

Exam : Isaca CISA

**Title : CISA Certified Information
Systems Auditor**

Version : V6.98

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

Explanation:

4GLs are usually not suitable for data intensive operations. Instead, they are used mainly for graphic user interface (GUI) design or as simple query/report generators.

Incorrect answers:

- A, B. Screen/report design facilities are one of the main advantages of 4GLs, and 4GLs have simple programming language subsets.
- C. Portability is also one of the main advantages of 4GLs.

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

Explanation:

A before-and-after maintenance report is the best answer because a visual review would provide the most positive verification that updating was proper.

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

Explanation:

A blackbox test is a dynamic analysis tool for testing software modules. During the testing of software modules a blackbox test works first in a cohesive manner as one single unit/entity, consisting of numerous modules and second, with the user data that flows across software modules. In some cases, this even drives the software behavior.

Incorrect answers:

In choices B, C and D, the software (design or code) remains static and somebody simply closely examines it by applying his/her mind, without actually activating the software. Hence, these cannot be referred to as dynamic analysis tools.

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

Explanation:

A BPR project more often leads to an increased number of people using technology, and this would be a cause for concern. Incorrect answers:

B. As BPR is often technology oriented, and this technology is usually more complex and volatile than in the past, cost savings do not often materialize in this area.

D. There is no reason for IP to conflict with a BPR project, unless the project is not run properly.

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

Explanation:

A bridge connects two separate networks to form a logical network (e.g., joining an ethernet and token network) and has the storage capacity to store frames and act as a storage and forward device. Bridges operate at the OSI data link layer by examining the media access control header of a data packet. Incorrect answers:

A. Routers are switching devices that operate at the OSI network layer by examining network addresses (i.e., routing information encoded in an IP packet). The router, by examining the IP address, can make intelligent decisions in directing the packet to its destination.

C. Repeaters amplify transmission signals to reach remote devices by taking a signal from a LAN, reconditioning and retiming it, and sending it to another. This functionality is hardware encoded and occurs at the OSI physical layer.

D. Gateways provide access paths to foreign networks.

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

Explanation:

A callback feature hooks into the access control software and logs all authorized and unauthorized access attempts, permitting the follow-up and further review of potential breaches. Call forwarding (choice D) is a means of potentially bypassing callback control. By dialing through an authorized phone number from an unauthorized phone number, a perpetrator can gain computer access. This vulnerability can be controlled through callback systems that are available.

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

Explanation:

A call-back system in a net centric environment would mean that a user with an id and password calls a remote server through a dial-up line first, and then the server disconnects and dials back to the user machine based on the user id and password using a telephone number from its database. Although the server can depend upon its own database, it cannot know the authenticity of the dialer when the user dials again. The server cannot depend upon the sender's database to dial back as the same could be manipulated.

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

Explanation:

A characteristic of structured programming is smaller, workable units. Structured programming has evolved because smaller, workable units are easier to maintain. Structured programming is a style of programming which restricts the kinds of control structures. This limitation is not crippling. Any program can be written with allowed control structures. Structured programming is sometimes referred to as go-to-less programming, since a go-to statement is not allowed. This is perhaps the most well known restriction of the style, since go-to statements were common at the time structured programming was becoming more

popular. Statement labels also become unnecessary, except in languages where subroutines are identified by labels.

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

Explanation:

A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered or an incorrect, but valid, value substituted.

This control is effective in detecting transposition and transcription errors.

Incorrect answers:

- A. A range check is checking data that matches a predetermined range of values.
- C. A validity check is programmed checking of the data validity in accordance with predetermined criteria.
- D. In a duplicate check, new or fresh transactions are matched to those previously entered to ensure that they are not already in the system.

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

Explanation:

A cold site is ready to receive equipment but does not offer any components at the site in advance of the need.

Incorrect answers:

B. A warm site is an offsite backup facility that is configured partially with network connections and selected peripheral equipment, such as disk and tape units, controllers and CPUs, to operate an information processing facility.

D. A duplicate information processing facility is a dedicated, self-developed recovery site that can back up critical applications.

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

Explanation:

A common system maintenance problem is that errors are often corrected quickly (especially when deadlines are tight) , units are tested by the programmer, and then transferred to the acceptance test area. This often results in system problems that should have been detected during integration or system testing. Integration testing aims at ensuring that the major components of the system interface correctly.

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

Explanation:

A communications handler transmits and receives electronic documents between trading partners and/or wide area networks (WANs).

Incorrect answers:

- B. An EDI translator translates data between the standard format and a trading partner's proprietary format.
- C. An application interface moves electronic transactions to, or from, the application system and performs data mapping.
- D. An EDI interface manipulates and routes data between the application system and the communications handler.

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

Explanation:

Company.com in the early stages of a BCP will incur the most significant level of program development effort, which will level out as the BCP moves into maintenance, testing and evaluation stages. It is during the planning stage that an IS auditor will play an important role in obtaining senior management's commitment to resources and assignment of BCP responsibilities.

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

Explanation:

A completely connected mesh configuration creates a direct link between any two host machines. Incorrect answers:

- A. A bus configuration links all stations along one transmission line.

- B. A ring configuration forms a circle, and all stations are attached to a point on the transmission circle.
- D. In a star configuration each station is linked directly to a main hub.

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

Explanation:

A completeness check is used to determine if a field contains data and not zeros or blanks. Incorrect answers:

- A. A check digit is a digit calculated mathematically to ensure original data was not altered.
- B. An existence check also checks entered data for agreement to predetermined criteria.
- D. A reasonableness check matches input to predetermined reasonable limits or occurrence rates.

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

Explanation:

A compliance test determines if controls are operating as designed and are being applied in a manner that complies with management policies and procedures. For example, if the IS auditor is concerned whether program library controls are working properly, the IS auditor might select a sample of programs to determine if the source and object versions are the same. In other words, the broad objective of any compliance test is to provide auditors with reasonable assurance that a particular control on which the

auditor plans to rely is operating as the auditor perceived it in the preliminary evaluation.

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

Explanation:

A data administrator is responsible for defining data elements, data names and their relationship. Choices A, C and D are functions of a database administrator (DBA)

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

Explanation:

A database administrator is responsible for creating and controlling the logical and physical database. Defining data ownership resides with the head of the user department or top management if the data is common to the organization. IS management and the data administrator are responsible for establishing operational standards for the data dictionary. Establishing ground rules for ensuring data integrity and security in line with the corporate security policy is a function of the security administrator.

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 Explanation:

A DBA only in rare instances should be mapping data elements from the data model to the internal schema (physical data storage definitions). To do so would eliminate data independence for application systems. Mapping of the data model occurs with the conceptual schema since the conceptual schema represents the enterprisewide view of data within an organization and is the basis for deriving an end-user department data model.

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