estimation is not the goal of risk management.

Explanation D. It is not possible to remove all risk without the organization ceasing to exist.

PrepLogic Question: 4293-712

40. Review Question p. 110

Answers: D

Explanation A. An objective of risk analysis is to identify risk.

Explanation B. An objective of risk analysis is to quantify the impact of each risk.

Explanation C. An objective of risk analysis is to evaluate the cost effectiveness of safeguards.

Explanation D. Risk analysis is used to compare safeguards, but it does not select the countermeasure to implement. Countermeasure selection is left to the decision makers; i.e., senior management or their delegated administrators.

PrepLogic Question: 4293-713

41. Review Question p. 111

Answers: C

Explanation A. Countermeasure selection is not a step in risk analysis. It is a task left up to senior management after risk analysis has taken place.

Explanation B. Cost/benefit analysis is the last step in risk analysis, other than reporting the findings to senior management. These are then used by senior management to select countermeasures.

Explanation C. Asset valuation is the first step in risk analysis. If assets have no value, there is no need to protect them.

Explanation D. Qualitative risk analysis is a method of risk analysis, but it is not the first step.

PrepLogic Question: 4293-714

42. Review Question p. 111

Answers: B

Explanation A. Private sector organizations are primarily concerned about data availability and integrity. Confidentiality is the primary concern of military organizations.

Explanation B. Private sector organizations are primarily concerned about data availability and integrity. Saying that availability and integrity are the primary concens does not means that confidentiality and other security aspects are of no concern, they are just no the top priorities of most private sector organizations.

Explanation C. Private sector organizations are primarily concerned about data availability and integrity. Non-repudiation is an aspect of accountability, and encryption is a security control used to ensure either confidentiality or integrity.

Explanation D. Private sector organizations are primarily concerned about data availability and integrity. Confidentiality is the primary concern of military organizations.

PrepLogic Question: 4293-715

43. Review Question p. 111

Answers: C

Explanation A. Private sector organizations are primarily concerned about data availability and integrity.

Explanation B. Non-repudiation is an aspect of accountability.

Explanation C. Confidentiality is the most important aspect of security to military organizations.

Explanation D. Private sector organizations are primarily concerned about data availability and integrity.

PrepLogic Question: 4293-716

44. Review Question p. 112

Answers: A

Explanation A. Tracking down intruders for prosecution is not a function or element of risk management, but it is possibly a factor in intrusion detection.

Explanation B. Analyzing the probability of attack occurrence is a mechanism used by risk management in an attempt to reduce risk to an acceptable level.

Explanation C. Predicting the impact of a breach is a mechanism used by risk management in an attempt to reduce risk to an acceptable level.

Explanation D. Evaluating safeguards is a mechanism used by risk management in an attempt to reduce risk to an acceptable level.

PrepLogic Question: 4293-717

45. Review Question p. 112

Answers: C

Explanation A. Human error is an example of a risk.

Explanation B. Equipment malfunction is an example of a risk.

Explanation C. Replacing human security guards with dogs is a change in a security access control, it is not an example of a risk.

Explanation D. Disgruntled insider is an example of a risk.

PrepLogic Question: 4293-718

46. Review Question p. 112

Answers: D

Explanation A. Risk is the possibility of something happening that will damage assets.

Explanation B. Risk is the possibility of something happening that will damage assets.

Explanation C. Risk is the possibility of something happening that will damage assets.

Explanation D. Risk is the possibility of something happening that will damage assets.

PrepLogic Question: 4293-719

47. Review Question p. 112

Answers: A

Explanation A. Risk will be totally eliminated only when the organization ceases to exist.

Explanation B. A security policy will reduce risk to an acceptable level when implemented properly, but there is always some level of risk.

Explanation C. Even with powered down systems, there is risk. One such risk is physical theft, while another is destruction via natural disaster.

Explanation D. Awareness training is important to reducing risk, but there is always some level of risk for an operating organization.

PrepLogic Question: 4293-720

48. Review Question p. 113

Answers: C

Explanation A. Risk analysis is used to determine whether safeguards are cost effective.

Explanation B. Risk analysis is used to determine whether safeguards are relevant.

Explanation C. No safeguard is exhaustive of all risks.

Explanation D. Risk analysis is used to determine whether safeguards are timely.

PrepLogic Question: 4293-721

49. Review Question p. 113

Answers: A

Explanation A. An effective safeguard from a risk analysis perspective is that the safeguard should cost less than the cost of the loss due to the risk.

Explanation B. An effective safeguard may not offer a complete solution for a specific risk.

Explanation C. Invisibility to the user is a desired characteristic of safeguards, but that is not a factor in risk analysis's evaluation of an effective safeguard.

Explanation D. Easy removal is a function of change and configuration management, it is not a factor in risk analysis's evaluation of an effective safeguard.

PrepLogic Question: 4293-722

50. Review Question p. 113

Answers: B

Explanation A. Senior management directs and supports risk analysis.

Explanation B. The Risk Assessment Team should be comprised of a representative from most or all departments, but not necessarily senior management.

Explanation C. Senior management acts appropriately upon the results.

Explanation D. Senior management reviews the outcome of the analysis.

PrepLogic Question: 4293-723

51. Review Question p. 114

Answers: A

Explanation A. Senior management is ultimately responsible and liable if the security perimeter of an organization is violated by an intruder and asset losses occur. Senior management is responsible for all aspects of security and is the primary decision maker. However, in most cases the implementation of security is delegated to lower levels of the authority hierarchy, such as the network or system administrators.

Explanation B. Senior management is ultimately responsible and liable if the security perimeter of an organization is violated by an intruder and asset losses occur. Network or system administrators are responsible for implementing the solutions selected by the security team and senior management.

Explanation C. Senior management is ultimately responsible and liable if the security perimeter of an organization is violated by an intruder and asset losses occur. Security

guards are responsible for carrying out their assigned duties and notifying the security team of any security breaches or attempts.

Explanation D. Senior management is ultimately responsible and liable if the security perimeter of an organization is violated by an intruder and asset losses occur. End users are responsible for completing their work tasks and complying with the security policy of the organization.

PrepLogic Question: 4293-724

52. Review Question p. 114

Answers: C

Explanation A. Confidentiality is one of the three fundamental principles of security included in the CIA triad, which includes Confidentiality, Integrity and Availability.

Explanation B. Integrity is one of the three fundamental principles of security included in the CIA triad, which includes Confidentiality, Integrity and Availability.

Explanation C. While accountability is an important part of IT security, it is not one of the three fundamental principles of security included in the CIA triad, namely, Confidentiality, Integrity and Availability.

Explanation D. Availability is one of the three fundamental principles of security included in the CIA triad, which includes Confidentiality, Integrity and Availability.

PrepLogic Question: 4293-726

53. Review Question p. 114

Answers: D

Explanation A. An example of sustaining confidentiality is preventing unauthorized access to a restricted document.

Explanation B. An example of sustaining integrity is preventing unauthorized alterations to a sensitive document.

Explanation C. Accountability is the result of the mechanisms of identification, authentication, authorization, access control, and auditing which is used to hold people responsible for their online activities.

Explanation D. The ability of a computer system to provide adequate capacity for predictable performance is an example of Availability.

PrepLogic Question: 4293-727

54. Review Question p. 115

Answers: A

Explanation A. Risk is the likelihood of a threat taking advantage of a vulnerability.

Explanation B. Exposure is an instance of being exposed to losses from a threat agent.

Explanation C. Mitigation is the removal or patching of a vulnerability.

Explanation D. An attack is the realization of a threat taking advantage of a vulnerability.

PrepLogic Question: 4293-728

55. Review Question p. 115

Answers: C

Explanation A. The creation of a clear and efficient reporting process is the responsibility of the security administration team.

Explanation B. Monitoring the security of an organization is the responsibility of the security administration team.

Explanation C. Approving the security policy is the responsibility of senior management, not the security administration team.

Explanation D. Identifying the strengths and weaknesses of a security solution is the responsibility of the security administration team.

PrepLogic Question: 4293-729

56. Review Question p. 115

Answers: D

Explanation A. Assigning classifications or values to data is a task that may be assigned to senior management, especially when they are an owner of a resource.

Explanation B. Dictating how information is to be protected is a task assigned to senior management. While the IT Security team may evaluate security and make recommendations, the decisions on what security to implement is the purview of senior management.

Explanation C. Delegating security responsibilities to data custodians is a task assigned to senior management.

Explanation D. Implementing security controls is the responsibility of the security administration team or data custodians, not senior management.

PrepLogic Question: 4293-730

57. Review Question p. 116

Answers: A

Explanation A. Executive is not a valid type of security control. The three valid types of security control are administrative, technical (or logical), and physical.

Explanation B. The three valid types of security control are administrative, technical (or logical), and physical.

Explanation C. The three valid types of security control are administrative, technical (or logical), and physical.

Explanation D. The three valid types of security control are administrative, technical (or logical), and physical.

PrepLogic Question: 4293-731

58. Review Question p. 116

Answers: B

Explanation A. Security guards are an example of a physical security control.

Explanation B. Policies are an example of an administrative security control.

Explanation C. Locks are an example of a physical security control.

Explanation D. Intrusion detection systems are examples of either physical or logical/technical security controls.

PrepLogic Question: 4293-732

59. Review Question p. 116

Answers: C

Explanation A. Standards are an example of an administrative security control.

Explanation B. Guidelines are an example of an administrative security control.

Explanation C. Identification is an example of a logical/technical security control.

Explanation D. Personnel screening are an example of an administrative security control.

PrepLogic Question: 4293-733

60. Review Question p. 117

Answers: D

Explanation A. Procedures are an example of an administrative security control.

Explanation B. Awareness training is an example of an administrative security control.

Explanation C. Perimeter lighting is an example of a physical security control.

Explanation D. Encryption is an example of a technical/logical security control.

PrepLogic Question: 4293-734

61. Review Question p. 117

Answers: A

Explanation A. Fire detection and suppression is an example of a physical security control.

Explanation B. Access control matrix is an example of a technical/logical security control.

Explanation C. Authorization is an example of a technical/logical security control.

Explanation D. Traffic filtering is an example of a technical/logical security control.

PrepLogic Question: 4293-735

62. Review Question p. 117

Answers: D

Explanation A. Evaluating the effect of a security solution on production is a valid activity of security management.

Explanation B. Managing access is a valid activity of security management.

Explanation C. Interacting with senior management about fine tuning the security policy is a valid activity of security management. However, only senior management has the authority to make decisions regarding altering security policy. Delegated authorities handling implementation and day-to-day management of the security policy only have the right to critique and make suggestions.

Explanation D. It is not a good security management practice to implement new security controls, especially in mission critical environments, before that control has been thoroughly tested.

PrepLogic Question: 4293-738

63. Review Question p. 118

Answers: A

Explanation A. The three fundamental principles of security are Confidentiality, Integrity, and Availability.

Explanation B. The three fundamental principles of security are Confidentiality, Integrity, and Availability. Confinement is not a security principle discussed in the CISSP CBK. Integrity is one of the CIA triad elements. Accessibility is a component of availability.

Explanation C. The three fundamental principles of security are Confidentiality, Integrity, and Availability. Corroboration and Interrogation are not security principles discussed in the CISSP CBK. Authorization is an important element in maintaining security to support the CIA triad.

Explanation D. The three fundamental principles of security are Confidentiality, Integrity, and Availability. Continuity and Intelligence are not security principles discussed in the CISSP CBK. Authentication is an important element in maintaining security to support the CIA triad.

PrepLogic Question: 4293-739

64. Review Question p. 118

Answers: B

Explanation A. Restricted access is an example of a security control that focuses on maintaining integrity.

Explanation B. Network traffic padding is an example of a security control that focuses on maintaining confidentiality.

Explanation C. Input validity verification is an example of a security control that focuses on maintaining integrity.

Explanation D. Backups are an example of a security control that focuses on maintaining availability.

PrepLogic Question: 4293-740

65. Review Question p. 118

Answers: C

Explanation A. Data encryption is an example of a security control that focuses on maintaining confidentiality.

Explanation B. Access control is an example of a security control that focuses on maintaining confidentiality.

Explanation C. Change restrictions is an example of a security control that focuses on maintaining integrity.

Explanation D. Personnel training is an example of a security control that focuses on maintaining confidentiality.

PrepLogic Question: 4293-741

66. Review Question p. 119

Answers: D

Explanation A. Trusted recovery is an example of a security control that focuses on maintaining availability and integrity. However, this is not the best selection for this specific question.

Explanation B. Denial of service attack protection is an example of a security control that focuses on maintaining availability.

Explanation C. Data classification is an example of a security control that focuses on maintaining confidentiality.

Explanation D. Hashing of data in transit is an example of a security control that focuses on maintaining integrity.

PrepLogic Question: 4293-742

67. Review Question p. 119

Answers: A

Explanation A. Network monitoring is an example of a security control that focuses on maintaining availability.

Explanation B. Managing alterations to data in a database is an example of a security control that focuses on maintaining integrity.

Explanation C. Validating input data to accepted data formats in a database is an example of a security control that focuses on maintaining integrity.

Explanation D. Preventing of unauthorized access to data in a database is an example of a security control that focuses on maintaining integrity.

PrepLogic Question: 4293-743

68. Review Question p. 119

Answers: B

Explanation A. Encrypted transport of data is an example of a security control that focuses on maintaining integrity.

Explanation B. Quick recovery from faults is an example of a security control that focuses on maintaining availability.

Explanation C. Fixed packet length transmissions is an example of a security control that focuses on maintaining confidentiality.

Explanation D. User awareness training of proper procedures in handling data is an example of a security control that focuses on maintaining confidentiality.

PrepLogic Question: 4293-744

69. Review Question p. 120

Answers: C

Explanation A. Secured state machines is an example of a security control that focuses on maintaining availability.

Explanation B. Avoiding single points of failure is an example of a security control that focuses on maintaining availability.

Explanation C. Implementing need to know access controls is an example of a security control that focuses on maintaining confidentiality.

Explanation D. Controlling the environmental characteristics is an example of a security control that focuses on maintaining availability.

PrepLogic Question: 4293-745

70. Review Question p. 120

Answers: D

Explanation A. Risk is the likelihood that a system will experience a security breach.

Explanation B. Exposure is an instance of being exposed to losses from a threat agent.

Explanation C. Threat is a potential danger to information or systems.

Explanation D. A vulnerability is a weakness or the absence of a safeguard that could be exploited.

PrepLogic Question: 4293-746

71. Review Question p. 120

Answers: A

Explanation A. Assigning all users access based on job descriptions is a valid form of security control and is thus not an example of a vulnerability.

Explanation B. Modems on clients is an example of a vulnerability.

Explanation C. Open ports is an example of a vulnerability.

Explanation D. Easy access to the server room is an example of a vulnerability.

PrepLogic Question: 4293-747

72. Review Question p. 120

Answers: B

Explanation A. Restricting access to authorized users is a safeguard, not a vulnerability.

Explanation B. Failing to enforce the password policy is an example of a vulnerability.

Explanation C. Filtering traffic at all communication borders to authorized users is a safeguard, not a vulnerability.

Explanation D. Implementing physical access restrictions to authorized users is a safeguard, not a vulnerability.

PrepLogic Question: 4293-748

73. Review Question p. 121

Answers: A

Explanation A. A quantitative risk analysis approach employs specific dollar values assigned to each risk.

Explanation B. A qualitative risk analysis approach employs opinions.

Explanation C. A qualitative risk analysis approach employs scenarios.

Explanation D. A qualitative risk analysis approach employs guesswork.

PrepLogic Question: 4293-749

74. Review Question p. 121

Answers: B

Explanation A. Quantitative analysis assigns real numbers and concrete probability percentages.

Explanation B. A purely quantitative risk analysis is not possible, since it is not possible to quantify all qualitative items.

Explanation C. Quantitative analysis can be automated.

Explanation D. Qualitative analysis involves significantly less time and effort than a quantitative approach.

PrepLogic Question: 4293-750

75. Review Question p. 121

Answers: C

Explanation A. Single loss expectancy is the amount of loss that would be incurred due to the compromise of an asset.

Explanation B. Exposure is the instance of being exposed to losses from a threat agent, not an exposure factor.

Explanation C. An exposure factor is the percentage of loss that a realized threat event would cause against a specific asset.

Explanation D. Risk is the likelihood that a system will experience a security breach.

PrepLogic Question: 4293-751

76. Review Question p. 122

Answers: D

Explanation A. Exposure factor multiplied by annualized rate of occurrence is not a valid equation in risk analysis.

Explanation B. Asset value multiplied by exposure factor is the equation for single loss expectancy.

Explanation C. Asset value multiplied by risk probability multiplied by safeguard benefit is not a valid equation in risk analysis.

Explanation D. The annualized loss expectancy can be calculated using asset value multiplied by exposure factor multiplied by annualized rate of occurrence. It can also be calculated using single loss expectancy multiplied by annualized rate of occurrence.

PrepLogic Question: 4293-752

77. Review Question p. 122

Answers: A

Explanation A. Single loss expectancy serves a dual purpose as an element in risk analysis cost/benefit calculations as well as a descriptive value in business impact analysis.

Explanation B. Exposure factor only has a single purpose in risk analysis.

Explanation C. Annualized rate of occurrence only has a single purpose in risk analysis.

Explanation D. Annualized loss expectancy only has a single purpose in risk analysis.

PrepLogic Question: 4293-753

78. Review Question p. 122

Answers: B

Explanation A. Reducing risk is an accepted response to the results of risk analysis.

Explanation B. Rejecting risk is not an accepted response to the results of risk analysis.

Explanation C. Assigning risk is an accepted response to the results of risk analysis.

Explanation D. Accepting risk is an accepted response to the results of risk analysis.

PrepLogic Question: 4293-754

79. Review Question p. 123

Answers: C

Explanation A. Reducing risk is implemented by deploying safeguards.

Explanation B. Rejecting risk is implemented by refusing to act on or ignoring the results of a risk analysis.

Explanation C. Assigning risk can be implemented by purchasing insurance against loss.

Explanation D. Accepting risk is implemented by understanding the possible loss due to a threat and accepting the consequences of not implementing safeguards.

PrepLogic Question: 4293-755

80. Review Question p. 123

Answers: D

Explanation A. Purchasing insurance is a valid example of assigning risk. Risk is assigned to the insurance company.

Explanation B. Implementing offsite backups is a valid example of assigning risk. Risk is assigned to the backup solution.

Explanation C. Crafting a disaster recovery plan is a valid example of assigning risk. Risk is assigned to the plan.

Explanation D. Delegating security policy implementation responsibilities is not a valid example of assigning risk. Risk remains the responsibility of senior management, and it cannot be delegated.

PrepLogic Question: 4293-756

81. Review Question p. 123

Answers: B

Explanation A. Need to know is usually not the most cost-effective security mechanism, but it is often necessary as part of a complete security solution.

Explanation B. Data classification is the security mechanism that is primarily responsible for implementing security controls that protect data in the most cost-effective manner.

Explanation C. Traffic filtering is usually not the most cost-effective security mechanism, but it is often necessary as part of a complete security solution.

Explanation D. Intrusion detection is usually not the most cost-effective security mechanism, but it is often necessary as part of a complete security solution.

PrepLogic Question: 4293-757

82. Review Question p. 124

Answers: D

Explanation A. The confidential data classification represents assets that, if disclosed, could serious impact an organization.

Explanation B. The private data classification represents assets that, if disclosed, could have an adverse affect.

Explanation C. The sensitive data classification represents assets that, if disclosed, may not have an adverse affect but must be protected from alteration.

Explanation D. The public data classification represents assets that, if disclosed, will not cause an adverse impact.

PrepLogic Question: 4293-758

83. Review Question p. 124

Answers: B

Explanation A. Focus group is a method used in qualitative risk analysis.

Explanation B. Quantitative, not qualitative, risk analysis can be automated with software.

Explanation C. One-on-one meeting is a method used in qualitative risk analysis.

Explanation D. Using checklists is a method used in qualitative risk analysis.

PrepLogic Question: 4293-759

84. Review Question p. 124

Answers: C

Explanation A. The value of a safeguard is calculated using the formula: (ALE before safeguard) - (ALE after implementing the safeguard) - (Annual cost of safeguard).

Explanation B. The value of a safeguard is calculated using the formula: (ALE before safeguard) - (ALE after implementing the safeguard) - (Annual cost of safeguard).

Explanation C. Residual risk is not used in the formula for calculating the value of a safeguard, instead it is the calculation of risk remaining after safeguards are implemented.

Explanation D. The value of a safeguard is calculated using the formula: (ALE before safeguard) - (ALE after implementing the safeguard) - (Annual cost of safeguard).

PrepLogic Question: 4293-760

85. Review Question p. 125

Answers: D

Explanation A. Risk can never be completely eliminated.

Explanation B. Additional safeguards always exist to reduce risk. Residual risk is what remains after selected safeguards are applied.

Explanation C. Risk is not absolutely quantifiable in concrete terms.

Explanation D. Residual risk is what remains after selected safeguards are applied (i.e., controls gap). Residual risk = total risk - controls gap.

PrepLogic Question: 4293-761

86. Review Question p. 125

Answers: A

Explanation A. Acceptable risk is the amount of risk an organization is willing to shoulder.

Explanation B. Residual risk includes acceptable risk, but not all residual risk is

acceptable. Residual risk is what remains after selected safeguards are applied. The residual risk may not be acceptable, so an organization may select additional safeguards or implement risk assignment.

Explanation C. Acceptable risk is not the collection of risks that cannot be addressed by safeguards, instead it is the risks that remain after available safeguards are not selected for implementation.

Explanation D. Acceptable risk is not defined by the exposure factor.

PrepLogic Question: 4293-762

87. Review Question p. 125

Answers: B

Explanation A. Procedures are compulsory, they outline detailed steps or tasks for implementing the security policy.

Explanation B. Guidelines are not compulsory, but describe the methodologies that should be employed for implementing the security policy.

Explanation C. Standards are compulsory, they outline the legal, industry, and best business practices of security.

Explanation D. Policies are compulsory, they define the overall outlook and focus for security within an organization.

PrepLogic Question: 4293-764

88. Review Question p. 125

Answers: D

Explanation A. Guidelines define recommended actions.

Explanation B. Guidelines are to be used when specific standards do not apply.

Explanation C. Guidelines serve as operational guides for IT staff.

Explanation D. Procedures detail step-by-step activities, items that guidelines do not address.

PrepLogic Question: 4293-765

89. Review Question p. 126

Answers: A

Explanation A. If a company does not practice due care and due diligence, managers can be held liable for negligence and held accountable for asset losses.

Explanation B. Properly implementing a security policy will help to ensure managers are not held directly liable. In most cases, security polices include risk mitigation and risk assignment to reduce personal risk.

Explanation C. Refusing to alter a security policy, especially if that change is seemed as a means to reduce security or increase risk, will not cause managers to be held personally responsible for losses.

Explanation D. Maintaining the business continuity plan is an important part of sustaining a security policy and thus requires due care and due diligence. But it is the responsibility of senior management, not the analysis team, to update and change plans and policies.

PrepLogic Question: 4293-766

90. Review Question p. 126

Answers: C

Explanation A. The military uses these five standard data classifications: top secret, secret, confidential, sensitive but unclassified, and unclassified.

Explanation B. The military uses these five standard data classifications: top secret, secret, confidential, sensitive but unclassified, and unclassified.

Explanation C. Private is a data classification used by the private sector (i.e. corporate business), not the military.

Explanation D. The military uses these five standard data classifications: top secret, secret, confidential, sensitive but unclassified, and unclassified.

PrepLogic Question: 4293-767

91. Review Question p. 126

Answers: D

Explanation A. Asset valuation is useful in the cost/benefit analysis of safeguards.

Explanation B. Asset valuation is useful in avoiding negligence by confirming to due care.

Explanation C. Asset valuation is useful as an insurance inventory.

Explanation D. Asset valuation is useful in assigning classifications to objects (i.e. assets), but is not directly useful in assigning classifications to subjects. Subject classification is often based on background checks and job descriptions.

PrepLogic Question: 4293-768

92. Review Question p. 127

Answers: A

Explanation A. The Delphi technique is a form of qualitative risk analysis that employs a group of people who reach a consensus through an anonymous means of voting and exchanging ideas.

Explanation B. Brainstorming is not anonymous, but is a public method of thinking outside of the box for new ideas.

Explanation C. Storyboarding is not anonymous and often ill-suited for reaching a consensus.

Explanation D. Surveys cannot be used to reach a consensus.

PrepLogic Question: 4293-769

93. Review Question p. 127

Answers: D

Explanation A. The value of an asset has little bearing on how much time is needed to perform any type of analysis.

Explanation B. The value of an asset has no bearing on whether a quantitative analysis is performed. A quantitative analysis is always performed.

Explanation C. The terms logical control and technical control are used to describe the same set of security controls.

Explanation D. The value of an asset helps to determine the relative strength and cost of the safeguard selected to protect it.

PrepLogic Question: 4293-770

94. Review Question p. 127

Answers: A

Explanation A. The cost to train personnel to employ the asset is not as relevant as the costs to develop, acquire, and maintain an asset when determining the cost of an asset. Training costs are often difficult to quantify since training on any specific asset is typically grouped in training regarding overall IT interaction. While this answer is technically correct, it is the least correct answer of those offered.

Explanation B. The cost to develop is an element in determining the cost of an asset.

Explanation C. The cost to acquire is an element in determining the cost of an asset.

Explanation D. The cost to maintain is an element in determining the cost of an asset.

PrepLogic Question: 4293-771

95. Review Question p. 128

Answers: B

Explanation A. The cost to protect is an element in determining the cost of an asset.

Explanation B. Amount in GB of hard drive storage requirements for a single asset is not as relevant as the cost for overall storage and maintenance in the determination of the cost of an asset. While this answer is technically correct, it is the least correct answer of those offered.

Explanation C. The value to owners and users is an element in determining the cost of an asset.

Explanation D. The value to competitors is an element in determining the cost of an asset.

PrepLogic Question: 4293-772

96. Review Question p. 128

Answers: C

Explanation A. The cost to replace a given asset is an element in determining the cost of that asset.

Explanation B. The cost in productivity if the asset becomes unavailable is an element in determining the cost of that asset.

Explanation C. The file formats used by the asset are typically not an element in determining the cost of an asset. This a compatiblity and usibility issue, not a cost issue.

Explanation D. Any liability incurred if asset is compromised is an element in determining the cost of an asset.

PrepLogic Question: 4293-773

Explanations: Chapter 6

1. Review Question p. 129

Answers: C

Explanation A. The U.S. Privacy Act of 1974 requires that federal agencies protect information about private individuals that is stored in government databases.

Explanation B. The Paperwork Reduction Act of 1995 requires Federal Agencies to assess the security of their non-classified information systems, to provide a risk assessment, and to report the security needs of its systems.

Explanation C. The U.S. National Information Infrastructure Protection Act of 1996 addresses confidentiality, integrity, and availability for both data and systems and encourages other countries to adopt the same framework.

Explanation D. The Gramm Leach Bliley Act of 1999 requires that banks give customers the option to prohibit the distribution of personal information with non-affiliated third parties.

PrepLogic Question: 4293-400

2. Review Question p. 129

Answers: D

Explanation A. The U.S. Privacy Act of 1974 requires that federal agencies protect information about private individuals that is stored in government databases.

Explanation B. The U.S. Computer Fraud and Privacy Act of 1986 defines the use of a federal interest computer in a crime as a federal offense and reduces the minimum damage required to declare a crime a federal offence.

Explanation C. The U.S. National Information Infrastructure Protection Act of 1996 addresses confidentiality, integrity, and availability for both data and systems and encourages other countries to adopt the same framework.

Explanation D. The Paperwork Reduction Act of 1995 requires Federal Agencies to assess the security of their non-classified information systems, to provide a risk assessment, and to report the security needs of its systems.

PrepLogic Question: 4293-401

3. Review Question p. 129

Answers: A

Explanation A. The U.S. Computer Fraud and Privacy Act of 1986 defines the trafficking in computer passwords as a federal crime if that activity affects interstate or foreign commerce or permits unauthorized access to government computers.

Explanation B. The Paperwork Reduction Act of 1995 requires Federal Agencies to assess the security of their non-classified information systems, to provide a risk assessment, and to report the security needs of its systems.

Explanation C. The U.S. National Information Infrastructure Protection Act of 1996 addresses confidentiality, integrity, and availability for both data and systems and encourages other countries to adopt the same framework.

Explanation D. The Gramm Leach Bliley Act of 1999 requires that banks give customers the option to prohibit the distribution of personal information with non-affiliated third parties.

PrepLogic Question: 4293-402

4. Review Question p. 130

Answers: C

Explanation A. A trademark is a form of intellectual property law that protects or establishes a word, name, symbol, etc. as an identifying mark for an organization or a product.

Explanation B. A patent is a form of intellectual property law that provides the owner with 17 years of exclusive use rights.

Explanation C. A copyright is a form of intellectual property law that protects original works of authorship for 50+ years.

Explanation D. A trade secret is a type of data defined by intellectual property law that is confidential and proprietary to a specific organization.

PrepLogic Question: 4293-403

5. Review Question p. 130

Answers: A

Explanation A. A trademark is a form of intellectual property law that protects or establishes a word, name, symbol, etc. as an identifying mark for an organization or a product.

Explanation B. A patent is a form of intellectual property law that provides the owner with 17 years of exclusive use rights.

Explanation C. A copyright is a form of intellectual property law that protects original works of authorship for 50+ years.

Explanation D. A trade secret is a type of data defined by intellectual property law that is confidential and proprietary to a specific organization.

PrepLogic Question: 4293-404

6. Review Question p. 130

Answers: B

Explanation A. The U.S. Privacy Act of 1974 is not an amendment to the U.S. Computer Fraud and Privacy Act of 1986. The U.S. Privacy Act of 1974 requires that federal agencies protect information about private individuals that is stored in government databases.

Explanation B. The U.S. National Information Infrastructure Protection Act of 1996 is an amendment to the U.S. Computer Fraud and Privacy Act of 1986. The U.S. National Information Infrastructure Protection Act of 1996 addresses confidentiality, integrity, and availability for both data and systems and encourages other countries to adopt the same framework.

Explanation C. The Paperwork Reduction Act of 1995 is not an amendment to the U.S. Computer Fraud and Privacy Act of 1986. The Paperwork Reduction Act of 1995 requires Federal Agencies to assess the security of their non-classified information systems, to provide a risk assessment, and to report the security needs of its systems.

Explanation D. The Gramm Leach Bliley Act of 1999 is not an amendment to the U.S. Computer Fraud and Privacy Act of 1986. The Gramm Leach Bliley Act of 1999 requires that banks give customers the option to prohibit the distribution of personal information with non-affiliated third parties.

PrepLogic Question: 4293-405

7. Review Question p. 131

Answers: D

Explanation A. A trademark is a form of intellectual property law that protects or establishes a word, name, symbol, etc. as an identifying mark for an organization or a product.

Explanation B. A patent is a form of intellectual property law that provides the owner with 17 years of exclusive use rights.

Explanation C. A copyright is a form of intellectual property law that protects original works of authorship for 50+ years.

Explanation D. A trade secret is a type of data defined by intellectual property law that is confidential and proprietary to a specific organization.

PrepLogic Question: 4293-406

8. Review Question p. 131

Answers: B

Explanation A. A trademark is a form of intellectual property law that protects or establishes a word, name, symbol, etc. as an identifying mark for an organization or a product.

Explanation B. A patent is a form of intellectual property law that provides the owner with 17 years of exclusive use rights.

Explanation C. A copyright is a form of intellectual property law that protects original works of authorship for 50+ years.

Explanation D. A trade secret is a type of data defined by intellectual property law that is confidential and proprietary to a specific organization.

PrepLogic Question: 4293-407

9. Review Question p. 131

Answers: C

Explanation A. European privacy laws are more restrictive than those of the United States.

Explanation B. European privacy laws are more restrictive than those of the United States.

Explanation C. European privacy laws are more restrictive than those of the United States.

Explanation D. European privacy laws are more restrictive than those of the United States. European privacy laws and United States privacy laws are, however, similar.

PrepLogic Question: 4293-408

10. Review Question p. 132

Answers: D

Explanation A. European privacy laws do require that data be collected in accordance with the law.

Explanation B. European privacy laws do prevent collected information from being disclosed to others without the consent of the individual.

Explanation C. European privacy laws do require that records kept about an individual be accurate and timely.

Explanation D. European privacy laws do not require consent for the collection of private data, just the distribution of such data.

PrepLogic Question: 4293-409

11. Review Question p. 132

Answers: A

Explanation A. The European privacy laws require that data be retained for a limited and reasonable period of time defined at the time of gathering the data.

Explanation B. The European privacy laws allow individuals to correct errors in the data collected about them.

Explanation C. The European privacy laws require that collected data be used only for the original purpose for which it was collected.

Explanation D. The European privacy laws state that individuals are entitled to a report detailing the information retained about them.

PrepLogic Question: 4293-410

12. Review Question p. 132

Answers: B

Explanation A. It is a common problem that too much access is granted to personal health and medical data.

Explanation B. Most systems do not have a high level of granular access control and thus they are vulnerable to security violations. So, the presence of strong security is not

a common problem with the storage of personal health and medical data.

Explanation C. It is a common problem that Internet connectivity increases vulnerabilities to integrity and privacy of data.

Explanation D. It is a common problem that the misuse of personal medical data can have a significant negative impact on the public perception of an organization.

PrepLogic Question: 4293-411

13. Review Question p. 133

Answers: C

Explanation A. Health care organizations should comply with the privacy principle of granting individuals the means to monitor and correct the data collected about them.

Explanation B. Health care organizations should comply with the privacy principle of restricting the uses of data to those outlined when the data was originally collected.

Explanation C. Health care organizations should comply with the privacy principle of making sure that databases containing personal health and medical information about individuals is kept secret except for those uses outlined when the data was originally collected.

Explanation D. Health care organizations should comply with the privacy principle of providing adequate protection for gathered data.

PrepLogic Question: 4293-412

14. Review Question p. 133

Answers: D

Explanation A. HIPPA establishes the rights for individuals who are subjects of individually identifiable health information.

Explanation B. HIPAA defines uses and disclosures of individually identifiable health information that should be authorized or required.

Explanation C. HIPPA requires an information security officer.

Explanation D. HIPAA does not provide specifics for a protecting solution, rather it outlines a framework to provide protecting for individually identifiable health information.

PrepLogic Question: 4293-413

15. Review Question p. 133

Answers: A

Explanation A. The same monitoring procedures and practices should be applied to senior management as to end users. Using different levels of monitoring for different users is not a recommended practice for the monitoring of e-mail on a company network.

Explanation B. Informing all users that monitoring is occurring via a clearly visible and frequent banner or similar warning system is a recommended practice for the monitoring of e-mail on a company network.

Explanation C. Monitoring should be performed in a lawful and consistent manner is a recommended practice for the monitoring of e-mail on a company network. The same monitoring procedures and practices should be applied to senior management as to end users.

Explanation D. Detailing who will be accessing and viewing the archived data and for how long the data will be retained is a recommended practice for the monitoring of e-mail on a company network.

PrepLogic Question: 4293-414

16. Review Question p. 134

Answers: B

Explanation A. The U.S. Federal Sentencing Guidelines do not provide a punishment of imprisonment.

Explanation B. The U.S. Federal Sentencing Guidelines provide for a punishment of a fine of up to $290 million.

Explanation C. The U.S. Federal Sentencing Guidelines do not provide a punishment of confiscation of assets.

Explanation D. The U.S. Federal Sentencing Guidelines do not provide a punishment of seizure of public stock offerings.

PrepLogic Question: 4293-415

17. Review Question p. 134

Answers: C

Explanation A. Often the lack of due diligence is used to further prosecute a suspect, but it does not relate directly to proving negligence.

Explanation B. Often the failure to comply with recognized standards is used to further prosecute a suspect, but it does not relate directly to proving negligence.

Explanation C. Negligence is proven in court by demonstrating a legally recognized obligation.

Explanation D. Often proximate causation that results in loss or injury is used to further prosecute a suspect, but it does not relate directly to proving negligence.

PrepLogic Question: 4293-416

18. Review Question p. 134

Answers: D

Explanation A. Physical access controls are one of many aspects of visible proof that an organization is practicing due care in regards to security.

Explanation B. Hardware backups are one of many aspects of visible proof that an organization is practicing due care in regards to security.

Explanation C. Security awareness training is one of many aspects of visible proof that an organization is practicing due care in regards to security.

Explanation D. Use of plenum cabling is often mandated by building code for proper fire rating; however, it is not an aspect of due care.

PrepLogic Question: 4293-417

19. Review Question p. 135

Answers: B

Explanation A. A well-organized and legitimate monitoring solution that records all e-mail on a business network does provide a means to track down violations of security policy.

Explanation B. A well-organized and legitimate monitoring solution that records all e-mail on a business network does not provide a guarantee of personal privacy.

Explanation C. A well-organized and legitimate monitoring solution that records all e-mail on a business network does clearly inform all users of the monitoring activity.

Explanation D. A well-organized and legitimate monitoring solution that records all e-mail on a business network does make employees aware of the acceptable use of e-mail.

PrepLogic Question: 4293-418

20. Review Question p. 135

Answers: C

Explanation A. The U.S. Computer Fraud and Privacy Act of 1986 defines the trafficking in computer passwords as a federal crime if that activity affects interstate or foreign commerce or permits unauthorized access to government computers.

Explanation B. The Paperwork Reduction Act of 1995 requires Federal Agencies to assess the security of their non-classified information systems, to provide a risk assessment, and to report the security needs of its systems.

Explanation C. The 1991 U.S. Federal Sentencing Guidelines treats the unauthorized possession of information, without the intent to profit from it, as a crime.

Explanation D. The Gramm Leach Bliley Act of 1999 requires that banks give customers the option to prohibit the distribution of personal information with non-affiliated third parties.

PrepLogic Question: 4293-419

21. Review Question p. 135

Answers: D

Explanation A. The 1991 U.S. Federal Sentencing Guidelines treats the unauthorized possession of information, without the intent to profit from it, as a crime.

Explanation B. The 1991 U.S. Federal Sentencing Guidelines applies to both individuals and organizations.

Explanation C. The 1991 U.S. Federal Sentencing Guidelines makes the degree of punishment a function of the extent to which the organization has demonstrated due diligence in establishing security.

Explanation D. The U.S. Computer Fraud and Abuse Act, not the 1991 U.S. Federal Sentencing Guidelines, makes the use of information that causes $1,000 or more in damages, or which impairs medical treatment, a federal crime.

PrepLogic Question: 4293-420

22. Review Question p. 136

Answers: A

Explanation A. The 1991 U.S. Federal Sentencing Guidelines invokes the prudent man rule that requires that senior management of an organization perform their duties with the same care that any normal person would exercise in the same circumstances.

Explanation B. The principle of least privilege states that users should only have sufficient privileges to perform their work tasks. It is not associated with the 1991 U.S. Federal Sentencing Guidelines.

Explanation C. The tenant of due care is that senior management should show that efforts were made to design a security solution. This is not what the 1991 U.S. Federal Sentencing Guidelines rely upon.

Explanation D. Separation of duties is the access control mechanism that is used to divide up privileged activities among several users so no single person has complete and total access to a system. It is not associated with the 1991 U.S. Federal Sentencing Guidelines.

PrepLogic Question: 4293-421

23. Review Question p. 136

Answers: A

Explanation A. The speed of networking devices is not evidence of due care.

Explanation B. Telecommunications encryption is one of many aspects of visible proof that an organization is practicing due care in regards to security.

Explanation C. Disaster recovery plans are one of many aspects of visible proof that an organization is practicing due care in regards to security.

Explanation D. The development of formalized security infrastructure documentation is one of many aspects of visible proof that an organization is practicing due care in regards to security.

PrepLogic Question: 4293-422

24. Review Question p. 136

Answers: B

Explanation A. CIRT may be responsible for managing and minimizing risks to an organization that can include managing public relations.

Explanation B. CIRT is not responsible for designing security policies.

Explanation C. CIRT is responsible for investigating intrusions.

Explanation D. CIRT is responsible for reporting incidents.

PrepLogic Question: 4293-423

25. Review Question p. 137

Answers: D

Explanation A. Espionage is a crime.

Explanation B. Fraud is a crime.

Explanation C. Piracy is a crime.

Explanation D. Resource waste is an inappropriate activity, acces abuse, and a violation of company policy, but not an actual crime.

PrepLogic Question: 4293-425

26. Review Question p. 137

Answers: B

Explanation A. Evidence must be reliable.

Explanation B. Evidence need not be sufficient.

Explanation C. Evidence must be relevant.

Explanation D. Evidence must be permissible.

PrepLogic Question: 4293-426

27. Review Question p. 137

Answers: C

Explanation A. Writing on printouts is a valid means to label evidence.

Explanation B. Recording serial numbers is a valid means to label evidence.

Explanation C. Writing a file to the hard drive may alter the evidence and therefore is an invalid means to label evidence.

Explanation D. Photographing a monitor is a valid means to collect/label data.

PrepLogic Question: 4293-427

28. Review Question p. 138

Answers: D

Explanation A. Hearsay evidence is not based on personal, first hand knowledge of the witness, but was obtained from another source.

Explanation B. Circumstantial evidence is merely inference of information from other intermediate, relevant facts.

Explanation C. Secondary evidence is a copy of evidence or oral description of its contents.

Explanation D. Direct evidence proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses.

PrepLogic Question: 4293-428

29. Review Question p. 138

Answers: C

Explanation A. The (ISC)^2 code of ethics does require that CISSP candidates conduct themselves with high standards of moral, ethical, and legal behavior.

Explanation B. The (ISC)^2 code of ethics does require that CISSP candidates not commit any unlawful acts.

Explanation C. The actual act of authoring malicious code is not a violation of the (ISC)^2 code of ethics. However, allowing that malicious code to affect systems is a violation.

Explanation D. The (ISC)^2 code of ethics does require that CISSP candidates report any unlawful activities they discover.

PrepLogic Question: 4293-429

30. Review Question p. 138

Answers: D

Explanation A. The ISC2's CISSP code of ethics does support that CISSP candidates promote understanding of security.

Explanation B. The ISC2's CISSP code of ethics does support that CISSP candidates provide competent service.

Explanation C. The ISC2's CISSP code of ethics does support that CISSP candidates do not disclose confidential information from clients.

Explanation D. The ISC2's CISSP code of ethics indicates that knowledge of crimes should be appropriately reported. Appropriately reporting crimes would be to inform the management of the organization and/or law enforcement. Informing ISC2 is not appropriate.

PrepLogic Question: 4293-430

31. Review Question p. 139

Answers: A

Explanation A. It is not a violation of computer ethics to work overtime.

Explanation B. It is a violation of computer ethics to browser files from other people unless your work tasks specifically require you to do so.

Explanation C. It is a violation of computer ethics to use proprietary software without compensation (i.e. commercial software without purchasing it).

Explanation D. It is a violation of computer ethics to use another's intellectual property without acknowledgement (i.e., plagiarizing).

PrepLogic Question: 4293-431

32. Review Question p. 139

Answers: B

Explanation A. Seeking to gain unauthorized access to resources is an unacceptable and inappropriate activity as defined by the Internet Activities Board of Ethics and the Internet.

Explanation B. Conducting commercial activities over the Internet is not defined as an unacceptable and inappropriate activity as defined by the Internet Activities Board of Ethics and the Internet.

Explanation C. Destroying the integrity of computer stored information is an unacceptable and inappropriate activity as defined by the Internet Activities Board of Ethics and the Internet.

Explanation D. Wasting resources is an unacceptable and inappropriate activity as defined by the Internet Activities Board of Ethics and the Internet.

PrepLogic Question: 4293-432

33. Review Question p. 139

Answers: A

Explanation A. The U.S. Privacy Act of 1974 requires that federal agencies protect information about private individuals that is stored in government databases.

Explanation B. The U.S. Computer Fraud and Privacy Act of 1986 defines the use of a federal interest computer in a crime as a federal offense and reduces the minimum damage required to declare a crime a federal offence.

Explanation C. The Paperwork Reduction Act of 1995 requires Federal Agencies to assess the security of their non-classified information systems, to provide a risk assessment, and to report the security needs of its systems.

Explanation D. The Gramm Leach Bliley Act of 1999 requires that banks give customers the option to prohibit the distribution of personal information with non-affiliated third parties.

PrepLogic Question: 4293-433

34. Review Question p. 140

Answers: B

Explanation A. The U.S. Privacy Act of 1974 requires that federal agencies protect information about private individuals that is stored in government databases.

Explanation B. The U.S. Computer Fraud and Privacy Act of 1986 defines the use of a federal interest computer in a crime as a federal offense and reduces the minimum damage required to declare a crime a federal offence.

Explanation C. The U.S. National Information Infrastructure Protection Act of 1996 addresses confidentiality, integrity, and availability for both data and systems and encourages other countries to adopt the same framework.

Explanation D. The Gramm Leach Bliley Act of 1999 requires that banks give

customers the option to prohibit the distribution of personal information with non-affiliated third parties.

PrepLogic Question: 4293-434

35. Review Question p. 140

Answers: D

Explanation A. The U.S. Department of Health, Education, and Welfare Code of Fair Information Practices requires that people be able to discover what information is retained about them and for what purposes it is used, not that they can remove any data item from the database.

Explanation B. The U.S. Department of Health, Education, and Welfare Code of Fair Information Practices requires that organizations ensure that personal data is not misused.

Explanation C. The U.S. Department of Health, Education, and Welfare Code of Fair Information Practices requires that data be reliable, but not necessarily timely.

Explanation D. The U.S. Department of Health, Education, and Welfare Code of Fair Information Practices requires that the existence of systems that maintain records of a personal nature cannot remain secret.

PrepLogic Question: 4293-436

36. Review Question p. 140

Answers: A

Explanation A. Illegally transferring money from one bank account to another over the Internet is a crime committed using a computer.

Explanation B. Erasing a hard drive using a degaussing magnet can be a crime committed against a computer.

Explanation C. Setting fire to a building can be a crime against a computer.

Explanation D. Theft of a notebook from an airport security checkpoint is a crime against a computer.

PrepLogic Question: 4293-437

37. Review Question p. 141

Answers: B

Explanation A. Social engineering can be a computer crime.

Explanation B. Surfing pornographic Web sites is inappropriate in most business environments and often grounds for termination, but it is not a crime.

Explanation C. Password sniffing is a computer crime.

Explanation D. Spoofing IP addresses is a computer crime.

PrepLogic Question: 4293-438

38. Review Question p. 141

Answers: C

Explanation A. Intercepting wireless network communications is a crime committed using a computer.

Explanation B. Installing software that has not been properly purchased is a crime committed using a computer.

Explanation C. Causing a blackout of the local power grid by damaging a power station can be considered a crime against a computer instead of a crime committed with a computer.

Explanation D. Testing an intrusion script against a competitor's Web site is a crime committed using a computer.

PrepLogic Question: 4293-439

39. Review Question p. 141

Answers: D

Explanation A. Spoofing, social engineering, and masquerading are all computer crimes where someone attempts to impersonate or assume the identity of someone else in order to gain access, control, or cause destruction.

Explanation B. Spoofing, social engineering, and masquerading are all computer crimes where someone attempts to impersonate or assume the identity of someone else in order to gain access, control, or cause destruction.

Explanation C. Spoofing, social engineering, and masquerading are all computer crimes where someone attempts to impersonate or assume the identity of someone else in order to gain access, control, or cause destruction.

Explanation D. Data diddling is the alteration of data, not the use of information to pretend to be something or someone else.

PrepLogic Question: 4293-440

40. Review Question p. 141

Answers: B

Explanation A. Espionage can be a computer crime.

Explanation B. While data may certainly be stolen, "theft by taking" as defined by the legal code is not, in and of itself, a computer crime.

Explanation C. Fraud can be a computer crime.

Explanation D. Embezzlement can be a computer crime.

PrepLogic Question: 4293-442

41. Review Question p. 142

Answers: C

Explanation A. Statutory law, or the United States code, is a form of law found in the US that can be used in court.

Explanation B. Administrative law, or the code of federal regulations, is a form of law found in the US that can be used in court.

Explanation C. Islamic law is a religious law that is found in some areas of the US, but it is not used in government courts.

Explanation D. Common law, case reports, and case digests is a form of law found in the US that can be used in court.

PrepLogic Question: 4293-443

42. Review Question p. 142

Answers: D

Explanation A. Statutory law is also known as the United States code, not the code of federal regulations.

Explanation B. Common law is also known as case reports or case digests, not the code of federal regulations.

Explanation C. Case digests are also known as common law or case reports, not the code of federal regulations.

Explanation D. Administrative laws are also known as the code of federal regulations.

PrepLogic Question: 4293-444

43. Review Question p. 142

Answers: A

Explanation A. Civil law is a category of common law that allows for financial penalties but not imprisonment.

Explanation B. Criminal law is a category of common law, but it does allow for both financial penalties and imprisonment.

Explanation C. Administrative law is a category of common law, but it does allow for both financial penalties and imprisonment.

Explanation D. Regulatory law is a category of common law, but it does allow for both financial penalties and imprisonment.

PrepLogic Question: 4293-445

44. Review Question p. 143

Answers: B

Explanation A. Civil law focuses on wrongs inflicted against an individual or organization.

Explanation B. Criminal law focuses on the violation of government laws focused on the protection of the public.

Explanation C. Administrative law (which is the same as regulatory law) focuses on enforcing standards of performance and conduct expected by the government.

Explanation D. Regulatory law (which is the same as administrative law) focuses on enforcing standards of performance and conduct expected by the government.

PrepLogic Question: 4293-446

45. Review Question p. 143

Answers: C

Explanation A. Administrative law, which is the same as regulatory law, is not known as tort.

Explanation B. Criminal law is not known as tort.

Explanation C. Civil law is also known as tort.

Explanation D. Regulatory law, which is the same as administrative law, is not known as tort.

PrepLogic Question: 4293-447

46. Review Question p. 143

Answers: D

Explanation A. The U.S. Privacy Act of 1974 requires that federal agencies protect information about private individuals that is stored in government databases.

Explanation B. The U.S. Computer Fraud and Privacy Act of 1986 defines the use of a federal interest computer in a crime as a federal offense and reduces the minimum damage required to declare a crime a federal offence.

Explanation C. The U.S. National Information Infrastructure Protection Act of 1996 addresses confidentiality, integrity, and availability for both data and systems and encourages other countries to adopt the same framework.

Explanation D. The Gramm Leach Bliley Act of 1999 requires that banks give customers the option to prohibit the distribution of personal information with non-affiliated third parties.

PrepLogic Question: 4293-448

47. Review Question p. 144

Answers: A

Explanation A. Maintaining individual privacy is often not possible when an investigation is being conducted. Thus, maintaining individual privacy is not an example of a negative consequence. In reality, individual privacy is often violated during an investigation.

Explanation B. If the subject becomes aware of the investigation, it is possible and likely that the subject will commit retaliatory acts. This is a negative consequence of an investigation.

Explanation C. Negative publicity resulting in loss of public confidence is a negative consequence of an investigation.

Explanation D. The interruption of business processes is a negative consequence of an investigation.

PrepLogic Question: 4293-450

48. Review Question p. 144

Answers: C

Explanation A. The FBI does, indeed, have jurisdiction over computer crimes in the U.S. Local law enforcement may be involved in some aspect of the investigation, such as assisting on arrests, but local agencies wouldn't have the jurisdiction to prosecute.

Explanation B. The Secret Service does have jurisdiction over computer crimes in the U.S.. The National Institute of Standards and Technology (NIST) is primarily a research laboratory responsibile for industry standards, technology and science in measurement. It's not involved in the legal process at all (except, perhaps, to provide expert witnesses).

Explanation C. The FBI and the Secret Service have jurisdiction over computer crimes in the U.S.

Explanation D. The Central Intelligence Agency (CIA) and the National Security Agency (NSA) are both responsible for protecting the US against foreign attacks. The CIA gathers intelligence that might, in some cases, be used in the prosecution of computer crimes, but doesn't have jurisdiction within in the country. The NSA provides cryptanalysis, signals intelligence and protects the nation's information systems from similar agencies.

PrepLogic Question: 4293-451

49. Review Question p. 144

Answers: D

Explanation A. Generating post incident reports is not the most important activity to perform once a computer crime is suspected. In fact, unless those reports were generated as a normal business task, they shouldn't be generated at all.

Explanation B. Triggering the emergency response team is not the most important activity to perform once a computer crime is suspected. Not all incidents require emergency response and doing so may alert the suspect.

Explanation C. Restoring non-critical business processes is not the most important

activity to perform once a computer crime is suspected.

Explanation D. The most important act once a computer crime is suspected is to not alert the suspect.

PrepLogic Question: 4293-452

50. Review Question p. 145

Answers: C

Explanation A. There is usually a compressed time frame within which to conduct the investigation when a computer crime incident is involved.

Explanation B. The investigation of a computer crime incident may interfere with the normal operations of business.

Explanation C. Evidence in a computer crime incident is usually intangible.

Explanation D. Evidence of a computer crime incident may be co-mingled with data needed for normal business activities.

PrepLogic Question: 4293-455

51. Review Question p. 145

Answers: D

Explanation A. Evidence of a computer crime incident can be difficult to gather.

Explanation B. Evidence of a computer crime incident may be damaged or altered by the normal operations of business.

Explanation C. Jurisdictional responsibility may be cloudy when investigating a computer crime incident.

Explanation D. In many instances, evidence gathering for a computer crime incident requires an expert or specialist.

PrepLogic Question: 4293-456

52. Review Question p. 145

Answers: D

Explanation A. In an interview, the goal is to gather information as well as to discern the subject's credibility.

Explanation B. In an interview, a subject becomes a witness.

Explanation C. In an interrogation, a witness becomes a suspect.

Explanation D. This is a false statement. In an interrogation, a witness becomes a suspect.

PrepLogic Question: 4293-458

53. Review Question p. 146

Answers: A

Explanation A. Whether the evidence is relevant is not an element of the chain of custody.

Explanation B. The time and location that the evidence was gathered is an element of the chain of custody.

Explanation C. Who discovered the evidence is an element of the chain of custody.

Explanation D. Who maintained possession of the evidence is an element of the chain of custody.

PrepLogic Question: 4293-459

54. Review Question p. 146

Answers: C

Explanation A. The correct order is discovery, protection, recording, collection, identification, preservation, transportation, presentation, and return.

Explanation B. The correct order is discovery, protection, recording, collection, identification, preservation, transportation, presentation, and return.

Explanation C. The correct order is discovery, protection, recording, collection, identification, preservation, transportation, presentation, and return.

Explanation D. The correct order is discovery, protection, recording, collection, identification, preservation, transportation, presentation, and return.

PrepLogic Question: 4293-460

55. Review Question p. 146

Answers: D

Explanation A. Evidence must be relevant to be presented in court.

Explanation B. Evidence must be legally permissible to be presented in court.

Explanation C. Evidence must be reliable to be presented in court.

Explanation D. Evidence need not be sufficient to be presented in court.

PrepLogic Question: 4293-461

56. Review Question p. 147

Answers: A

Explanation A. Whether evidence has been altered is not an aspect of relevance but an aspect of reliability.

Explanation B. An aspect of the relevance of evidence is that it must show that a crime has been committed.

Explanation C. An aspect of the relevance of evidence is that it must show some aspect of the perpetrator's motives.

Explanation D. An aspect of the relevance of evidence is that it must verify or demonstrate what has occurred.

PrepLogic Question: 4293-462

57. Review Question p. 147

Answers: D

Explanation A. Evidence made during the normal process of business activity is an exception to the hearsay rule.

Explanation B. Evidence in the custody of the witness on a regular basis is an exception to the hearsay rule.

Explanation C. Evidence made at or near the time of the incident being investigated is an exception to the hearsay rule.

Explanation D. Evidence is inadmissible as hearsay if the documents are generated after the incident for the sole purpose of producing evidence about the incident.

PrepLogic Question: 4293-463

58. Review Question p. 147

Answers: B

Explanation A. Best evidence is the original or primary evidence.

Explanation B. Direct evidence is the oral testimony of a witness.

Explanation C. Hearsay evidence is not based on first-hand knowledge but obtained from another source.

Explanation D. Conclusive evidence is incontrovertible evidence, such as DNA.

PrepLogic Question: 4293-464

59. Review Question p. 148

Answers: C

Explanation A. Best evidence is generally admissible in court.

Explanation B. Direct evidence is generally admissible in court.

Explanation C. Hearsay evidence is generally inadmissible in court.

Explanation D. Expert opinion is generally admissible in court.

PrepLogic Question: 4293-465

60. Review Question p. 148

Answers: B

Explanation A. Writing on paper printouts with permanent markers is considered a valid means of identification.

Explanation B. Writing to a storage media in any way alters that media and can destroy evidence. This is not a valid means of identifying evidence.

Explanation C. Recording the serial numbers from devices is considered a valid means of identification.

Explanation D. Placing evidence in sealed and marked containers is a valid means of identification.

PrepLogic Question: 4293-466

61. Review Question p. 148

Answers: C

Explanation A. Avoiding smoke and dust is a valid action to take when preserving evidence.

Explanation B. Write protecting media is a valid action to take when preserving evidence.

Explanation C. Storing electronic media in plastic bags is not a valid action since these bags can cause static discharge and condensation. Paper, cardboard, or special anti-static bags should be used.

Explanation D. Avoiding magnetic fields is a valid action to take when preserving evidence.

PrepLogic Question: 4293-467

62. Review Question p. 149

Answers: D

Explanation A. Running tripwire on a system will provide no useful function, plus tripwire will alter the storage device by creating a database file to store the message digests it creates. This is not a means by which to preserve evidence.

Explanation B. Encrypting the storage device alters it and therefore is not a means to preserve evidence.

Explanation C. Defragmenting a storage device alters it and therefore is not a means to preserve evidence.

Explanation D. Creating a SHA message digest of a storage device, as long as that digest is not written to the device itself, can be used to validate the integrity of the storage device at a later time, thus preserving the evidence.

PrepLogic Question: 4293-468

63. Review Question p. 149

Answers: A

Explanation A. Best evidence is the original or primary evidence.

Explanation B. Direct evidence is the oral testimony of a witness.

Explanation C. Secondary evidence is a copy or an oral description of evidence.

Explanation D. Conclusive evidence is incontrovertible evidence, such as DNA.

PrepLogic Question: 4293-469

64. Review Question p. 149

Answers: A

Explanation A. Intention is not one of the standard discriminators.

Explanation B. The standard discriminator is to evaluate motive, opportunity, and means.

Explanation C. The standard discriminator is to evaluate motive, opportunity, and means.

Explanation D. The standard discriminator is to evaluate motive, opportunity, and means.

PrepLogic Question: 4293-470

65. Review Question p. 150

Answers: B

Explanation A. The goal of an interrogation is to establish enough evidence to consider a subject a witness.

Explanation B. The goal of an interview is to find the answers to who, what, when, where, why, and how.

Explanation C. The goal of an investigation is to gather sufficient evidence to reconstruct the incident.

Explanation D. The goal of interpretation is to properly read the gathered evidence.

PrepLogic Question: 4293-471

66. Review Question p. 150

Answers: C

Explanation A. The goal of an investigation is to gather sufficient evidence to

reconstruct the incident.

Explanation B. The goal of an interview is to find the answers to who, what, when, where, why, and how.

Explanation C. The goal of an interrogation is to establish enough evidence to consider a subject a witness.

Explanation D. The goal of interpretation is to properly read the gathered evidence.

PrepLogic Question: 4293-472

67. Review Question p. 150

Answers: B

Explanation A. Gathering all relevant storage media is a valid collection means.

Explanation B. Using degaussing equipment is not a valid collection means, in most cases this will destroy the electronically stored evidence data.

Explanation C. Imaging the hard drive is a valid collection means.

Explanation D. Printing out the screen is a valid collection means.

PrepLogic Question: 4293-473

68. Review Question p. 151

Answers: B

Explanation A. Advisory security policies outline acceptable and expected behavior and activities for an organization.

Explanation B. Regulatory security policies outline the laws and industry restrictions placed upon an organization.

Explanation C. Information security policies outline a company's goals and missions.

Explanation D. Organizational security policies outline scope and direction for security solutions within the company.

PrepLogic Question: 4293-763

Explanations: Chapter 7

1. Review Question p. 152

   Answers: D

   Explanation A. Only end users are audited is a poor security practice and is not the primary element of the supervisory structure access control method.

   Explanation B. All employees need performance reviews is generally true, but it is not the primary element of the supervisory structure access control method.

   Explanation C. Senior management is always liable, but it is not the primary element of the supervisory structure access control method.

   Explanation D. Every employee has a boss is the primary element of the supervisory structure access control method. Every employee has to report to someone who oversees their activities.

   PrepLogic Question: 4293-119

2. Review Question p. 152

   Answers: B

   Explanation A. A clipping level is not the threshold of unauthorized activity. Unauthorized activity can occur above and below the clipping level.

   Explanation B. A clipping level is the baseline of normal activity. Events above the clipping level are more likely to be abnormal or unauthorized.

   Explanation C. A clipping level is not the collection of abnormal activity. Abnormal activity can occur above and below the clipping level.

   Explanation D. A clipping level is not the saturation point above which only violations occur. Violations and normal activity can occur above and below the clipping level.

   PrepLogic Question: 4293-160

3. Review Question p. 152

   Answers: C

   Explanation A. Normal activity occurs below the clipping leve. However, some unauthorized activity may occur below a clipping level.

Explanation B. The clipping level itself is the point at which additional activity is more suspect than otherwise.

Explanation C. A violation record is recorded when the clipping level is exceeded.

Explanation D. Violation records are only recorded when the clipping level is exceeded, not at all times.

PrepLogic Question: 4293-161

4. Review Question p. 153

Answers: D

Explanation A. Exceeding the authority of a user account is a repetitive mistake that will exceed clipping levels.

Explanation B. Too many users with unrestricted access is a repetitive mistake that will exceed clipping levels.

Explanation C. Repeated high-volume intrusion detection attempts is a repetitive mistake that will exceed clipping levels.

Explanation D. Failing to submit logon credentials to access resources is a failure to transmit anything. The absence of activity will not exceed the clipping level.

PrepLogic Question: 4293-162

5. Review Question p. 153

Answers: A

Explanation A. Encryption can be used to protect the confidentiality of audit logs.

Explanation B. Write-once media protects the integrity, not the confidentiality, of audit logs.

Explanation C. Redundant event recording will ensure integrity and availability, but not confidentiality.

Explanation D. Digital signatures protect the integrity of audit logs, not the confidentiality.

PrepLogic Question: 4293-167

6. Review Question p. 153

Answers: B

Explanation A. Erasing media using native OS tools will usually leave remanence.

Explanation B. Cremation of media (i.e., complete destruction) is the only assured means to prevent remanence.

Explanation C. Degaussing media may leave remanence if the degaussing equipment is faulty or not working properly.

Explanation D. Performing a single format will usually leave remanence.

PrepLogic Question: 4293-168

7. Review Question p. 154

Answers: D

Explanation A. Object reuse may result in disclosure.

Explanation B. Object reuse may allow unauthorized users to access or extract remanence (i.e., the remains of previously stored data) even after erasure of a media.

Explanation C. Object reuse may seem like cost effective resource management at first, but the cost of the security violation is always much more significant.

Explanation D. The act of recycling a backup tape for another purpose is known as object reuse.

PrepLogic Question: 4293-171

8. Review Question p. 154

Answers: A

Explanation A. Clearing is the process of removing data from media so that it can be reused within the same security environment.

Explanation B. Purging should be performed when media is to be reused in a different security environment.

Explanation C. Overwriting is a common form of data deletion that may leave remanence on media.

Explanation D. Destruction is the proper action to take when media is no longer needed within a security environment. Media reuse should be avoided.

PrepLogic Question: 4293-172

9. Review Question p. 154

Answers: C

Explanation A. CIRT is responsible for managing network logs.

Explanation B. CIRT is responsible for resolving vulnerabilities.

Explanation C. CIRT is not responsible for risk assessment.

Explanation D. CIRT is responsible for minimizing the costs of incidents to an organization.

PrepLogic Question: 4293-424

10. Review Question p. 155

Answers: C

Explanation A. Computer security supports the mission of an organization is a true statement according to GASSP.

Explanation B. Computer security should be cost effective is a true statement according to GASSP.

Explanation C. Computer security is restrained by society according to GASSP.

Explanation D. Computer security should be periodically reassessed is a true statement according to GASSP.

PrepLogic Question: 4293-435

11. Review Question p. 155

Answers: D

Explanation A. Deciding how an incident should be reported is an aspect of emergency response planning.

Explanation B. Deciding when management should be informed of an incident is an aspect of emergency response planning.

Explanation C. Deciding what action should be taken when an incident is detected is an aspect of emergency response planning.

Explanation D. Locating the facility is an aspect of initial security policy and solution design. It is not an aspect of emergency response planning.

PrepLogic Question: 4293-449

12. Review Question p. 155

Answers: A

Explanation A. Determining the criteria for a federal crime is the responsibility of the federal government, not your organization's emergency response planning team.

Explanation B. Deciding what is an incident is an aspect of emergency response planning.

Explanation C. Deciding to whom to report incidents is an aspect of emergency response planning.

Explanation D. Deciding who will respond to incidents is an aspect of emergency response planning.

PrepLogic Question: 4293-453

13. Review Question p. 156

Answers: B

Explanation A. Determining how much damage was caused by an incident is a valid action to take after an incident actually occurs.

Explanation B. Backup solutions should be deployed before an incident, not after. Granted, they may need adjustment after an incident, but if they are not present beforehand you may not be able to recover.

Explanation C. Determining whether additional remedial safeguards are required to improve the security of an environment is a valid action to take after an incident actually occurs.

Explanation D. Determining if recovery procedures should be triggered to recover from an incident is a valid action to take after an incident actually occurs.

PrepLogic Question: 4293-454

14. Review Question p. 156

Answers: B

Explanation A. The committee should establish a liaison with law enforcement.

Explanation B. In most instances, post-incident reports, especially those generated outside the normal business practices of the organization, are not permissible in court, thus the committee should not produce them.

Explanation C. The committee should design a procedure for reporting IT crimes.

Explanation D. The committee should inform senior management and other affected parties of the progress of an investigation.

PrepLogic Question: 4293-457

15. Review Question p. 156

Answers: C

Explanation A. Procedural security defines the processes by which various security related activities should be accomplished.

Explanation B. Oversight security is the supervision of managers to ensure that users are complying with security policy.

Explanation C. Operations security controls focus on day to day activities for the protection of IT and the support of the security policy.

Explanation D. Physical security control focus on protecting physical assets and limiting physical access to a facility.

PrepLogic Question: 4293-474

16. Review Question p. 157

Answers: D

Explanation A. Hardware, software, and data resources must be addressed in the resource protection scheme of an organization.

Explanation B. Hardware, software, and data resources must be addressed in the resource protection scheme of an organization.

Explanation C. Hardware, software, and data resources must be addressed in the resource protection scheme of an organization.

Explanation D. Transitive resources, those provided by other organizations, need not be included in the resource protection scheme for an organization.

PrepLogic Question: 4293-475

17. Review Question p. 157

Answers: A

Explanation A. Recertification may be necessary after a repair, but it is not an element of the actual maintenance and repair process.

Explanation B. Trusted offsite technicians are often required for maintaining security while hardware undergoes maintenance or repair.

Explanation C. Bonded escorts are often required for maintaining security while hardware undergoes maintenance or repair.

Explanation D. Accredited supervision is often required for maintaining security while hardware undergoes maintenance or repair.

PrepLogic Question: 4293-476

18. Review Question p. 157

Answers: B

Explanation A. Vendor maintenance accounts are not any account that has administrative level privileges.

Explanation B. Vendor maintenance accounts are supervisory level factory installed accounts. These accounts should be disabled or be assigned strong passwords.

Explanation C. Vendor maintenance accounts are not accounts used by hardware repair technicians that are created and maintained by your IT staff.

Explanation D. Vendor maintenance accounts are not those administrator accounts involved in the daily support of user accounts and access.

PrepLogic Question: 4293-477

19. Review Question p. 158

Answers: C

Explanation A. Changing passwords is an effective countermeasure against the unauthorized use of maintenance accounts.

Explanation B. Disabling accounts is an effective countermeasure against the unauthorized use of maintenance accounts.

Explanation C. Network traffic logging is not an effective or valid countermeasure against the unauthorized use of maintenance accounts. Such monitoring may detect the use of maintenance accounts, but monitoring is not a countermeasure against their use.

Explanation D. Maintaining physical access control over devices is an effective countermeasure against the unauthorized use of maintenance accounts.

PrepLogic Question: 4293-478

20. Review Question p. 158

Answers: D

Explanation A. Software testing is an operational security software control.

Explanation B. Managed storage of software media is an operational security software control.

Explanation C. Backup are operational security software controls.

Explanation D. Diagnostic port controls are physical security controls for hardware, not software.

PrepLogic Question: 4293-479

21. Review Question p. 158

Answers: B

Explanation A. Maintaining inventory is one of the elements of media security controls, but it is not the primary goal.

Explanation B. The primary goal of media security controls is to prevent loss or disclosure of sensitive data while it is stored on removable media.

Explanation C. Maintaining chain of custody information is useful in tracking usage and preventing disclosure. The mechanism used in media security controls is distinct from the chain of custody used in evidence gathering during a computer crime investigation.

Explanation D. Media security controls do not deal with access restrictions to prevent users from employing removable media.

PrepLogic Question: 4293-481

22. Review Question p. 159

Answers: C

Explanation A. Logging, chain of custody, and inventory management are all aspects of maintaining media security controls.

Explanation B. Logging, chain of custody, and inventory management are all aspects of maintaining media security controls.

Explanation C. Deploying security guard is not an element of maintaining media security controls. Security guards are used to provide physical access control to facilities.

Explanation D. Logging, chain of custody, and inventory management are all aspects of maintaining media security controls.

PrepLogic Question: 4293-482

23. Review Question p. 159

Answers: D

Explanation A. This is not a true statement. Only users with the same or higher clearance can use the removable media.

Explanation B. This is not a true statement. The removable media can only store data with the same clearance level.

Explanation C. This is not a true statement. Confidentiality and integrity are maintained through security labeling, not availability.

Explanation D. This is a true statement. The removable media must be protected under the same restrictions as data with the same classification.

PrepLogic Question: 4293-483

24. Review Question p. 159

Answers: A

Explanation A. At the end of the useful lifetime of a removable media with a high security classification level, that media should be destroyed, such as by incineration.

Explanation B. Purging for re-use is not satisfactory for high classification environments. Plus, at the end of its useful life, purging will not restore it to usefulness.

Explanation C. Cleaning is never sufficient to re-use media in different security

domains.

Explanation D. Once the useful lifetime of media is expired, it should be destroyed not stored. Once a media has reached the end of its useful lifetime, it cannot be used for archival purposes as it will not provide reliable access to the data it was once used to store.

PrepLogic Question: 4293-484

25. Review Question p. 160

Answers: D

Explanation A. Penetration testing is a monitoring or reconnaisance technique.

Explanation B. Demon (war) dialing is a monitoring or reconnaisance technique.

Explanation C. Sniffing is a monitoring or reconnaisance technique.

Explanation D. Static firewall rules are an access control mechanism, not a monitoring or reconnaisance technique.

PrepLogic Question: 4293-487

26. Review Question p. 160

Answers: A

Explanation A. Biometrics are an identification or authentication technique, not a monitoring or reconnaisance technique.

Explanation B. Scanning is a monitoring or reconnaisance technique.

Explanation C. Violation analysis is a monitoring or reconnaisance technique.

Explanation D. Social engineering is a monitoring or reconnaisance technique.

PrepLogic Question: 4293-488

27. Review Question p. 160

Answers: C

Explanation A. When the clipping level is exceeded a violation report is generated. Since clipping levels are associated with tracking the number of errors in a system, it is primarily used for auditing rather than directly reponding to unwanted user activities.

Explanation B. When the clipping level is exceeded a violation report is generated. Since clipping levels are associated with tracking the number of errors in a system, it is primarily used for auditing rather than directly reponding to unwanted user activities.

Explanation C. When the clipping level is exceeded a violation report is generated.

Explanation D. When the clipping level is exceeded a violation report is generated. Since clipping levels are associated with tracking the number of errors in a system, it is primarily used for auditing rather than directly reponding to unwanted user activities.

PrepLogic Question: 4293-490

28. Review Question p. 161

Answers: D

Explanation A. Repetitive mistakes are easily detected through the use of clipping levels.

Explanation B. Individuals exceeding their authorized privileges are easily detected through the use of clipping levels.

Explanation C. Serious intrusion attempts are easily detected through the use of clipping levels.

Explanation D. Slow low-traffic attacks are typically not detected through the use of clipping levels. Slow low-traffic attacks are lost in the bulk of normal expected activity.

PrepLogic Question: 4293-491

29. Review Question p. 161

Answers: A

Explanation A. Monitoring should already be enabled before users begin logging on to the system.

Explanation B. Monitoring should begin after application installation, system configuration, and operation system patching.

Explanation C. Monitoring should begin after application installation, system configuration, and operation system patching.

Explanation D. Monitoring should begin after application installation, system configuration, and operation system patching.

PrepLogic Question: 4293-492

30. Review Question p. 161

Answers: B

Explanation A. Monitoring should focus on violation tracking, processing, and analysis.

Explanation B. Monitoring is not directly concerned with the resolution of violations. That is a secondary result of the monitoring process. If there is to be a resoution to violations, it is a result of violation analysis.

Explanation C. Monitoring should focus on violation tracking, processing, and analysis.

Explanation D. Monitoring should focus on violation tracking, processing, and analysis.

PrepLogic Question: 4293-493

31. Review Question p. 162

Answers: B

Explanation A. Developing an attack plan should come after obtaining management approval and before collecting attack tools.

Explanation B. Obtaining management approval is always the first step when using penetration testing.

Explanation C. Collecting attack tools should come after developing an attack plan.

Explanation D. Producing a results report should occur at the end of the penetration testing process.

PrepLogic Question: 4293-497

32. Review Question p. 162

Answers: C

Explanation A. The goal of penetration testing is to evaluate the existing security protection. The actions taken based on the results of a penetration test may result in altering the security policy.

Explanation B. The goal of penetration testing is to evaluate the existing security

protection. Blame is not important, evaluating and improving security is important.

Explanation C. The goal of penetration testing is to evaluate the existing security protection.

Explanation D. The goal of penetration testing is to evaluate the existing security protection. Reliable reports on an organization's state of security and properly evaluating all the optiosn and their costs should be sufficient to encourage management into making prudent decisions.

PrepLogic Question: 4293-498

33. Review Question p. 162

Answers: C

Explanation A. Enabling rollback is a part of configuration or change management, but it is not the primary goal.

Explanation B. Duplicating changes on multiple systems is a part of configuration or change management, but it is not the primary goal.

Explanation C. The primary goal of configuration or change management is to ensure that security is not diminished.

Explanation D. Informing users of changes is a part of configuration or change management, but it is not the primary goal.

PrepLogic Question: 4293-500

34. Review Question p. 162

Answers: A

Explanation A. Biometric enrollment is not a form of monitoring. Biometric enrollment is often a determining factor in whether or not a biometric identification or authenticating device will be accepted by the user community. If enrollment takes longer than 2 minutes, most users will be unwilling to use it.

Explanation B. Port scanning is a form of monitoring. Port scanning monitors for open ports which may not have adequate security and access controls.

Explanation C. Intrusion detection is a form of monitoring. Intrusion detection monitors for unauthorized access.

Explanation D. Penetration testing is a form of monitoring. Penetration testing

monitors for vulnerabilities in a security policy.

PrepLogic Question: 4293-502

35. Review Question p. 163

Answers: B

Explanation A. Transaction processing is the act of executing instructions to exchange information or data.

Explanation B. Trend or traffic analysis is the examination of traffic patterns rather than packet contents.

Explanation C. Sniffing is the act of gathering packets for content inspection.

Explanation D. Port scanning is the act of testing devices and communication links for open connection pathways.

PrepLogic Question: 4293-503

36. Review Question p. 163

Answers: C

Explanation A. Implementing the change is one of the five generally recognized procedural steps to implement configuration or change control management.

Explanation B. Applying to introduce a change is one of the five generally recognized procedural steps to implement configuration or change control management.

Explanation C. Since changes are not supposed to alter the security environment, there should be no need to change or alter the security policy. Therefore, updating the security policy is not one of the five generally recognized procedural steps to implement configuration or change control management.

Explanation D. Cataloging the intended change is one of the five generally recognized procedural steps to implement configuration or change control management.

PrepLogic Question: 4293-504

37. Review Question p. 163

Answers: D

Explanation A. Updating new employee training materials is not one of the most important features or mechanisms of configuration or change control management.

Explanation B. Revising the organization's security policy is not one of the most important features or mechanisms of configuration or change control management, especially since the goal of configuration or change control management is to prevent alterations to the security environment.

Explanation C. Compliance with configuration or change control management is typically not a specific features or mechanisms of compliance with due care requirements.

Explanation D. One of the most important features or mechanisms of configuration or change control management is the ability to rollback changes to a previous state.

PrepLogic Question: 4293-505

38. Review Question p. 164

Answers: A

Explanation A. The purpose of trusted recovery is to ensure that security is not breached during the recovery from a system failure.

Explanation B. The purpose of trusted recovery is to ensure that security is not breached during the recovery from a system failure. Maintaining accreditation requires periodic re-assessment after a length of time or after significant changes to a system.

Explanation C. The purpose of trusted recovery is to ensure that security is not breached during the recovery from a system failure. Testing backups and using verification features are used to guarantee the reliability of backups.

Explanation D. The purpose of trusted recovery is to ensure that security is not breached during the recovery from a system failure. The disaster recovery plan and the salvage team are responsible for returning an organization to the primary site after a disaster.

PrepLogic Question: 4293-518

39. Review Question p. 164

Answers: B

Explanation A. Rebooting into a single user mode is an element of trusted recovery.

Explanation B. The TCB is not re-validated by the trusted recovery process. Instead, the trusted recovery process relied upon the TCB to provide its capability of returning the system to a secure state after a failure.

Explanation C. Recovering all file systems that were active at the time of failure is an element of trusted recovery.

Explanation D. Verifying the integrity of system level security critical files is an element of trusted recovery.

PrepLogic Question: 4293-519

40. Review Question p. 164

Answers: D

Explanation A. A primary function of configuration or change control management is to provide a means to track and audit changes to a system.

Explanation B. A primary function of configuration or change control management is to ensure formalized testing of all system changes.

Explanation C. A primary function of configuration or change control management is to analyze the effects of changes on a system.

Explanation D. A primary function of configuration or change control management is to keep users informed of system changes.

PrepLogic Question: 4293-521

41. Review Question p. 165

Answers: A

Explanation A. The top priority of configuration or change control management is to prevent changes from diminishing security.

Explanation B. A primary function, but not the top priority, of configuration or change control management is to analyze the effects of changes on a system.

Explanation C. A primary function, but not the top priority, of configuration or change control management is to provide a means to track and audit changes to a system.

Explanation D. A primary function, but not the top priority, of configuration or change control management is to ensure formalized testing of all system changes.

PrepLogic Question: 4293-522

42. Review Question p. 165

Answers: B

Explanation A. Applying to introduce a change is one of the five generally recognized procedural steps to implement configuration or change control management.

Explanation B. Updating the configuration item is an aspect of software development life cycle change control management, not overall configuration or change control management.

Explanation C. Scheduling the change is one of the five generally recognized procedural steps to implement configuration or change control management.

Explanation D. Reporting the change to the appropriate parties is one of the five generally recognized procedural steps to implement configuration or change control management.

PrepLogic Question: 4293-523

43. Review Question p. 165

Answers: D

Explanation A. A partial or full knowledge team would already know considerable details about the environment, which would taint the results of the test.

Explanation B. There is not a knowledge level labeled disclosed in regards to penetration attack teams.

Explanation C. A partial or full knowledge team would already know considerable details about the environment, which would taint the results of the test.

Explanation D. A penetration attack team with zero knowledge will be able to clearly demonstrate how much information can be discovered about your environment from the outside.

PrepLogic Question: 4293-524

44. Review Question p. 166

Answers: A

Explanation A. Safeguard tuning is not an element of penetration testing.

Explanation B. Discovery, enumeration, and exploitation are steps in penetration testing.

Explanation C. Discovery, enumeration, and exploitation are steps in penetration

testing.

Explanation D. Discovery, enumeration, and exploitation are steps in penetration testing.

PrepLogic Question: 4293-525

45. Review Question p. 166

Answers: B

Explanation A. Footprinting occurs in the discovery phase of penetration testing.

Explanation B. Social engineering requires some level of data knowledge in order to be effective. Social engineering can be performed in the enumeration, vulnerability mapping, or exploitation phases of penetration testing.

Explanation C. Scavenging occurs in the discovery phase of penetration testing.

Explanation D. Dumpster diving occurs in the discovery phase of penetration testing.

PrepLogic Question: 4293-526

46. Review Question p. 166

Answers: C

Explanation A. The deployment of new safeguards is a step after risk analysis, which is itself a task performed after the completion of penetration testing.

Explanation B. The reporting of findings of penetration testing is used to guide risk analysis on the discovered problems. However, the risk analysis itself is not considered part of the penetration testing process.

Explanation C. The final step in penetration testing is reporting findings.

Explanation D. Exploiting discovered vulnerabilities is not the last step of penetration testing.

PrepLogic Question: 4293-527

47. Review Question p. 167

Answers: A

Explanation A. Purging of audit media should be avoided in most situations. Audit details are usually retained for historical comparisons.

Explanation B. Retention and protection of audit media is an important security issue related to audit trails.

Explanation C. Protection against alteration is an important security issue related to audit trails.

Explanation D. Support of availability of audit media is an important security issue related to audit trails.

PrepLogic Question: 4293-529

48. Review Question p. 167

Answers: B

Explanation A. Findings reports must be in writing.

Explanation B. Oral reports can be used for interim reports only.

Explanation C. Final reports must be in writing.

Explanation D. Objectives definition reports must be in writing.

PrepLogic Question: 4293-530

49. Review Question p. 167

Answers: D

Explanation A. Viewing another user's files is a browsing attack.

Explanation B. Shoulder surfing is a browsing attack.

Explanation C. Going through someone's trash is a browsing attack.

Explanation D. Extracting data from purged media is a scavenging attack, not a browsing attack.

PrepLogic Question: 4293-532

50. Review Question p. 168

Answers: D

Explanation A. Accessing and distributing controversial political content is an inappropriate activity.

Explanation B. Conducting personal business on company resources is an inappropriate activity.

Explanation C. Abusing your privileges is an inappropriate activity.

Explanation D. Performing a work task is always an appropriate activity, even if the results are not always desirable.

PrepLogic Question: 4293-542

51. Review Question p. 168

Answers: A

Explanation A. Violating the confidentiality of sensitive data is an abuse of privileges.

Explanation B. Violating the confidentiality of sensitive data is not considered wasting company resources.

Explanation C. Violating the confidentiality of sensitive data does not address the appropriateness of content.

Explanation D. Vandalism generally does not violate the confidentiality of sensitive data.

PrepLogic Question: 4293-543

52. Review Question p. 168

Answers: B

Explanation A. Fraud is always a computer crime.

Explanation B. An input error or omission is not a computer crime even if it results in a serious financial loss to your organization. It is simply an unwanted activity.

Explanation C. Eavesdropping can be a computer crime if it results in a serious financial loss to your organization.

Explanation D. War dialing can be a computer crime if it results in a serious financial loss to your organization.

PrepLogic Question: 4293-544

53. Review Question p. 169

Answers: D

Explanation A. Message padding, transmission of noise, and covert channel analysis are all valid countermeasures to traffic or trend analysis.

Explanation B. Message padding, transmission of noise, and covert channel analysis are all valid countermeasures to traffic or trend analysis.

Explanation C. Message padding, transmission of noise, and covert channel analysis are all valid countermeasures to traffic or trend analysis.

Explanation D. Encrypting individual messages is not an effective countermeasure to traffic or trend analysis.

PrepLogic Question: 4293-546

54. Review Question p. 169

Answers: A

Explanation A. Traffic or trend analysis is primarily concerned with the amount of data traveling to another system.

Explanation B. Traffic or trend analysis is not concerned with the content of network packets.

Explanation C. Traffic or trend analysis is not concerned with the application used in a communication.

Explanation D. Traffic or trend analysis is not concerned with the user account and password associated with a communication session.

PrepLogic Question: 4293-547

55. Review Question p. 169

Answers: D

Explanation A. Some components may need replacement more or less often than once per year.

Explanation B. Components should be repaired not replaced when necessary up to when their mean time between failure (MTBF) time period expires.

Explanation C. Components should be repaired not replaced when necessary up to when their mean time between failure (MTBF) time period expires.

Explanation D. Hardware components should be replaced before their mean time between failure (MTBF) time period expires.

PrepLogic Question: 4293-550

56. Review Question p. 170

Answers: C

Explanation A. The mean time to repair (MTTR) is used to describe the typical time it takes to repair a component once it experiences a failure.

Explanation B. The mean time between failures is used to determine when to replace a device.

Explanation C. The mean time to repair (MTTR) is used to describe how long it takes to repair a component once it experiences a failure.

Explanation D. The MTTR and MTBF have no such formulaic relationship.

PrepLogic Question: 4293-551

57. Review Question p. 170

Answers: D

Explanation A. The mean time to repair is how long it takes to repair hardware, not the length of time before hardware should be replaced.

Explanation B. Every two years may be a longer or shorter time span than the mean time between failures.

Explanation C. The capacity utilization has little to do with replacing hardware before failure to maintain availability.

Explanation D. Hardware should be replaced before it reaches its age of mean time between failures.

PrepLogic Question: 4293-577

58. Review Question p. 170

Answers: B

Explanation A. When performed properly, degaussing can destroy data on magnetic media.

Explanation B. OS based deletion will not usually destroy the data on media in most cases. Often, an OS deletion only removes the filename from the directory structure but leaves the data on the sectors of the drive unchanged.

Explanation C. Overwriting data on magnetic media at least seven times is considered sufficient to prevent extraction of data remanace. Thus, data can then be considered reliably destroyed.

Explanation D. Purging is the use of degaussing and / or overwriting the media seven times or more to properly, completely, and reliably destroy data.

PrepLogic Question: 4293-620

59. Review Question p. 171

Answers: C

Explanation A. Purging is often sufficient to destroy data, but it is not absolutely guaranteed to be effective every time.

Explanation B. Formatting usually only changes the file table and does not remove the data from the medium.

Explanation C. The only way to absolutely prevent data remenance from being extracted from electronic media is to destroy it by incineration.

Explanation D. Overwrite at least seven times is often sufficient to destroy data, but it is not absolutely guaranteed to be effective every time.

PrepLogic Question: 4293-622

60. Review Question p. 171

Answers: D

Explanation A. Purging is more than sufficient and is not the minimally sufficient solution offered.

Explanation B. Destroying the media by cremation will prevent that medias re-use.

Explanation C. Overwriting at least seven times is more than sufficient and is not the minimally sufficient solution offered.

Explanation D. Clearing is the process of overwriting a media so it can be re-used in the same environment. It is not as thorough as a purge, but sufficient as long as the security classification remains constant.

PrepLogic Question: 4293-623

61. Review Question p. 171

Answers: A

Explanation A. RAID 1 is basic mirroring.

Explanation B. RAID 3 is disk striping with byte level parity.

Explanation C. RAID 5 is disk striping with interleave parity.

Explanation D. RAID 6 is a combination of mirroring and interleave parity (i.e., RAID 1 with RAID 5).

PrepLogic Question: 4293-798

Explanations: Chapter 8

1. Review Question p. 172

   Answers: A

   Explanation A. Notebook cable locks are physical mechanisms to directly prevent physical computer theft.

   Explanation B. Work area separation does not directly protect against physical computer theft, rather it restricts access to secured areas within a facility.

   Explanation C. Lighting does not directly protect against physical computer theft, but rather is used as a deterrent for casual trespassers.

   Explanation D. Control zones do not directly protect against physical computer theft, but are used to protect against electronic emissions.

   PrepLogic Question: 4293-120

2. Review Question p. 172

   Answers: A

   Explanation A. Backups are not considered a form of preventative access control. Backups are a form of recovery access control.

   Explanation B. Locks are an example of preventative access controls.

   Explanation C. Lighting is an example of preventative access controls.

   Explanation D. Security guards are an example of preventative access controls.

   PrepLogic Question: 4293-151

3. Review Question p. 172

   Answers: A

   Explanation A. Clipping levels is a preventative logical/technical access control that is the baseline of normal activity on a system.

   Explanation B. Badges are an example of a preventative physical access control.

   Explanation C. Dogs are an example of a preventative physical access control.

Explanation D. Mantraps are an example of a preventative physical access control.

PrepLogic Question: 4293-155

4. Review Question p. 173

Answers: C

Explanation A. Cutting through a wire fence is not an example of piggybacking.

Explanation B. Re-transmitting intercepted packets is not an example of piggybacking.

Explanation C. Passing through a door opened by another person who used a key is an example of piggybacking.

Explanation D. Decrypting the content of secured communication sessions is not an example of piggybacking.

PrepLogic Question: 4293-545

5. Review Question p. 173

Answers: B

Explanation A. A UPS (uninterruptible power supply) is a useful and recommended power protection device for a mission critical server.

Explanation B. A surge protector, while useful and recommended, is not the best option, from this list devices, for a mission critical server.

Explanation C. An alternate power supply is a useful and recommended power protection device for a mission critical server.

Explanation D. A backup generator is a useful and recommended power protection device for a mission critical server.

PrepLogic Question: 4293-552

6. Review Question p. 173

Answers: C

Explanation A. A brownout is an extended loss of voltage.

Explanation B. A spike is a momentary high voltage.

Explanation C. A fault is a momentary loss of power.

Explanation D. A sag is a momentary loss of voltage.

PrepLogic Question: 4293-553

7. Review Question p. 173

Answers: A

Explanation A. Transient noise is a short duration of an interfering disturbance in the power line.

Explanation B. A spike is momentarily high voltage.

Explanation C. Noise is steadily interfering disturbance in the power line.

Explanation D. A sag is a complete, but momentary loss of voltage.

PrepLogic Question: 4293-554

8. Review Question p. 174

Answers: B

Explanation A. A transient noise is a short duration of an interfering disturbance in the power line.

Explanation B. Traverse mode noise is the radiation generated by the difference in power of the hot and neutral wires of a circuit.

Explanation C. Common mode noise is the radiation generated by the difference in power of the hot and ground wires of a circuit.

Explanation D. A brownout is an extended loss of voltage, not a form of interference.

PrepLogic Question: 4293-555

9. Review Question p. 174

Answers: C

Explanation A. Moving power lines away from strong magnetic sources is an effective means to eliminate or reduce power line noise.

Explanation B. Ensuring proper grounding is an effective means to eliminate or reduce power line noise.

Explanation C. Cables with fewer twists will increase the likelihood of power line

noise.

Explanation D. Adding cable shielding is an effective means to eliminate or reduce power line noise.

PrepLogic Question: 4293-556

10. Review Question p. 174

Answers: D

Explanation A. The ANSI standard for brownouts makes no reference to a value of 1.2%.

Explanation B. The ANSI standard for brownouts makes no reference to a value of 10%.

Explanation C. The ANSI standard for brownouts makes no reference to a value of 3.5%.

Explanation D. According to the ANSI standard, at a drop of 8% in power between the power source and the meter is a brownout declared.

PrepLogic Question: 4293-557

11. Review Question p. 175

Answers: A

Explanation A. A gas discharge system suppresses fires by means of oxygen displacement.

Explanation B. A Preaction system may be dry or wet pipe. This system is used to prevent an accidental discharge of water by providing an advance alarm.

Explanation C. A Deluge system employs open sprinklers attached to a dry pipe. The pipe, in turn, is attached to a tank full of water that is opened by a detection system. When a fire is detected, it releases the water in the tank and discharges.

Explanation D. A Dry Pipe system employs sprinklers attached to a piping system filled with air. When the air is released, this opens a valve that allows water to fill the pipes and then be disbursed through the open sprinklers.

PrepLogic Question: 4293-558

12. Review Question p. 175

Answers: B

Explanation A. Too little humidity can cause static electricity buildup.

Explanation B. The ideal operating humidity for a data center room is 40 - 60%.

Explanation C. Too much humidity can result in corrosion.

Explanation D. Extremely high levels of humidity can result in corrosion and pooling condensation.

PrepLogic Question: 4293-559

13. Review Question p. 175

Answers: C

Explanation A. Actually, static electricty can discharge at a much higher voltage than 1,000 volts.

Explanation B. Even with low-static carpeting and low humidity, static electricty can discharge at a higher voltage than 5,000 volts.

Explanation C. Static electricity discharges over 20,000 volts are possible on low-static carpeting in an environment with very low humidity.

Explanation D. 150,000 volts is a little more than static electricity can produce. Most commercial stun guns output at around 150,000 volts.

PrepLogic Question: 4293-560

14. Review Question p. 175

Answers: D

Explanation A. A static discharge of 2,000 volts is sufficient to cause a system shutdown.

Explanation B. A static discharge of 1,500 volts is sufficient to destroy data on a hard drive.

Explanation C. A static discharge of 17,000 volts is sufficient to permenantly damage microchips.

Explanation D. A static discharge of 1,000 volts is sufficient to scramble a CRT monitor display.

PrepLogic Question: 4293-561

15. Review Question p. 176

Answers: A

Explanation A. A static discharge of only 4,000 volts is sufficient to cause a printer jam or serious malfunction.

Explanation B. A static discharge of 1,000 volts is sufficient to cause the scrambling of a monitor display.

Explanation C. A static discharge of 55,000 volts is more than sufficient to destroy any part of an electronic device or computer.

Explanation D. A static discharge of 17,000 volts is sufficient to cause permanent damage to microchips.

PrepLogic Question: 4293-562

16. Review Question p. 176

Answers: B

Explanation A. Electric cables can cause radio frequency interference (RFI).

Explanation B. Cement walls do not cause radio frequency interference (RFI), but may actually reduce it due to internal steel reinforcements that may absorb EMI and RFI.

Explanation C. Fluorescent lights cause radio frequency interference (RFI).

Explanation D. Electric space heaters can cause radio frequency interference (RFI).

PrepLogic Question: 4293-563

17. Review Question p. 176

Answers: C

Explanation A. Reference checks are an element of the pre-employment screening process.

Explanation B. Drug screening is an element of the pre-employment screening process.

Explanation C. A supervisor review can only occur after a worker has been employed for a length of time. This is not an element of the pre-employment screening process.

Explanation D. Education history verification is an element of the pre-employment screening process.

PrepLogic Question: 4293-564

18. Review Question p. 177

Answers: D

Explanation A. Security clearance verification should be part of ongoing employee security compliance checks.

Explanation B. Supervisor reviews should be part of ongoing employee security compliance checks.

Explanation C. Drug testing should be part of ongoing employee security compliance checks.

Explanation D. Termination of physical access should occur as an element of the post-employment or termination procedures, not as part of on-going employee security compliance checks.

PrepLogic Question: 4293-565

19. Review Question p. 177

Answers: A

Explanation A. The issuing of photo ID is an element of the employment or hiring procedures, not the termination procedures.

Explanation B. An escort off the premises can be part of the termination process.

Explanation C. Review of non-disclosure agreements can be part of the termination process.

Explanation D. The return of equipment can be part of the termination process.

PrepLogic Question: 4293-566

20. Review Question p. 177

Answers: B

Explanation A. Fire drills are an administrative control for maintaining physical security.

Explanation B. Assigning a user account logon rights is a logical or technical control for maintaining logical or technical security.

Explanation C. Exit interviews are an administrative control for maintaining both physical and logical security.

Explanation D. Employment record verification is an administrative control for maintaining physical security.

PrepLogic Question: 4293-567

21. Review Question p. 178

Answers: C

Explanation A. Clearly documenting the steps of procedures is important to maintaining administrative controls to protect physical security in the event of a disaster or emergency.

Explanation B. Personnel training and drills are important to maintaining administrative controls to protect physical security in the event of a disaster or emergency.

Explanation C. Risk analysis is not an element of maintaining administrative controls to protect physical security. Instead, risk analysis is used to select the safeguards to implement and re-evaluate their effectiveness, not in the maintenance of a selected security solution.

Explanation D. Periodic review of the recovery plan is important to maintaining administrative controls to protect physical security in the event of a disaster or emergency.

PrepLogic Question: 4293-568

22. Review Question p. 178

Answers: C

Explanation A. Vandalism is a human threat to physical security.

Explanation B. Strikes are a human threat to physical security.

Explanation C. Utility loss is a threat of physical security that can be caused by humans, but it can also be caused by natural disasters. This is the best answer for this question.

Explanation D. Sabotage is a human threat to physical security.

PrepLogic Question: 4293-569

23. Review Question p. 178

Answers: D

Explanation A. Cost effectiveness of mechanisms is not the most important factor when designing and implementing physical security solutions. Security measures should not b implemented if they are not cost effective.

Explanation B. Efficiency of solutions is not the most important factor when designing and implementing physical security solutions. The efficiency of a solution will often influence its cost effectiveness.

Explanation C. Automation of controls is not the most important factor when designing and implementing physical security solutions. Security controls can be effective even if they do not offer automated controls.

Explanation D. Personnel safety is always the most important factor when designing and implementing physical security solutions.

PrepLogic Question: 4293-570

24. Review Question p. 179

Answers: A

Explanation A. The cost benefits of a physical security mechanism are the second most important after human safety. If a mechanism costs more to implement and maintain that the assets it is protecting, then it should not be deployed.

Explanation B. Compliance with industry standards is often important, but the cost benefits is of higher importance.

Explanation C. Similarity with existing solutions may be beneficial when leveraging existing expertise, but it could also be a disadvantage if the similarity means it is as ineffective as previous solutions.

Explanation D. The amount of user training required can be important if its related costs are high, but these costs are taken into account with all other costs related to the new solution implementation.

PrepLogic Question: 4293-571

25. Review Question p. 179

Answers: B

Explanation A. Physical security mechanisms are not always invisible to the user; often visible physical security mechanisms are more effective.

Explanation B. Physical security mechanisms should always comply with laws and regulations.

Explanation C. Physical security mechanisms need not be automated to be effective.

Explanation D. Only approval by upper management is actually required for the deployment of a security mechanism.

PrepLogic Question: 4293-572

26. Review Question p. 179

Answers: D

Explanation A. A surge is prolonged, high voltage.

Explanation B. A spike is a momentary high voltage.

Explanation C. Noise is a steady, interfering disturbance in the power line.

Explanation D. An inrush is the momentary increase in power often experienced at the moment when a device or a power system is turned on.

PrepLogic Question: 4293-573

27. Review Question p. 180

Answers: A

Explanation A. Cost is the least important aspect when evaluating the security of a new facility or site.

Explanation B. Location is a very important aspect when evaluating the security of a new facility or site.

Explanation C. The fire rating is a very important aspect when evaluating the security of a new facility or site.

Explanation D. Local emergency services is a very important aspect when evaluating the security of a new facility or site.

PrepLogic Question: 4293-574

28. Review Question p. 180

Answers: B

Explanation A. Fire suppression systems are very important for secured server rooms.

Explanation B. Human compatibility is the least important aspect of a secured server room. In fact, server rooms are often very incompatible for humans.

Explanation C. Temperature control systems are very important for secured server rooms.

Explanation D. Efficient use of space is important for secured server rooms.

PrepLogic Question: 4293-575

29. Review Question p. 180

Answers: C

Explanation A. Protection of human safety is always the most important aspect of any security control. Cost is usually the last factor when selecting access controls; it is always more important that an access control functions reliability.

Explanation B. Protection of human safety is always the most important aspect of any security control. Ease of maintenance is one of the selection factors when choosing access controls.

Explanation C. Protection of human safety is always the most important aspect of any security control.

Explanation D. Protection of human safety is always the most important aspect of any security control. The reliability of an access control is one of the primary selection factors.

PrepLogic Question: 4293-576

30. Review Question p. 181

Answers: C

Explanation A. Subject classification levels are determined either by the industry (i.e., military/government or private sector) or by the data owner, not by critical path analysis.

Explanation B. Control zones are developed by the data owner, not through critical path analysis.

Explanation C. Critical path analysis is used in the area of physical security to determine the value of each element of infrastructure.

Explanation D. Vulnerability testing and penetration testing, not critical path analysis, is used to determine whether a security solution is sufficient.

PrepLogic Question: 4293-578

31. Review Question p. 181

Answers: D

Explanation A. Training is an example of a physical security administrative control.

Explanation B. Facility management is an example of a physical security administrative control.

Explanation C. Emergency response procedures is an example of a physical security administrative control.

Explanation D. Alarms are examples of physical security technical controls.

PrepLogic Question: 4293-579

32. Review Question p. 181

Answers: A

Explanation A. Facility construction design is an example of a physical security administrative control.

Explanation B. Fencing is an example of a physical security physical control.

Explanation C. Man traps are an example of a physical security physical control.

Explanation D. Security guards are an example of a physical security physical control.

PrepLogic Question: 4293-580

33. Review Question p. 182

Answers: A

Explanation A. Security guards are an example of a physical security physical control.

Explanation B. CCTV monitoring is an example of a physical security technical control.

Explanation C. Power supply management is an example of a physical security technical control.

Explanation D. Intrusion detection is an example of a physical security technical control.

PrepLogic Question: 4293-581

34. Review Question p. 182

Answers: B

Explanation A. Surrounding terrain is an important aspect when considering a location for a secure facility.

Explanation B. Cost is the least important aspect, from this list of options, when considering a location for a secure facility.

Explanation C. Access to emergency services is an important aspect when considering a location for a secure facility.

Explanation D. Proximity to residential areas is an important aspect when considering a location for a secure facility.

PrepLogic Question: 4293-582

35. Review Question p. 182

Answers: C

Explanation A. Access to means of transportation is an important aspect when considering a location for a secure facility. Transportation supports safe evacuation as well as ease of worker access.

Explanation B. Frequency of earthquakes is an important aspect when considering a location for a secure facility. Earthquake danger will require earthquake proofing your bulding and equipment as well as expensive insurance.

Explanation C. Size suitable for future growth is the least important aspect, from this list of options, when considering a location for a secure facility. Size suitable for future growth is important before final selection, but it is not as critical as elements that threaten the safety and security of your organization.

Explanation D. Direction of door openings is an important aspect when considering a location for a secure facility. Doors opening from the inside out are considered safer for personnel but doors that open from the outside in provide greater safety for equipment.

PrepLogic Question: 4293-583

36. Review Question p. 183

Answers: D

Explanation A. Load rating is an important factor to consider when designing security of a facility's interior.

Explanation B. Fire resistance is an important factor to consider when designing security of a facility's interior.

Explanation C. Accessibility is an important factor to consider when designing security of a facility's interior.

Explanation D. The number of offices with doors is the least important aspect of a facility's interior when designing security. Doors with secure locking mechanisms will be important for the server vault and for separating different classifications of workers, but whether there are plenty of offices for those high-up in the organization's personnel heirarchy is not a security concern.

PrepLogic Question: 4293-584

37. Review Question p. 183

Answers: A

Explanation A. UV reflection or blocking is the least important factor in regards to security when considering windows.

Explanation B. Translucency vs. opaqueness is an important physical security factor when considering the security of windows.

Explanation C. Shatterproofness is an important physical security factor when considering the security of windows.

Explanation D. Placement is an important physical security factor when considering the security of windows.

PrepLogic Question: 4293-585

38. Review Question p. 183

Answers: B

Explanation A. The load rating is an important physical security factor when considering the security of flooring.

Explanation B. The texture of following is the least important physical security factor when considering the security of flooring.

Explanation C. Conductivity of the surface is an important physical security factor when considering the security of flooring.

Explanation D. Combustibility is an important physical security factor when considering the security of flooring.

PrepLogic Question: 4293-586

39. Review Question p. 184

Answers: C

Explanation A. Partitions are insufficient for creating divisions between work and visitor spaces. Permanent floor to ceiling walls and/or buildings are needed to create separate work and visitor spaces.

Explanation B. Partitions are insufficient for creating fire barriers. Fire rated permanent floor to ceiling walls are need to create fire barriers.

Explanation C. Partitions are useful for creating separation between individual work spaces and desks.

Explanation D. Partitions are insufficient for creating a distinction between areas of different sensitivity. Floor to ceiling permanent walls are needed to protect sensitive areas.

PrepLogic Question: 4293-587

40. Review Question p. 184

Answers: D

Explanation A. Partitions are useful for creating separate work spaces, but they are not sufficient to provide security and separation of areas with various levels of sensitivity and confidentiality.

Explanation B. Windows may be used to separate work areas while maintaining separate HVAC environments, but they are not sufficient to provide security and

separation of areas with various levels of sensitivity and confidentiality.

Explanation C. Boundaries outlined by colored tape may be useful in separating work areas in some situations, but they are not sufficient to provide security and separation of areas with various levels of sensitivity and confidentiality.

Explanation D. Floor to ceiling permanent walls should be used to provide sufficient security and separation of areas with various levels of sensitivity and confidentiality.

PrepLogic Question: 4293-588

41. Review Question p. 184

Answers: D

Explanation A. Fencing is a physical control for protecting physical security.

Explanation B. Dogs are a physical control for protecting physical security.

Explanation C. Lighting is a physical control for protecting physical security.

Explanation D. CCTV is considered a technical or logical access control, even though it is used for providing physical security.

PrepLogic Question: 4293-589

42. Review Question p. 185

Answers: B

Explanation A. Biometric door locks are an example of physical security technical controls.

Explanation B. Visitor sign-in sheet are an example of a physical security administrative control.

Explanation C. Intrusion detection is an example of physical security technical controls.

Explanation D. HVAC management is an example of physical security technical controls.

PrepLogic Question: 4293-590

43. Review Question p. 185

Answers: C

Explanation A. Lighting is an example of a physical security physical control.

Explanation B. Facility construction materials are an example of physical security physical controls.

Explanation C. Fire detection and suppression is an example of physical security technical control.

Explanation D. Facility selection is an example of physical security administrative control.

PrepLogic Question: 4293-591

44. Review Question p. 185

Answers: D

Explanation A. Guard dogs are an example of a physical security physical control.

Explanation B. Man traps are an example of a physical security physical control.

Explanation C. Fencing is an example of a physical security physical control.

Explanation D. Data backups are an example of a physical security technical control.

PrepLogic Question: 4293-592

45. Review Question p. 186

Answers: A

Explanation A. The mission critical data center should be placed in the center or core of a facility for the maximum protection from threats to physical security.

Explanation B. Locating the mission critical data center off site will not adequately provide protection against threats to physical security since the issues will still exist at the second location.

Explanation C. Placing the mission critical data center in the basement is not the best choice in all situations, especially when flooding is prevalent.

Explanation D. Distributing the mission critical data center will require event greater security precautions and will not provide the same level of protection as locating it in the core or center of the facility.

PrepLogic Question: 4293-593

46. Review Question p. 186

Answers: B

Explanation A. The load rating of the floor is important to prevent too much equipment from being stored on a floor that is not designed to support it, but when specifically discussing sensitive electrical equipment, dealing with static electricity is more important.

Explanation B. The most important factor when protecting sensitive electrical equipment is the electrical conductance of the flooring material or the likelihood of generation and sparking of static electricity.

Explanation C. The presence of raising flooring is not as significant an issue for protecting sensitive electrical equipment, as is dealing with static electricity.

Explanation D. The physical dimensions of the data center room are inconsequential to the protection of sensitive electrical equipment.

PrepLogic Question: 4293-594

47. Review Question p. 186

Answers: C

Explanation A. A computer room or data center should have restricted access to be secure and protected.

Explanation B. A computer room or data center should have an electronic equipment compatible fire suppression system to be secure and protected.

Explanation C. A computer room or data center need not be human compatible to be secure and protected.

Explanation D. A computer room or data center should be located in the center or core of the facility to be secure and protected.

PrepLogic Question: 4293-595

48. Review Question p. 187

Answers: A

Explanation A. The theft of a notebook would represent a threat to all three aspects of the security triad.

Explanation B. Physical destruction of access terminals is a direct physical threat to maintaining the availability of hosted data, but not to confidentiality or integrity.

Explanation C. Unauthorized publication of a trade secret to a public Web site is a threat to maintaining the confidentiality of hosted data, but not to availability or integrity.

Explanation D. Termination of power to the supporting systems is a direct physical threat to maintaining the availability of hosted data, but not to confidentiality or integrity.

PrepLogic Question: 4293-596

49. Review Question p. 187

Answers: C

Explanation A. Unauthorized disclosure is a direct threat to maintaining the confidentiality of hosted data.

Explanation B. Termination of power to the supporting systems is a direct threat to maintaining the availability of hosted data.

Explanation C. Using storage devices from unknown/untrusted sources can result in a direct threat to maintaining the integrity of hosted data.

Explanation D. Severe physical damage to an access terminal is a direct threat to maintaining the availability of hosted data.

PrepLogic Question: 4293-597

50. Review Question p. 187

Answers: B

Explanation A. Toxic material release is a physical security emergency.

Explanation B. Intrusion attempts through communication links are a technical or logical security emergency, not physical.

Explanation C. Facility fire is a physical security emergency.

Explanation D. Flooding is a physical security emergency.

PrepLogic Question: 4293-598

51. Review Question p. 188

Answers: A

Explanation A. CO2 or Halon are most effective against electrical fires. Type C fire extinguishers use CO2, Halon, or a Halon replacement to suppress electrical fires.

Explanation B. Soda acid is not an effective suppressant medium for electrical fires.

Explanation C. Water is not an effective suppressant medium for electrical fires.

Explanation D. Soda ash is not an effective suppressant medium for electrical fires.

PrepLogic Question: 4293-599

52. Review Question p. 188

Answers: D

Explanation A. CO2, soda acid, and Halon found in Type B fire extinguishers are designed for use against burning liquids.

Explanation B. CO2, soda acid, and Halon found in Type B fire extinguishers are designed for use against burning liquids.

Explanation C. CO2, soda acid, and Halon found in Type B fire extinguishers are designed for use against burning liquids.

Explanation D. Water should never be used to attempt to extinguish burning liquids. In most cases, water will help spread the fire rather than suppress it.

PrepLogic Question: 4293-600

53. Review Question p. 188

Answers: B

Explanation A. A bucket of sand is not effective enough as a suppressant for electrical fires and can cause additional damage to electrical components.

Explanation B. Type C fire extinguishers use CO2, Halon, or a Halon replacement to suppress electrical fires. Type C is the best choice for a data center.

Explanation C. A bucket of water is not effective as a suppressant for electrical fires and can cause additional damage to electrical components.

Explanation D. CO2, soda acid, and Halon found in Type B fire extinguishers are designed for use against burning liquids, not for use on electrical fires.

PrepLogic Question: 4293-601

54. Review Question p. 189

Answers: C

Explanation A. Fire detectors respond to a fire through a sensor that may detect heat (i.e., a sharp rise in temperature).

Explanation B. Fire detectors respond to a fire through a sensor that may detect light (i.e., the flickering illumination of flames).

Explanation C. Fire detectors do not sense the sound of fire. Intrusion detection alarms or certain types of motion detectors use sound (such as glass breaking or the change in a steadily broadcast frequency) to detect movement.

Explanation D. Fire detectors respond to a fire through a sensor that may detect smoke (i.e., a significant change in the electrical conductivity of the air).

PrepLogic Question: 4293-602

55. Review Question p. 189

Answers: D

Explanation A. Smoke actuated fire detectors are the most common; however, they are inexpensive and not the fastest detection method.

Explanation B. Fixed temperature, heat actuated detectors do not detect fires quickly, but only after the room's temperature reaches a pre-determined level. That level needs to be high enough not to be triggered falsely by the heating system or a failure of the A/C.

Explanation C. Rate of rise heat actuated cause many false alarms.

Explanation D. Flame actuated fire detectors are considered the most expensive but also the fastest in detecting fires.

PrepLogic Question: 4293-603

56. Review Question p. 189

Answers: A

Explanation A. Deluge systems are a form of dry pipe system, but with a larger volume of water. Deluge systems are not recommended for data centers.

Explanation B. A preaction system fills the pipes when the fire is initially detected,

then releases the water after a second level of detection is triggered. A preaction system gives site operators the chance to disable the system before the water is released in the event of a false alarm or a small fire that is brought under control quickly. A preaction system is the most recommended system for data centers.

Explanation C. A dry pipe system holds compressed air that keeps water out of the system. Once a fire is detected, the air is released allowing the pipes to fill with and release water. A dry pipe system is not recommended for data centers since no intervention mechanism is built into the system: once it is triggered, water will be released.

Explanation D. A wet pipe system always contain water. A wet pipe system is not recommended for data centers since no intervention mechanism is built into the system: once it is triggered, water will be released.

PrepLogic Question: 4293-604

57. Review Question p. 190

Answers: B

Explanation A. A preaction system fills the pipes when the fire is initially detected, then releases the water after a second level of detection is triggered. A preaction system gives site operates the chance to disable the system before the water is released in the event of a false alarm or a small fire that is brought under control quickly. A preaction system is the most recommended water-based system for data centers, but only if a gas discharge system is not available. Water is a poor selection of a suppression medium for a data center, especially since a false alarm release could cause significant damage to equipment.

Explanation B. A gas discharge system is most appropriate for data centers since a gas can be selected that will cause the least damage to the equipment in the event of a real or a false alarm release of the suppression medium.

Explanation C. Deluge systems are a form of dry pipe system, but with a larger volume of water. Deluge systems are not recommended for data centers. Water is a poor selection of a suppression medium for a data center, especially since a false alarm release will cause significant damage to equipment.

Explanation D. A dry pipe system holds compressed air that keeps water out of the system. Once a fire is detected, the air is released allowing the pipes to fill with and release water. A dry pipe system is not recommended for data centers since no intervention mechanism is built into the system: once it is triggered, water will be released. Water is a poor selection of a suppression medium for a data center, especially since a false alarm release could cause significant damage to equipment.

PrepLogic Question: 4293-605

58. Review Question p. 190

Answers: C

Explanation A. A water based system suppresses fires by means of heat reduction.

Explanation B. A foaming agent based system suppresses fires by means of isolating or separating the fuel from the fire.

Explanation C. A gas discharge system primarily suppresses fires by means of oxygen displacement.

Explanation D. There is no known means of interrupting the chemical reaction of burning other than by removing heat, fuel, or oxygen.

PrepLogic Question: 4293-606

59. Review Question p. 190

Answers: D

Explanation A. Halon is extremely effective against all types of fires, including electrical.

Explanation B. Halon is not as expensive as some of the ecological replacements being used, but it is more expensive than water, soda ash, or CO2 based systems.

Explanation C. Halon is no more difficult to manage than any other medium in a gas discharge suppression system.

Explanation D. Halon degrades into toxic chemicals at 900 degrees. Also, Halon uses CFCs which are thought to damage the ozone layer. Due to these issues, Halon has been restricted by the Montreal Protocol.

PrepLogic Question: 4293-607

60. Review Question p. 191

Answers: A

Explanation A. FM-200 is the most commonly used ecological replacement for Halon in gas discharge systems.

Explanation B. Low pressure waters mists is an ecological replacement, but it requires a change from a gas discharge system to a water based system.

Explanation C. CO2 is reasonably effective against most fires and is considerably less expensive than Halon, but it is not the most common ecological replacement for Halon in gas discharge systems.

Explanation D. Halon 1301 is the gas suppression medium that is being replaced.

PrepLogic Question: 4293-608

61. Review Question p. 191

Answers: B

Explanation A. Argon is an ecological replacement for Halon in gas discharge fire suppression systems.

Explanation B. Neon is not a fire suppressant, thus it is an inappropriate replacement for Halon.

Explanation C. Inergen is an ecological replacement for Halon in gas discharge fire suppression systems.

Explanation D. NAF-S-III is an ecological replacement for Halon in gas discharge fire suppression systems.

PrepLogic Question: 4293-609

62. Review Question p. 191

Answers: C

Explanation A. Smoke is often a significant cause of damage to computer equipment.

Explanation B. Combustion is often a significant cause of damage to computer equipment, since it causes both smoke and heat. Plus, if the fuel is the computer or its components, destruction is direct.

Explanation C. The suppression medium, Halon or its replacement equivalents, are designed to cause little or no damage to electrical equipment.

Explanation D. Heat is often a significant cause of damage to computer equipment.

PrepLogic Question: 4293-610

63. Review Question p. 192

Answers: D

Explanation A. A benefit of security guards is their ability to respond to changing situations.

Explanation B. A benefit of security guards is their ability to detect unique intrusions and attacks.

Explanation C. A benefit of security guards is their ability to make value judgments in the midst of an incident.

Explanation D. Being susceptible to social engineering or any form of intrusion or attack is a disadvantage of any security mechanism, include security guards.

PrepLogic Question: 4293-611

64. Review Question p. 192

Answers: A

Explanation A. A benefit of security guards is their ability to offer discriminating judgment on site.

Explanation B. A disadvantage of security guards is they are not appropriate in all environments.

Explanation C. A disadvantage of security guards is they may include fraudulent information on their job application or resume that results in them obtaining a job position that they are not qualified for.

Explanation D. A disadvantage of security guards is they may get sick. This can result in poor performance on site, the necessity to leave their post, or their not showing up for work altogether.

PrepLogic Question: 4293-612

65. Review Question p. 192

Answers: B

Explanation A. Rarely is lighting a sufficient replacement or alternative for security guards.

Explanation B. For certain situations, dogs are the most suitable replacement or alternative for security guards. Dogs are suitable replacements for security guards when the primary need is to prevent tresspassing.

Explanation C. Rarely is fencing a sufficient replacement or alternative for security

guards.

Explanation D. Rarely are proximity detectors a sufficient replacement or alternative for security guards.

PrepLogic Question: 4293-613

66. Review Question p. 193

Answers: C

Explanation A. Dogs are often expensive, this is a disadvantage.

Explanation B. Dogs are very high maintenance, this is a disadvantage.

Explanation C. Guard dogs are excellent tools for perimeter security control.

Explanation D. Dogs require insurance and have a significant liability associated with them; this is a disadvantage.

PrepLogic Question: 4293-614

67. Review Question p. 193

Answers: D

Explanation A. Lighting is the most commonly used physical security mechanism, but few non-security professionals recognize it as a defining structure to indicate the outer perimeter of a secured or controlled area.

Explanation B. Proximity detectors are an invisible means of establishing a security perimeter, therefore they are not recognized by the unauthorized or uninformed observer.

Explanation C. Locked doors are often used inside a secured or controlled area, not as the defining mechanism for the outer perimeter.

Explanation D. Fencing is the most recognized physical security mechanism used to define the outer perimeter of a secured or controlled area.

PrepLogic Question: 4293-615

68. Review Question p. 193

Answers: A

Explanation A. Casual trespassers are usually deterred by a fence a minimum of 3 to 4

feet high. They are also deterred by stronger or higher means, such as a fence 6 feet high. However, this question asked only for a deterrent against just casual trespassers, not stronger mechanisms of trespassing protection.

Explanation B. A lighted perimeter discouraged prowlers and casual intruders, but not casual trespassers (i.e., those making a choice to violate a perimeter, but who are not intent on completing a destructive activity or further crime).

Explanation C. A wooden fence 6 feet high is more than sufficient to deter casual trespassers. However, this question asked only for a deterrent against just casual trespassers, not stronger mechanisms of trespassing protection.

Explanation D. Posted "authorized entry only" signs, unless posted on a sufficiently high fence, are as in effective as lighting in preventing casual trespassers.

PrepLogic Question: 4293-616

69. Review Question p. 194

Answers: B

Explanation A. A gate offers no means to control a subject during or after the authentication process.

Explanation B. A mantrap is the most effective means to contain a subject while the authentication process is performed, so that in the event of a failure, a security guard response can result in the capture of the subject. In a mantrap, a subject must enter a small room that has both doors locked. Only after a successful authentication is the inner door opened for entry. If the authentication fails, a security guard is notified and the subject is detained within the enclosure.

Explanation C. A turnstile offers no means to control a subject during or after the authentication process. A turnstile merely provides a means to control the direction of flow of traffic.

Explanation D. A proximity detector offers no means to control a subject during or after the authentication process. Proximity detectors open a door or gate when an authorized user approaches.

PrepLogic Question: 4293-617

70. Review Question p. 194

Answers: C

Explanation A. Fencing is the most clearly recognized form of perimeter protection and

boundary definition, but it is not the most widely deployed mechanism.

Explanation B. Guard dogs are effective only within a fenced area. Dogs cannot provide the flexibility of lighting.

Explanation C. The most commonly deployed form of perimeter protection is lighting.

Explanation D. CCTV is spreading in the level of deployment, but it still trails far behind the deployment of lighting.

PrepLogic Question: 4293-618

71. Review Question p. 194

Answers: A

Explanation A. The use of closed circuit television (CCTV) for monitoring live events is considered a preventative form of security control. There is a small distinction in the use of CCTV: viewing live events is preventative; recording events is detective. If a subject knows they are being watched, they are less likley to commit a violation. Recorded video simply helps detect violations.

Explanation B. The use of closed circuit television (CCTV) for monitoring live events is considered a preventative form of security control. There is a small distinction in the use of CCTV: viewing live events is preventative; recording events is detective. If a subject knows they are being watched, they are less likley to commit a violation. Recorded video simply helps detect violations.

Explanation C. The use of closed circuit television (CCTV) that is actively monitored by security guards who can react to a situation is considered a responsive form of security control.

Explanation D. There is no corrective security control mechanism that involves the use of closed circuit television (CCTV). Corrective security controls self-adjust to changing situations to maintain security.

PrepLogic Question: 4293-619

72. Review Question p. 195

Answers: D

Explanation A. 8 candle feet power at 2 feet in height is incorrect. The NIST standard for perimeter protection provided by light is that critical areas should be illuminated by 2 candle feet power at 8 feet in height.

Explanation B. Fencing is not addressed by the NIST standard. A chain link fence 3 to 4 feet tall without barbed wire is sufficient to deter casual trespassers.

Explanation C. Fencing is not addressed by the NIST standard. A chain link fence 8 feet tall with 3 strands of barbed wire is sufficient to deter intruders.

Explanation D. The NIST standard for perimeter protection provided by light is that critical areas should be illuminated by 2 candle feet power at 8 feet in height.

PrepLogic Question: 4293-621

73. Review Question p. 195

Answers: B

Explanation A. Rules based access controls is an example of a technical/logical security control.

Explanation B. CCTV is an example of a physical security control.

Explanation C. Exit interviews is an example of an administrative security control.

Explanation D. Traffic tunneling is an example of a technical/logical security control.

PrepLogic Question: 4293-736

74. Review Question p. 195

Answers: C

Explanation A. Dogs are an example of a physical security control.

Explanation B. Fencing is an example of a physical security control.

Explanation C. Biometric authentication is an example of a technical/logical security control.

Explanation D. Badge IDs are an example of a physical security control.

PrepLogic Question: 4293-737

75. Review Question p. 196

Answers: B

Explanation A. Plenum cable is not any more resistant to wire tapping than any other form of copper wire based cabling.

Explanation B. Plenum cable should be used when wiring any facility since it won't produce toxic fumes when burned.

Explanation C. Plenum cable is available in multiple category types or throughput ratings. The fact that it is Plenum does not directly improve overall throughput.

Explanation D. Plenum cable is inexpensive, but there are other less expensive forms of cabling (most of which do produce toxic fumes when burned).

PrepLogic Question: 4293-817

Explanations: Chapter 9

1. Review Question p. 197

   Answers: C

   Explanation A. Data remanence is the data that remains after a media has been improperly purged.

   Explanation B. Data diddling is the alteration of data.

   Explanation C. Data hiding is the use of a covert channel, such as a fake bad sector on a hard drive, to store and transmit data.

   Explanation D. Data reduction is the automated task of locating significant information within a large collection of data.

   PrepLogic Question: 4293-173

2. Review Question p. 197

   Answers: C

   Explanation A. Screening applets at firewalls is an effective means to mitigate the threat of malicious code in a DCE.

   Explanation B. Configuring browsers to accept code only from trusted servers is an effective means to mitigate the threat of malicious code in a DCE.

   Explanation C. Avoiding the use of FTP is the least effective means to mitigate the threat of malicious code in a DCE.

   Explanation D. Training users regarding mobile code is an effective means to mitigate the threat of malicious code in a DCE.

   PrepLogic Question: 4293-199

3. Review Question p. 197

   Answers: A

   Explanation A. C2 does not require configuration and change control management.

   Explanation B. B2, B3, and A1 all require configuration and change control management.

Explanation C. B2, B3, and A1 all require configuration and change control management.

Explanation D. B2, B3, and A1 all require configuration and change control management.

PrepLogic Question: 4293-506

4. Review Question p. 198

Answers: B

Explanation A. The Orange book defines Operational and Life Cycle assurance.

Explanation B. The Orange book defines Operational and Life Cycle assurance.

Explanation C. The Orange book defines Operational and Life Cycle assurance.

Explanation D. The Orange book defines Operational and Life Cycle assurance.

PrepLogic Question: 4293-511

5. Review Question p. 198

Answers: C

Explanation A. System architecture, system integrity, covert channel analysis, trusted facility management, and trusted recovery are all elements of operational assurance as defined by the Orange book.

Explanation B. System architecture, system integrity, covert channel analysis, trusted facility management, and trusted recovery are all elements of operational assurance as defined by the Orange book.

Explanation C. Security testing, design specification and testing, configuration management, and trusted distribution are all elements of Life cycle assurance as defined by the Orange book.

Explanation D. System architecture, system integrity, covert channel analysis, trusted facility management, and trusted recovery are all elements of operational assurance as defined by the Orange book.

PrepLogic Question: 4293-512

6. Review Question p. 198

Answers: D

Explanation A. Security testing, design specification and testing, configuration management, and trusted distribution are all elements of Life cycle assurance as defined by the Orange book.

Explanation B. Security testing, design specification and testing, configuration management, and trusted distribution are all elements of Life cycle assurance as defined by the Orange book.

Explanation C. Security testing, design specification and testing, configuration management, and trusted distribution are all elements of Life cycle assurance as defined by the Orange book.

Explanation D. System architecture, system integrity, covert channel analysis, trusted facility management, and trusted recovery are all elements of operational assurance as defined by the Orange book.

PrepLogic Question: 4293-513

7. Review Question p. 199

Answers: C

Explanation A. The Common Criteria define the three types of trusted recovery as manual, automated, and automated without undo loss.

Explanation B. The Common Criteria define the three types of trusted recovery as manual, automated, and automated without undo loss.

Explanation C. The Common Criteria does not define a type of trusted recovery named asynchronous assisted recovery.

Explanation D. The Common Criteria define the three types of trusted recovery as manual, automated, and automated without undo loss.

PrepLogic Question: 4293-520

8. Review Question p. 199

Answers: A

Explanation A. Resource isolation provides for auditing and tracking of all events, including minor ones.

Explanation B. Resource isolation allows for the subject and object to be clearly identified.

Explanation C. Resource isolation provides for enforced accountability.

Explanation D. Resource isolation provides for independent assignment of permissions and rights.

PrepLogic Question: 4293-624

9. Review Question p. 199

Answers: B

Explanation A. Trusted computing base does not require physical separation of memory. Trusted computing base is founded on the notion that a collection of computer components work in unison to support a security policy.

Explanation B. The separation of memory physically instead of just logically is an example of and a requirement for hardware segmentation.

Explanation C. A division between user mode and kernel mode is not founded upon physical memory separation. Such a division is designed into the OS based on the use of the theory of protection rings.

Explanation D. Data classification levels have nothing to do with physical memory separation. Data classification levels are defined by the security policy and objects are assigned a classification by the data owner.

PrepLogic Question: 4293-625

10. Review Question p. 200

Answers: D

Explanation A. Data diddling is the alteration of data.

Explanation B. Data hiding is placing restricted data in a different security domain so a specific subject is unaware of its existence.

Explanation C. Abstraction is the grouping of subjects or objects into classes for bulk control or privilege assignment.

Explanation D. Layering restricts communications so that they only occur through controlled interfaces in order to maintain the security.

PrepLogic Question: 4293-627

11. Review Question p. 200

Answers: A

Explanation A. Data hiding is placing restricted data in a different security domain so a specific subject is unaware of its existence. Data hiding is also the absence of a communication interface between security layers in order to prevent subjects from obtaining knowledge of a confidential resource.

Explanation B. Laying restricts communications to detailed and controlled interfaces in order to maintain the security.

Explanation C. Data classification is the labeling of a resource so it can be properly managed and positioned within a security infrastructure.

Explanation D. Abstraction is the grouping of subjects or objects into classes for bulk control or privilege assignment.

PrepLogic Question: 4293-628

12. Review Question p. 200

Answers: B

Explanation A. A state machine model is secure in every instance of its existence.

Explanation B. A state machine model executes commands and transactions securely.

Explanation C. A state machine model boots into a secure state, even after an error is encountered.

Explanation D. A state machine model restricts subjects to access resources.

PrepLogic Question: 4293-629

13. Review Question p. 201

Answers: C

Explanation A. A row of an access control matrix is known as a capability list.

Explanation B. A tuple is a row in a database table.

Explanation C. A column of an access control matrix is known as an access control list.

Explanation D. An ordinal set is a fake distracter, as no such entity associated with an access control matrix is called an ordinal set. In mathematics, an ordinal set is a series of numbers that begins with 0.

PrepLogic Question: 4293-630

14. Review Question p. 201

Answers: D

Explanation A. The Bell-LaPadula model is a lattice model that protects confidentiality.

Explanation B. The Biba model is a lattice model that protects integrity.

Explanation C. The Clark-Wilson model protects against unauthorized modifications.

Explanation D. The Take-Grant model defines the relationships that allow a subject to transfer rights to objects. It also defines the rights that a subject can take from another subject.

PrepLogic Question: 4293-631

15. Review Question p. 201

Answers: A

Explanation A. The Bell-LaPadula security model is primarily concerned with confidentiality.

Explanation B. The Biba security model is primarily concerned with integrity.

Explanation C. No security model is focused on protecting non-repudiation. Non-repudiation is provided for by digital signatures.

Explanation D. No security model is focused on protecting accountability. Accountability is made possible through identification, authentication, authorization, and auditing.

PrepLogic Question: 4293-632

16. Review Question p. 202

Answers: B

Explanation A. The * (star) integrity axiom, no write up, is the primary regulation of the Biba security model.

Explanation B. The * (star) property rule, no write down, is the primary regulation of the Bell-LaPadula security model.

Explanation C. No write up, or the * (star) integrity axiom, is the primary regulation of the Biba security model.

Explanation D. No read down, the simple security axiom, is the secondary regulation of the Biba security model.

PrepLogic Question: 4293-633

17. Review Question p. 202

Answers: C

Explanation A. No write up, the * (star) integrity axiom, is the primary regulation of the Biba security model.

Explanation B. No write down, the * (star) integrity axiom, is the primary regulation of the Biba security model.

Explanation C. No read up, the simple security rule, is the secondary regulation of the Bell-LaPadula security model.

Explanation D. No read down, the simple security axiom, is the secondary regulation of the Biba security model.

PrepLogic Question: 4293-634

18. Review Question p. 202

Answers: D

Explanation A. Bell-LaPadula does not address covert channels. This is a weakness.

Explanation B. Bell-LaPadula does not address file sharing. This is a weakness.

Explanation C. Bell-LaPadula does not specifically define what a secure state transition actually is. This is a flaw or oversight.

Explanation D. Bell-LaPadula is based on a multilevel security policy. This is a feature and usually a benefit.

PrepLogic Question: 4293-635

19. Review Question p. 203

Answers: A

Explanation A. The Biba security model is primarily concerned with integrity.

Explanation B. The Bell-LaPadula security model is primarily concerned with confidentiality or disclosure.

Explanation C. No security model is focused on protecting availability. Availability is the assurance that a resource will be accessible in a timely manner.

Explanation D. The Bell-LaPadula security model is primarily concerned with confidentiality.

PrepLogic Question: 4293-636

20. Review Question p. 203

Answers: B

Explanation A. No write down is the primary regulation of the Bell-LaPadula security model.

Explanation B. No write up, the * (star) integrity axiom, is the primary regulation of the Biba security model.

Explanation C. No read down, the simple security axiom, is the secondary regulation of the Biba security model.

Explanation D. No read up is the secondary regulation of the Bell-LaPadula security model.

PrepLogic Question: 4293-637

21. Review Question p. 203

Answers: C

Explanation A. The Take-Grant model defines the relationships that allow a subject to transfer rights to objects. It also defines the rights that a subject can take from another subject. It is not an analog to the Bell-LaPadula security model.

Explanation B. Clark-Wilson model protects against unauthorized modifications. It is not an analog to the Bell-LaPadula security model.

Explanation C. The Biba security model developed as the integrity analog to the Bell-LaPadula security model.

Explanation D. The Information Flow model controls how data is moved to and from approved levels. It is not an analog to the Bell-LaPadula security model.

PrepLogic Question: 4293-638

22. Review Question p. 204

Answers: D

Explanation A. The Clark Wilson model is not a lattice based model. The boundary controls of LUB and GLB are related to lattice based models.

Explanation B. The non-interference model is not lattice based.

Explanation C. The Biba is an integrity model that is a lattice based model, but not all lattice based models are integrity focused.

Explanation D. The lattice model uses the boundary controls of least upper bound (LUB) and greatest lower bound (GLB).

PrepLogic Question: 4293-639

23. Review Question p. 204

Answers: A

Explanation A. Clark-Wilson model is focused on preventing authorized users from making unauthorized modifications to data.

Explanation B. The Bell-LaPadula security model is primarily concerned with confidentiality.

Explanation C. The Biba security model is primarily concerned with integrity.

Explanation D. The Take-Grant model defines the relationships that allow a subject to transfer rights to objects. It also defines the rights that a subject can take from another subject.

PrepLogic Question: 4293-640

24. Review Question p. 204

Answers: B

Explanation A. Within the Clark-Wilson security model subjects can access resources only through authorized interfaces.

Explanation B. The Biba security model uses three levels of integrity axioms: high, medium, and low. Clark-Wilson does not.

Explanation C. Within the Clark-Wilson security model separation of duties is compulsory.

Explanation D. Within the Clark-Wilson security model auditing is mandatory.

PrepLogic Question: 4293-641

25. Review Question p. 205

Answers: C

Explanation A. The Biba security model is primarily concerned with integrity. However, it is based on the information flow model which manages the movement of data between levels. While this may be a technically correct answer, it is not the best answer for this specific question and answer option set.

Explanation B. Clark-Wilson model is focused on preventing authorized users from making unauthorized modifications to data.

Explanation C. The Information Flow model controls how data is moved to and from approved levels.

Explanation D. The Noninterference model is concerned with preventing the actions of subjects at one security level from being noticed by or affecting subjects at a different security level.

PrepLogic Question: 4293-642

26. Review Question p. 205

Answers: D

Explanation A. The Biba security model is primarily concerned with integrity.

Explanation B. Clark-Wilson model is focused on preventing authorized users from making unauthorized modifications to data.

Explanation C. The Information Flow model controls how data is moved to and from approved levels.

Explanation D. The Noninterference model is concerned with preventing the actions of subjects at one security level from being noticed by or affecting subjects at a different security level.

PrepLogic Question: 4293-643

27. Review Question p. 205

Answers: A

Explanation A. Dedicated security mode is represented by the state when all users have the clearance or need to know for all information stored on a system.

Explanation B. System-high security mode is represented by the state when all users have the clearance, but not the need to know, for all information stored on a system.

Explanation C. Compartmented security mode is represented by the state when users are limited to resource access based on need to know and formal access approval (i.e., real-time clearance for access by a superior).

Explanation D. Multilevel security mode is represented by the state when a user can process data from two or more different security classifications when that user does not have full clearance access for all data in all reference security classifications.

PrepLogic Question: 4293-644

28. Review Question p. 206

Answers: B

Explanation A. Multilevel security mode is represented by the state when a user can process data from two or more different security classifications when that user does not have full clearance access for all data in all reference security classifications.

Explanation B. Compartmentalized security mode is represented by the state when users are limited to resource access based on need to know and formal access approval (i.e., real-time clearance for access by a superior). And, users of a compartmentalized security mode system are limited to processing data from a single level of classification.

Explanation C. System-high security mode is represented by the state when all users have the clearance but not the need to know for all information stored on a system.

Explanation D. Dedicated security mode is represented by the state when all users have the clearance or need to know for all information stored on a system.

PrepLogic Question: 4293-645

29. Review Question p. 206

Answers: C

Explanation A. A system within the system-high security mode function at a single security level, but users do not necessarily have all the need to know for all data on the

system.

Explanation B. A system within the multilevel security mode can function at multiple security levels and users do not necessarily have all the need to know for all data on the system.

Explanation C. A system within the dedicated security mode functions at a single security level, but users do not necessarily have all the need to know for all data on the system.

Explanation D. A system within the compartmented security mode can function at multiple security levels and users do not necessarily have all the need to know for all data on the system.

PrepLogic Question: 4293-646

30. Review Question p. 206

Answers: D

Explanation A. A system is labeled as having assurance when a high level of confidence can be placed in the security of a system since its trust has been more thoroughly verified.

Explanation B. A system is labeled as having certification when it meats the checklist of criteria required for a specific level of security certification.

Explanation C. A system is accredited when it has passed a thorough examination to verify its compliance with a specific certification checklist.

Explanation D. A system is labeled as trusted when all of the security protection mechanism work in concert to process and handle sensitive data without violating the trusted computer base or the applicable security policy.

PrepLogic Question: 4293-647

31. Review Question p. 207

Answers: A

Explanation A. Information Technology Security Evaluation Criteria (ITSEC) is the set of European standards.

Explanation B. Common Criteria (CC) is the newly developed set of standards that were designed to replace TCSEC and ITSEC.

Explanation C. European Union Trusted Computer System Evaluation Criteria (EU TCSEC) is a fake distracter. There is no such standard.

Explanation D. Trusted Computer System Evaluation Criteria (TCSEC) is the standards for the US.

PrepLogic Question: 4293-648

32. Review Question p. 207

Answers: C

Explanation A. A denial of service may be implemented after a buffer overflow, but DoS is not the best choice.

Explanation B. A logic bomb may be planted onto a system due to the access gained by a buffer overflow attack, but logic bomb is not the best choice.

Explanation C. Failing to control input may result in a buffer overflow.

Explanation D. A virus infection may result due to the system violations that occur after a buffer overflow, but virus infection is not the best choice.

PrepLogic Question: 4293-649

33. Review Question p. 207

Answers: D

Explanation A. The ready state is the state of a process that is standing by to resume processing.

Explanation B. The wait state is the state of a process waiting for a specific event to finish.

Explanation C. A supervisory state is the state of a process executing a privileged activity or performing a system-level function.

Explanation D. The problem state is the state of a process performing normal execution.

PrepLogic Question: 4293-650

34. Review Question p. 208

Answers: A

Explanation A. Data hiding is the placement of data in a different security level than a given subject in order to hide it from that subject.

Explanation B. Layering is the method used to establish security levels where only adjacent levels can communicate and exchange information, and that through limiting or restrictive interfaces.

Explanation C. Data diddling is the act of altering data.

Explanation D. Abstraction is the process of grouping similar objects or subjects into a container so security mechanisms can act on them as a whole rather than as individual elements.

PrepLogic Question: 4293-651

35. Review Question p. 208

Answers: B

Explanation A. The Biba model is focused on protecting integrity.

Explanation B. The Bell-LaPadula model is focused on protecting confidentiality.

Explanation C. The Take-Grant model is focused on the exchange of rights between subjects.

Explanation D. The Clark-Wilson model is focused on protecting integrity by preventing authorized users from making unauthorized modifications.

PrepLogic Question: 4293-652

36. Review Question p. 208

Answers: C

Explanation A. The orange book (i.e. ITSEC) is concerned with stand-alone systems.

Explanation B. The tan book is concerned with auditing.

Explanation C. The red book (i.e. TNI) is concerned with the interactions of computers over a communication medium.

Explanation D. The purple book is concerned with development of production-quality formal verification systems.

PrepLogic Question: 4293-653

37. Review Question p. 209

Answers: A

Explanation A. Adding security as an afterthought is not an effective means to provide adequate, functional, or even reliable security.

Explanation B. Security should be integrated into a product at the design stage.

Explanation C. Security should be engineered into the product.

Explanation D. Security should be implemented by default in the product.

PrepLogic Question: 4293-654

38. Review Question p. 209

Answers: B

Explanation A. Once security has been implemented into a product, it should be tested.

Explanation B. Security should not be disabled once it has been integrated into a product.

Explanation C. Once security has been implemented into a product, it should be certified.

Explanation D. Once security has been implemented into a product, it should be audited.

PrepLogic Question: 4293-655

39. Review Question p. 209

Answers: C

Explanation A. Session hijacking occurs when a malicious entity takes over a communication session between two systems.

Explanation B. Access grabbing occurs when a user account exploits a flaw in the OS or software to access greater privileges than those which are assigned to them.

Explanation C. Failing to define boundaries for input can result in a buffer overflow error.

Explanation D. Information disclosure may occur as a result of a buffer overflow, but not all information disclosures occur because of a buffer overflow or a failure to set boundaries on input. Information disclosure occurs whenever a user without specific

access is able to access confidential resources.

PrepLogic Question: 4293-656

40. Review Question p. 210

Answers: A

Explanation A. Network throttling is usually not a function, symptom, or effect of a buffer overflow. Network throttling is a control feature to limit the bandwidth consumed by a specific application or service.

Explanation B. Buffer overflows can cause system freezing.

Explanation C. Buffer overflows can cause system reboots.

Explanation D. Buffer overflows can cause data corruption.

PrepLogic Question: 4293-658

41. Review Question p. 210

Answers: B

Explanation A. Primary storage is the memory area that is directly accessed by the CPU.

Explanation B. Once data has been processed by the CPU, it is moved into memory areas known as real storage. Real storage is the memory address space allocated for use by programs.

Explanation C. Secondary storage is any non-volitile data storage device, including hard drives, floppy disks, CD-ROMs, etc.

Explanation D. Virtual storage (also known as virtual memory) is the memory storage space created by combining physical RAM with a paging file stored on secondary storage devices. Real storage is part of virtual memory, but this answer option is not as accurate since it also includes a paging file. Data from the CPU must go into real storage first, then it may be moved to a paging file.

PrepLogic Question: 4293-659

42. Review Question p. 210

Answers: D

Explanation A. Ring 0 is the protection ring that hosts the OS kernel. It is not the

collection of mechanisms that support a security policy.

Explanation B. An assurance package is a system with verified compliance with a certified level of security. It is not the collection of mechanisms that support a security policy.

Explanation C. A white box system is a pre-built computer supplied by a manufacturer to a reseller who customizes the system and repackages it as their own. It is not the collection of mechanisms that support a security policy.

Explanation D. The collection of mechanisms within a computer system that work in harmony to enforce and support a security policy is known as the trusted computing base or TCB.

PrepLogic Question: 4293-660

43. Review Question p. 211

Answers: C

Explanation A. Static RAM or Random Access Memory stores data without needing to be refreshed.

Explanation B. ROM or Read Only Memory is permanent memory storage and does not need refreshing.

Explanation C. Dynamic RAM or Random Access Memory requires constant updates because the data it stores dissipates and decays.

Explanation D. EPROM or Erasable and Programmable Read Only Memory is permanent memory storage that does not need refreshing, but which can be erased and re-written.

PrepLogic Question: 4293-661

44. Review Question p. 211

Answers: D

Explanation A. Secondary storage is often 10 to 10,000 slower than cache.

Explanation B. Virtual storage includes secondary storage and therefore is slower than cache.

Explanation C. Real storage is slower than cache.

Explanation D. Cache memory is a form of high-speed memory accessed directly by the CPU and that operates at a higher rate than real memory.

PrepLogic Question: 4293-662

45. Review Question p. 211

Answers: A

Explanation A. The CPU is the most trusted component of a computer system.

Explanation B. Memory is not the most trusted component of a computer system.

Explanation C. Storage devices are not the most trusted component of a computer system.

Explanation D. Network interfaces are not the most trusted component of a computer system.

PrepLogic Question: 4293-663

46. Review Question p. 212

Answers: B

Explanation A. A memory mapper/manager does not prevent buffer overflows. Buffer overflows are only prevented by implementing boundary controls on input.

Explanation B. Software is not trusted, therefore it is isolated from managing hardware (i.e., memory) directly.

Explanation C. A memory mapper/manager does not address how software uses secondary storage except when it concerns virtual storage or memory.

Explanation D. The D1 TCSEC certification has no such restriction or requirement for a memory mapper.

PrepLogic Question: 4293-664

47. Review Question p. 212

Answers: C

Explanation A. Ring 0 hosts the OS kernel.

Explanation B. Ring 1 hosts the remainder of the core OS.

Explanation C. Device drivers are typically located in Ring 2.

Explanation D. Ring 3 hosts applications and programs.

PrepLogic Question: 4293-665

48. Review Question p. 212

Answers: D

Explanation A. Buffer overflows are errors caused by failing to validate input, they have nothing to do with processes in different protection rings communicating.

Explanation B. A change or shift in execution priority will not affect the need for a system call to be used to communicate from a higher numbered protection ring to a lower numbered one.

Explanation C. Processes are not moved between protection rings.

Explanation D. A system call is required for a a process in a higher ring number needs to communicate with a process or resource in a lower ring number.

PrepLogic Question: 4293-666

49. Review Question p. 213

Answers: A

Explanation A. The wait state is the state of a process waiting for a specific event to finish, such as a print job.

Explanation B. The ready state is the state of a process that is standing by to resume processing, but not waiting on some event to finish.

Explanation C. The problem state is the state of a process performing normal execution.

Explanation D. A supervisory state is the state of a process executing a privileged activity or performing a system-level function.

PrepLogic Question: 4293-667

50. Review Question p. 213

Answers: B

Explanation A. Multithreading is where a process has multiple execution threads.

Explanation B. Multitasking is where a computer system can execute more than one process simultaneously.

Explanation C. Multiprocessing is where a computer system has more than one CPU which can execute processes independently.

Explanation D. Multiplexing is the ability to transmit multiple signals on the same transmission or communications medium.

PrepLogic Question: 4293-668

51. Review Question p. 213

Answers: C

Explanation A. The more complex a security system, the less assurance it provides.

Explanation B. The more complex a security system, the less assurance it provides. Less complexity does not directly offer more assurance.

Explanation C. The more complex a security system, the less assurance it provides.

Explanation D. The more complex a security system, the less assurance it provides.

PrepLogic Question: 4293-669

52. Review Question p. 214

Answers: A

Explanation A. No system is fully secure. TCB provides a means to measure and evaluate the level of security offered.

Explanation B. If the TCB meets specific requirements, it can be said to provide a specific level of trust.

Explanation C. TCB can be built into a system, evaluated, and certified.

Explanation D. TCB certification provides a standardized system to compare the security capabilities between different systems and to provide a standardized label of the level of security it provides.

PrepLogic Question: 4293-670

53. Review Question p. 214

Answers: B

Explanation A. The tan book is concerned with auditing.

Explanation B. The orange book (TCSEC) is concerned with stand-alone systems.

Explanation C. The red book is concerned with the interactions of computers over a communication medium.

Explanation D. The purple book is concerned with development of production-quality formal verification systems.

PrepLogic Question: 4293-671

54. Review Question p. 214

Answers: C

Explanation A. This is a true statement. In order to ensure tight security, any congress between a security domain and the operating system kernel---or Trusted Control Block (TCB)---must be strictly regulated.

Explanation B. This is a true statement. A security domain entails everything a given subject can access.

Explanation C. This is NOT a true statement. Kernel mode---sometimes called supervisor mode---can basically perform any function. Essentially, a piece of software running in user mode that needs to perform some specialized function must place a call into kernel mode before it can function. Therefore, user mode can't have a larger security domain than kernel mode.

Explanation D. This is a true statement and a basic part of security planning and development. Security domains must be clearly identified, separated, and enforced.

PrepLogic Question: 4293-672

55. Review Question p. 215

Answers: D

Explanation A. Applications executing in user mode cannot access hardware directly.

Explanation B. Applications executing in user mode have their memory needs handled by a mediator process.

Explanation C. Applications executing in user mode can access resources only within its own security domain.

Explanation D. Applications executing in user mode do not have direct access to sensitive resources. Only application in kernel mode have such access.

PrepLogic Question: 4293-673

56. Review Question p. 215

Answers: B

Explanation A. Trusted Computer System Evaluation Criteria (TCSEC) security label A requires verified protection mechanisms and controls. Label A includes the requirements of label B, thus label B is the lowest level that requires mandatory protection control mechanisms.

Explanation B. Trusted Computer System Evaluation Criteria (TCSEC) security label B is the lowest level that requires mandatory protection mechanisms and controls.

Explanation C. Trusted Computer System Evaluation Criteria (TCSEC) security label C requires discretionary protection mechanisms and controls.

Explanation D. Trusted Computer System Evaluation Criteria (TCSEC) security label D requires minimal protection mechanisms and controls.

PrepLogic Question: 4293-674

57. Review Question p. 215

Answers: C

Explanation A. A1 is the Trusted Computer System Evaluation Criteria (TCSEC) security label that represents those systems with the highest degree of trust.

Explanation B. B2 is the Trusted Computer System Evaluation Criteria (TCSEC) security label that represents those systems with a slightly greater degree of trust than B1.

Explanation C. B1 is the Trusted Computer System Evaluation Criteria (TCSEC) security label that represents those systems with the least degree of trust (among those labels listed in this question).

Explanation D. B3 is the Trusted Computer System Evaluation Criteria (TCSEC) security label that represents those systems with the a greater degree of trust than B1 and B2, but not as much as A1.

PrepLogic Question: 4293-675

58. Review Question p. 216

Answers: D

Explanation A. Continuous protection is an evaluation criteria for establishing Trusted Computer System Evaluation Criteria (TCSEC) security labels. Other evaluation criteria not listed here include security policy, labels, documentation, and life cycle assurance.

Explanation B. Identification is an evaluation criteria for establishing Trusted Computer System Evaluation Criteria (TCSEC) security labels. Other evaluation criteria not listed here include security policy, labels, documentation, and life cycle assurance.

Explanation C. Accountability is an evaluation criteria for establishing Trusted Computer System Evaluation Criteria (TCSEC) security labels. Other evaluation criteria not listed here include security policy, labels, documentation, and life cycle assurance.

Explanation D. Task based access controls is not an evaluation criteria.

PrepLogic Question: 4293-676

59. Review Question p. 216

Answers: A

Explanation A. A is the highest Trusted Computer System Evaluation Criteria (TCSEC) label for security.

Explanation B. B is high, but not the highest Trusted Computer System Evaluation Criteria (TCSEC) label for security.

Explanation C. C is low, but not the lowest Trusted Computer System Evaluation Criteria (TCSEC) label for security.

Explanation D. D is the lowest Trusted Computer System Evaluation Criteria (TCSEC) label for security.

PrepLogic Question: 4293-677

60. Review Question p. 216

Answers: B

Explanation A. C1 is the Trusted Computer System Evaluation Criteria (TCSEC) security label that represents systems that employ discretionary protection.

Explanation B. B3 is the Trusted Computer System Evaluation Criteria (TCSEC) security label that represents systems that employ security domains.

Explanation C. C2 is the Trusted Computer System Evaluation Criteria (TCSEC) security label that represents systems that employ controlled access protection.

Explanation D. B2 is the Trusted Computer System Evaluation Criteria (TCSEC) security label that represents systems that employ structured protection.

PrepLogic Question: 4293-678

61. Review Question p. 217

Answers: C

Explanation A. C2 does not address covert channels.

Explanation B. B1 does not address covert channels.

Explanation C. B2 is the minimum Trusted Computer System Evaluation Criteria (TCSEC) security level that directly addresses covert channels.

Explanation D. A1 directly addresses covert channels, but it is not the minimum Trusted Computer System Evaluation Criteria (TCSEC) security level that does so.

PrepLogic Question: 4293-679

62. Review Question p. 217

Answers: A

Explanation A. Port blocking is not an effective countermeasure against buffer overflows. Buffer overflows occur because too much invalid data is submitted over an otherwise legitimate communications session.

Explanation B. Verifying input data is an effective countermeasure against buffer overflows.

Explanation C. Auditing can be an effective countermeasure against buffer overflows by catching patterns and indications of buffer overflow attacks.

Explanation D. Host based intrusion detection system can be an effective countermeasure against buffer overflows, by means of watching for suspicious behavior on the system.

PrepLogic Question: 4293-680

63. Review Question p. 217

Answers: B

Explanation A. ITSEC evaluates functionality and assurance separately while TCSEC evaluates them together.

Explanation B. ITSEC evaluates functionality and assurance separately while TCSEC evaluates them together.

Explanation C. ITSEC evaluates functionality and assurance separately while TCSEC evaluates them together.

Explanation D. ITSEC evaluates functionality and assurance separately while TCSEC evaluates them together.

PrepLogic Question: 4293-681

64. Review Question p. 218

Answers: D

Explanation A. Trusted Computer System Evaluation Criteria (TCSEC) addresses confidentiality only, not integrity or assurance.

Explanation B. Trusted Computer System Evaluation Criteria (TCSEC) works only with government data classifications.

Explanation C. Trusted Computer System Evaluation Criteria (TCSEC) employs only a few specific ratings and therefore is limited in its scope and depth.

Explanation D. Trusted Computer System Evaluation Criteria (TCSEC) does not address network connectivity, rather is only addresses stand alone systems. Trusted Computer System Evaluation Criteria (TCSEC) is the orange book.

PrepLogic Question: 4293-682

65. Review Question p. 218

Answers: A

Explanation A. The Red book (Trusted Network Interpretation) only addresses centralized networks with a single accreditation authority.

Explanation B. The Red book (Trusted Network Interpretation) addresses network connectivity.

Explanation C. The Red book (Trusted Network Interpretation) rates confidentiality and integrity.

Explanation D. The Red book (Trusted Network Interpretation) addresses denial of service protection.

PrepLogic Question: 4293-683

66. Review Question p. 218

Answers: C

Explanation A. TEMPEST is the study and control of stray electrical signals.

Explanation B. A backdoor is a maintenance hook installed by developers in software.

Explanation C. A covert channel is an information path that is not normally used to communicate information and therefore unprotected by the system's security mechanisms. Covert channels are a means by which data can be secretly disclosed to other systems or users. The two types of covert channels are storage and timing.

Explanation D. Data remanence is the data leftover after an incomplete purging (such as a delete or a single formatting) that may be used to extract the original content.

PrepLogic Question: 4293-684

67. Review Question p. 219

Answers: A

Explanation A. Bell-LaPadula is an example of a multi-level security model.

Explanation B. Information flow is not a multi-level security model, instead it analyses data movements. Information flow can be applied to multi-level models, but it can also apply to single-level models.

Explanation C. Clark-Wilson is not a multi-level security model, instead it focuses on preventing authorized users from making unauthorized modifications to data.

Explanation D. Take-Grant is not a multi-level security model, instead it focuses on the exchange of privileges between subjects and objects.

PrepLogic Question: 4293-685

68. Review Question p. 219

Answers: B

Explanation A. An expert system is a computing system that uses reasoning similar to that of a human. It is not a security focused system.

Explanation B. A state machine model is secure in each and every instance of its existence.

Explanation C. A neural network is a computer system modeled after the functioning of human neurons. It is not a security focused system.

Explanation D. A trusted computing base is the collection of security mechanisms within a computer system that enforces a security policy. It does not necessarily indicate that the system is secure in each and every instance of its existence.

PrepLogic Question: 4293-686

69. Review Question p. 219

Answers: D

Explanation A. A blinking light on a device could be used as a covert channel by altering the pattern of the blinks, disabling the blinking, or causing an otherwise steady light to blink.

Explanation B. Using a fraudulently marked bad sector to store data is a form of covert channel.

Explanation C. Using the timing of network packet transmissions is a form of covert channel.

Explanation D. A dedicated VPN is not a covert channel.

PrepLogic Question: 4293-687

70. Review Question p. 220

Answers: A

Explanation A. NIACAP does not offer a domain accreditation.

Explanation B. NIACAP offers site, type, and system accreditations.

Explanation C. NIACAP offers site, type, and system accreditations.

Explanation D. NIACAP offers site, type, and system accreditations.

PrepLogic Question: 4293-688

71. Review Question p. 220

Answers: C

Explanation A. B1 has a classification evaluation criteria that each object must have a classification label.

Explanation B. B1 has a classification evaluation criteria that each subject must have a clearance label.

Explanation C. B2 is the level which requires restrictions against cover channels, not B1.

Explanation D. B1 has a classification evaluation criteria that data leaving the system must have an accurate security label.

PrepLogic Question: 4293-689

72. Review Question p. 220

Answers: D

Explanation A. C2 TCSEC certification has a requirement of discretionary protection.

Explanation B. B2 TCSEC certification has a requirement of structured protection.

Explanation C. B3 TCSEC certification has a requirement of security domains.

Explanation D. A1 TCSEC certification has a requirement of verified protection.

PrepLogic Question: 4293-690

73. Review Question p. 221

Answers: B

Explanation A. The Information Technology Security Evaluation Criteria (ITSCE) E2 rating is roughly the equivalent of the Trusted Computer System Evaluation Criteria (TCSEC) B1 rating.

Explanation B. The Information Technology Security Evaluation Criteria (ITSCE) E4 rating is roughly the equivalent of the Trusted Computer System Evaluation Criteria (TCSEC) B2 rating.

Explanation C. The Information Technology Security Evaluation Criteria (ITSCE) E5 rating is roughly the equivalent of the Trusted Computer System Evaluation Criteria (TCSEC) B3 rating.

Explanation D. The Information Technology Security Evaluation Criteria (ITSCE) E6

rating is roughly the equivalent of the Trusted Computer System Evaluation Criteria (TCSEC) A1 rating.

PrepLogic Question: 4293-691

74. Review Question p. 221

Answers: C

Explanation A. The Trusted Computer System Evaluation Criteria (TCSEC) security evaluation method does not employ protection profiles to specify security requirements.

Explanation B. The Information Technology Security Evaluation Criteria (ITSEC)security evaluation method does not employ protection profiles to specify security requirements.

Explanation C. The Common Criteria (CC) security evaluation method employs protection profiles to specify security requirements.

Explanation D. European Union Trusted Computer System Evaluation Criteria (EU TCSEC) is a fake distracter. There is no such standard.

PrepLogic Question: 4293-692

75. Review Question p. 221

Answers: D

Explanation A. Both Certification and Accreditation must be rechecked or reverified after a specific period of time or after significant changes occur.

Explanation B. Both Certification and Accreditation must be rechecked or reverified after a specific period of time or after significant changes occur.

Explanation C. Both Certification and Accreditation must be rechecked or reverified after a specific period of time or after significant changes occur.

Explanation D. Both Certification and Accreditation must be rechecked or reverified after a specific period of time or after significant changes occur.

PrepLogic Question: 4293-693

76. Review Question p. 222

Answers: A

Explanation A. Department of Defense Information Assurance Certification and

Accreditation Process (DIACAP) is the certification and accreditation method employed by the department of defense.

Explanation B. National Information Assurance Certification and Accreditation Process (NIACAP) certification and accreditation method is employed by non-DoD (department of defense) sections of the government.

Explanation C. Commercial Information Security Analysis Process (CIAP) is a commercial version of the NIACAP being developed for the private sector.

Explanation D. Common Criteria (CC) is the newly developed set of evaluation standards that were designed to replace TCSEC and ITSEC.

PrepLogic Question: 4293-694

77. Review Question p. 222

Answers: B

Explanation A. Closed systems are proprietary.

Explanation B. Open systems, not closed systems, have published specifications for easy 3rd party component development.

Explanation C. Closed systems offers some level of security through obscurity.

Explanation D. Microsoft, Apple, and UNIX operating systems are not examples of closed systems, they are all open systems.

PrepLogic Question: 4293-695

78. Review Question p. 222

Answers: D

Explanation A. Firewalls are not effective safeguards against covert channels.

Explanation B. Vulnerabilility scanners are not effective safeguards against covert channels.

Explanation C. Anti-virus software is not an effective safeguard against covert channels.

Explanation D. Noise and traffic generation are the most effective means to protect against the use of covert channels. Traffic and trend analysis are the most effective means to detect the use of covert channels.

PrepLogic Question: 4293-696

79. Review Question p. 223

Answers: B

Explanation A. A maintenance hook is a back door that is installed by the original programmers and developers.

Explanation B. Back door is software or a break in a system's security imposed by a hacker that allows them to reconnect to a system at a later date.

Explanation C. A Trojan horse may be used to deposit back door software onto a system, but it is not the back door itself.

Explanation D. The term covert channel is sometimes incorrectly used to describe the means by which a hacker gains access to a system using malicious software or a security hole. However, a covert channel is a means of exchanging data that is not normally used to do so and therefore outside the range of protection by the security solution.

PrepLogic Question: 4293-697

80. Review Question p. 223

Answers: C

Explanation A. Encryption is an effective countermeasure against backdoors and maintenance hooks.

Explanation B. Network based intrusion detection system is an effective countermeasure against backdoors and maintenance hooks.

Explanation C. Strong authentication is not an effective countermeasure against backdoors and maintenance hooks since these subversive means to gain access to a system usually bypass the identification and authentication processes.

Explanation D. Strong access controls are an effective countermeasure against backdoors and maintenance hooks.

PrepLogic Question: 4293-698

Explanations: Chapter 10

1. Review Question p. 224

Answers: C

Explanation A. SQL operates at layer 5 the Session layer.

Explanation B. SQL operates at layer 5 the Session layer.

Explanation C. SQL operates at layer 5 the Session layer.

Explanation D. SQL operates at layer 5 the Session layer.

PrepLogic Question: 4293-242

2. Review Question p. 224

Answers: A

Explanation A. SSH-2 is a secure replacement for telnet.

Explanation B. S/MIME is a secure e-mail enhancement, not a telnet replacement.

Explanation C. SET is a secure e-commerce transaction system, not a telnet replacement.

Explanation D. S/WAN is a VPN using IPSec for security, not a telnet replacement.

PrepLogic Question: 4293-377

3. Review Question p. 224

Answers: B

Explanation A. WTLS provides Class 1: Anonymous authentication.

Explanation B. WTLS does not directly provide for challenge-response authentication.

Explanation C. WTLS provides Class 3: Two-way client and server authentication.

Explanation D. WTLS provides Class 2: Server authentication.

PrepLogic Question: 4293-390

4. Review Question p. 225

Answers: C

Explanation A. Data moving across a Wireless Application Protocol (WAP) gateway will be converted from WTLS to SSL.

Explanation B. Data is temporarily in the clear on a Wireless Application Protocol (WAP) gateway.

Explanation C. The Wireless Application Protocol (WAP) protocol stack does not include IPSec.

Explanation D. Authentication and authorization can be performed by wireless devices through PKI enabled transactions.

PrepLogic Question: 4293-391

5. Review Question p. 225

Answers: D

Explanation A. WAP is not primarily focused on security, but rather it is the entire wireless protocol stack. Also, WAP is a technology for portable devices, such as cell phones, any is not used for 802.11 wireless networking.

Explanation B. WTLS is an authentication protocol, but it does not provide encryption. WTLS is a protocol in the WAP protocol stack.

Explanation C. WDP is a transport protocol in the WAP protocol stack.

Explanation D. WEP is the algorithm used to provide encryption and authentication for 802.11b wireless networks.

PrepLogic Question: 4293-392

6. Review Question p. 225

Answers: A

Explanation A. WEP is an optional element of 802.11b.

Explanation B. WEP is reasonably strong. Or at least at the time of its selection it was considered reasonably strong. Today, WEP is considered fairly weak.

Explanation C. WEP is self-synchronizing.

Explanation D. WEP is computationally efficient.

PrepLogic Question: 4293-393

7. Review Question p. 226

Answers: B

Explanation A. 802.11 does not define an authentication form called "anonymous".

Explanation B. Open system authentication is also known as null authentication in the 802.11 specification.

Explanation C. Shared key is a form of authentication defined by the 802.11 specification; it is not, however, referred to as "null authentication".

Explanation D. 802.11 does not define an authentication form called "closed system".

PrepLogic Question: 4293-394

8. Review Question p. 226

Answers: A

Explanation A. A gateway can link two or more networks together even if they use different protocols.

Explanation B. A hub links systems together that are all using the same protocol and networking technology.

Explanation C. A bridge can link together networks using different networking technologies but the same protocol.

Explanation D. A router can link together networks using the same protocol and networking topology.

PrepLogic Question: 4293-774

9. Review Question p. 226

Answers: B

Explanation A. A screened-host or sacrificial-host firewall uses packet filtering.

Explanation B. A screened-host or sacrificial-host firewall provides network and application layer filtering.

Explanation C. A screened-host or sacrificial-host firewall uses a bastion host.

Explanation D. A screened-host or sacrificial-host firewall is a first generation firewall.

PrepLogic Question: 4293-775

10. Review Question p. 227

Answers: C

Explanation A. An application level firewall or application layer gateway is also known as a proxy server.

Explanation B. An application level firewall or application layer gateway is also known as a circuit level firewall.

Explanation C. An application level firewall or application layer gateway is not a dynamic firewall, it is a static firewall.

Explanation D. An application level firewall or application layer gateway is also known as a second generation firewall.

PrepLogic Question: 4293-776

11. Review Question p. 227

Answers: D

Explanation A. A static packet filtering firewall examines individual packets regardless of the communication session.

Explanation B. A stateful inspection firewall performs detailed inspections of the content of packets regardless of the communication session.

Explanation C. A kernel proxy firewall is a fifth generation firewall.

Explanation D. A second generation firewall (also known as an application level firewall, an application layer gateway, a circuit level firewall, or a proxy server) creates a virtual circuit between the workstation/client system and the server.

PrepLogic Question: 4293-777

12. Review Question p. 227

Answers: A

Explanation A. Third generation firewalls, or stateful inspection firewalls, may cause performance decreases, in comparison with first and second generation firewalls, due to the depth and extent of the stateful inspection process.

Explanation B. Third generation firewalls are stateful inspection firewalls.

Explanation C. Third generation firewalls, or stateful inspection firewalls, operate primarily at the network layer, but do perform data inspections at all layers of the OSI model.

Explanation D. Third generation firewalls, or stateful inspection firewalls, examine the state and content of data.

PrepLogic Question: 4293-778

13. Review Question p. 228

Answers: B

Explanation A. A fifth generation firewall is a kernel proxy.

Explanation B. A fourth generation firewall is a dynamic packet filtering firewall.

Explanation C. A third generation firewall is a stateful inspection firewall.

Explanation D. A second generation firewall is an application level firewall.

PrepLogic Question: 4293-779

14. Review Question p. 228

Answers: C

Explanation A. A host system must have at least two NICs in different networks to operate as a firewall.

Explanation B. All connected networks must used the same protocol in order for a host system to serve as a firewall. To convert between different protocols requires a gateway service.

Explanation C. The connected networks need not use the same networking topology. As long as the NICs support the correct topology and the networks use the same protocol, a host server can act as a firewall.

Explanation D. IP forwarding must be disabled, otherwise the system serves as a router instead of a firewall. As a firewall, packets must be inspected and subjected to filtering before being passed onto another network.

PrepLogic Question: 4293-780

15. Review Question p. 228

Answers: D

Explanation A. A DMZ may be used to allow Internet users to access systems placed within it, or it can be used as an extranet for a limited set of visitors, such as business partners. The primary purpose is to provide a double barrier to protect the private network. A DMZ is created by placing a router on either side of a multi-homed firewall host. Internet accessible systems can be connected to the firewall host, but all access is still filtered by the firewall.

Explanation B. A DMZ provides security against intrusions from the Internet, it is not primarily deployed to grant access for internal users to the Internet. However, such a configuration is possible and common.

Explanation C. A DMZ is not required to configure VPNs. In many cases, the presence of a DMZ can make VPN configuration more difficult.

Explanation D. A DMZ provides a high level of security for the private network by hiding the network behind itself.

PrepLogic Question: 4293-781

16. Review Question p. 229

Answers: A

Explanation A. Network address translation (NAT) allows private network clients to initiate communications with Internet services, but it does not allow Internet users to initiate communicates into the private network nor to extract network configuration information about the private network from any communications intercepted by external users.

Explanation B. A router often allows users connected to one port to extrapolate the network configuration off of other ports.

Explanation C. A firewall is used to block selecting communications but does not directly prohibit the ability to extract internal network configuration information from interactions.

Explanation D. Virtual private networking is used to securely connect remote system together using a public communication network, such as the Internet. VPNs do not prevent users at the end-points of the links from extracting internal network configuration information from interactions.

PrepLogic Question: 4293-782

17. Review Question p. 229

Answers: B

Explanation A. NAT does not offer proxy services. However, many proxy server products (hardware and software, including firewalls) offer NAT as a feature.

Explanation B. NAT allows private IP addresses to be used in a private network and still support communications with the Internet.

Explanation C. NAT does not offer traffic throttling. Some firewalls, ruters, proxy servers, and network interfaces offer traffic throttling features.

Explanation D. NAT does not perform packet filtering in the sense of a firewall. Firewalls provide packet filtering features.

PrepLogic Question: 4293-783

18. Review Question p. 229

Answers: C

Explanation A. Redirection is not another name for NAT. Redirection is the function of a router or switch.

Explanation B. Traffic routing is not another name of NAT. Traffic routing is performed by a router.

Explanation C. IP masking is another name for NAT. NAT masks the assigned IP address of its internal clients from all external users and services.

Explanation D. Virtual circuits is not another name for NAT. A virtual circuit is used to logically connect the end-points of a communication over a switched network.

PrepLogic Question: 4293-784

19. Review Question p. 230

Answers: D

Explanation A. The seven original top-level domain names used on the Internet are .com, .edu, .gov, .mil, .net, .org, and .int.

Explanation B. The seven original top-level domain names used on the Internet are .com, .edu, .gov, .mil, .net, .org, and .int.

Explanation C. The seven original top-level domain names used on the Internet are .com, .edu, .gov, .mil, .net, .org, and .int.

Explanation D. .biz is not one of the seven original top-level domain names used on the Internet.

PrepLogic Question: 4293-785

20. Review Question p. 230

Answers: A

Explanation A. The country codes or geographic top-level domain names are standardized 2 character names.

Explanation B. The seven original top-level domain names used on the Internet are all 3 characters long.

Explanation C. Many of the newer top-level domain names being used on the Internet contain 4 or more letters, such as .name, .corp, and .aero.

Explanation D. Many of the newer top-level domain names being used on the Internet contain 5 or more letters, such as .museum.

PrepLogic Question: 4293-786

21. Review Question p. 230

Answers: B

Explanation A. Caller ID is a valid remote access security method for authenticating connecting users. Caller ID verifies the phone number of the user before the connection is allowed.

Explanation B. Digital signatures is not a valid remote access security method for authenticating connecting users. Digital signatures are used to verify the identity of the source of a transmission, they are not used in the initial connection establishment authentication process.

Explanation C. Callback is a valid remote access security method for authenticating connecting users. Callback hangs up on the connection, then dials the user back to establish the communication session.

Explanation D. Restricted access is a valid remote access security method for authenticating connecting users. Restricted access verifies the IP address of the connecting system.

PrepLogic Question: 4293-787

22. Review Question p. 231

Answers: B

Explanation A. SONET does use fiber optic cable, but fiber optics alone does not provide for its ability to self-heal.

Explanation B. SONET is self-healing due to its use of redundant rings.

Explanation C. SONET does use token passing, but token passing alone does not provide for its ability to self-heal.

Explanation D. SONET does support numerous protocol types, but the use of various protocols does not provide for its ability to self-heal.

PrepLogic Question: 4293-788

23. Review Question p. 231

Answers: C

Explanation A. Circuit switching networks use physical permanent connections from one point to another.

Explanation B. Circuit switching networks have a single switched communication path.

Explanation C. Packet switching networks, not circuit switching ones, route data based on best path available.

Explanation D. Circuit switching networks are primarily voice oriented. The public telephone system is an example of a circuit switching network.

PrepLogic Question: 4293-789

24. Review Question p. 231

Answers: D

Explanation A. Packet switching networks transmit bursty or inconsistent levels of traffic. Circuit switching networks support only constant or consistent levels of traffic.

Explanation B. Packet switching networks incorporates variable delays in the transmission of data. Circuit switching networks have fixed delays in transmission.

Explanation C. Packet switching networks are sensitive to the loss of data. Circuit switching networks are sensitive to the loss of connection, not data.

Explanation D. Circuit switching networks are connection oriented. Packet switching

networks are data oriented or at least are not physical connection oriented.

PrepLogic Question: 4293-790

25. Review Question p. 232

Answers: A

Explanation A. The Internet's switching mechanisms can overall be described as a switched virtual circuit. Switched virtual circuits (SVC) are used for highly inconsistent transmissions. Switched virtual circuits are built when needed and torn down after use.

Explanation B. Circuit switching is only used on the Internet when users employ dial-up connections. Overall the Internet is not a circuit switching mechanism.

Explanation C. Packet switching is used extensively throughout the Internet, but overall it operates more like switched virtual circuits.

Explanation D. The Internet does have some permanent virtual circuits, but this does not describe it overall. Permanent virtual circuits (PVC) always exist once they are established.

PrepLogic Question: 4293-791

26. Review Question p. 232

Answers: B

Explanation A. Frame relay was not the first packet switching network, but it generally offers the fastest WAN connectivity.

Explanation B. X.25 was the first packet switching network.

Explanation C. ATM was not the first packet switching network, but it offers high bandwidth transmission with little delay.

Explanation D. SMDS was not the first packet switching network, but it offers bandwidth on demands and is a connectionless solution.

PrepLogic Question: 4293-792

27. Review Question p. 232

Answers: C

Explanation A. In a VPN in tunnel mode the original header and the data is encrypted and a new header is added to the packet for transport.

Explanation B. There is no such VPN mode as header throughput.

Explanation C. In a VPN in transport mode the data contained in the IP packet is encrypted but the header of the IP packet is not encrypted.

Explanation D. There is not such VPN mode as link hop.

PrepLogic Question: 4293-793

28. Review Question p. 233

Answers: D

Explanation A. L2TP enables a single point to point connection.

Explanation B. L2TP operates at the Data Link layer.

Explanation C. L2TP supports the encryption of multiple protocols.

Explanation D. PPTP (Point to Point Tunneling Protocol) uses PPP authentication and encryption services. L2TP uses IPSec.

PrepLogic Question: 4293-794

29. Review Question p. 233

Answers: A

Explanation A. IPSec is built into IPv6, but not the currently used IPv4. However, add-ons by many OSes enable IPSec to be used over IPv4.

Explanation B. IPSec encrypts and authenticates IP data.

Explanation C. IPSec is used to establish network to network connectivity.

Explanation D. IPSec supports multiple simultaneous tunnels.

PrepLogic Question: 4293-795

30. Review Question p. 233

Answers: C

Explanation A. No callback is the least secure selection from this list. Without callback, dial-up connections are subjected only to the logon authentication process.

Explanation B. Using callback to a user provided number is actually less secure than

not using callback at all. This feature should only be used when long distance charges are to be reversed for traveling users.

Explanation C. Using callback to a predetermined number is the most secure option. Ways to attack a predetermined callback is to hack the phone company and hijack a phone number or to use call forwarding at the predetermined number site.

Explanation D. There is no such thing as multilink callback. Callback only functions with a single line connection.

PrepLogic Question: 4293-796

31. Review Question p. 234

Answers: D

Explanation A. PAP does have a wide range of compatibility, but that is not a reason to avoid PAP.

Explanation B. PAP is an authentication protocol but it is not used exclusively by remote access systems. But even if it was, that is not a reason to avoid PAP.

Explanation C. PAP does not require the presence of a CA. But even if it did, that is not a reason to avoid PAP.

Explanation D. PAP transmits logon credentials in plain text and therefore provides no security or protection for the username and password. For this reason, PAP should be avoided. Challenge Handshake Authentication Protocol (CHAP) should be used instead.

PrepLogic Question: 4293-797

32. Review Question p. 234

Answers: A

Explanation A. TCP is connection-oriented, not connectionless.

Explanation B. TCP is full duplex.

Explanation C. TCP does use acknowledgements.

Explanation D. TCP does use sequenced segments.

PrepLogic Question: 4293-799

33. Review Question p. 234

Answers: B

Explanation A. At the application layer data is called a message.

Explanation B. At the Host-to-Host or Transport layer data is called a segment.

Explanation C. At the Internet or Network layer data is called a packet.

Explanation D. At the Network Access layer data is called a frame.

PrepLogic Question: 4293-800

34. Review Question p. 235

Answers: C

Explanation A. Attenuation is the signal loss due to wire length.

Explanation B. Noise is the signal interference caused by external EMI or RF sources.

Explanation C. Crosstalk is the occurrence of electronic signals spilling over from one wire to another.

Explanation D. Superzapping is the use of a tool to bypass security to recover a crashed system.

PrepLogic Question: 4293-801

35. Review Question p. 235

Answers: D

Explanation A. Ethernet is a baseband LAN transmission protocol. The opposite of baseband communication is broadband.

Explanation B. Ethernet is a CSMA/CD Carrier-Sense multiple Access with Collision Detection LAN transmission protocol. Many wireless communication protocols are CSMA based.

Explanation C. Ethernet is a CSMA/CD Carrier-Sense multiple Access with Collision Detection LAN transmission protocol. The Macintosh protocol LocalTalk is an example of a CSMA/CA protocol.

Explanation D. Ethernet is a CSMA/CD Carrier-Sense multiple Access with Collision Detection LAN transmission protocol.

PrepLogic Question: 4293-802

36. Review Question p. 235

Answers: A

Explanation A. A dynamic packet filtering firewall is able to self-modify its traffic filters.

Explanation B. A kernel proxy firewall is not able to self-modify. A kernel proxy operates at the protocol level to enforce the security policy via packet filtering.

Explanation C. A stateful inspection firewall is not able to self-modify. A stateful inspection firewall is able to analyze the contents of traffic to make filtering decisions.

Explanation D. An application level firewall is not able to self-modify. An application level firewall is able to filter traffic based on valid messages from a specified application or service.

PrepLogic Question: 4293-803

37. Review Question p. 236

Answers: C

Explanation A. UDP is an unreliable communications protocol since it does not use acknowledgements.

Explanation B. IP is an unreliable communications protocol since it does not use acknowledgements.

Explanation C. TCP is a reliable communications protocol since it uses acknowledgements.

Explanation D. TFTP is an application layer protocol, not network or transport one, and therefore does not include a mechanism, such as acknowledgements, to ensure data delivery.

PrepLogic Question: 4293-804

38. Review Question p. 236

Answers: D

Explanation A. FTP can be used to exchange files.

Explanation B. NFS can be used to exchange files.

Explanation C. TFTP can be used to exchange files.

Explanation D. Telnet cannot be used to exchange files, rather it is limited to running applications or commands remotely.

PrepLogic Question: 4293-805

39. Review Question p. 236

Answers: A

Explanation A. SMTP or Simple Mail Transport Protocol is used to transmit e-mail from server to server and from client to server.

Explanation B. LPD or Line Printer Daemon is a print server service that waits for print jobs to be submitted to it.

Explanation C. SNMP or Simple Network Management Protocol is used to monitor and gather information about the activities of various components on a network.

Explanation D. BootP or Bootstrap Protocol is used to obtain IP addressing information for systems without statically defined addresses and it is also used on diskless workstations to download a working terminal OS upon bootup.

PrepLogic Question: 4293-806

40. Review Question p. 236

Answers: A

Explanation A. Logical communication between peer layers of the OSI model are made possible through the use of encapsulation.

Explanation B. Remote procedure calls are not used by the OSI model to support logical communications between peer layers.

Explanation C. Direct addressing is not used by the OSI model to support logical communications between peer layers.

Explanation D. Broadcasts are not used by the OSI model to support logical communications between peer layers.

PrepLogic Question: 4293-807

41. Review Question p. 237

Answers: B

Explanation A. The Clark-Wilson model is a security model that focuses on preventing authorized users from making unauthorized modifications.

Explanation B. The OSI model is the abstract protocol model that is widely used as the standard framework for designing applications and network protocols and describing how they function.

Explanation C. NetBIOS is not a theoretical model, but a network protocol developed by IBM and used extensively by Microsoft.

Explanation D. MAC addressing is not a protocol model, rather it is the unique six digit hexadecimal addresses assigned to each network interface.

PrepLogic Question: 4293-808

42. Review Question p. 237

Answers: C

Explanation A. The Session layer is the fifth layer of the OSI model.

Explanation B. The Transport layer is the fourth layer of the OSI model.

Explanation C. The Network layer is the third layer of the OSI model.

Explanation D. The Data Link layer is the second layer of the OSI model.

PrepLogic Question: 4293-809

43. Review Question p. 237

Answers: D

Explanation A. The Network layer of the OSI model supports elements such as IP, ICMP, RIP, and OSPF.

Explanation B. The Transport layer of the OSI model supports elements such as TCP, UDP, and SPX.

Explanation C. The Data Link layer of the OSI model supports elements such as ARP, PPP, and SLIP.

Explanation D. SSL (secure sockets layer) and NFS (network file system) operate at the Session level of the OSI model. Note: Some may define SSL as operating in the Transport layer of the OSI model. This is also a valid definition as the OSI model does

not exactly match up with the actual functions of TCP/IP. However, the CISSP exam assumes SSL operates at the Session layer of the OSI model.

PrepLogic Question: 4293-810

44. Review Question p. 238

Answers: A

Explanation A. Auditing is not a security service used to protect OSI communications.

Explanation B. Authentication is a security service used to protect OSI communications.

Explanation C. Data integrity is a security service used to protect OSI communications.

Explanation D. Non-repudiation is a security service used to protect OSI communications.

PrepLogic Question: 4293-811

45. Review Question p. 238

Answers: B

Explanation A. TCP provides for full-duplex communications.

Explanation B. TCP is connection oriented, UDP is connectionless.

Explanation C. TCP provides for data flow management through sliding windows.

Explanation D. TCP provides reliable virtual circuits.

PrepLogic Question: 4293-812

46. Review Question p. 238

Answers: B

Explanation A. FIN is the start of the termination handshake to end a TCP/IP session.

Explanation B. ACK is the third and final element of the three-way handshake that establishes a communication link between two systems. Once the ACK is received, actual data can be communicated.

Explanation C. SYN/ACK is the second element of the three-way handshake that establishes a communication link between two systems.

Explanation D. SYN is the first element of the three-way handshake that establishes a communication link between two systems.

PrepLogic Question: 4293-813

47. Review Question p. 239

Answers: C

Explanation A. Networks are deployed to enable the sharing of resources.

Explanation B. Networks are deployed to enable communications between systems.

Explanation C. Networks are inherently less secure than stand alone systems. Therefore, deploying a network is a reduction in security, not an improvement.

Explanation D. Networks are deployed to enable centralized administration.

PrepLogic Question: 4293-814

48. Review Question p. 239

Answers: D

Explanation A. CAT 1 cable is rated for supporting voice communications only.

Explanation B. CAT 3 cable is rated for 10Mbps.

Explanation C. CAT 5 cable is rated for 100Mbps.

Explanation D. CAT 7 cable is rated for 1Gbps. The CISSP exam may also present CAT 6 or CAT 5e as other valid answers to this question.

PrepLogic Question: 4293-815

49. Review Question p. 239

Answers: A

Explanation A. Attenuation is the loss of signal strength caused by excessive cable length. This situation is most likely caused by attenuation.

Explanation B. Since a heavily insulated cable is used to connect the two floors, noise is probably not the issue.

Explanation C. Since a heavily insulated cable is used to connect the two floors, crosstalk is probably not the issue.

Explanation D. Protocol mismatch is not a potential problem since both networks are fully compatible, which implies they are using the same protocols. Plus, since communication does occur, even though poorly, the protocol is working properly.

PrepLogic Question: 4293-816

50. Review Question p. 240

Answers: C

Explanation A. Asynchronous transmissions require that the receiver always be in the read to receive state since transmissions can be sent at any time.

Explanation B. Asynchronous transmissions are used primarily for small amounts of data.

Explanation C. Synchronous transmissions uses a clocking mechanism, asynchronous transmissions do not.

Explanation D. Asynchronous transmissions often used stop and start delimiter bits to clearly signal the boundaries of individual messages or transmissions.

PrepLogic Question: 4293-818

51. Review Question p. 240

Answers: D

Explanation A. ATM, ISDN, and DSL along with cable TV/cable modems, T1, and T3s are broadband based communication mechanisms.

Explanation B. ATM, ISDN, and DSL along with cable TV/cable modems, T1, and T3s are broadband based communication mechanisms.

Explanation C. ATM, ISDN, and DSL along with cable TV/cable modems, T1, and T3s are broadband based communication mechanisms.

Explanation D. Ethernet is a baseband communication mechanism.

PrepLogic Question: 4293-819

52. Review Question p. 240

Answers: A

Explanation A. Multicast is a type of network transmission that originates from a single source but is directed toward multiple specific destinations.

Explanation B. Broadcast is a type of network transmission that originates from a single source and is directed toward all destinations.

Explanation C. Unicast is a type of network transmission that originates from a single source to a single destination.

Explanation D. Polling is a feature of some LAN transmission protocols where a secondary host must obtain permission from a primary host before they can communicate over the network.

PrepLogic Question: 4293-820

53. Review Question p. 241

Answers: B

Explanation A. Gigabit Ethernet is a LAN media access method, but it has a distance limit of 100m, supports transmission rates up to 1Gbps, and is susceptible to RFI.

Explanation B. Fiber Distributed Data Interface (FDDI) is a LAN media access method that can be used to connect systems up to 2 km apart, support transmission rates up to 100Mbps, is highly resistant to electromagnetic and radio frequency interference, and which does not use virtual circuits. FDDI is a two-ring based token-passing media access topology.

Explanation C. Copper Distributed Data Interface (CDDI) is a two-ring based token-passing media access topology that has a limited distance (100m) and is susceptible to RFI.

Explanation D. Asynchronous Transfer Mode (ATM) is a WAN cell-switching connectivity technology, not a LAN media access method. ATM offers high speed connections, WAN connections over great distances, and is generally deployed on fiber optic networks and therefore highly resistant to electromagnetic and radio frequency interference.

PrepLogic Question: 4293-821

54. Review Question p. 241

Answers: C

Explanation A. A hub is a network device used to connect multiple segments together. Hubs operate at layer 1 of the OSI model.

Explanation B. A bridge is a network device used to connect different LAN segments of the same topology. Bridges operate at layer 2 of the OSI model.

Explanation C. A repeater is a network device used specifically to safeguard against attenuation. Repeaters operate at layer 1 of the OSI model.

Explanation D. A router is a network device used to control traffic flow and to connect LAN segments using similar or different topologies. Routers operate at layer 3 of the OSI model.

PrepLogic Question: 4293-822

55. Review Question p. 241

Answers: D

Explanation A. Bridges operate at layer 2 of the OSI model.

Explanation B. Repeaters operate at layer 1 of the OSI model.

Explanation C. Switches operate at layer 2 and 3 of the OSI model.

Explanation D. Routers operate at layer 3 of the OSI model.

PrepLogic Question: 4293-823

56. Review Question p. 242

Answers: B

Explanation A. DNS round robin pointing to duplicate servers is a form of server fault tolerance. If any one of the servers fails, the others continue to function. DNS will need to be altered to remove the IP address of the failed server while it is being repaired.

Explanation B. Automated remote journaling to an offline server provides for a backup of a server, but it does not offer fault tolerance. If the primary server goes down, there is no means by which the backup server can be quickly and easily brought back online to support the network activities.

Explanation C. A mirrored pair of servers with hot rollover capability is a form of server fault tolerance. If the primary server fails, the backup server automatically takes over.

Explanation D. Server clustering is a form of server fault tolerance. If any member of the cluster fails, the other members compensate to support the network activities.

PrepLogic Question: 4293-824

57. Review Question p. 242

Answers: B

Explanation A. Termination is not a problem of twisted pair cabling, but of coax.

Explanation B. Excess cable length is a common cabling failure for twisted pair cabling.

Explanation C. Audio interference is not a common problem for twisted pair cabling. EMI and RFI can be problems for twisted pair cabling that is not properly insulated.

Explanation D. Installation is usually not a problem for twisted pair cabling. Twisted pair installation is simple and straightforward. Fiber optic cabling, on the other hand, is difficult to install.

PrepLogic Question: 4293-828

58. Review Question p. 242

Answers: C

Explanation A. Ethernet is extremely resistant to failure.

Explanation B. FDDI is fault tolerant by design. It uses two rings instead of just one.

Explanation C. Token Ring is not fault tolerant. Its single ring design is a single point of failure.

Explanation D. Frame Relay is extremely fault tolerant. Within the Frame Relay cloud are numerous possible pathways for data to travel.

PrepLogic Question: 4293-829

59. Review Question p. 243

Answers: D

Explanation A. Attempted logon break-ins are focused on authentication.

Explanation B. Masquerading is focused on authentication.

Explanation C. Identity theft is focused on authentication.

Explanation D. Eavesdropping is not necessarily focused on authentication, it could be focused on confidentiality violations.

PrepLogic Question: 4293-830

60. Review Question p. 243

Answers: C

Explanation A. The use of false source identity, using a debugging account, and gain access to a secured area using someone else's credentials are not examples of eavesdropping.

Explanation B. The use of false source identity, using a debugging account, and gain access to a secured area using someone else's credentials arenot examples of network resource saturation or denial of service.

Explanation C. The use of false source identity, using a debugging account, and gain access to a secured area using someone else's credentials are examples of spoofing, piggybacking, and backdoors.

Explanation D. The use of false source identity, using a debugging account, and gain access to a secured area using someone else's credentials are not examples of sniffing and probing a network.

PrepLogic Question: 4293-831

61. Review Question p. 243

Answers: A

Explanation A. A smurf attack requires the three components of a source site, bounce site, and target site to perpetrate its attack. A smurf attack sends a spoofed ping to the broadcast address of a high-volume bounce site that responds with a large flood to the target site.

Explanation B. The ping of death is a form of buffer overflow attack where larger than expected ping packets are sent to the victim. A bounce site is not needed by this attack.

Explanation C. The SYN flood attack works by requesting TCP sessions by initializing the handshake process, but instead of completing the process, it quickly attempts to initiate another TCP session. A bounce site is not needed by this attack.

Explanation D. A teardrop attack is a flood of fragmented IP packets sent to a victim. If the system is not properly patched to drop fragmented packets, it can cause a denial of service state. A bounce site is not needed by this attack.

PrepLogic Question: 4293-832

62. Review Question p. 244

Answers: A

Explanation A. When a switch is proving communiction services between VLANs (i.e. routing services), it is performing operations at layer 3 of the OSI model.

Explanation B. When a switch is proving communiction services between VLANs (i.e. routing services), it is performing operations at layer 3 of the OSI model. Layer 2 is where most other switch services are performed.

Explanation C. When a switch is proving communiction services between VLANs (i.e. routing services), it is performing operations at layer 3 of the OSI model. A switch does not provide serivces at layer 4.

Explanation D. When a switch is proving communiction services between VLANs (i.e. routing services), it is performing operations at layer 3 of the OSI model. A switch does not provide services at layer 7.

PrepLogic Question: 4293-833

63. Review Question p. 244

Answers: B

Explanation A. A switch divides collision domains but it does not divide broadcast domains.

Explanation B. A routers divides collision domains and divides broadcast domains.

Explanation C. A bridge divides collision domains but it does not divide broadcast domains.

Explanation D. A hub does not divide collision domains nor does it divide broadcast domains.

PrepLogic Question: 4293-834

64. Review Question p. 244

Answers: D

Explanation A. Sending a victim large e-mail attachments can be a denial of service attack.

Explanation B. Tasking all TCP ports for illegitimate traffic is a denial of service attack.

Explanation C. Submitting a large stream of fragmented IP packets to a system can be a denial of service attack.

Explanation D. Attempting to break a logon using a brute force password attack is an intrusion attack or a password attack, it is not considered a denial of service attack.

PrepLogic Question: 4293-835

65. Review Question p. 245

Answers: B

Explanation A. CHAP (Challenge Handshake Authentication Protocol) is an authentication protocol, not a VPN protocol.

Explanation B. L2TP or Layer 2 Tunneling Protocol is the replacement for PPTP in VPNs.

Explanation C. PPP (Point to Point Protocol) is an asynchronous connectivity protocol (used over modem dialup links), it is not a VPN protocol.

Explanation D. HDLC (High level Data Link Control) protocol is a WAN protocol from which PPP is derived. HDLC is not a VPN protocol.

PrepLogic Question: 4293-836

66. Review Question p. 245

Answers: C

Explanation A. A bridge is not a network device used as a boundary protection and security mechanism. A bridge is used to connect two or more similar networks.

Explanation B. A router is not a network device used as a boundary protection and security mechanism. A router is used to direct and control the flow of traffic between networks using the same protocol.

Explanation C. A firewall is a network device used as a boundary protection and security mechanism.

Explanation D. A switch is not a network device used as a boundary protection and security mechanism. A switch is used to create a temporary direct communication pathway between two nodes on a network.

PrepLogic Question: 4293-837

67. Review Question p. 245

Answers: D

Explanation A. SMTP operates at Layer 7 (Application) of the OSI model.

Explanation B. UDP operates at Layer 4 (Transport) of the OSI model.

Explanation C. ARP operates at Layer 2 (Data Link) of the OSI model.

Explanation D. DSSS (Direct Sequence Spread Spectrum) operates at Layer 1 (Physical) of the OSI model.

PrepLogic Question: 4293-838

68. Review Question p. 246

Answers: A

Explanation A. BootP or bootstrap protocol is used in a diskless workstation environment to initiate the startup process of terminals.

Explanation B. X Windows is a protocol used to provide support for GUI based applications.

Explanation C. LPD or Line Printer Daemon is the protocol that waits for print jobs to be submitted to a print server.

Explanation D. FTP is used for file transfers, but it is not used to initiate the startup of terminals. TFTP might be considered as a mechanism to perform this task, as it is often used in this manner for routers, switches, and firewalls as a backup configuration server that can be accessed upon bootup in the event of a local loss of configuration data.

PrepLogic Question: 4293-839

69. Review Question p. 246

Answers: B

Explanation A. CAT 5 is 100Mbps rated twisted pair cabling.

Explanation B. ThinNet coax cabling is also known as RG-58 cabling.

Explanation C. Twisted pair can be CAT 1 - 7 rated cabling for voice through gigabit throughput.

Explanation D. ThinNet cabling can be Plenum cabling. But not all types of Plenum cabling is ThinNet RG-58. Plenum is cabling that is encased in a shielding that does not

produce toxic fumes when burned.

PrepLogic Question: 4293-840

70. Review Question p. 246

Answers: A

Explanation A. Firewalls offer the best control over security and traffic when combined with routers. Routers include some access control and traffic filtering capabilities that complement the security features of a firewall.

Explanation B. Bridges provide nothing in the way of traffic or security control, therefore they offer nothing to complement a firewall. Bridges are used to connect two or more similar networks.

Explanation C. Hubs provide nothing in the way of traffic or security control, therefore they offer nothing to complement a firewall. Hubs are used to connect multiple clients to the network.

Explanation D. Repeaters provide nothing in the way of traffic or security control, therefore they offer nothing to complement a firewall. Repeaters are used to strengthen the network signal to compensate for attenuation due to lengthy cable segments.

PrepLogic Question: 4293-841

71. Review Question p. 246

Answers: B

Explanation A. Coax is affected by RFI and EMI.

Explanation B. Fiber optic is the only form of cabling which is resistant to EMI and RFI.

Explanation C. Twisted pair is affected by RFI and EMI.

Explanation D. Shielded twisted pair is affected by RFI and EMI.

PrepLogic Question: 4293-842

72. Review Question p. 247

Answers: C

Explanation A. Neither the TCP/IP nor the OSI model contains 8 layers.

Explanation B. Neither the TCP/IP nor the OSI model contains 5 layers.

Explanation C. The TCP/IP protocol stack or protocol model contains 4 layers.

Explanation D. The OSI model, not the TCP/IP model, contains 7 layers.

PrepLogic Question: 4293-843

73. Review Question p. 247

Answers: D

Explanation A. Repeaters forward broadcast storms.

Explanation B. Hubs forward broadcast storms.

Explanation C. Bridges forward broadcast storms.

Explanation D. Routesr block broadcast storms.

PrepLogic Question: 4293-844

74. Review Question p. 247

Answers: A

Explanation A. A gateway is a networking device that is primarily software and can be used to connect networks that use different protocols.

Explanation B. A switch has software, but it is not primarily software. Moreover, it can only be used to connect networks that use the same protocol.

Explanation C. A router has software, but it is not primarily software. It can only be used to connect networks that use the same protocol.

Explanation D. A bridge is primarily hardware and can only be used to connect networks that use the same protocol.

PrepLogic Question: 4293-845

75. Review Question p. 248

Answers: B

Explanation A. The presentation layer of the OS model provides for compression, encryption, and establishing a relationship between data format and the packet or protocol format.

Explanation B. The transport layer of the OSI model provides end-to-end conveyance services and establishes a logical connection between server and client.

Explanation C. The network layer of the OSI model provides packet routing, error detection, and traffic control.

Explanation D. The data link layer of the OSI model formats messages into data frames for transmission on the physical network media.

PrepLogic Question: 4293-846

76. Review Question p. 248

Answers: C

Explanation A. Power loss is a rare cause of hardware failures. In many cases, power loss is protected against using UPSes and alternate power sources.

Explanation B. Router tables may cause significant problems, but this is a software issue not hardware. Routing tables only become a problem when incorrect information is added to them.

Explanation C. Cabling is the most common cause of network hardware failures. Cables are fragile and are easily damaged. They should be thoroughly tested before and after initial deployment.

Explanation D. Protocol mis-configuration is a common problem, but it is a software issue not a hardware issue.

PrepLogic Question: 4293-847

77. Review Question p. 248

Answers: D

Explanation A. There are two protocols within TCP/IP, namely UDP and TCP, that use ports, but the total number of ports they offer together is 130,072.

Explanation B. 1024 is the number of well-known ports used within TCP and/or UDP. This is not the total number of ports available within TCP/IP as a whole.

Explanation C. 65,536 is the number of ports that TCP and UDP have separately. When combined together, there are 130,072 available ports.

Explanation D. TCP/IP includes both TCP and UDP, both of which have 65,536 available ports. Thus the total number of ports is 130,072.

PrepLogic Question: 4293-848