Practice test for certified information systems auditor

Profession, Student

Isaca CISA CISA Certified Information Systems Auditor Practice Test Version 3. 8 Isaca CISA: Practice Exam 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 " Pass Any Exam. Any Time. " - www. actualtests. com Ac tua lTe sts . co m 2 Isaca CISA: Practice Exam 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 Answer: A

Explanation: A BPR project more often leads to an increased number of people usingtechnology, 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 " Pass Any Exam. Any Time. " - www. actualtests. com 3 Ac tua lTe 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 lessaccountabilityD. Increased information protection (IP) risk will increase sts Which of the following is MOST likely to

result from a business process reengineering (BPR) project? . co m Isaca CISA: Practice Exam C. Repeater D. Gateway Answer: B Explanation: A bridge connects two separate networks to form a logical network (e. . , 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 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: " Pass Any Exam. Any Time. " - www. actualtests. com Ac Answer: A tua A. Provide an

audit trail B. Can be used in a switchboardenvironmentC. Permit unlimited user mobility D. Allow call forwarding lTe

Which of the following is a benefit of using callback devices? sts . co m 4 Isaca CISA: Practice Exam 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 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 tructured programming was becoming more popular. Statement labels also become unnecessary, except in languages where subroutines are identified by labels. " Pass Any Exam. Any Time. " - www. actualtests. com Ac tua 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. lTe

Structured programming is BEST described as a technique that: sts . co m 5 Isaca CISA: Practice Exam 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 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. " Pass Any Exam. Any Time. " - www. actualtests. com 6 Ac tua An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a: lTe sts . co m Isaca CISA: Practice Exam

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. " Pass Any Exam. Any Time. " - www. actualtests. com 7 Ac tua lTe sts . co m Isaca CISA: Practice Exam 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. arly 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 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 " Pass Any Exam. Any Time. " - www. actualtests. com Ac A. Bus B. Ring C. Star D. Completely connected (mesh) tua lTe Which of the following network configuration options contains a direct link between any two host machines? sts . co m 8 Isaca CISA: Practice Exam 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 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: " Pass Any Exam. Any Time. " - www. actualtests. com Ac tua 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 lTe sts 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? . co m 9 Isaca CISA: Practice Exam A. maintaining database system software. B. efining 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 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 conceptualschemA. B. defining security and integrity checks. C. liaising with users in developing

data model. D. mapping data model with the internalschemA. Answer: D " Pass Any Exam. Any Time. " - www. actualtests. com Ac tua 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. lTe sts . co m 10 Isaca CISA: Practice Exam 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. ny 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 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. " Pass Any Exam. Any Time. " - www. actualtests. com

Ac 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. ua lTe sts . co m 11 Isaca CISA: Practice Exam 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. pecial 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 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 " Pass Any Exam. Any Time. " - www. actualtests. com 12

Ac 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. tua lTe sts . co m Isaca CISA: Practice Exam Explanation: A front-end processor is a hardware device that connects allcommunicationlines 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. " Pass Any Exam. Any Time. " - www. actualtests. com 13 Ac tua lTe sts . co m Isaca CISA: Practice Exam 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: 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. " Pass Any Exam. Any Time. - www. actualtests. com Ac 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. tua lTe sts . co m 14 Isaca CISA: Practice Exam 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 Answer: B 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 " Pass Any Exam. Any Time. " - www. actualtests. com 15 Ac Explanation: A modem is a device that translates data from digital to analog and back to digital. tua lTe A. Multiplexer B. Modem C. Protocol converter D. Concentrator sts Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital? . co m Isaca CISA: Practice Exam 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 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. " Pass Any Exam. Any Time. " - www. actualtests. com 16 Ac tua 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. lTe sts . co m Isaca CISA: Practice Exam 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 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. " Pass Any Exam. Any Time. " - www. actualtests. com Ac tua lTe A. logic bomb. B. stealth virus. C. trojan horse. D. polymorphic virus. sts A malicious code that changes itself with each file it infects is called a: . co m 17 Isaca CISA: Practice Exam 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. Incorrect answers: " Pass Any Exam. Any Time. " - www. actualtests. com 18 Ac tua lTe sts . co m Isaca CISA: Practice Exam A. A full operational test is conducted after the paper and preparedness test. C. A paper test is a structured walkthrough of the DRP and should be conducted before a preparedness test.

D. A regression test is not a DRP test and is used in software maintenance. QUESTION NO: 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 QUESTION NO: 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 Explanation: A quality plan is an essential element of all projects. It is critical that the contracted supplier be required to produce such a plan. The quality plan for the roposed development contract should " Pass Any Exam. Any Time. " - www. actualtests. com 19 Ac tua Explanation: A protective cover over the switch would allow it to be accessible and visible, but would prevent accidental activation. Incorrect Answers: A: Relocating the shut off switch would defeat the purpose of having it readily accessible. C: Escorting the personnel moving the equipment may not have prevented this incident. D: Logging of environmental failures would provide management with a report of incidents, but reporting alone would not prevent a reoccurrence. lTe sts . co m

Isaca CISA: Practice Exam be comprehensive and encompass all phases of the development and include which business functions will be included and

when. Acceptance is normally managed by the user area, since they must be satisfied that the new system will meet their requirements. If the system is large, a phased-in approach to implementing the application is a reasonable approach. Prototyping is a valid method of ensuring that the system will meet business requirements. QUESTION NO: 39 In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i. . , certificate subjects) is the: A. registration authority (RA). B. issuing certification authority (CA). C. subject CA. D. policy management authority. Answer: A QUESTION NO: 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 Explanation: A reasonableness check is a data validation edit and control, used to ensure that data conforms to predetermined criteriA . Incorrect answers: A.

A hash total is a total of any numeric data field or series of data elements in a data file. This " Pass Any Exam. Any Time. " - www. actualtests. com 20 Ac tua Explanation: A RA is an entity that is responsible for identification and authentication of certificate subjects, but the RA does not sign or issue certificates. The certificate subject usually interacts with the RA for completing the process of subscribing to the services of the certification authority in terms of getting identity validated with standard identification documents, as detailed in the certificate policies of the CA.

In the context of a particular certificate, the issuing CA is the CA that issued the certificate. In the context of a particular CA certificate, the subject CA is

the CA whose public key is certified in the certificate. lTe sts . co m Isaca CISA: Practice Exam total is checked against a control total of the same field or fields to ensure completeness of processing. B. Online access controls are designed to prevent unauthorized access to the system and datA . C. Before and after image reporting is a control over data files that makes it possible to trace changes.

QUESTION NO: 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 QUESTION NO: 42 . What is the primary objective of a control self-assessment (CSA) program? A. Enhancement of the auditresponsibilityB. Elimination of the audit responsibility C. Replacement of the audit responsibility D. Integrity of the audit responsibility Answer: A Explanation: Audit responsibility enhancement is an objective of a control self-assessment (CSA) program. Pass Any Exam. Any Time. " - www. actualtests. com Ac tua Explanation: A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of datA . Incorrect answers: A. A reasonableness check compares data to predefined reasonability limits or occurrence rates established for the datA . B. A parity check is a hardware control that detects data errors when data are read from one computer to another, from memory or during transmission. D. Check digits detect transposition and transcription errors. lTe sts . co m 21 Isaca CISA: Practice Exam QUESTION NO: 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 Explanation: 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. Think of it this way: If any reliance is placed on internal controls, that reliance must be validated through compliance testing.

High control risk results in little reliance on internal controls, which results in additional substantive testing. QUESTION NO: 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 Explanation: Prior audit reports are considered of lesser value to an IS auditor attempting to gain an understanding of an organization's IT process than evidence directly collected. QUESTION NO: 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 " Pass Any Exam. Any Time. " - www. actualtests. com Ac tua lTe sts . co m 22 Isaca CISA: Practice Exam Answer: C Explanation: The primary purpose of audit trails is to establish accountability and responsibility for processed transactions. QUESTION NO:

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. QUESTION NO: 47 Answer: A Explanation: After an IS auditor has identified threats and potential impacts, the auditor should then identify and evaluate the existing controls. QUESTION NO: 48 . The use of statistical sampling procedures helps minimize: A. Detection risk " Pass Any Exam. Any Time. " - www. actualtests. com 23 Ac A. Identify and evaluate the existing controls B. Conduct a business impact analysis (BIA) C. Report on existing controls D. Propose new controls ua . After an IS auditor has identified threats and potential impacts, the auditor should: lTe sts Explanation: Allocation of auditing resources to the areas of highest concern is a benefit of a risk-based approach to audit planning. . co Answer: B m Isaca CISA: Practice Exam B. Business risk C. Controls risk D. Compliance risk Answer: A Explanation: The use of statistical sampling procedures helps minimize detection risk. QUESTION NO: 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 QUESTION NO: 50 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 Explanation: A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can identify high-risk areas that might need a detailed review later. " Pass

Any Exam. Any Time. " - www. actualtests. com Ac . A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can: tua Te Explanation: Detection risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist. sts . co m 24 Isaca CISA: Practice Exam QUESTION NO: 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 Explanation: A bottom-up approach to the development of organizational policies is often driven by risk assessment. . 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 QUESTION NO: 53 . Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false? A. True B. False Answer: A Explanation: Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. " Pass Any Exam. Any Time. " - www. actualtests. com 25 Ac Explanation: Data and systems owners are accountable for maintaining appropriate security measures over information assets. tua lTe sts . co QUESTION NO: 52 Isaca CISA: Practice Exam QUESTION NO: 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 Explanation: If an IS auditor observes that project-approval procedures do not exist, the IS auditor should recommend to management that formal approval procedures be adopted and ocumented. QUESTION NO: 55 Answer: A QUESTION NO: 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 Explanation: Proper segregation of duties normally prohibits a LAN administrator from also having programming responsibilities. " Pass Any Exam. Any Time. " - www. actualtests. com 26 Ac Explanation: The board of directors is ultimately accountable for the development of an IS security policy. tua lTe A. The board of directors B. Middle management C. Security administrators D.

Network administrators sts . Who is ultimately accountable for the development of an IS security policy? . co m Isaca CISA: Practice Exam QUESTION NO: 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 Explanation: Above all else, an IS strategy must support the business objectives of the organization. Answer: D QUESTION NO: 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 "

Pass Any Exam. Any Time. " - www. actualtests. com Ac Explanation: Batch control reconciliations is a compensatory control for mitigating risk of inadequate segregation of duties. tua lTe A. Detective B. Corrective C. Preventative D. Compensatory sts . Batch control reconciliation is a _____ (fill in the blank) control for mitigating risk of inadequate segregation of duties. . co QUESTION NO: 58 m 27

Isaca CISA: Practice Exam Explanation: Key verification is one of the best controls for ensuring that data is entered correctly. QUESTION NO: 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 Explanation: A company's implementation of IT will be less likely to succeed if senior management is not committed to strategic planning.

QUESTION NO: 61 Answer: A Explanation: Lack of employee awareness of a company's information security policy could lead to an unintentional loss of confidentiality. QUESTION NO: 62 . What topology provides the greatest redundancy of routes and the greatest network fault tolerance? A. A star network topology " Pass Any Exam. Any Time. " - www. actualtests. com Ac A. Lack of employee awareness of a company's information security policy B. Failureto comply with a company's information security policy C. A momentary lapse of reason D. Lack of security policy enforcement procedures tua lTe Which of the following could lead to an unintentional loss

of confidentiality? Choose the BEST answer. sts . co m 28 Isaca CISA: Practice Exam B. A mesh network topology with packet forwarding enabled at each host C. A bus network topology D. A ring network topology Answer: B Explanation: A mesh network topology provides a point-to-point link between every network host. If each host is configured to route and forward communication, this topology provides the greatest redundancy of routes and the greatest network fault tolerance. QUESTION NO: 63 . An IS auditor usually places more reliance on evidence directly collected.

What is an example of such evidence? A. Evidence collected through personalobservationB. 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 Explanation: An IS auditor usually places more reliance on evidence directly collected, such as through personal observation. . 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 Explanation: The transport layer of the TCP/IP protocol suite provides for connection-oriented protocols to ensure reliable communication. " Pass Any Exam. Any Time. " - www. actualtests. com Ac QUESTION NO: 64 tua lTe sts . co m 29 Isaca CISA: Practice Exam QUESTION NO: 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 Explanation: Electronic data interface (EDI) supports intervendor communication while decreasing the time necessary for review because it is usually configured to readily identify errors requiring follow-up. QUESTION NO: 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 QUESTION NO: 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 Explanation: " Pass Any Exam. Any Time. " - www. actualtests. com 30 Ac Explanation: An IS auditor can expect to find system errors to be detailed in the console log. tua lTe sts . co m Isaca CISA: Practice Exam 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.

QUESTION NO: 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 Explanation: When trying to determine the existence of unauthorized access to data by a user or program, the IS auditor will often review the system logs. . 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 Explanation: A graphical interface to the map of the network topology is essential for the IS auditor to obtain a clear understanding of network management. QUESTION NO: 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. Pass Any Exam. Any Time. " - www. actualtests. com 31 Ac tua lTe sts QUESTION NO: 69 . co m Isaca CISA: Practice Exam D. Risk of unauthorized and untraceable changes to the database decreases. Answer: B Explanation: If users have direct access to a database at the system level, risk of unauthorized and untraceable changes to the database increases. QUESTION NO: 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. QUESTION NO: 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 Explanation: " Pass Any Exam. Any Time. " - www. actualtests. com Ac tua Explanation: 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. lTe Answer: A sts co m 32 Isaca CISA: Practice Exam Using capacity-monitoring software to monitor usage patterns and trends enables management to properly allocate resources and ensure continuous efficiency of operations. QUESTION NO: 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 Explanation: A system downtime log can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program. QUESTION NO: 74

Answer: A Explanation: Concurrency controls are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information. QUESTION NO: 75 . What increases encryption overhead and cost the most? A. A long symmetric encryption key B. A long asymmetric encryption key " Pass Any Exam. Any Time. " - www. actualtests. com Ac A. Referential integrity controls B. Normalization controls C. Concurrency controls D. Run-to-run totals tua lTe . 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. sts . co m 33 Isaca CISA: Practice Exam C. A long Advance Encryption Standard (AES) key D. A long Data Encryption Standard (DES) key Answer: B Explanation: A long asymmetric encryption key (public key encryption) increases encryption overhead and cost. All other answers are single shared symmetric keys. QUESTION NO: 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 macroenabled Word documents Answer: A QUESTION NO: 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 Explanation: Identifying network applications such as mail, web, or FTP servers to be externally accessed is an initial step in creating a proper firewall policy. " Pass Any Exam. Any Time. " - www. actualtests. com Ac tua lTe Explanation: Worms are malicious programs that can run independently and can propagate without the aid of a carrier program such as email. sts . co m 34 Isaca CISA: Practice Exam QUESTION NO: 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 Explanation: With public key encryption or asymmetric encryption, data is encrypted by the sender using the recipient's public key; the data is then decrypted using the recipient's private key. . How does the SSL network protocol provide confidentiality? Answer: D QUESTION NO: 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 Explanation: " Pass Any Exam. Any Time. " - www. actualtests. com Ac Explanation: The SSL protocol provides confidentiality through symmetric encryption such as Data Encryption Standard, or DES. tua lTe 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 sts . co QUESTION NO: 79 m 35 Isaca CISA: Practice Exam Information systems security policies are used as the framework for developing logical access controls. QUESTION NO: 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 Explanation: Time stamps are an effective control for detecting duplicate transactions such as payments made or received.

QUESTION NO: 82 Answer: C Explanation: File encryption is a good control for protecting confidential data residing on a PC. QUESTION NO: 83 . Which of the following is a guiding best practice for implementing logical access controls? A. Implementing theBiba 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 " Pass Any Exam. Any Time. " - www. actualtests. com Ac tua A. Personal firewall B. File encapsulation C. File encryption D.

Host-based intrusion detection lTe . Which of the following is a good control for protecting confidential data residing on a PC? sts . co m 36 Isaca CISA: Practice Exam Answer: B Explanation: Logical access controls should be reviewed to ensure that access is granted on a least-privilege basis, per the organization's data owners. QUESTION NO: 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 QUESTION NO: 85 Answer: A Explanation: The primary purpose of digital signatures is to provide authentication and integrity of datA . QUESTION NO: 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. " Pass Any Exam. Any Time. " - www. actualtests. com 37 Ac A. Authentication and integrity of data B. Authentication and confidentiality of data C. Confidentiality and integrity of data D. Authentication and availability of data tua . Which of the following do digital

signatures provide? lTe sts Explanation: PKI uses a combination of public-key cryptography and digital certificates to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions. co Answer: C m Isaca CISA: Practice Exam 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 Explanation: 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 its own message digest from the data for comparison and data integrity validation.

Public and private are used to enforce confidentiality. Hashing algorithms are used to enforce integrity. QUESTION NO: 87 Explanation: A fingerprint scanner facilitating biometric access control can provide a very high degree of server access control. QUESTION NO: 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 " Pass Any Exam. Any Time. " - www. actualtests. com 38 Ac Answer: D tua A. A mantrap-monitored entryway to the server room B.

Host-based intrusion detection combined withCCTVC. Network-based intrusion detection D. A fingerprint scanner facilitating biometric access control lTe . Which of the following would provide the highest degree of server access control? sts . co m Isaca CISA: Practice Exam Answer: B Explanation: Logical access controls are often the primary safeguards for systems software and datA . QUESTION NO: 89 . Which of the following is often used as a detection and deterrent control against Internet attacks? A. Honeypots B. CCTV C. VPN D. VLAN QUESTION NO: 90 Answer: A

Explanation: A monitored double-doorway entry system, also referred to as a mantrap or deadman door, is used as a deterrent control for the vulnerability of piggybacking. QUESTION NO: 91 . 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 notstateful inspection firewalls B. An application-layer gateway, or proxy firewall " Pass Any Exam. Any Time. " - www. actualtests. com 39 Ac tua 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 lTe . Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking? sts . co Explanation: Honeypots are often used as a detection

and deterrent control against Internet attacks. m Answer: A Isaca CISA: Practice Exam C. A circuit-level gateway D. A first-generation packet-filtering firewall Answer: B Explanation: Application-layer gateways, or proxy firewalls, are an effective method for controlling downloading of files via FTP.

Because FTP is an OSI application-layer protocol, the most effective firewall needs to be capable of inspecting through the application layer. QUESTION NO: 92 . 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 . 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 Explanation: Screensaver passwords are an effective control to implement as a countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off. QUESTION NO: 94 " Pass Any Exam. Any Time. " - www. actualtests. com Ac tua QUESTION NO: 93 lTe Explanation: Biometrics can be used to provide excellent physical access control. sts . co m 40 Isaca CISA: Practice Exam . 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 Explanation: ISPs can use access control lists to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources. Answer: B QUESTION NO: 96 . Which of the following is BEST characterized by unauthorized modification of data before or during systems data entry? A. Data diddling B. Skimming C.