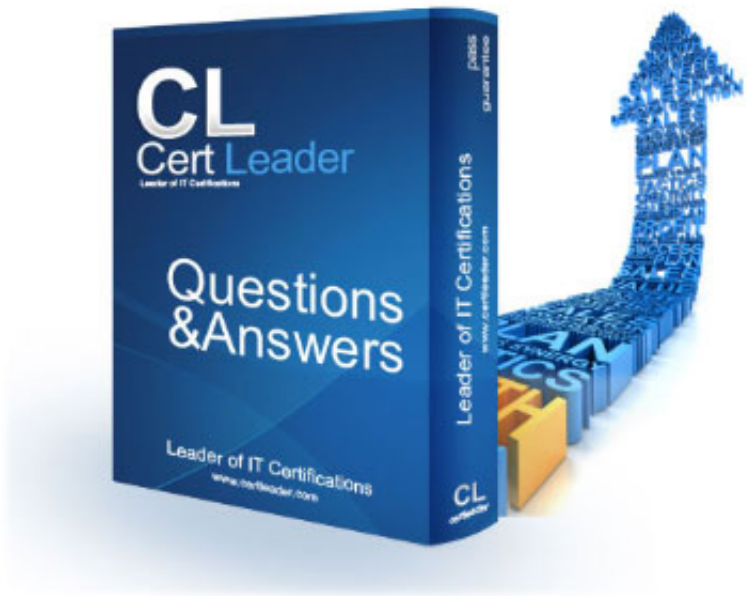
# CISA - Isaca CISA

## http://www.certleader.com/CISA-dumps.html



1. IS management has decided to rewrite a legacy customer relations system using fourth generation languages (4GLs). Which of the following risks is MOST often associated with system development using 4GLs?

A. Inadequate screen/report design facilities

B. Complex programming language subsets

C. Lack of portability across operating systems

D. Inability to perform data intensive operations

**Answer:** D

2. Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?

A. Field checks

B. Control totals

C. Reasonableness checks

D. A before-and-after maintenance report

**Answer:** D

3. Which of the following is a dynamic analysis tool for the purpose of testing software modules?

A. Blackbox test

B. Desk checking

C. Structured walk-through

D. Design and code

**Answer:** A

4. Which of the following is MOST likely to result from a business process reengineering (BPR) project?

A. An increased number of people using technology

B. Significant cost savings, through a reduction in the complexity of information technology

C. A weaker organizational structures and less accountability

D. Increased information protection (IP) risk will increase

**Answer:** A

5. Which of the following devices extends the network and has the capacity to store frames and act as a storage and forward device?

A. Router

B. Bridge

C. Repeater

D. Gateway

**Answer:** B

6. Which of the following is a benefit of using callback devices?

A. Provide an audit trail

B. Can be used in a switchboard environment

C. Permit unlimited user mobility

D. Allow call forwarding

**Answer:** A

7. A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

A. dials back to the user machine based on the user id and password using a telephone number from its database.

B. dials back to the user machine based on the user id and password using a telephone number provided by the user during this connection.

C. waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using its database.

D. waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using the sender\'s database.

**Answer:** A

8. Structured programming is BEST described as a technique that:

A. provides knowledge of program functions to other programmers via peer reviews.

B. reduces the maintenance time of programs by the use of small-scale program modules.

C. makes the readable coding reflect as closely as possible the dynamic execution of the program.

D. controls the coding and testing of the high-level functions of the program in the development process.

**Answer:** B

9. Which of the following data validation edits is effective in detecting transposition and transcription errors?

A. Range check

B. Check digit

C. Validity check

D. Duplicate check

**Answer:** B

10. An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

A. cold site.

B. warm site.

C. dial-up site.

D. duplicate processing facility.

**Answer:** A

11. A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

A. Unit testing

B. Integration testing

C. Design walk-throughs

D. Configuration management

**Answer:** B

12. In an EDI process, the device which transmits and receives electronic documents is the:

A. communications handler.

B. EDI translator.

C. application interface.

D. EDI interface.

**Answer:** A

13. The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

A. testing stage.

B. evaluation stage.

C. maintenance stage.

D. early stages of planning.

**Answer:** D

14. Which of the following network configuration options contains a direct link between any two host machines?

A. Bus

B. Ring

C. Star

D. Completely connected (mesh)

**Answer:** D

15. Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

A. Check digit

B. Existence check

C. Completeness check

D. Reasonableness check

**Answer:** C

16. Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

A. A substantive test of program library controls

B. A compliance test of program library controls

C. A compliance test of the program compiler controls

D. A substantive test of the program compiler controls

**Answer:** B

17. A data administrator is responsible for:

A. maintaining database system software.

B. defining data elements, data names and their relationship.

C. developing physical database structures.

D. developing data dictionary system software.

**Answer:** B

18. A database administrator is responsible for:

A. defining data ownership.

B. establishing operational standards for the data dictionary.

C. creating the logical and physical database.

D. establishing ground rules for ensuring data integrity and security.

**Answer:** C

19. An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

A. defining the conceptual schemA.

B. defining security and integrity checks.

C. liaising with users in developing data model.

D. mapping data model with the internal schemA.

**Answer:** D

20. To affix a digital signature to a message, the sender must first create a message digest by applying a cryptographic hashing algorithm against:

A. the entire message and thereafter enciphering the message digest using the sender\'s private key.

B. any arbitrary part of the message and thereafter enciphering the message digest using the sender\'s private key.

C. the entire message and thereafter enciphering the message using the sender\'s private key.

D. the entire message and thereafter enciphering the message along with the message digest using the sender\'s private key.

**Answer:** A

21. A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

A. digest signature.

B. electronic signature.

C. digital signature.

D. hash signature.

**Answer:** C

22. A critical function of a firewall is to act as a:

A. special router that connects the Internet to a LAN.

B. device for preventing authorized users from accessing the LAN.

C. server used to connect authorized users to private trusted network resources.

D. proxy server to increase the speed of access to authorized users.

**Answer:** B

23. Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?

A. Spool

B. Cluster controller

C. Protocol converter

D. Front end processor

**Answer:** D

24. The use of a GANTT chart can:

A. aid in scheduling project tasks.

B. determine project checkpoints.

C. ensure documentation standards.

D. direct the post-implementation review.

**Answer:** A

25. Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

A. Gateway

B. Protocol converter

C. Front-end communication processor

D. Concentrator/multiplexor

**Answer:** A

26. Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

A. Specific developments only

B. Business requirements only

C. All phases of the installation must be documented

D. No need to develop a customer specific documentation

**Answer:** C

27. A hub is a device that connects:

A. two LANs using different protocols.

B. a LAN with a WAN.

C. a LAN with a metropolitan area network (MAN).

D. two segments of a single LAN.

**Answer:** D

28. A LAN administrator normally would be restricted from:

A. having end-user responsibilities.

B. reporting to the end-user manager.

C. having programming responsibilities.

D. being responsible for LAN security administration.

**Answer:** C

29. Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital?

A. Multiplexer

B. Modem

C. Protocol converter

D. Concentrator

**Answer:** B

30. Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

A. A neural network

B. Database management software

C. Management information systems

D. Computer assisted audit techniques

**Answer:** A

31. A hardware control that helps to detect errors when data are communicated from one computer to another is known as a:

A. duplicate check.

B. table lookup.

C. validity check.

D. parity check.

**Answer:** D

32. For which of the following applications would rapid recovery be MOST crucial?

A. Point-of-sale system

B. Corporate planning

C. Regulatory reporting

D. Departmental chargeback

**Answer:** A

33. The initial step in establishing an information security program is the:

A. development and implementation of an information security standards manual.

B. performance of a comprehensive security control review by the IS auditor.

C. adoption of a corporate information security policy statement.

D. purchase of security access control software.

**Answer:** C

34. A malicious code that changes itself with each file it infects is called a:

A. logic bomb.

B. stealth virus.

C. trojan horse.

D. polymorphic virus.

**Answer:** D

35. Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan\'s effectiveness?

A. Paper test

B. Post test

C. Preparedness test

D. Walk-through

**Answer:** C

36. An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST costeffective test of the DRP?

A. Full operational test

B. Preparedness test

C. Paper test

D. Regression test

**Answer:** B

37. The IS auditor learns that when equipment was brought into the data center by a vendor, the emergency power shutoff switch was accidentally pressed and the UPS was engaged. Which of the following audit recommendations should the IS auditor suggest?

A. Relocate the shut off switch.

B. Install protective covers.

C. Escort visitors.

D. Log environmental failures.

**Answer:** B

38. Company.com has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

A. Acceptance testing is to be managed by users.

B. A quality plan is not part of the contracted deliverables.

C. Not all business functions will be available on initial implementation.

D. Prototyping is being used to confirm that the system meets business requirements.

**Answer:** B

39. In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

A. registration authority (RA).

B. issuing certification authority (CA).

C. subject CA.

D. policy management authority.

**Answer:** A

40. Which of the following is a data validation edit and control?

A. Hash totals

B. Reasonableness checks

C. Online access controls

D. Before and after image reporting

**Answer:** B

41. A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

A. reasonableness check.

B. parity check.

C. redundancy check.

D. check digits.

**Answer:** C

42. What is the primary objective of a control self-assessment (CSA) program?

A. Enhancement of the audit responsibility

B. Elimination of the audit responsibility

C. Replacement of the audit responsibility

D. Integrity of the audit responsibility

**Answer:** A

43. IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?

A. True

B. False

**Answer:** A

44. As compared to understanding an organization\'s IT process from evidence directly collected, how valuable are prior audit reports as evidence?

A. The same value.

B. Greater value.

C. Lesser value.

D. Prior audit reports are not relevant.

**Answer:** C

45. What is the PRIMARY purpose of audit trails?

A. To document auditing efforts

B. To correct data integrity errors C. To establish accountability and responsibility for processed transactions

D. To prevent unauthorized access to data

**Answer:** C

46. How does the process of systems auditing benefit from using a risk-based approach to audit planning?

A. Controls testing starts earlier.

B. Auditing resources are allocated to the areas of highest concern.

C. Auditing risk is reduced.

D. Controls testing is more thorough.

**Answer:** B

47. After an IS auditor has identified threats and potential impacts, the auditor should:

A. Identify and evaluate the existing controls

B. Conduct a business impact analysis (BIA)

C. Report on existing controls

D. Propose new controls

**Answer:** A

48. The use of statistical sampling procedures helps minimize:

A. Detection risk B. Business risk

C. Controls risk

D. Compliance risk

**Answer:** A

49. What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?

A. Business risk

B. Detection risk

C. Residual risk

D. Inherent risk

**Answer:** B

50. A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:

A. Identify high-risk areas that might need a detailed review later

B. Reduce audit costs

C. Reduce audit time

D. Increase audit accuracy

**Answer:** C

51. What type of approach to the development of organizational policies is often driven by risk assessment?

A. Bottom-up

B. Top-down

C. Comprehensive

D. Integrated

**Answer:** B

52. Who is accountable for maintaining appropriate security measures over information assets?

A. Data and systems owners

B. Data and systems users

C. Data and systems custodians

D. Data and systems auditors

**Answer:** A

53. Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

A. True

B. False

**Answer:** A

54. What should an IS auditor do if he or she observes that project-approval procedures do not exist?

A. Advise senior management to invest in project-management training for the staff

B. Create project-approval procedures for future project implementations

C. Assign project leaders

D. Recommend to management that formal approval procedures be adopted and documented

**Answer:** D

55. Who is ultimately accountable for the development of an IS security policy?

A. The board of directors

B. Middle management

C. Security administrators

D. Network administrators

**Answer:** A

56. Proper segregation of duties normally does not prohibit a LAN administrator from also having programming responsibilities. True or false?

A. True

B. False

**Answer:** B

57. A core tenant of an IS strategy is that it must:

A. Be inexpensive

B. Be protected as sensitive confidential information

C. Protect information confidentiality, integrity, and availability

D. Support the business objectives of the organization

**Answer:** D

58. Batch control reconciliation is a _____ (fill in the blank) control for mitigating risk of inadequate segregation of duties.

A. Detective

B. Corrective

C. Preventative

D. Compensatory

**Answer:** D

59. Key verification is one of the best controls for ensuring that:

A. Data is entered correctly

B. Only authorized cryptographic keys are used

C. Input is authorized

D. Database indexing is performed properly

**Answer:** A

60. If senior management is not committed to strategic planning, how likely is it that a company\'s implementation of IT will be successful?

A. IT cannot be implemented if senior management is not committed to strategic planning.

B. More likely.

C. Less likely.

D. Strategic planning does not affect the success of a company\'s implementation of IT.

**Answer:** C

61. Which of the following could lead to an unintentional loss of confidentiality? Choose the BEST answer.

A. Lack of employee awareness of a company\'s information security policy

B. Failure to comply with a company\'s information security policy

C. A momentary lapse of reason

D. Lack of security policy enforcement procedures

**Answer:** A

62. What topology provides the greatest redundancy of routes and the greatest network fault tolerance?

A. A star network topology

B. A mesh network topology with packet forwarding enabled at each host

C. A bus network topology

D. A ring network topology

**Answer:** B

63. An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

A. Evidence collected through personal observation

B. Evidence collected through systems logs provided by the organization\'s security administration

C. Evidence collected through surveys collected from internal staff

D. Evidence collected through transaction reports provided by the organization\'s IT administration

**Answer:** A

64. What kind of protocols does the OSI Transport Layer of the TCP/IP protocol suite provide to ensure reliable communication?

A. Nonconnection-oriented protocols

B. Connection-oriented protocols

C. Session-oriented protocols

D. Nonsession-oriented protocols

**Answer:** B

65. How is the time required for transaction processing review usually affected by properly implemented Electronic Data Interface (EDI)?

A. EDI usually decreases the time necessary for review.

B. EDI usually increases the time necessary for review.

C. Cannot be determined.

D. EDI does not affect the time necessary for review.

**Answer:** A

66. What would an IS auditor expect to find in the console log? Choose the BEST answer.

A. Evidence of password spoofing

B. System errors

C. Evidence of data copy activities

D. Evidence of password sharing

**Answer:** B

67. Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing. True or false?

A. True

B. False

**Answer:** A

68. Why does the IS auditor often review the system logs?

A. To get evidence of password spoofing

B. To get evidence of data copy activities

C. To determine the existence of unauthorized access to data by a user or program

D. To get evidence of password sharing

**Answer:** C

69. What is essential for the IS auditor to obtain a clear understanding of network management?

A. Security administrator access to systems

B. Systems logs of all hosts providing application services

C. A graphical map of the network topology

D. Administrator access to systems

**Answer:** C

70. How is risk affected if users have direct access to a database at the system level?

A. Risk of unauthorized access increases, but risk of untraceable changes to the database decreases.

B. Risk of unauthorized and untraceable changes to the database increases.

C. Risk of unauthorized access decreases, but risk of untraceable changes to the database increases.

D. Risk of unauthorized and untraceable changes to the database decreases.

**Answer:** B

71. What is the most common purpose of a virtual private network implementation?

A. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over an otherwise unsecured channel such as the Internet.

B. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a dedicated T1 connection.

C. A virtual private network (VPN) helps to secure access within an enterprise when communicating over a dedicated T1 connection between network segments within the same facility.

D. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a wireless connection.

**Answer:** A

72. What benefit does using capacity-monitoring software to monitor usage patterns and trends provide to management? Choose the BEST answer.

A. The software can dynamically readjust network traffic capabilities based upon current usage.

B. The software produces nice reports that really impress management.

C. It allows users to properly allocate resources and ensure continuous efficiency of operations.

D. It allows management to properly allocate resources and ensure continuous efficiency of operations.

**Answer:** D

73. What can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program? Choose the BEST answer.

A. Network-monitoring software

B. A system downtime log

C. Administration activity reports

D. Help-desk utilization trend reports

**Answer:** B

74. What are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information? Choose the BEST answer.

A. Referential integrity controls

B. Normalization controls

C. Concurrency controls

D. Run-to-run totals

**Answer:** A

75. What increases encryption overhead and cost the most?

A. A long symmetric encryption key

B. A long asymmetric encryption key

C. A long Advance Encryption Standard (AES) key

D. A long Data Encryption Standard (DES) key

**Answer:** B

76. Which of the following best characterizes "worms"?

A. Malicious programs that can run independently and can propagate without the aid of a carrier program such as email

B. Programming code errors that cause a program to repeatedly dump data

C. Malicious programs that require the aid of a carrier program such as email

D. Malicious programs that masquerade as common applications such as screensavers or macro-enabled Word documents

**Answer:** A

77. What is an initial step in creating a proper firewall policy?

A. Assigning access to users according to the principle of least privilege

B. Determining appropriate firewall hardware and software

C. Identifying network applications such as mail, web, or FTP servers

D. Configuring firewall access rules

**Answer:** C

78. What type of cryptosystem is characterized by data being encrypted by the sender using the recipient\'s public key, and the data then being decrypted using the recipient\'s private key?

A. With public-key encryption, or symmetric encryption

B. With public-key encryption, or asymmetric encryption

C. With shared-key encryption, or symmetric encryption

D. With shared-key encryption, or asymmetric encryption

**Answer:** B

79. How does the SSL network protocol provide confidentiality?

A. Through symmetric encryption such as RSA

B. Through asymmetric encryption such as Data Encryption Standard, or DES

C. Through asymmetric encryption such as Advanced Encryption Standard, or AES

D. Through symmetric encryption such as Data Encryption Standard, or DES

**Answer:** D

80. What are used as the framework for developing logical access controls?

A. Information systems security policies

B. Organizational security policies

C. Access Control Lists (ACL)

D. Organizational charts for identifying roles and responsibilities

**Answer:** A

81. Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

A. Concurrency controls

B. Reasonableness checks

C. Time stamps

D. Referential integrity controls

**Answer:** C

82. Which of the following is a good control for protecting confidential data residing on a PC?

A. Personal firewall

B. File encapsulation

C. File encryption

D. Host-based intrusion detection

**Answer:** C

83. Which of the following is a guiding best practice for implementing logical access controls?

A. Implementing the Biba Integrity Model

B. Access is granted on a least-privilege basis, per the organization\'s data owners

C. Implementing the Take-Grant access control model

D. Classifying data according to the subject\'s requirements

**Answer:** B

84. What does PKI use to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions?

A. A combination of public-key cryptography and digital certificates and two-factor authentication

B. A combination of public-key cryptography and two-factor authentication

C. A combination of public-key cryptography and digital certificates

D. A combination of digital certificates and two-factor authentication

**Answer:** C

85. Which of the following do digital signatures provide?

A. Authentication and integrity of data

B. Authentication and confidentiality of data

C. Confidentiality and integrity of data

D. Authentication and availability of data

**Answer:** A

86. Regarding digital signature implementation, which of the following answers is correct?

A. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender\'s private key. Upon receiving the data, the recipient can decrypt the data using the sender\'s public key.

B. A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient\'s public key. Upon receiving the data, the recipient can decrypt the data using the recipient\'s public key.

C. A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value or message digest from the entire message contents. Upon receiving the data, the recipient can independently create it.

D. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender\'s public key. Upon receiving the data, the recipient can decrypt the data using the recipient\'s private key.

**Answer:** C

87. Which of the following would provide the highest degree of server access control?

A. A mantrap-monitored entryway to the server room

B. Host-based intrusion detection combined with CCTV

C. Network-based intrusion detection

D. A fingerprint scanner facilitating biometric access control

**Answer:** D

88. What are often the primary safeguards for systems software and data?

A. Administrative access controls

B. Logical access controls

C. Physical access controls

D. Detective access controls

**Answer:** B

89. Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

A. A monitored double-doorway entry system

B. A monitored turnstile entry system

C. A monitored doorway entry system

D. A one-way door that does not allow exit after entry

**Answer:** A

90. Which of the following is an effective method for controlling downloading of files via FTP? Choose the BEST answer.

A. An application-layer gateway, or proxy firewall, but not stateful inspection firewalls

B. An application-layer gateway, or proxy firewall

C. A circuit-level gateway

D. A first-generation packet-filtering firewall

**Answer:** B

91. Which of the following provides the strongest authentication for physical access control?

A. Sign-in logs

B. Dynamic passwords

C. Key verification

D. Biometrics

**Answer:** D

92. What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off? Choose the BEST answer.

A. Employee security awareness training

B. Administrator alerts

C. Screensaver passwords

D. Close supervision

**Answer:** C

93. What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources? Choose the BEST answer.

A. OSI Layer 2 switches with packet filtering enabled

B. Virtual Private Networks

C. Access Control Lists (ACL)

D. Point-to-Point Tunneling Protocol

**Answer:** C

94. What is the key distinction between encryption and hashing algorithms?

A. Hashing algorithms ensure data confidentiality.

B. Hashing algorithms are irreversible.

C. Encryption algorithms ensure data integrity.

D. Encryption algorithms are not irreversible.

**Answer:** B

95. Which of the following is BEST characterized by unauthorized modification of data before or during systems data entry?

A. Data diddling

B. Skimming

C. Data corruption

D. Salami attack

**Answer:** A

96. Which of the following is used to evaluate biometric access controls?

A. FAR

B. EER

C. ERR

D. FRR

**Answer:** B

97. Who is ultimately responsible and accountable for reviewing user access to systems?

A. Systems security administrators

B. Data custodians

C. Data owners

D. Information systems auditors

**Answer:** C

98. Establishing data ownership is an important first step for which of the following processes? Choose the BEST answer.

A. Assigning user access privileges

B. Developing organizational security policies

C. Creating roles and responsibilities

D. Classifying data

**Answer:** D

99. Which of the following is MOST is critical during the business impact assessment phase of business continuity planning?

A. End-user involvement

B. Senior management involvement

C. Security administration involvement

D. IS auditing involvement

**Answer:** A

100. What type of BCP test uses actual resources to simulate a system crash and validate the plan\'s effectiveness?

A. Paper

B. Preparedness

C. Walk-through

D. Parallel

**Answer:** B

101. Which of the following typically focuses on making alternative processes and resources available for transaction processing?

A. Cold-site facilities

B. Disaster recovery for networks

C. Diverse processing

D. Disaster recovery for systems

**Answer:** D

102. Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

A. Parallel

B. Preparedness

C. Walk-thorough

D. Paper

**Answer:** C

103. What influences decisions regarding criticality of assets?

A. The business criticality of the data to be protected

B. Internal corporate politics

C. The business criticality of the data to be protected, and the scope of the impact upon the organization as a whole

D. The business impact analysis

**Answer:** C

104. Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

A. Cold site

B. Alternate site

C. Hot site

D. Warm site

**Answer:** A

105. With the objective of mitigating the risk and impact of a major business interruption, a disasterrecovery plan should endeavor to reduce the length of recovery time necessary, as well as costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs. True or false?

A. True

B. False

**Answer:** A

106. Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

A. Cold site

B. Hot site

C. Alternate site

D. Warm site

**Answer:** A

107. Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following? Choose the BEST answer.

A. IT strategic plan

B. Business continuity plan

C. Business impact analysis

D. Incident response plan

**Answer:** B

108. Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive

management, such as the _____. (fill-in-the-blank)

A. Security administrator

B. Systems auditor

C. Board of directors

D. Financial auditor

**Answer:** C

109. Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

A. True

B. False

**Answer:** A

110. Library control software restricts source code to:

A. Read-only access

B. Write-only access

C. Full access

D. Read-write access

**Answer:** A

111. When is regression testing used to determine whether new application changes have

introduced any errors in the remaining unchanged code?

A. In program development and change management

B. In program feasibility studies

C. In program development

D. In change management

**Answer:** A

112. What is often the most difficult part of initial efforts in application development? Choose the BEST answer.

A. Configuring software

B. Planning security

C. Determining time and resource requirements

D. Configuring hardware

**Answer:** C

113. What is a primary high-level goal for an auditor who is reviewing a system development project?

A. To ensure that programming and processing environments are segregated

B. To ensure that proper approval for the project has been obtained

C. To ensure that business objectives are achieved

D. To ensure that projects are monitored and administrated effectively

**Answer:** C

114. Whenever an application is modified, what should be tested to determine the full impact of the change? Choose the BEST answer.

A. Interface systems with other applications or systems

B. The entire program, including any interface systems with other applications or systems

C. All programs, including interface systems with other applications or systems

D. Mission-critical functions and any interface systems with other applications or systems

**Answer:** B

115. The quality of the metadata produced from a data warehouse is _____ in the warehouse\'s design. Choose the BEST answer.

A. Often hard to determine because the data is derived from a heterogeneous data environment

B. The most important consideration

C. Independent of the quality of the warehoused databases

D. Of secondary importance to data warehouse content

**Answer:** B

116. Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system\'s inputs and outputs. True or false?

A. True

B. False

**Answer:** B

117. Who assumes ownership of a systems-development project and the resulting system?

A. User management

B. Project steering committee

C. IT management

D. Systems developers

**Answer:** A

118. If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

A. Documentation development

B. Comprehensive integration testing

C. Full unit testing

D. Full regression testing

**Answer:** B

119. When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

A. True

B. False

**Answer:** B

120. What is a reliable technique for estimating the scope and cost of a software-development project?

A. Function point analysis (FPA)

B. Feature point analysis (FPA)

C. GANTT

D. PERT

**Answer:** A

121. Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

A. Function Point Analysis (FPA)

B. GANTT

C. Rapid Application Development (RAD)

D. PERT

**Answer:** D

122. If an IS auditor observes that an IS department fails to use formal documented

methodologies, policies, and standards, what should the auditor do? Choose the BEST answer.

A. Lack of IT documentation is not usually material to the controls tested in an IT audit.

B. The auditor should at least document the informal standards and policies. Furthermore, the IS auditor should create formal documented policies to be implemented.

C. The auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemented.

D. The auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should create formal documented policies to be implemented.

**Answer:** C

# Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

## 100% Pass Your CISA Exam with Our Prep Materials Via below:

http://www.certleader.com/CISA-dumps.html