

Section: 1178 Questions

QUESTION NO: 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.

QUESTION NO: 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.

**QUESTION NO: 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.

**QUESTION NO: 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.

**QUESTION NO: 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.

### QUESTION NO: 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.

### QUESTION NO: 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.

**QUESTION NO: 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.

**QUESTION NO: 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.

**QUESTION NO: 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.

**QUESTION NO: 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.

**QUESTION NO: 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.

**QUESTION NO: 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.

**QUESTION NO: 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.

**QUESTION NO: 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.

**QUESTION NO: 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.

**QUESTION NO: 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)

**QUESTION NO: 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.

**QUESTION NO: 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.

**QUESTION NO: 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**

**Explanation:**

A digital signature is a cryptographic method that ensures data integrity, authentication of the message, and non-repudiation. To ensure these, the sender first creates a message digest by applying a cryptographic hashing algorithm against the entire message and thereafter enciphers the message digest using the sender's private key. A message digest is created by applying a cryptographic hashing algorithm against the entire message not on any arbitrary part of the message. After creating the message digest, only the message digest is enciphered using the sender's private key, not the message.

**QUESTION NO: 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**

**Explanation:**

A digital signature through the private cryptographic key authenticates a transmission from a sender through the private cryptographic key. It is a string of bits that uniquely represent another string of bits, a digital document. An electronic signature refers to the string of bits that digitally represents a handwritten signature captured by a computer system when a human applies it on an electronic pen pad, connected to the system.

**QUESTION NO: 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 unauthorized 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**

**Explanation:**

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users of other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling the outside resources to which its own users have access. Basically, a firewall, working closely with a router program, filters all network packets to determine whether or not to forward them toward their destination. A firewall includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so no incoming request can get directed to private network resources.

**QUESTION NO: 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 Explanation:**

A front-end processor is a hardware device that connects all communication lines to a central

computer to relieve the central computer.

**QUESTION NO: 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**

**Explanation:**

A GANTT chart is used in project control. It may aid in the identification of needed checkpoints but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the post-implementation review.

**QUESTION NO: 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**

**Explanation:**

A gateway performs the job of translating e-mail formats from one network to another so messages can make their way through all the networks.

Incorrect answers:

B. A protocol converter is a hardware device that converts between two different types of transmissions, such as asynchronous and synchronous transmissions.

C. A front-end communication processor connects all network communication lines to a central computer to relieve the central computer from performing network control, format conversion and message handling tasks.

D. A concentrator/multiplexor is a device used for combining several lower-speed channels into a higher-speed channel.

**QUESTION NO: 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**

**Explanation:**

A global enterprise product reengineering (EPR) software package can be applied to a business to replace, simplify and improve the quality of IS processing. Documentation is intended to help understand how, why and which solutions that have been selected and implemented, and therefore must be specific to the project. Documentation is also intended to support quality assurance and must be comprehensive.

**QUESTION NO: 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**

**Explanation:**

A hub is a device that connects two segments of a single LAN. A hub is a repeater. It provides transparent connectivity to users on all segments of the same LAN. It is a level 1 device. Incorrect answers:

- A. A bridge operates at level 2 of the OSI layer and is used to connect two LANs using different protocols (e.g., joining an ethernet and token network) to form a logical network.
- B. A gateway, which is a level 7 device, is used to connect a LAN to a WAN.
- C. A LAN is connected with a MAN using a router, which operates in the network layer.

**QUESTION NO: 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**

**Explanation:**

A LAN administrator should not have programming responsibilities but may have end-user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator also may be responsible for security administration over the LAN.

**QUESTION NO: 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**

**Explanation:**

A modem is a device that translates data from digital to analog and back to digital.

**QUESTION NO: 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 Explanation:**

A neural network will monitor and learn patterns, reporting exceptions for investigation.

Incorrect answers:

- B. Database management software is a method of storing and retrieving data .
- C. Management information systems provide management statistics but do not normally have a monitoring and detection function.
- D. Computer-assisted audit techniques detect specific situations, but are not intended to learn patterns and detect abnormalities.

**QUESTION NO: 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**

**Explanation:**

A parity check will help to detect data errors when data are read from memory or communicated from one computer to another. A one-bit digit (either 0 or 1) is added to a data item to indicate whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, an error report is generated.

Incorrect answers:

Choices A, B and C are types of data validation and editing controls.

**QUESTION NO: 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**

**Explanation:**

A point-of-sale system is a critical online system that when inoperable will jeopardize the ability of Company.com to generate revenue and track inventory properly.

**QUESTION NO: 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**

**Explanation:**

A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

**QUESTION NO: 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**

**Explanation:**

A polymorphic virus has the capability of changing its own code, enabling it to have many different variants. Since they have no consistent binary pattern, such viruses are hard to identify.

Incorrect answers:

A. A logic bomb is code that is hidden in a program or system which will cause something to happen when the user performs a certain action or when certain conditions are met. A logic bomb, which can be downloaded along with a corrupted shareware or freeware program, may destroy data, violate system security, or erase the hard drive.

B. A stealth virus is a virus that hides itself by intercepting disk access requests. When an antivirus program tries to read files or boot sectors to find the virus, the stealth virus feeds the antivirus program a clean image of the file or boot sector.

C. A trojan horse is a virus program that appears to be useful and harmless but which has harmful side effects such as destroying data or breaking the security of the system on which it is run.

**QUESTION NO: 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**

**Explanation:**

A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments. Incorrect answers:

- A. A paper test is a walkthrough of the plan, involving major players in the plan's execution who attempt to determine what might happen in a particular type of service disruption. A paper test usually precedes the preparedness test.
- B. A post-test is actually a test phase and is comprised of a group of activities, such as returning all resources to their proper place, disconnecting equipment, returning personnel and deleting all company data from third- party systems.
- D. A walk-through is a test involving a simulated disaster situation that tests the preparedness and understanding of management and staff, rather than the actual resources.

**QUESTION NO: 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**

**Explanation:**

A preparedness test is performed by each local office/area to test the adequacy of the preparedness of local operations for the disaster recovery.