

ISACA.CISA.v2026-01-26.q999

Exam Code:	CISA
Exam Name:	Certified Information Systems Auditor
Certification Provider:	ISACA
Free Question Number:	999
Version:	v2026-01-26
# of views:	110
# of Questions views:	9990
https://www.exam-tests.com/CISA-exam/ISACA.CISA.v2026-01-26.q999.html	

NEW QUESTION: 1

Which of the following findings should be of GREATEST concern to an IS auditor assessing the risk associated with end-user computing (EUC) in an organization?

- A. Insufficient processes to track ownership of each EUC application?
- B. Insufficient processes to test for version control
- C. Lack of awareness training for EUC users
- D. Lack of defined criteria for EUC applications

Answer: D (LEAVE A REPLY)

The finding that should be of greatest concern to an IS auditor assessing the risk associated with end-user computing (EUC) in an organization is the lack of defined criteria for EUC applications. EUC applications are applications that are developed and maintained by end-users, rather than by IT professionals, to support their business functions and processes. Examples of EUC applications include spreadsheets, databases, reports, and scripts. The lack of defined criteria for EUC applications means that the organization does not have clear and consistent standards or guidelines to identify, classify, and manage EUC applications. This can lead to various risks, such as:

Inaccurate or unreliable data and results from EUC applications that are not validated, verified, or tested
Unauthorized or inappropriate access or use of EUC applications that are not secured, controlled, or monitored
Inconsistent or incompatible data and results from EUC applications that are not integrated, documented, or updated
Loss or corruption of data and results from EUC applications that are not backed up, recovered, or archived
Therefore, the IS auditor should be most concerned about the lack of defined criteria for EUC applications, as it can affect the quality, integrity, and availability of the EUC applications and the data they produce.

Insufficient processes to track ownership of each EUC application is a finding that should be of concern to an IS auditor assessing the risk associated with EUC in an organization, but it is not the greatest concern. The ownership of an EUC application refers to the person or group who is responsible for creating, maintaining, and using the EUC application. Insufficient processes to

track ownership of each EUC application means that the organization does not have adequate mechanisms or records to identify and communicate who owns each EUC application. This can lead to risks, such as:

Lack of accountability or ownership for the quality and accuracy of the EUC application and its data
Lack of support or maintenance for the EUC application when the owner leaves or changes roles
Lack of awareness or training for the users of the EUC application on its purpose and functionality
However, these risks are less severe than those caused by the lack of defined criteria for EUC applications.

Insufficient processes to test for version control is a finding that should be of concern to an IS auditor assessing the risk associated with EUC in an organization, but it is not the greatest concern. Version control is a process that tracks and manages the changes made to an EUC application over time. Insufficient processes to test for version control means that the organization does not have adequate procedures or tools to ensure that the changes made to an EUC application are authorized, documented, and tested. This can lead to risks, such as:

Errors or inconsistencies in the data and results from different versions of the EUC application
Conflicts or confusion among the users of the EUC application on which version is current or correct
Loss or overwrite of data and results from previous versions of the EUC application
However, these risks are less severe than those caused by the lack of defined criteria for EUC applications.

Lack of awareness training for EUC users is a finding that should be of concern to an IS auditor assessing the risk associated with EUC in an organization, but it is not the greatest concern.

Awareness training for EUC users is a process that educates and informs the users of the EUC applications on their roles, responsibilities, and risks. Lack of awareness training for EUC users means that the organization does not have adequate programs or materials to raise the knowledge and skills of the users on how to use and manage the EUC applications effectively and securely. This can lead to risks, such as:

Misuse or abuse of the EUC applications by users who are not aware of their impact or implications
Non-compliance or violation of policies or regulations by users who are not aware of their requirements or expectations
Dissatisfaction or frustration among users who are not aware of their benefits or limitations
However, these risks are less severe than those caused by the lack of defined criteria for EUC applications.

References:

End-user computing - Wikipedia 1

How to Manage the Risks Associated with End User Computing 2

Managing end user computing risks - KPMG UK 3

NEW QUESTION: 2

Which of the following helps to ensure the integrity of data for a system interface?

- A.** System interface testing
- B.** user acceptance testing (UAT)
- C.** Validation checks

D. Audit logs

Answer: ([SHOW ANSWER](#))

Validation checks are a type of data quality control that helps to ensure the integrity of data for a system interface. Validation checks verify that the data entered or transferred between systems is correct, consistent, and conforms to predefined rules or standards. Validation checks can prevent or detect errors, anomalies, or inconsistencies in the data that may affect the system's functionality, performance, or security.

Option C is correct because validation checks are a common and effective method of ensuring data integrity for a system interface. Validation checks can be performed at various stages of the data lifecycle, such as input, processing, output, or storage. Validation checks can also be applied to different types of data, such as data types, codes, ranges, formats, consistency, and uniqueness.

Option A is incorrect because system interface testing is a type of software testing that verifies the interaction between two separate systems or components of a system. System interface testing does not directly ensure the integrity of data for a system interface, but rather the functionality and reliability of the interface itself.

System interface testing may use validation checks as part of its test cases, but it is not the same as validation checks.

Option B is incorrect because user acceptance testing (UAT) is a type of software testing that evaluates whether the system meets the user's expectations and requirements. UAT does not directly ensure the integrity of data for a system interface, but rather the usability and acceptability of the system from the user's perspective. UAT may use validation checks as part of its test scenarios, but it is not the same as validation checks.

Option D is incorrect because audit logs are records of events and activities that occur within a system or network. Audit logs do not directly ensure the integrity of data for a system interface, but rather provide evidence and accountability for the system's operations and security. Audit logs may use validation checks as part of their analysis or reporting, but they are not the same as validation checks.

References:

CISA Online Review Course¹, Module 5: Protection of Information Assets, Lesson 4: Data Quality Management, slide 5-6.

CISA Review Manual (Digital Version)², Chapter 5: Protection of Information Assets, Section 5.3: Data Quality Management, p. 281-282.

CISA Review Manual (Print Version), Chapter 5: Protection of Information Assets, Section 5.3: Data Quality Management, p. 281-282.

CISA Questions, Answers & Explanations Database³, Question ID: QAE_CISA_722.

Data Validation - Overview, Types, Practical Examples⁴

Data Validity: The Best Practice for Your Business⁵

Validation - Data validation⁶

What is Data Validation? Types, Techniques, Tools⁷

NEW QUESTION: 3

An IS auditor discovers that a developer has used the same key to grant access to multiple applications making calls to an application programming interface (API). Which of the following is the BEST recommendation to address this situation?

- A. Authorize the API key to allow read-only access by all applications.
- B. Coordinate an API key rotation exercise with all impacted application owners.
- C. Implement a process to expire the API key after a previously agreed-upon period of time.
- D. Replace the API key with time-limited tokens that grant least privilege access.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 4

To mitigate the risk of exposing data through application programming interface (API) queries, which of the following design considerations is MOST important?

- A. Data retention
- B. Data minimization
- C. Data quality
- D. Data integrity

Answer: ([SHOW ANSWER](#)**)**

Explanation

The answer B is correct because data minimization is the most important design consideration to mitigate the risk of exposing data through application programming interface (API) queries. An API is a set of rules and protocols that allows different software components or systems to communicate and exchange data. API queries are requests sent by users or applications to an API to retrieve or manipulate data. For example, a user may query an API to get information about a product, a service, or a location.

Data minimization is the principle of collecting, processing, and storing only the minimum amount of data that are necessary for a specific purpose. Data minimization can help to reduce the risk of exposing data through API queries by limiting the amount and type of data that are available or accessible through the API. Data minimization can also help to protect the privacy and security of the data subjects and the data providers, as well as to comply with the relevant laws and regulations.

Some of the benefits of data minimization for API design are:

Privacy: Data minimization can enhance the privacy of the data subjects by ensuring that only the data that are relevant and essential for the API purpose are collected and processed. This can prevent unnecessary or excessive collection or disclosure of personal or sensitive data, such as names, addresses, phone numbers, email addresses, etc. Data minimization can also help to comply with the privacy laws and regulations that require data protection by design and by default, such as GDPR (General Data Protection Regulation) or CCPA (California Consumer Privacy Act).

Security: Data minimization can improve the security of the data providers by reducing the attack surface and the potential damage of a data breach. If less data are stored or transmitted through

the API, there are fewer opportunities for attackers to access or compromise the data. Data minimization can also help to implement security controls such as encryption, access control, or logging more efficiently and effectively.

Performance: Data minimization can increase the performance of the API by optimizing the use of resources and bandwidth. If less data are stored or transmitted through the API, there are less storage space and network traffic required. Data minimization can also help to improve the speed and reliability of the API responses.

Some of the techniques for data minimization in API design are:

Define clear and specific purposes for the API and document them in the API specification or documentation.

Identify and classify the data that are needed for each purpose and assign them appropriate labels or levels, such as public, internal, confidential, or restricted.

Implement filters or parameters in the API queries that allow users or applications to specify or limit the data fields or attributes they want to retrieve or manipulate.

Use pagination or throttling in the API responses that limit the number or size of data items returned per request.

Use anonymization or pseudonymization techniques that remove or replace any identifying information from the data before sending them through the API.

Some examples of web resources that discuss data minimization in API design are:

Data Minimization in Web APIs - World Wide Web Consortium (W3C)

Adding Privacy by Design in Secure Application Development

Chung-ju/Data-Minimization: A repository of related papers. - GitHub

NEW QUESTION: 5

Which procedure provides the GREATEST assurance that corrective action to an audit report has been taken?

- A.** Inquiring about the current status of the recommendation
- B.** Reporting to the audit committee or the board of directors concerning specific action taken or lack thereof
- C.** Requesting a written management reply to the audit report identifying corrective action for each deficiency
- D.** Performing subsequent audit tests to verify resolution of the deficiencies

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 6

An organization is disposing of a number of laptop computers. Which of the following data destruction methods would be the MOST effective?

- A.** Run a low-level data wipe utility on all hard drives
- B.** Erase all data file directories
- C.** Format all hard drives
- D.** Physical destruction of the hard drive

Answer: D ([LEAVE A REPLY](#))

The most effective method is physical destruction. Running a low-level data wipe utility may leave some residual data that could be recovered; erasing data directories and formatting hard drives are easily reversed, exposing all data on the drive to unauthorized individuals.

NEW QUESTION: 7

Which of the following is the BEST way for an IS auditor to maintain visibility of a new system implementation project when faced with resource limitations

- A. Evaluate the project plan and milestones
- B. Assess user acceptance test (UAT) results.
- C. Review the target control environment
- D. Attend steering committee meetings.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 8

An IS auditor performing an independent classification of systems should consider a situation where functions could be performed manually at a tolerable cost for an extended period of time as:

- A. critical.
- B. vital.
- C. sensitive.
- D. noncritical.

Answer: C ([LEAVE A REPLY](#))

Sensitive functions are best described as those that can be performed manually at a tolerable cost for an extended period of time. Critical functions are those that cannot be performed unless they are replaced by identical capabilities and cannot be replaced by manual methods. Vital functions refer to those that can be performed manually but only for a brief period of time; this is associated with lower costs of disruption than critical functions. Noncritical functions may be interrupted for an extended period of time at little or no cost to the company, and require little time or cost to restore.

NEW QUESTION: 9

Which of the following should an IS auditor consider the MOST significant risk associated with a new health records system that replaces a legacy system?

- A. Staff were not involved in the procurement process, creating user resistance to the new system.
- B. Data is not converted correctly, resulting in inaccurate patient records.
- C. The deployment project experienced significant overruns, exceeding budget projections.
- D. The new system has capacity issues, leading to slow response times for users.

Answer: B ([LEAVE A REPLY](#))

The most significant risk associated with a new health records system that replaces a legacy system is data not being converted correctly, resulting in inaccurate patient records. Data conversion is the process of transferring data from one format or system to another. Data conversion is a critical step in implementing a new health records system, as it ensures that the patient data are consistent, complete, accurate, and accessible in the new system. Data not being converted correctly may cause errors, discrepancies, or losses in patient records, which may have serious implications for patient safety, quality of care, legal compliance, and privacy protection.

Staff not being involved in the procurement process, creating user resistance to the new system; the deployment project experiencing significant overruns, exceeding budget projections; and the new system having capacity issues, leading to slow response times for users are also risks associated with a new health records system implementation, but they are not as significant as data not being converted correctly. References: [ISACA CISA Review Manual 27th Edition], page 281.

NEW QUESTION: 10

When storing data archives off-site, what must be done with the data to ensure data completeness?

- A. The data must be normalized.
- B. The data must be validated.
- C. The data must be parallel-tested.
- D. The data must be synchronized.

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

When storing data archives off-site, data must be synchronized to ensure data completeness.

NEW QUESTION: 11

Which of the following is a standard secure email protection protocol?

- A. S/MIME
- B. SSH
- C. SET
- D. S/HTTP

Answer: ([SHOW ANSWER](#)**)**

Section: Protection of Information Assets

Explanation:

Secure Multipurpose Internet Mail Extension (S/MIME) is a standard secure email protocol that authenticates the identity of the sender and receiver, verifies message integrity, and ensures the privacy of message's content's, including attachments.

The following were incorrect answers:

SSH - A client server program that opens a secure, encrypted command-line shell session from the Internet for remote logon. Similar to a VPN, SSH uses strong cryptography to protect data,

including password, binary files and administrative commands, transmitted between system on a network. SSH is typically implemented between two parties by validating each other's credential via digital certificates. SSH is useful in securing Telnet and FTP services, and is implemented at the application layer, as opposed to operating at network layer (IPSec Implementation) SET - SET is a protocol developed jointly by VISA and Master Card to secure payment transaction among all parties involved in credit card transactions among all parties involved in credit card transactions on behalf of cardholders and merchants. As an open system specification, SET is a application-oriented protocol that uses trusted third party's encryption and digital-signature process, via PKI infrastructure of trusted third party institutions, to address confidentiality of information, integrity of data, cardholders authentication, merchant authentication and interoperability.

Secure Hypertext Transfer Protocol (S/HTTP) - As an application layer protocol, S/HTTP transmits individual messages or pages securely between a web client and server by establishing SSL-type connection. Using the https:// designation in the URL, instead of the standard http://, directs the message to a secure port number rather than the default web port address. This protocol utilizes SSL secure features but does so as a message rather than the session-oriented protocol.

Reference:

CISA review manual 2014 Page number 352 and 353

NEW QUESTION: 12

When using public key encryption to secure data being transmitted across a network:

- A. both the key used to encrypt and decrypt the data are public.
- B. the key used to encrypt is private, but the key used to decrypt the data is public.
- C. the key used to encrypt is public, but the key used to decrypt the data is private.
- D. both the key used to encrypt and decrypt the data are private.

Answer: [\(SHOW ANSWER\)](#)

Public key encryption, also known as asymmetric key cryptography, uses a public key to encrypt the message and a private key to decrypt it.

NEW QUESTION: 13

Which of the following type of a computer network is a WAN that are limited to a city?

- A. LAN
- B. MAN
- C. SAN
- D. PAN

Answer: [B \(LEAVE A REPLY\)](#)

Section: Information System Operations, Maintenance and Support

Explanation:

MAN - A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same

metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN.

For your exam you should know below information about computer networks:

Local Area Network (LAN)

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

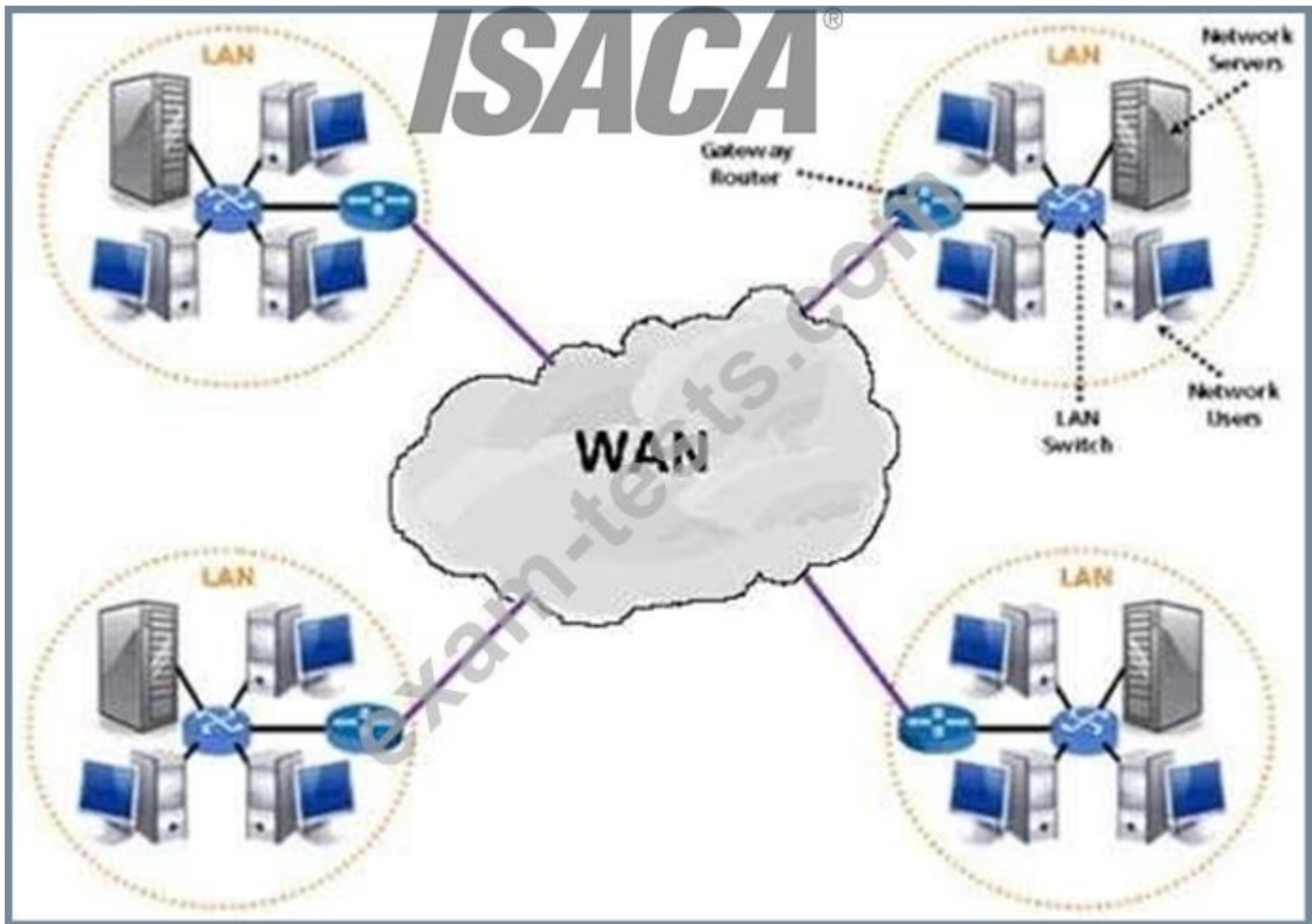
Local Area Network



Wide Area Network

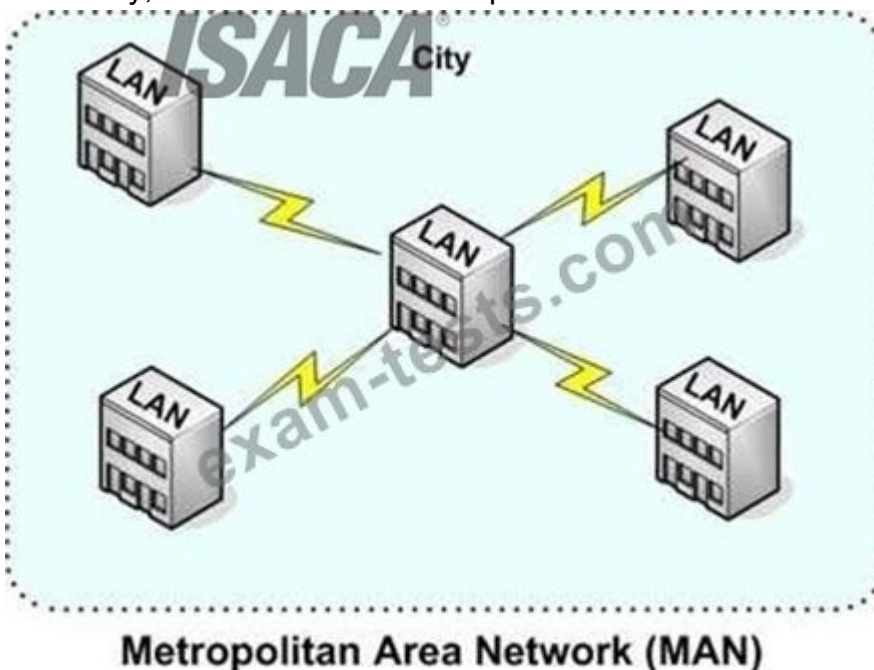
A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

Wide Area Network



Metropolitan Area Network

A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN Metropolitan Area Network



Personal Area Network

A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

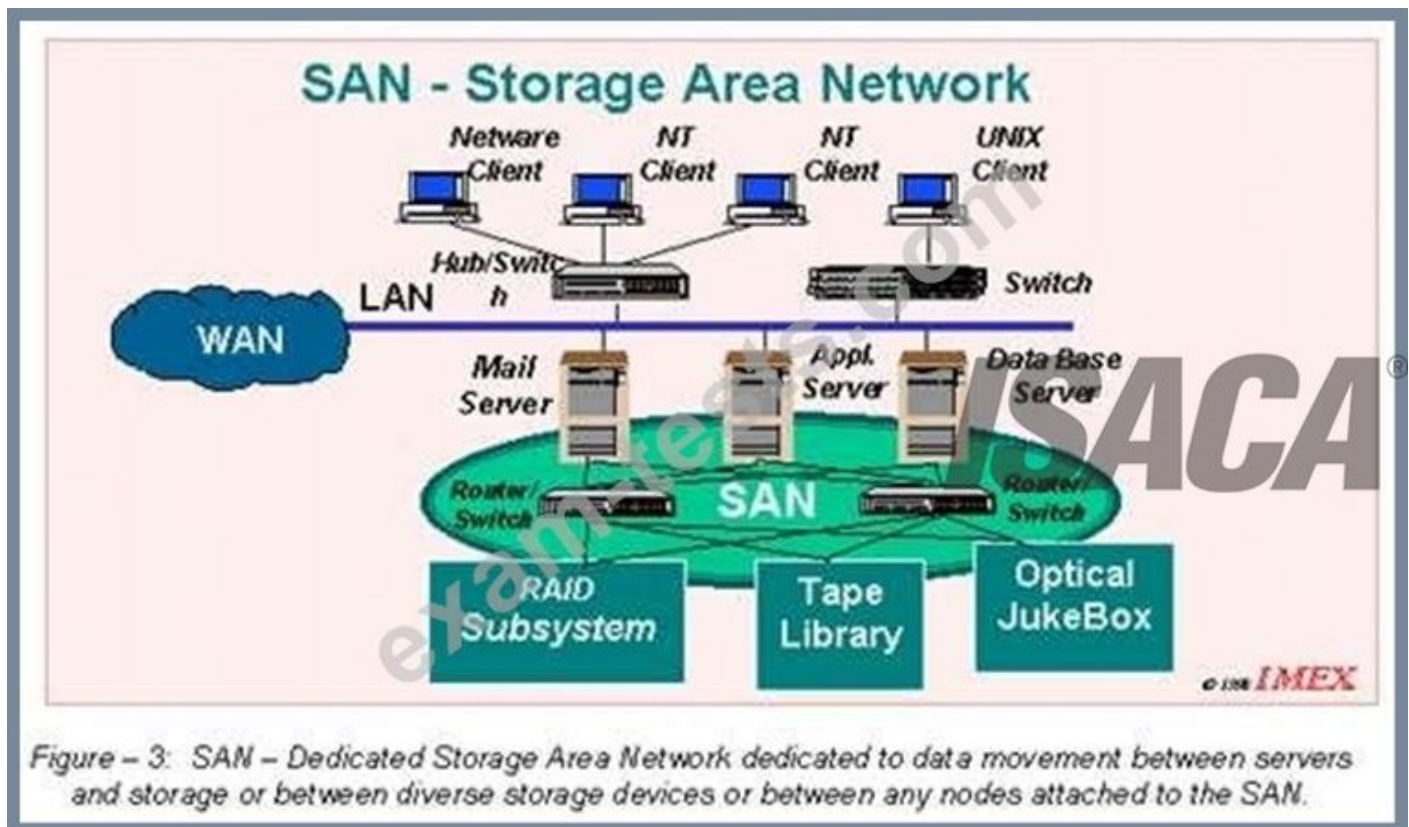
Personal Area Network



Storage Area Network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network



The following were incorrect answers:

PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

LAN - A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

SAN - A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Reference:

CISA review manual 2014 Page number 258

NEW QUESTION: 14

When using a wireless device, which of the following BEST ensures confidential access to email via web mail?

- A. Simple object access protocol (SOAP)
- B. Wired equivalent privacy (WEP)
- C. Extensible markup language (XML)
- D. Hypertext transfer protocol secure (HTTPS)

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 15

An IS auditor is reviewing a software-based configuration. Which of the following represents the GREATEST vulnerability? The firewall software:

- A. is configured with an implicit deny rule as the last rule in the rule base.
- B. is installed on an operating system with default settings.
- C. has been configured with rules permitting or denying access to systems or networks.
- D. is configured as a virtual private network (VPN) endpoint.

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Default settings are often published and provide an intruder with predictable configuration information, which allows easier system compromise. To mitigate this risk, firewall software should be installed on a system using a hardened operating system that has limited functionality, providing only the services necessary to support the firewall software. Choices A, C and D are normal or best practices for firewall configurations.

NEW QUESTION: 16

In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

- A. Diskless workstations
- B. Data encryption techniques
- C. Network monitoring devices
- D. Authentication systems

Answer: C ([LEAVE A REPLY](#))

Network monitoring devices may be used to inspect activities from known or unknown users and can identify client addresses, which may assist in finding evidence of unauthorized access. This serves as a detective control. Diskless workstations prevent access control software from being bypassed. Data encryption techniques can help protect sensitive or propriety data from unauthorized access, thereby serving as a preventive control. Authentication systems may provide environmentwide , logical facilities that can differentiate among users, before providing access to systems.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 17

In an environment that automatically reports all program changes, which of the following is the MOST efficient way to detect unauthorized changes to production programs?

- A. Reviewing the last compile date of production programs
- B. Manually comparing code in production programs to controlled copies
- C. Periodically running and reviewing test data against production programs
- D. Verifying user management approval of modifications

Answer: ([SHOW ANSWER](#))

Reviewing the last compile date of production programs is the most efficient way to detect unauthorized changes to production programs, as it can quickly identify any discrepancies between the expected and actual dates of program modification. The last compile date is a timestamp that indicates when a program was last compiled or translated from source code to executable code. Any changes to the source code would require a recompilation, which would update the last compile date. The IS auditor can compare the last compile date of production programs with the authorized change requests and reports to verify that only approved changes were implemented. The other options are not as efficient as option A, as they are more time-consuming, labor-intensive or error-prone. Manually comparing code in production programs to controlled copies is a method of verifying that the code in production matches the code in a secure repository or library, but it requires access to both versions of code and a tool or technique to compare them line by line. Periodically running and reviewing test data against production programs is a method of verifying that the programs produce the expected outputs and results, but it requires designing, executing and evaluating test cases for each program. Verifying user management approval of modifications is a method of verifying that the changes to production programs were authorized and documented, but it does not ensure that the changes were implemented correctly or accurately. References: CISA Review Manual (Digital Version) , Chapter 4:

Information Systems Operations and Business Resilience, Section 4.3: Change Management Practices.

NEW QUESTION: 18

Which of the following is MOST important to include in a contract to outsource data processing that involves customer personally identifiable information (Pit)?

- A. The vendor must compensate the organization if nonperformance occurs.
- B. The vendor must provide an independent report of its data processing facilities.
- C. The vendor must sign a nondisclosure agreement with the organization.
- D. The vendor must comply with the organization is legal and regulatory requirement.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 19

An employee transfers from an organization's risk management department to become the lead IS auditor.

While in the risk management department, the employee helped develop the key performance indicators (KPIs) now used by the organization. Which of the following would pose the GREATEST threat to the independence of this auditor?

- A. Developing KPIs to measure the internal audit team
- B. Training the IT audit team on IT risk management process
- C. Recommending controls to address the IT risks identified by KPIs
- D. Evaluating the effectiveness of IT risk management process

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 20

During a new system implementation, an IS auditor has been assigned to review risk management at each milestone. The auditor finds that several risks to project benefits have not been addressed. Who should be accountable for managing these risks?

- A. Enterprise risk manager
- B. Project sponsor
- C. Information security officer
- D. Project manager

Answer: D ([LEAVE A REPLY](#))

Explanation

The project manager should be accountable for managing the risks to project benefits. Project benefits are the expected outcomes or value that a project delivers to its stakeholders, such as improved efficiency, quality, customer satisfaction, or revenue. Project risks are uncertain events or conditions that may affect the project objectives, scope, budget, schedule, or quality. The project manager is responsible for identifying, analyzing, prioritizing, responding to, and monitoring project risks throughout the project life cycle. The other options are not accountable for managing project risks, as they have different roles and responsibilities. The enterprise risk manager is responsible for overseeing the organization's overall risk management framework and strategy, but not for managing specific project risks. The project sponsor is responsible for initiating, approving, and supporting the project, but not for managing project risks. The information security officer is responsible for ensuring that the project complies with the organization's information security policies and standards, but not for managing project risks.

References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION: 21

Which of the following tests is MOST likely to detect an error in one subroutine resulting from a recent change in another subroutine?

- A. Stress testing
- B. Regression testing
- C. User acceptance testing
- D. Black-box testing

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 22

Which of the following is the BEST type of backup to minimize the associated time and media?

- A. Compressed full
- B. Incremental
- C. Differential
- D. Mirror

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 23

What is the BEST action to prevent loss of data integrity or confidentiality in the case of an e-commerce application running on a LAN, processing electronic fund transfers (EFT) and orders?

- A. Using virtual private network (VPN) tunnels for data transfer
- B. Enabling data encryption within the application
- C. Auditing the access control to the network
- D. Logging all changes to access lists

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

The best way to ensure confidentiality and integrity of data is to encrypt it using virtual private network (VPN) tunnels. This is the most common and convenient way to encrypt the data traveling over the network. Data encryption within the application is less efficient than VPN. The other options are good practices, but they do not directly prevent the loss of data Integrity and confidentiality during communication through a network.

NEW QUESTION: 24

Which of the following should be of PRIMARY concern to an IS auditor reviewing the management of external IT service providers?

- A. Minimizing costs for the services provided
- B. Prohibiting the provider from subcontracting services
- C. Evaluating the process for transferring knowledge to the IT department
- D. Determining if the services were provided as contracted

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

From an IS auditor's perspective, the primary objective of auditing the management of service providers should be to determine if the services that were requested were provided in a way that is acceptable, seamless and in line with contractual agreements. Minimizing costs, if applicable and achievable (depending on the customer's need) is traditionally not part of an IS auditor's job. This would normally be done by a line management function within the IT department.

Furthermore, during an audit, it is too late to minimize the costs for existing provider arrangements. Subcontracting providers could be a concern, but it would not be the primary concern. Transferring knowledge to the internal IT department might be desirable under certain circumstances, but should not be the primary concern of an IS auditor when auditing IT service providers and the management thereof.

NEW QUESTION: 25

An IS auditor examining the configuration of an operating system to verify the controls should review the:

- A.** transaction logs.
- B.** authorization tables.
- C.** parameter settings.
- D.** routing tables.

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Parameters allow a standard piece of software to be customized for diverse environments and are important in determining how a system runs. The parameter settings should be appropriate to an organization's workload and control environment, improper implementation and/or monitoring of operating systems can result in undetected errors and corruption of the data being processed, as well as lead to unauthorized access and inaccurate logging of system usage. Transaction logs are used to analyze transactions in master and/or transaction files. Authorization tables are used to verify implementation of logical access controls and will not be of much help when reviewing control features of an operating system. Routing tables do not contain information about the operating system and, therefore, provide no information to aid in the evaluation of controls.

NEW QUESTION: 26

Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

- A.** Function point analysis
- B.** PERT chart
- C.** Rapid application development
- D.** Object-oriented system development

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

A PERT chart will help determine project duration once all the activities and the work involved with those activities are known. Function point analysis is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries, logical internal files, etc. While this will help determine the size of individual activities, it will not assist in determining project duration since there are many overlapping tasks. Rapid application development is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality, while object-oriented system development is the process of solution specification and modeling.

NEW QUESTION: 27

An IS auditor is reviewing the remote access methods of a company used to access system remotely.

Which of the following is LEAST preferred remote access method from a security and control point of view?

- A. RADIUS
- B. TACACS
- C. DIAL-UP
- D. DIAMETER

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation/Reference:

Dial-up connectivity not based on centralized control and least preferred from security and control standpoint.

Remote access user can connect remotely to their organization's networks with the same level of functionality as if they would access from within their office.

In connecting to an organization's network, a common method is to use dial-up lines. Access is granted

through the organization's network access server (NAS) working in concert with an organization network

firewall and router. The NAS handle user authentication, access control and accounting while maintaining

connectivity. The most common protocol for doing this is the Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Controller System (TACACS).

Remote access Controls include:

Policy and standard

Proper authorization

Identification and authentication mechanism

Encryption tool and technique such as use of VPN

System and network management

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 334

NEW QUESTION: 28

The purpose of business continuity planning and disaster-recovery planning is to:

- A. Transfer the risk and impact of a business interruption or disaster
- B. Mitigate, or reduce, the risk and impact of a business interruption or disaster
- C. Accept the risk and impact of a business
- D. Eliminate the risk and impact of a business interruption or disaster

Answer: B ([LEAVE A REPLY](#))

The primary purpose of business continuity planning and disaster-recovery planning is to mitigate, or reduce, the risk and impact of a business interruption or disaster. Total elimination of risk is impossible.

NEW QUESTION: 29

Which of the following areas of responsibility would cause the GREATEST segregation of duties conflict if the individual who performs the related tasks also has approval authority?

- A. Purchase requisitions and purchase orders
- B. Invoices and reconciliations
- C. Goods receipts and payments
- D. Vendor selection and statements of work

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 30

Which of the following is the most fundamental step in preventing virus attacks?

- A. Adopting and communicating a comprehensive antivirus policy
- B. Implementing antivirus protection software on users' desktop computers
- C. Implementing antivirus content checking at all network-to-Internet gateways
- D. Inoculating systems with antivirus code

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Adopting and communicating a comprehensive antivirus policy is the most fundamental step in preventing virus attacks. All other antivirus prevention efforts rely upon decisions established and communicated via policy.

NEW QUESTION: 31

Which of the following provides the BEST assurance that vendor-supported software remains up to date?

- A. Licensing agreement and escrow

- B. Software asset management
- C. Version management
- D. Release and patch management

Answer: D ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 32

Which of the following BEST demonstrates to an IS auditor that an organization has implemented effective risk management processes?

- A. The risk register is reviewed periodically.
- B. Critical business assets have additional controls.
- C. A business impact analysis (BIA) has been completed.
- D. The inventory of IT assets includes asset classification.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 33

When participating as a member of a system development team, the IS auditor should be aware that:

- A. the auditor's ability to perform an independent evaluation of the application after implementation will be impaired.
- B. for ongoing evaluation capability, the auditor should ensure that computer audit software is implemented in all applications.
- C. as a control specialist, the auditor can provide significant value to the project team by making the final decision on specific controls.
- D. the auditor should sign a statement of independence prior to participating in the project team.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 34

Following a recent internal data breach, an IS auditor was asked to evaluate information security practices within the organization. Which of the following findings would be MOST important to report to senior management?

- A. Employees are not required to sign a non-compete agreement.
- B. Security education and awareness workshops have not been completed.

- C. Users lack technical knowledge related to security and data protection.
- D. Desktop passwords do not require special characters.

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 35

When designing metrics for information security, the MOST important consideration is that the metrics:

- A. provide actionable data.
- B. track trends over time.
- C. are easy to understand.
- D. apply to all business units.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 36

.Why does an IS auditor review an organization chart?

- A. To optimize the responsibilities and authority of individuals
- B. To control the responsibilities and authority of individuals
- C. To better understand the responsibilities and authority of individuals
- D. To identify project sponsors

Answer: C ([LEAVE A REPLY](#))

The primary reason an IS auditor reviews an organization chart is to better understand the responsibilities and authority of individuals.

NEW QUESTION: 37

Of the following, who should authorize a project management team's request to take a mission-critical application offline to implement a new release and configuration?

- A. Project manager
- B. Chief information security officer (CISO)
- C. Business process owner
- D. Application administrator

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 38

Which of the following BEST enables an organization to improve the effectiveness of its incident response team?

- A. Conducting periodic testing and incorporating lessons learned
- B. Increasing the mean resolution time and publishing key performance indicator (KPI) metrics
- C. Disseminating incident response procedures and requiring signed acknowledgment by team members
- D. Ensuring all team members understand information systems technology

Answer: A ([LEAVE A REPLY](#))

Explanation

Conducting periodic testing and incorporating lessons learned is the best way to improve the effectiveness of an incident response team. This allows the team to practice their response procedures, identify any gaps or weaknesses in their response, and learn from their mistakes. It also helps to keep the team's skills sharp and up-to-date. The lessons learned from these tests can then be used to improve the team's procedures and performance¹². While understanding information systems technology, disseminating incident response procedures, and publishing KPI metrics can contribute to the effectiveness of the team, they do not provide the same level of continuous improvement as periodic testing and learning from experience.

NEW QUESTION: 39

During a security audit of IT processes, an IS auditor found that there were no documented security

procedures. The IS auditor should:

- A.** create the procedures document.
- B.** terminate the audit.
- C.** conduct compliance testing.
- D.** identify and evaluate existing practices.

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

One of the main objectives of an audit is to identify potential risks; therefore, the most proactive approach

would be to identify and evaluate the existing security practices being followed by the organization. IS

auditors should not prepare documentation, as doing so could jeopardize their independence.

Terminating

the audit may prevent achieving one of the basic audit objectives, i.e., identification of potential risks. Since

there are no documented procedures, there is no basis against which to test compliance.

NEW QUESTION: 40

Which of the following is the BEST way to ensure email confidentiality in transit?

- A.** Encryption of corporate network traffic
- B.** End-to-end encryption
- C.** Digital signatures
- D.** Complex user passwords

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 41

Which of the following is MOST important for the improvement of an organization's incident response processes?

- A. Post-event reviews by the incident response team
- B. Regular upgrades to incident management software
- C. Ongoing incident response training for users
- D. Periodic walk-through of incident response procedures

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 42

Which of the following is the PRIMARY purpose of batch processing monitoring?

- A. To prevent an incident that may result from batch failure
- B. To summarize the batch processing reporting
- C. To comply with security standards
- D. To log error events in batch processing

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 43

Which of the following should be of GREATEST concern for an IS auditor reviewing an organization's bring your own device (BYOD) policy?

- A. A mobile device management (MDM) solution is not implemented.
- B. Not all devices are approved for BYOD.
- C. The policy does not include the right to audit BYOD devices.
- D. The policy is not updated annually.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 44

Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance program?

- A. A system downtime log
- B. Vendors' reliability figures
- C. Regularly scheduled maintenance log
- D. A written preventive maintenance schedule

Answer: A ([LEAVE A REPLY](#))

A system downtime log provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

NEW QUESTION: 45

Which of the following should be of MOST concern to an IS auditor reviewing the public key infrastructure (PKI) for enterprise email?

- A. The PKI policy has not been updated within the last year.

- B. The certificate revocation list has not been updated.
- C. The certificate practice statement has not been published
- D. The private key certificate has not been updated.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 46

An external IS auditor is reviewing the continuous monitoring system for a large bank and notes several potential issues. Which of the following would present the GREATEST concern regarding the reliability of the monitoring system?

- A. The system results are not reviewed by senior management.
- B. The alert threshold is updated periodically.
- C. The monitoring thresholds are not subject to change management.
- D. The monitoring system was configured by a third party.

Answer: C ([LEAVE A REPLY](#))

Monitoring systems rely heavily on thresholds to detect anomalies or incidents. If thresholds can be changed without proper change management controls, the entire system's reliability is compromised because unauthorized or improper changes could either suppress critical alerts or generate excessive false positives.

While senior management review (A) is important for governance, it does not directly affect the accuracy of monitoring results. Periodic threshold updates (B) are actually good practice as long as they are controlled.

Third-party configuration (D) can be acceptable if properly governed. ISACA's COBIT BAI06 (Managed IT Changes) stresses that all changes to production systems-including monitoring thresholds-must follow formal change control processes to maintain integrity and reliability.

References (ISACA): COBIT 2019, BAI06 Managed IT Changes.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As

Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 47

When reviewing an organization's information security policies, an IS auditor should verify that the policies have been defined PRIMARILY on the basis of:

- A. a risk management process.
- B. an information security framework.
- C. past information security incidents.

D. industry best practices.

Answer: A ([LEAVE A REPLY](#))

Explanation

Information security policies are high-level statements that define the organization's approach to protecting its information assets from threats and risks. They should be based primarily on a risk management process, which is a systematic method of identifying, analyzing, evaluating, treating, and monitoring information security risks. A risk management process can help ensure that the policies are aligned with the organization's risk appetite, business objectives, legal and regulatory requirements, and stakeholder expectations. An information security framework is a set of standards, guidelines, and best practices that provide a structure for implementing information security policies. It can support the risk management process, but it is not the primary basis for defining the policies. Past information security incidents and industry best practices can also provide valuable inputs for defining the policies, but they are not sufficient to address the organization's specific context and needs. References: Insights and Expertise, CISA Review Manual (Digital Version)

NEW QUESTION: 48

During the implementation of an upgraded enterprise resource planning (ERP) system, which of the following is the MOST important consideration for a go-live decision?

- A. Rollback strategy
- B. Test cases
- C. Post-implementation review objectives
- D. Business case

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 49

When conducting a penetration test of an IT system, an organization should be MOST concerned with:

- A. the confidentiality of the report.
- B. finding all possible weaknesses on the system.
- C. restoring all systems to the original state.
- D. logging all changes made to the production system.

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

All suggested items should be considered by the system owner before agreeing to penetration tests, but the most important task is to be able to restore all systems to their original state. Information that is created and/or stored on the tested systems should be removed from these systems. If for some reason, at the end of the penetration test, this is not possible, all files (with their location) should be identified in the technical report so that the client's technical staff will be able to remove these after the report has been received.

NEW QUESTION: 50

Which of the following findings from a database security audit presents the GREATEST risk of critical security exposures?

- A. Legacy data has not been purged.
- B. Admin account passwords are not set to expire.
- C. Default settings have not been changed.
- D. Database activity logging is not complete.

Answer: ([SHOW ANSWER](#))

Explanation

Admin accounts typically have the highest level of privileges and access to sensitive data. If the passwords for these accounts are not set to expire, it increases the risk of unauthorized access and potential security breaches. This is especially true if an admin's credentials are compromised, as the attacker could have ongoing access to critical systems and data1.

References:

Database Auditing - Satori

NEW QUESTION: 51

Which of the following would be of GREATEST concern to an IS auditor evaluating an organization's change management process?

- A. A list of authorized requestors for emergency changes does not exist.
- B. Changes are approved after being moved to production.
- C. Change requests are not subject to prioritization.
- D. Change management meeting minutes are not available for several meetings.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 52

The cost of ongoing operations when a disaster recovery plan is in place, compared to not having a

disaster recovery plan, will MOST likely:

- A. increase.
- B. decrease.
- C. remain the same.
- D. be unpredictable.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Due to the additional cost of disaster recovery planning (DRP) measures, the cost of normal operations for any organization will always increase after a DRP implementation, i.e., the cost of normal operations during

a nondisaster period will be more than the cost of operations during a nondisaster period when no disaster recovery plan was in place.

NEW QUESTION: 53

Which of the following is the MOST important benefit of involving IS audit when implementing governance of enterprise IT?

- A.** Identifying relevant roles for an enterprise IT governance framework
- B.** Making decisions regarding risk response and monitoring of residual risk
- C.** Verifying that legal, regulatory, and contractual requirements are being met
- D.** Providing independent and objective feedback to facilitate improvement of IT processes

Answer: D ([LEAVE A REPLY](#))

The most important benefit of involving IS audit when implementing governance of enterprise IT is providing independent and objective feedback to facilitate improvement of IT processes. Governance of enterprise IT is the process of ensuring that IT supports the organization's strategy, goals, and objectives in an effective, efficient, ethical, and compliant manner. IS audit can provide value to governance of enterprise IT by assessing the alignment of IT with business needs, evaluating the performance and value delivery of IT, identifying risks and issues related to IT, recommending corrective actions and best practices, and monitoring the implementation and effectiveness of IT governance activities. IS audit can also provide assurance that IT governance processes are designed and operating in accordance with relevant standards, frameworks, laws, regulations, and contractual obligations. Identifying relevant roles for an enterprise IT governance framework is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help define and clarify the roles and responsibilities of various stakeholders involved in IT governance, such as board members, senior management, business units, IT function, external parties, etc. IS audit can also help ensure that these roles are aligned with the organization's strategy, goals, and objectives, and that they have adequate authority, accountability, communication, and reporting mechanisms. However, this benefit is more related to the design phase of IT governance implementation than to the ongoing monitoring and improvement phase. Making decisions regarding risk response and monitoring of residual risk is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help identify and assess the risks associated with IT activities and processes, such as strategic risks, operational risks, compliance risks, security risks, etc. IS audit can also help evaluate the effectiveness of risk management practices and controls implemented by management to mitigate or reduce these risks. However, this benefit is more related to the assurance function of IS audit than to its advisory function. Verifying that legal, regulatory, and contractual requirements are being met is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help verify that IT activities and processes comply with applicable laws, regulations, and contractual obligations, such as data protection laws, privacy laws, cybersecurity laws, industry standards, service level agreements, etc. IS audit can also help

identify and report any instances of noncompliance or violations that could result in legal or reputational consequences for the organization. However, this benefit is more related to the assurance function of IS audit than to its advisory function. References: ISACA CISA Review Manual 27th Edition, page 283

NEW QUESTION: 54

An IS auditor finds that conference rooms have active network ports. Which of the following is MOST important to ensure?

- A. The corporate network is using an intrusion prevention system (IPS)
- B. This part of the network is isolated from the corporate network
- C. A single sign-on has been implemented in the corporate network
- D. Antivirus software is in place to protect the corporate network

Answer: B ([LEAVE A REPLY](#))

If the conference rooms have access to the corporate network, unauthorized users may be able to connect to the corporate network; therefore, both networks should be isolated either via a firewall or being physically separated. An IPS would detect possible attacks, but only after they have occurred. A single sign-on would ease authentication management. Antivirus software would reduce the impact of possible viruses; however, unauthorized users would still be able to access the corporate network, which is the biggest risk.

NEW QUESTION: 55

Which of the following observations should be of GREATEST concern to an IS auditor reviewing an organization's enterprise architecture (EA) program?

- A. The architecture review board is chaired by the CIO
- B. IT application owners have sole responsibility for architecture approval
- C. The EA program governs projects that are not IT-related
- D. Information security requirements are reviewed by the EA program

Answer: B ([LEAVE A REPLY](#))

IT application owners having sole responsibility for architecture approval (B) is a major concern because it indicates a lack of oversight and segregation of duties. EA decisions should be reviewed by a cross-functional governance body to ensure alignment with security, compliance, and business objectives.

Other options:

The CIO chairing the review board (A) may indicate centralized leadership but is not inherently a risk.

EA governing non-IT projects (C) may indicate scope expansion but is not a security risk.

Security requirements being reviewed (D) is a best practice and not a concern.

Reference: ISACA CISA Review Manual, IT Governance and Management of IT

NEW QUESTION: 56

Which of the following would be the PRIMARY benefit of replacing physical keys with an electronic entry system for a data center?

- A. Creates an audit trail
- B. Enables data mining
- C. Ensures compliance
- D. Reduces cost

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

NEW QUESTION: 57

An organization having a number of offices across a wide geographical area has developed a disaster recovery plan. Using actual resources, which of the following is the MOST cost-effective test of the disaster recovery plan?

- A. Full operational test
- B. Preparedness test
- C. Paper test
- D. Regression test

Answer: B ([LEAVE A REPLY](#))

A preparedness test is performed by each local office/area to test the adequacy of the preparedness of local operations for disaster recovery. A paper test is a structured walk-through of the disaster recovery plan and should be conducted before a preparedness test. A full operational test is conducted after the paper and preparedness test. A regression test is not a disaster recovery planning (DRP) test and is used in software maintenance.

NEW QUESTION: 58

Which of the following should be the FIRST step in an organization's forensics process to preserve evidence?

- A. Determine which forensic tools to use
- B. Create the forensics analysis reporting template
- C. Duplicate digital evidence and validate it using a hash function
- D. Perform analytics on digital evidence obtained using forensic methods

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 59

Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?

- A. Engaging an independent third party to perform the forensic investigation
- B. Restricting evidence access to professionally certified forensic investigators
- C. Documenting evidence handling by personnel throughout the forensic investigation

D. Performing investigative procedures on the original hard drives rather than images of the hard drives

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 60

The FIRST course of action an investigator should take when a computer is being attacked is to:

- A. terminate all active processes.
- B. copy the contents of the hard drive.
- C. disconnect it from the network.
- D. disconnect the power source.

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

NEW QUESTION: 61

Which of the following observations should be of GREATEST concern to an IS auditor performing a review of an organization's IT governance structure?

- A. The chief risk officer is also the chief information officer.
- B. The chief information officer is prohibited from making capital decisions regarding IT.
- C. The IT steering committee has oversight of the IT budget.
- D. There are no IT subject matter experts on the board of directors.

Answer: A ([LEAVE A REPLY](#))

Section: Governance and Management of IT

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As

Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 62

The PRIMARY objective of a logical access control review is to:

- A. review access controls provided through software.
- B. ensure access is granted per the organization's authorities.
- C. walk through and assess the access provided in the IT environment.
- D. provide assurance that computer hardware is adequately protected against abuse.

Answer: B ([LEAVE A REPLY](#))

The scope of a logical access control review is primarily to determine whether or not access is granted per the organization's authorizations. Choices A and C relate to procedures of a logical

access control review, rather than objectives. Choice D is relevant to a physical access control review.

NEW QUESTION: 63

An organization recently implemented a data loss prevention (DLP) solution to control data in transit. Which of the following would be the GREATEST risk related to the DLP implementation?

- A. Inadequate data classification
- B. Improperly configured DLP modules
- C. Scanning end-points during peak hours
- D. DLP false positive alerts

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 64

What is the BEST way to control updates to the vendor master file in an accounts payable system?

- A. Periodically reviewing the entire vendor master file
- B. Having only one person updating the master file
- C. Using prenumbered and authorized request forms
- D. Comparing updates against authorization

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 65

An IS auditor is reviewing the release management process for an in-house software development solution. In which environment is the software version MOST likely to be the same as production?

- A. Staging
- B. Testing
- C. Integration
- D. Development

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 66

A company requires that all program change requests (PCRs) be approved and all modifications be automatically logged. Which of the following IS audit procedures will BEST determine whether unauthorized changes have been made to production programs?

- A. Trace a sample of complete PCR forms to the log of all program changes
- B. Use source code comparison software to determine whether any changes have been made to a sample of programs since the last audit date
- C. Review a sample of PCRs for proper approval throughout the program change process
- D. Trace a sample of program change from the log to completed PCR forms

Answer: B ([LEAVE A REPLY](#))

Explanation

The best way to determine whether unauthorized changes have been made to production programs is to use source code comparison software to compare the current version of the programs with the previous version or the approved version. This will identify any changes that have been made without proper authorization or documentation. Tracing PCR's to logs or vice versa will only verify that the authorized changes have been recorded, but not detect any unauthorized changes. References: Standards, Guidelines, Tools and Techniques - ISACA, section "IS Audit and Assurance Tools and Techniques"

NEW QUESTION: 67

Which of the following method is recommended by security professional to PERMANENTLY erase sensitive data on magnetic media?

- A. Degaussing
- B. Overwrite every sector of magnetic media with pattern of 1's and 0's
- C. Format magnetic media
- D. Delete File allocation table

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

PERMANENTLY is the keyword used in the question. You need to find out data removal method which remove data permanently from magnetic media.

Degaussing is the most effective method out of all provided choices to erase sensitive data on magnetic media provided magnetic media is not require to be reuse. Some degausses can destroy drives. The security professional should exercise caution when recommending or using degausses on media for reuse.

A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment).

For your exam you should know the information below:

When media is to be reassigned (a form of object reuse), it is important that all residual data is carefully removed.

Simply deleting files or formatting the media does not actually remove the information. File deletion and media formatting often simply remove the pointers to the information. Providing assurance for object reuse requires specialized tools and techniques according to the type of media on which the data resides.

Specialized hardware devices known as degausses can be used to erase data saved to magnetic media.

The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity. It is important to make sure that the coercivity of the degasser is of

sufficient strength to meet object reuse requirements when erasing data. If a degasser is used with insufficient coercivity, then a remanence of the data will exist.

Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over. Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse. Some degausses can destroy drives.

The security professional should exercise caution when recommending or using degausses on media for reuse.

Software tools also exist that can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media. There is a drawback to using overwrite software. During normal write operations with magnetic media, the head of the drive moves back-and-forth across the media as data is written. The track of the head does not usually follow the exact path each time.

The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten.

To provide higher assurance in this case, it is necessary to overwrite each sector multiple times. Security practitioners should keep in mind that a one-time pass may be acceptable for noncritical information, but sensitive data should be overwritten with multiple passes. Overwrite software can also be used to clear the sectors within solid-state media such as USB thumb drives. It is suggested that physical destruction methods such as incineration or secure recycling should be considered for solid-state media that is no longer used.

The last form of preventing unauthorized access to sensitive data is media destruction.

Shredding, burning, grinding, and pulverizing are common methods of physically destroying media. Degaussing can also be a form of media destruction. High-power degausses are so strong in some cases that they can literally bend and warp the platters in a hard drive.

Shredding and burning are effective destruction methods for non-rigid magnetic media. Indeed, some shredders are capable of shredding some rigid media such as an optical disk. This may be an effective alternative for any optical media containing nonsensitive information due to the residue size remaining after feeding the disk into the machine.

However, the residue size might be too large for media containing sensitive information.

Alternatively, grinding and pulverizing are acceptable choices for rigid and solid-state media.

Specialized devices are available for grinding the face of optical media that either sufficiently scratches the surface to render the media unreadable or actually grinds off the data layer of the disk. Several services also exist which will collect drives, destroy them on site if requested and provide certification of completion. It will be the responsibility of the security professional to help, select, and maintain the most appropriate solutions for media cleansing and disposal.

The following answers are incorrect:

Overwrite every sector of magnetic media with pattern of 1's and 0's-Less effective than degaussing provided magnetic media is not require to be reuse.

Format magnetic media - Formatting magnetic media does not erase all data. Data can be recoverable after formatting using software tools.

Delete File allocation table-It will not erase all data. Data can be recoverable using software tools.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 338

Official ISC2 guide to CISSP CBK 3rd Edition Page number 720.

NEW QUESTION: 68

When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator to ensure that the:

- A. hardware is protected against power surges.
- B. integrity is maintained if the main power is interrupted.
- C. immediate power will be available if the main power is lost.
- D. hardware is protected against long-term power fluctuations.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

A voltage regulator protects against short-term power fluctuations. It normally does not protect against long-term surges, nor does it maintain the integrity if power is interrupted or lost.

NEW QUESTION: 69

An organization uses multiple offsite data center facilities Which of the following is MOST important to consider when choosing related backup devices and media?

- A. Backup media capacity
- B. Associated costs
- C. Restoration speed
- D. Standardization

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 70

An IS auditor finds a computer that is suspected to have been involved in a cyber crime. Which of the following activities is MOST critical to ensure data collected is admissible in a court of law?

- A. Collect audit logs from the affected computer.
- B. Power off the computer to ensure data is not changed.
- C. Track possession of the computer.
- D. Notify law enforcement upon detection.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 71

Providing security certification for a new system should include which of the following prior to the system's implementation?

- A. External audit sign-off on financial controls
- B. End-user authorization to use the system in production
- C. An evaluation of the configuration management practices
- D. Testing of the system within the production environment

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 72

Who is ultimately responsible for providing requirement specifications to the software-development team?

- A. The project sponsor
- B. The project members
- C. The project leader
- D. The project steering committee

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

Explanation:

The project sponsor is ultimately responsible for providing requirement specifications to the software- development team.

NEW QUESTION: 73

An IS audit manager has been asked to perform a quality review on an audit that the same manager also supervised. Which of the following is (he manager's BEST response to this situation?

- A. Discuss with the audit team to understand how conclusions were reached.
- B. Escalate the situation to senior audit leadership.
- C. Notify the audit committee of the situation.
- D. Determine whether audit evidence supports audit conclusions.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 74

A characteristic of a digital signature is that it:

- A. has a reproducible hashing algorithm
- B. is under control of the receiver.
- C. unique to the message
- D. Is validated when data are changed.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 75

An IS auditor has completed the fieldwork phase of a network security review and is preparing the initial draft of the audit report. Which of the following findings should be ranked as the HIGHEST risk?

- A. The network device inventory is incomplete.
- B. Network firewall rules have not been documented.
- C. Network penetration tests are not performed.
- D. The network firewall policy has not been approved by the information security officer.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 76

Which of the following is the BEST detective control for a job scheduling process involving data transmission?

- A. Jobs are scheduled to be completed daily and data is transmitted using a Secure File Transfer Protocol (SFTP).
- B. Jobs are scheduled and a log of this activity is retained for subsequent review.
- C. Failure alerts are automatically generated and routed to support personnel
- D. Metrics denoting the volume of monthly job failures are reported and reviewed by senior management

Answer: C ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As

Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 77

During an exit interview, senior management disagrees with some of the facts presented in the draft audit report and wants them removed from the report. Which of the following would be the auditor's BEST course of action?

- A. Revise the assessment based on senior management's objections.
- B. Escalate the issue to audit management.
- C. Finalize the draft audit report without changes.
- D. Gather evidence to analyze senior management's objections

Answer: D ([LEAVE A REPLY](#))

The auditor's best course of action when senior management disagrees with some of the facts presented in the draft audit report is to gather evidence to analyze senior management's objections. The auditor should not revise the assessment, escalate the issue, or finalize the report without changes until they have evaluated the validity and relevance of senior management's objections and resolved any discrepancies or misunderstandings. The auditor should maintain a

professional and objective attitude and seek to present a fair and accurate audit report based on sufficient and appropriate evidence. References:

* CISA Review Manual (Digital Version), page 372

* CISA Questions, Answers & Explanations Database, question ID 3338

NEW QUESTION: 78

What is the PRIMARY reason for conducting a risk assessment when developing an annual IS audit plan?

- A. Decide which audit procedures and techniques to use
- B. Identify and prioritize audit areas
- C. Determine the existence of controls in audit areas
- D. Provide assurance material items will be covered

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 79

Which of the following is the BEST way to ensure an organization's data classification policies are preserved during the process of data transformation?

- A. Map data classification controls to data sets.
- B. Control access to extract, transform, and load (ETL) tools.
- C. Conduct a data discovery exercise across all business applications.
- D. Implement classification labels in metadata during data creation.

Answer: (SHOW ANSWER)

Explanation

Data classification is the process of tagging data according to its type, sensitivity, and value to the organization. Data transformation is the process of changing the structure and format of data to make it usable for analysis and visualization. Both processes are important for data security and compliance, but they also pose some challenges.

One of the challenges is to ensure that the organization's data classification policies are preserved during the process of data transformation. This means that the data should retain its original classification level and labels after it is transformed, and that the appropriate controls and protections are applied to the transformed data.

The best way to ensure this is to implement classification labels in metadata during data creation (D).

Metadata is data that describes other data, such as its source, format, content, and context. By adding classification labels to metadata, the data can be easily identified and tracked throughout its lifecycle, including during data transformation. The labels can also help enforce the proper access rights and encryption standards for the data, regardless of its state or location.

NEW QUESTION: 80

Which of the following is the MOST important area of focus for an IS auditor when developing a risk-based audit strategy?

- A. Recent audit results
- B. Existing IT controls
- C. Critical business applications
- D. Business processes

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 81

When reviewing an organization's strategic IT plan an IS auditor should expect to find:

- A. an assessment of the fit of the organization's application portfolio with business objectives.
- B. actions to reduce hardware procurement cost.
- C. a listing of approved suppliers of IT contract resources.
- D. a description of the technical architecture for the organization's network perimeter security.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

An assessment of how well an organization's application portfolio supports the organization's business objectives is a key component of the overall IT strategic planning process. This drives the demand side of IT planning and should convert into a set of strategic IT intentions. Further assessment can then be made of how well the overall IT organization, encompassing applications, infrastructure, services, management processes, etc., can support the business objectives. Operational efficiency initiatives belong to tactical planning, not strategic planning. The purpose of an IT strategic plan is to set out how IT will be used to achieve or support an organization's business objectives. A listing of approved suppliers of IT contract resources is a tactical rather than a strategic concern. An IT strategic plan would not normally include detail of a specific technical architecture.

NEW QUESTION: 82

The GREATEST advantage of using web services for the exchange of information between two systems is:

- A. secure communications.
- B. improved performance.
- C. efficient interfacing.
- D. enhanced documentation.

Answer: C ([LEAVE A REPLY](#))

Web services facilitate the exchange of information between two systems, regardless of the operating system or programming language used. Communication is not necessarily securer or faster, and there is no documentation benefit in using web services.

NEW QUESTION: 83

An organization's disposal policy emphasizes obtaining maximum value for surplus IT media. The IS

auditor should obtain assurance that:

- A. the media is returned to the vendor for credit
- B. any existing data is removed before disposal
- C. identification labels are removed
- D. the media is recycled to other groups within the organization

Answer: D ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

NEW QUESTION: 84

Which of the following is MOST useful when planning to audit an organization's compliance with cybersecurity regulations in foreign countries?

- A. Prioritize the audit to focus on the country presenting the greatest amount of operational risk.
- B. Follow the cybersecurity regulations of the country with the most stringent requirements.
- C. Develop a template that standardizes the reporting of findings from each country's audit team
- D. Map the different regulatory requirements to the organization's IT governance framework

Answer: D ([LEAVE A REPLY](#))

The most useful thing to do when planning to audit an organization's compliance with cybersecurity regulations in foreign countries is to map the different regulatory requirements to the organization's IT governance framework. This is because an IT governance framework is a roadmap that defines the methods used by an organization to implement, manage and report on IT governance within said organization¹. IT governance helps align business and IT strategies using a solid and formal framework². By mapping the different regulatory requirements to the IT governance framework, the auditor can:

- * Identify the commonalities and differences among the various cybersecurity regulations that apply to the organization's operations in different countries.
- * Assess the level of compliance and maturity of the organization's IT governance practices against each regulatory requirement.
- * Evaluate the risks and gaps associated with non-compliance or partial compliance with any of the regulatory requirements.
- * Recommend appropriate actions or improvements to enhance the organization's IT governance and cybersecurity posture.

Option D is correct because mapping the different regulatory requirements to the organization's IT governance framework is a systematic and effective way to plan and conduct an audit of compliance with cybersecurity regulations in foreign countries.

NEW QUESTION: 85

Which of the following technique is NOT used by a preacher against a Private Branch Exchange (PBX)?

- A. Eavesdropping
- B. Illegal call forwarding
- C. Forwarding a user's to an unused or disabled number

D. SYN Flood

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

The word NOT the keyword used in the question. You need to find out the technique which preacher do not use to exploit PBX.

SYN Flood -Sends a flood of TCP/SYN packets with forged sender address, causing half-open connections and saturates available connection capacity on the target machine.

For CISA Exam you should know below mentioned techniques used by preacher for illegal purpose of PBX.

Eavesdropping on conversation, without the other parties being aware of it Eavesdropping on conference call

Illegal forwarding calls from specific equipment to remote numbers

Forwarding a user's to an unused or disabled number, thereby making it unreachable by external calls.

The following were incorrect answers:

The other options presented correctly describes the techniques used preacher for illegal purpose of PBX.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 357

NEW QUESTION: 86

Which of the following BEST enables an IS auditor to understand the shared control requirements between multiple cloud service providers and the customer organization?

- A.** An industry-accepted cloud security framework for which all parties have obtained certification
- B.** Roles and responsibilities of the IT professionals working under a shared responsibility model
- C.** A risk and controls matrix that documents a clear set of actions for each party
- D.** Logs produced by a cloud access security broker (CASB) monitoring the multi-cloud solution

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 87

A small business unit is implementing a control self-assessment (CSA) program and leveraging the internal audit function to test its internal controls annually. Which of the following is the MOST significant benefit of this approach?

- A.** Compliance costs are reduced.
- B.** Risks are detected earlier.
- C.** Business owners can focus more on their core roles.
- D.** Line management is more motivated to avoid control exceptions.

Answer: B ([LEAVE A REPLY](#))

The most significant benefit of implementing a control self-assessment (CSA) program and leveraging the internal audit function to test its internal controls annually is that risks are detected earlier. A CSA program is a process that enables business owners and managers to assess and

improve their own internal controls on a regular basis, without relying on external auditors or consultants. A CSA program can help identify and mitigate risks, enhance performance, increase accountability, and foster a culture of control within the organization. By leveraging the internal audit function to test its internal controls annually, a small business unit can also obtain independent assurance and validation of its CSA results, as well as recommendations for improvement. This approach can help reduce compliance costs, as external audits may be less frequent or extensive. However, this is not the most significant benefit, as compliance costs are only one aspect of the total cost of risk. Business owners can also focus more on their core roles, as they can delegate some of their control responsibilities to their staff or teams through CSA. However, this is not the most significant benefit, as business owners still need to oversee and monitor their CSA activities and results, and ensure that they align with their strategic objectives and priorities. Line management may also be more motivated to avoid control exceptions, as they are directly involved in assessing and improving their own controls through CSA. However, this is not the most significant benefit, as motivation alone may not be sufficient to ensure effective control design and operation. References: Info Technology & Systems Resources | COBIT, Risk, Governance
... - ISACA, IT Governance and Process Maturity

NEW QUESTION: 88

Which of the following is a PRIMARY function of an intrusion detection system (IDS)?

- A. Blocking malicious network traffic
- B. Predicting an attack before it occurs
- C. Alerting when a scheduled backup job fails
- D. Warning when executable programs are modified

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 89

Which of the following is the BEST indication that an information security program is effective?

- A. The security team has performed a risk assessment to understand the organization's risk appetite.
- B. The security team is knowledgeable and uses the best available tools.
- C. The security awareness program was developed following industry best practices.
- D. The number of reported and confirmed security incidents has increased after awareness training.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 90

To help determine whether a controls-reliant approach to auditing financial systems in a company should be used, which sequence of IS audit work is MOST appropriate?

- A. Review of major financial applications followed by a review of IT governance processes
- B. Review of application controls followed by a test of key business process controls

- C. Detailed examination of financial transactions followed by review of the general ledger
- D. Review of the general IS controls followed by a review of the application controls

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 91

When is it MOST important for an IS auditor to apply the concept of materiality in an audit?

- A. When planning an audit engagement
- B. When gathering information for the fieldwork
- C. When evaluating representations from the auditee
- D. When a violation of a regulatory requirement has been identified

Answer: D ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 92

An IS auditor is determining the scope for an upcoming audit. Which of the following BEST enables the auditor to ensure appropriate controls are considered?

- A. Using an IT-related framework
- B. Reviewing previous audit reports
- C. Reading recent industry journal articles
- D. Conducting interviews with IT staff

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 93

Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

- A. Test data run
- B. Code review
- C. Automated code comparison
- D. Review of code migration procedures

Answer: ([SHOW ANSWER](#)**)**

An automated code comparison is the process of comparing two versions of the same program to determine whether the two correspond. It is an efficient technique because it is an automated procedure. Test data runs permit the auditor to verify the processing of preselected transactions,

but provide no evidence about unexercised portions of a program. Code review is the process of reading program source code listings to determine whether the code contains potential errors or inefficient statements. A code review can be used as a means of code comparison but it is inefficient. The review of code migration procedures would not detect program changes.

NEW QUESTION: 94

Which of the following is the MOST important prerequisite for the protection of physical information assets in a data center?

- A.** Segregation of duties between staff ordering and staff receiving information assets
- B.** Complete and accurate list of information assets that have been deployed
- C.** Availability and testing of onsite backup generators
- D.** Knowledge of the IT staff regarding data protection requirements

Answer: ([SHOW ANSWER](#))

The most important prerequisite for the protection of physical information assets in a data center is a complete and accurate list of information assets that have been deployed. Information assets are any data, devices, systems, or software that have value for the organization and need to be protected from unauthorized access, use, disclosure, modification, or destruction⁴. A data center is a facility that houses various information assets such as servers, storage devices, network equipment, etc., that support the organization's IT operations and services⁵. A complete and accurate list of information assets that have been deployed in a data center can help to identify and classify the assets based on their importance, sensitivity, or criticality for the organization. This can help to determine the appropriate level of protection and security measures that need to be applied to each asset. A complete and accurate list of information assets can also help to track and monitor the location, status, ownership, usage, configuration, maintenance, etc., of each asset. This can help to prevent or detect any unauthorized or inappropriate changes or movements of assets that may compromise their security or integrity. Segregation of duties between staff ordering and staff receiving information assets, availability and testing of onsite backup generators, and knowledge of the IT staff regarding data protection requirements are also important prerequisites for the protection of physical information assets in a data center, but not as important as a complete and accurate list of information assets that have been deployed. These factors are more related to the implementation and maintenance of security controls and procedures that depend on having a complete and accurate list of information assets as a starting point. References:

ISACA CISA Review Manual 27th Edition, page 308

NEW QUESTION: 95

Which of the following mechanisms for process improvement involves examination of industry best practice?

- A.** Business process reengineering (BPR)
- B.** Continuous improvement
- C.** Benchmarking

D18912E1457D5D1DDCBD40AB3BF70D5D

D. Knowledge management

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 96

Which of the following will BEST ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure?

- A. Maintaining system console logs in electronic format
- B. Ensuring bisynchronous capabilities on all transmission lines
- C. Using a database management system (DBMS) to dynamically back-out partially processed transactions
- D. Rotating backup copies of transaction files offsite

Answer: C ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 97

Which of the following is MOST helpful for measuring benefits realization for a new system?

- A. Function point analysts
- B. Balanced scorecard review
- C. Business impact analysis (BIA)
- D. Post-implantation review

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 98

Which of the following would BEST provide assurance of the integrity of new staff?

- A. background screening
- B. References
- C. Bonding
- D. Qualifications listed on a resume

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

A background screening is the primary method for assuring the integrity of a prospective staff member.

References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligence compliance, not at integrity, and qualifications listed on a resume may not be accurate.

NEW QUESTION: 99

In which of the following RFID risks competitor potentially could gain unauthorized access to RFID- generated information and use it to harm the interests of the organization implementing the RFID system?

- A. Business Process Risk
- B. Business Intelligence Risk
- C. Privacy Risk
- D. Externality Risk

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system. RFID is a powerful technology, in part, because it supports wireless remote access to information about assets and people that either previously did not exist or was difficult to create or dynamically maintain.

While this wireless remote access is a significant benefit, it also creates a risk that unauthorized parties could also have similar access to that information if proper controls are not in place. This risk is distinct from the business process risk because it can be realized even when business processes are functioning as intended.

A competitor or adversary can gain information from the RFID system in a number of ways, including eavesdropping on RF links between readers and tags, performing independent queries on tags to obtain relevant data, and obtaining unauthorized access to a back-end database storing information about tagged items. Supply chain applications may be particularly vulnerable to this risk because a variety of external entities may have read access to the tags or related databases.

The risk of unauthorized access is realized when the entity engaging in the unauthorized behavior does something harmful with that information. In some cases, the information may trigger an immediate response. For example, someone might use a reader to determine whether a shipping container holds expensive electronic equipment, and then break into the container when it gets a positive reading. This scenario is an example of targeting. In other cases, data might also be aggregated over time to provide intelligence regarding an organization's operations, business strategy, or proprietary methods.

For instance, an organization could monitor the number of tags entering a facility to provide a reasonable indication of its business growth or operating practices. In this case, if someone determined that a warehouse recently received a number of very large orders, then that might trigger an action in financial markets or prompt a competitor to change its prices or production schedule.

For your exam you should know the information below:

Radio-frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects.

The tags contain electronically stored information. Some tags are powered by and read at short ranges (a few meters) via magnetic fields (electromagnetic induction). Others use a local power source such as a battery, or else have no battery but collect energy from the interrogating EM field, and then act as a passive transponder to emit microwaves or UHF radio waves (i.e., electromagnetic radiation at high frequencies). Battery powered tags may operate at hundreds of meters. Unlike a barcode, the tag does not necessarily need to be within line of sight of the reader, and may be embedded in the tracked object.

RFID tags are used in many industries. An RFID tag attached to an automobile during production can be used to track its progress through the assembly line. Pharmaceuticals can be tracked through warehouses. Livestock and pets may have tags injected, allowing positive identification of the animal.

RFID RISKS

RFID technology enables an organization to significantly change its business processes to: Increase its efficiency, which results in lower costs, Increase its effectiveness, which improves mission performance and makes the implementing organization more resilient and better able to assign accountability, and Respond to customer requirements to use RFID technology to support supply chains and other applications.

The RFID technology itself is complex, combining a number of different computing and communications technologies to achieve the desired objectives. Unfortunately, both change and complexity generate risk.

For RFID implementations to be successful, organizations need to effectively manage that risk, which requires an understanding of its sources and its potential characteristics. This section reviews the major high-level business risks associated with RFID systems so that organizations planning or operating these systems can better identify, characterize, and manage the risk in their environments.

The risks are as follows:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood.

The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

Externality Risk -RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

An important characteristic of RFID that impacts all of these risks is that RF communication is invisible to operators and users.

The following answers are incorrect:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Externality Risk -RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood.

The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 248

NIST SP 800-98 RFID 2007 -

http://www.csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf

NEW QUESTION: 100

Attribute sampling is BEST suited to estimate:

- A. compliance with approved procedures.
- B. the true monetary value of a population.
- C. the total error amount in the population.
- D. whether a recorded balance is within limits of materiality.

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation/Reference:

NEW QUESTION: 101

internal IS auditor recommends that incoming accounts payable payment files be encrypted. Which type of control is the auditor recommending?

- A. Detective
- B. Directive
- C. Corrective
- D. Preventive

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 102

An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

- A. conclude that the controls are inadequate.
- B. expand the scope to include substantive testing.
- C. place greater reliance on previous audits.
- D. suspend the audit.

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

If the answers provided to an IS auditor's questions are not confirmed by documented procedures or job descriptions, the IS auditor should expand the scope of testing the controls and include additional substantive tests. There is no evidence that whatever controls might exist are either inadequate or adequate. Placing greater reliance on previous audits or suspending the audit are inappropriate actions as they provide no current knowledge of the adequacy of the existing controls.

NEW QUESTION: 103

Which of the following control is intended to discourage a potential attacker?

- A. Deterrent
- B. Preventive
- C. Corrective
- D. Recovery

Answer: A ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

Explanation:

Deterrent Control are intended to discourage a potential attacker

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to

threats and attacks by the simple fact that the existence of the control is enough to keep some potential

attackers from attempting to circumvent the control. This is often because the effort required to circumvent

the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative

implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing

the identification and authentication of a user, service, or application, and all that it implies, the potential for

incidents associated with the system is significantly reduced because an attacker will fear association with

the incident. If there are no controls for a given access path, the number of incidents and the potential

impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process.

This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally

perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities

are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are

based on the anonymity of the threat agent, and any potential for identification and association with their

actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers.

Deterrents also take the form of potential punishment if users do something unauthorized. For example, if

the organization policy specifies that an employee installing an unauthorized wireless access point will be

fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a

user from performing some activity or function. Preventative controls differ from deterrent controls in that

the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is

easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides

with the user (or the attacker). Preventative controls place the power of action with the system, obeying the

control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the

requirement of a policy. Compensating controls can be technical, procedural, or managerial.

Although an

existing system may not support the required controls, there may exist other technology or processes that

can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when

performed over the Internet. Adjusting an application to natively support encryption for authentication

purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and

layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain

tasks to compensate for technical limitations in the system and ensure the security of transactions. In

addition, management processes, such as authorization, supervision, and administration, can be used to

compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident

timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful

incidents through the application of least privilege. However, the detective nature of access controls can

provide significant visibility into the access environment and help organizations manage their access

strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the

ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated

user has. However, there are few options to control what a user can perform once privileges are provided.

For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise

negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer

visibility into the transaction. The control environment can be established to log activity regarding the

identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to

validate when provided credentials were exercised. The logging system as a detective device provides

evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions.

Corrective controls are actions that seek to alter the security posture of an environment to correct any

deficiencies and return the environment to a secure state. A security incident signals the failure of one or

more directive, deterrent, preventative, or compensating controls. The detective controls may have

triggered an alarm or notification, but now the corrective controls must work to stop the incident in its

tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the

particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer

temporary compensating controls, need to be accurately reinstated and returned to normal operations.

There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and

full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may

adversely affect controls placed on system files or even have default administrative accounts unknowingly

implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy

requirements regarding separation of duties. An attack on systems may have resulted in the implantation of

a Trojan horse program, potentially exposing private user information, such as credit card information and

financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and

controls returned to normal operations.

The following answers are incorrect:

Preventive - Preventive controls are intended to avoid an incident from occurring

Corrective - Corrective control fixes components or systems after an incident has occurred

Recovery - Recovery controls are intended to bring the environment back to regular operations

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

NEW QUESTION: 104

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 (LEAVE A REPLY)

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 proposed development contract should 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.

NEW QUESTION: 105

During the implementation of an enterprise resource planning (ERP) system, an IS auditor is reviewing the results of user acceptance testing (UAT). The auditor's PRIMARY focus should be to determine if:

- A. application interfaces have been satisfactorily tested.
- B. all errors found in the testing process have been corrected.
- C. the business process owner has signed off on the results.
- D. system integration testing was performed.

Answer: C (LEAVE A REPLY)

During the review of user acceptance testing (UAT) results, the IS auditor's primary focus should be to determine if the business process owner has signed off on the results. This ensures that the

ERP system meets the business requirements and that the business process owner is satisfied with the performance of the system.

NEW QUESTION: 106

An IS auditor discovers an option in a database that allows the administrator to directly modify any table. This option is necessary to overcome bugs in the software, but is rarely used. Changes to tables are automatically logged. The IS auditor's FIRST action should be to:

- A. recommend that the option to directly modify the database be removed immediately.
- B. recommend that the system require two persons to be involved in modifying the database.
- C. determine whether the log of changes to the tables is backed up.
- D. determine whether the audit trail is secured and reviewed.

Answer: D ([LEAVE A REPLY](#))

Explanation

The IS auditor's first action after discovering an option in a database that allows the administrator to directly modify any table should be to determine whether the audit trail is secured and reviewed. This is because direct modification of database tables can pose a significant risk to data integrity, security, and accountability. An audit trail is a record of all changes made to database tables, including who made them, when they were made, and what was changed. An audit trail can help to detect unauthorized or erroneous changes, provide evidence for investigations or audits, and support data recovery or restoration. The IS auditor should assess whether the audit trail is protected from tampering or deletion, and whether it is regularly reviewed for anomalies or exceptions.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 107

During an implementation review of a multiuser distributed application, an IS auditor finds minor weaknesses in three areas-the initial setting of parameters is improperly installed, weak passwords are being used and some vital reports are not beingchecked properly. While preparing the audit report, the IS auditor should:

- A. record the observations separately with the impact of each of them marked against each respective finding.
- B. advise the manager of probable risks without recording the observations, as the control weaknesses are minor ones.

- C. record the observations and the risk arising from the collective weaknesses.
- D. apprise the departmental heads concerned with each observation and properly document it in the report.

Answer: ([SHOW ANSWER](#))

Individually the weaknesses are minor; however, together they have the potential to substantially weaken the overall control structure. Choices A and D reflect a failure on the part of an IS auditor to recognize the combined affect of the control weakness. Advising the local manager without reporting the facts and observations would conceal the findings from other stakeholders.

NEW QUESTION: 108

An IS auditor observes that routine backups of operational databases are taking longer than before. Which of the following would MOST effectively help to reduce backup and recovery times for operational databases?

- A. Utilizing database technologies to achieve efficiencies
- B. Using solid storage device (SSD) media
- C. Requiring a combination of weekly full backups and daily differential backups
- D. Archiving historical data in accordance with the data retention policy

Answer: C ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 109

Which of the following is MOST important to ensure during computer forensics investigations?

- A. Effective backup schemes are in place to preserve digital evidence.
- B. Personnel undertaking the investigation process are certified to collect digital evidence.
- C. The contents of digital evidence are preserved in their original form.
- D. The analysis is performed against the original digital evidence.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 110

To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to:

- A. rely on senior management to enforce security
- B. promote the relevance and contribution of security
- C. reiterate the necessity of security
- D. focus on compliance

Answer: B ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 111

Which of the following should be done FIRST to minimize the risk of unstructured data?

- A. Identify repositories of unstructured data.

- B. Purchase tools to analyze unstructured data.
- C. Implement strong encryption for unstructured data.
- D. Implement user access controls to unstructured data.

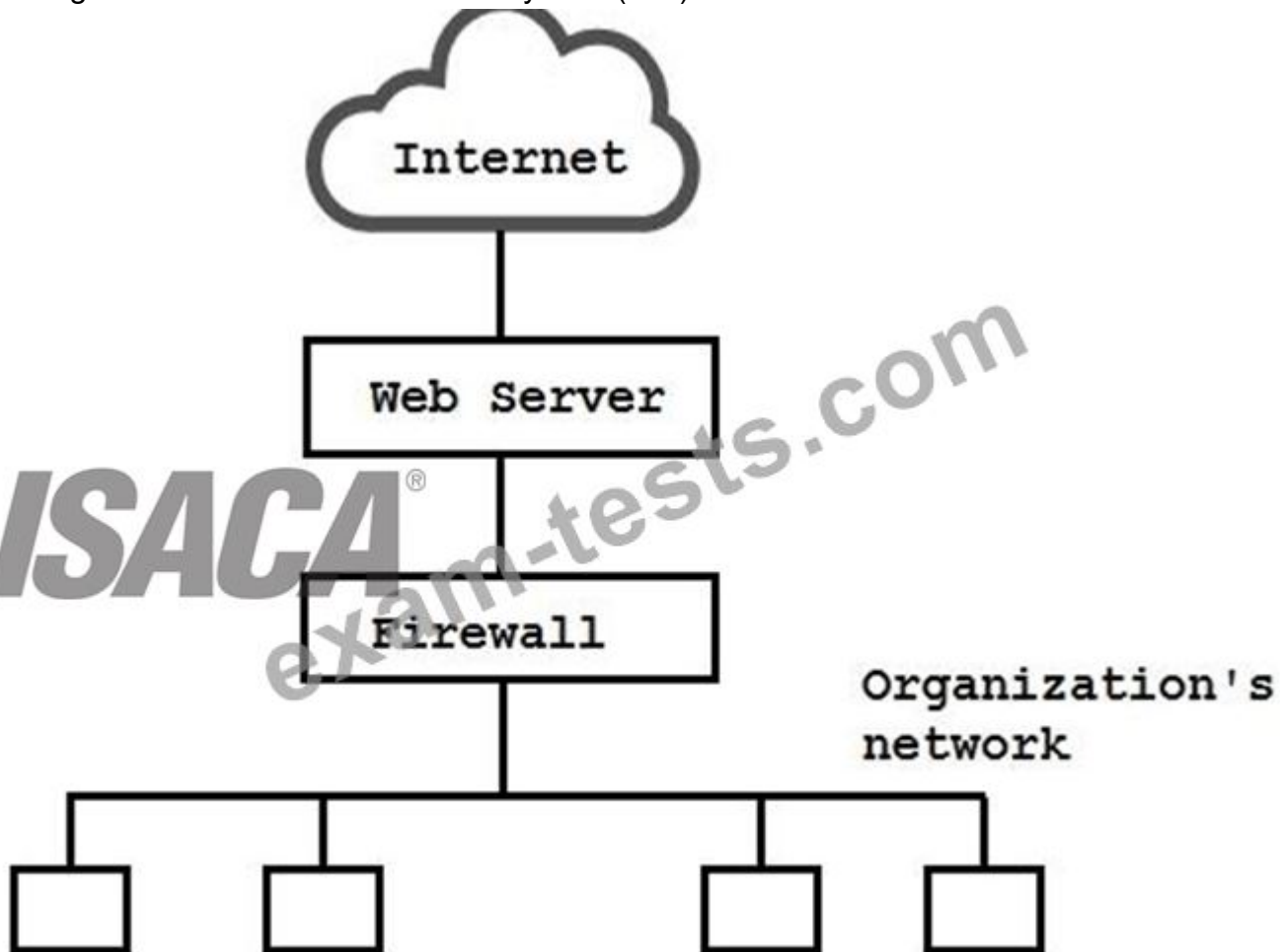
Answer: A ([LEAVE A REPLY](#))

Explanation

Unstructured data is data that does not have a predefined model or organization, making it difficult to store, process, and analyze using traditional relational databases or spreadsheets. Unstructured data can pose a risk to an organization if it contains sensitive, confidential, or regulated information that is not properly secured, managed, or governed. To minimize the risk of unstructured data, the first step is to identify the repositories of unstructured data, such as file servers, cloud storage, email systems, social media platforms, etc. This will help to understand the scope, volume, and nature of unstructured data in the organization, and to prioritize the areas that need further analysis and action. References: Unstructured data - Wikipedia

NEW QUESTION: 112

To detect attack attempts that the firewall is unable to recognize, an IS auditor should recommend placing a network intrusion detection system (IDS) between the:



- A. Firewall and the organization's network.
- B. Internet and the firewall.
- C. Internet and the web server.

D. Web server and the firewall.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Attack attempts that could not be recognized by the firewall will be detected if a network-based intrusion detection system is placed between the firewall and the organization's network. A network-based intrusion detection system placed between the internet and the firewall will detect attack attempts, whether they do or do not enter the firewall.

NEW QUESTION: 113

Which of the following would BEST guide an IS auditor when determining an appropriate time to schedule the follow-up of agreed corrective actions for reported audit issues?

- A. Progress updates indicate that the implementation of agreed actions is on track.
- B. Sufficient time has elapsed since implementation to provide evidence of control operation.
- C. Business management has completed the implementation of agreed actions on schedule.
- D. Regulators have announced a timeline for an inspection visit.

Answer: B ([LEAVE A REPLY](#))

This is because the follow-up of agreed corrective actions for reported audit issues should be done after the auditee has had enough time to implement the corrective actions and demonstrate their effectiveness and sustainability. The follow-up audit should not be too soon or too late, but based on a reasonable and realistic timeframe that allows for adequate testing and verification of the control operation¹².

A). Progress updates indicate that the implementation of agreed actions is on track. is not the best answer, because progress updates are not sufficient to guide the follow-up audit timing. Progress updates are useful for monitoring and communicating the status and challenges of the corrective actions, but they do not provide conclusive evidence of the control operation. The follow-up audit should be based on actual results and outcomes, not on expectations or projections¹².

C). Business management has completed the implementation of agreed actions on schedule. is not the best answer, because the completion of the implementation of agreed actions is not enough to guide the follow-up audit timing. The completion of the implementation only indicates that the auditee has taken the necessary steps to address the audit issues, but it does not guarantee that the corrective actions are effective and sustainable. The follow-up audit should be based on the evaluation and validation of the control operation, not on the completion of the control implementation¹².

D). Regulators have announced a timeline for an inspection visit. is not the best answer, because the regulators' inspection visit is not relevant to guide the follow-up audit timing. The regulators' inspection visit is an external factor that may or may not coincide with the internal follow-up audit schedule. The follow-up audit should be based on the internal audit plan and objectives, not on the external audit requirements or expectations¹².

NEW QUESTION: 114

Which of the following would BEST detect that a distributed denial of service (DDoS) attack is occurring?

- A. Customer service complaints
- B. Automated monitoring of logs
- C. Server crashes
- D. Penetration testing

Answer: ([SHOW ANSWER](#))

Explanation

The best way to detect that a distributed denial of service (DDoS) attack is occurring is to use automated monitoring of logs. A DDoS attack disrupts the operations of a server, service, or network by flooding it with unwanted Internet traffic². Automated monitoring of logs can help pinpoint potential DDoS attacks by analyzing network traffic patterns, monitoring traffic spikes or other unusual activity, and alerting administrators or security teams of any anomalies or malicious requests, protocols, or IP blocks³. Automated monitoring of logs can also help identify the source, type, and impact of the DDoS attack, and provide evidence for further investigation or mitigation. The other options are not as effective as automated monitoring of logs for detecting DDoS attacks. Customer service complaints are an indirect and delayed indicator of a DDoS attack, as they rely on users reporting problems with accessing a website or service. Customer service complaints may also be caused by other factors unrelated to DDoS attacks, such as server errors or network issues. Server crashes are an extreme and undesirable indicator of a DDoS attack, as they indicate that the server has already been overwhelmed by the attack and has stopped functioning. Server crashes may also result in data loss or corruption, service disruption, or reputational damage. Penetration testing is a proactive and preventive measure for assessing the security posture of a system or network, but it does not detect ongoing DDoS attacks. Penetration testing may involve simulating DDoS attacks to test the resilience or vulnerability of a system or network, but it does not monitor real-time traffic or identify actual attackers.

References:

ISACA CISA Review Manual 27th Edition (2019), page 254

How to prevent DDoS attacks | Methods and tools | Cloudflare²

Understanding Denial-of-Service Attacks | CISA³

NEW QUESTION: 115

Which of the following is the MOST effective way to assess whether an outsourcer's controls are following the service level agreement (SLA)?

- A. Perform an onsite review of the outsourcer.
- B. Review the outsourcer's monthly service reports.
- C. Perform a review of penalty clauses for non-performance.
- D. Review an internal audit report from the outsourcer's auditor.

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

NEW QUESTION: 116

During a follow-up audit, an IS auditor concludes that a previously identified issue has not been adequately remediated. The auditee insists the risk has been addressed. The auditor should:

- A. recommend an independent assessment by a third party
- B. report the disagreement according to established procedures
- C. follow-up on the finding next year
- D. accept the auditee's position and close the finding

Answer: A ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

NEW QUESTION: 117

Which of the following is MOST effective against system intrusions?

- A. Continuous monitoring
- B. Layered protection
- C. Penetration testing
- D. Two-factor authentication

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 118

Which of the following encryption methods uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message?

- A. Blowfish
- B. Tripwire
- C. certificate
- D. DES
- E. one-time pad
- F. None of the choices.

Answer: E ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

It's possible to protect messages in transit by means of cryptography. One method of encryption - the one-time pad - has been proven to be unbreakable when correctly used. This method uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

NEW QUESTION: 119

Which of the following BEST enables the timely identification of risk exposure?

- A. External audit review

- B. Internal audit review
- C. Control self-assessment (CSA)
- D. Stress testing

Answer: C ([LEAVE A REPLY](#))

Explanation

Control self-assessment (CSA) is a technique that enables business managers and staff to assess and improve the effectiveness of their own controls and risk management processes. CSA can best enable the timely identification of risk exposure, as it allows for continuous monitoring and reporting of risks by those who are closest to the business processes and activities. External audit review, internal audit review, and stress testing are also useful methods for identifying risk exposure, but they are not as timely as CSA, as they are performed periodically or on demand by external or internal parties who may not have as much insight into the business operations and environment. References: ISACA CISA Review Manual 27th Edition, page 95.

NEW QUESTION: 120

An audit group is conducting a risk assessment as part of a risk-based audit strategy. To help ensure the risk assessment results are relevant to the organization, it is MOST important to:

- A. understand the organization's objectives and risk appetite.
- B. include operational departments and processes.
- C. determine both the inherent risk and detection risk.
- D. understand the organization's controls.

Answer: ([SHOW ANSWER](#)**)**

Section: The process of Auditing Information System

NEW QUESTION: 121

An IS auditor is reviewing the remote access methods of a company used to access system remotely.

Which of the following is LEAST preferred remote access method from a security and control point of view?

- A. RADIUS
- B. TACACS
- C. DIAL-UP
- D. DIAMETER

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Dial-up connectivity not based on centralized control and least preferred from security and control standpoint.

Remote access user can connect remotely to their organization's networks with the same level of functionality as if they would access from within their office.

In connecting to an organization's network, a common method is to use dial-up lines. Access is granted through the organization's network access server (NAS) working in concert with an organization network firewall and router. The NAS handle user authentication, access control and accounting while maintaining connectivity. The most common protocol for doing this is the Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Controller System (TACACS).

Remote access Controls include:

Policy and standard

Proper authorization

Identification and authentication mechanism

Encryption tool and technique such as use of VPN

System and network management

Reference:

CISA Review Manual 2014 Page number 334

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 122

As part of an IS audit, the auditor notes the practices listed below. Which of the following would be a segregation of duties concern?

- A. Operators are degaussing magnetic tapes during night shifts.
- B. System programmers have logged access to operating system parameters.
- C. System programmers are performing the duties of operators.
- D. Operators are acting as tape librarians on alternate shifts.

Answer: (SHOW ANSWER)

Section: The process of Auditing Information System

NEW QUESTION: 123

Which of the following attack involves sending forged ICMP Echo Request packets to the broadcast

address on multiple gateways in order to illicit responses from the computers behind the gateway where

they all respond back with ICMP Echo Reply packets to the source IP address of the ICMP Echo Request

packets?

- A. Reflected attack
- B. Brute force attack
- C. Buffer overflow
- D. Pulsing Zombie

Answer: A (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation/Reference:

Reflected attack involves sending forged requests to a large number of computers that will reply to the requests. The source IP address is spoofed to that of the targeted victim, causing replies to flood. A distributed denial of service attack may involve sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet Protocol address spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target.

(This reflected attack form is sometimes called a "DRDOS".

ICMP Echo Request attacks (Smurf Attack) can be considered one form of reflected attack, as the flooding

host(s) send Echo Requests to the broadcast addresses of mis-configured networks, thereby enticing hosts

to send Echo Reply packets to the victim. Some early DDoS programs implemented a distributed form of this attack.

In the smurf attack, the attacker sends an ICMP ECHO REQUEST packet with a spoofed source address to

a victim's network broadcast address. This means that each system on the victim's subnet receives an

ICMP ECHO REQUEST packet. Each system then replies to that request with an ICMP ECHO REPLY

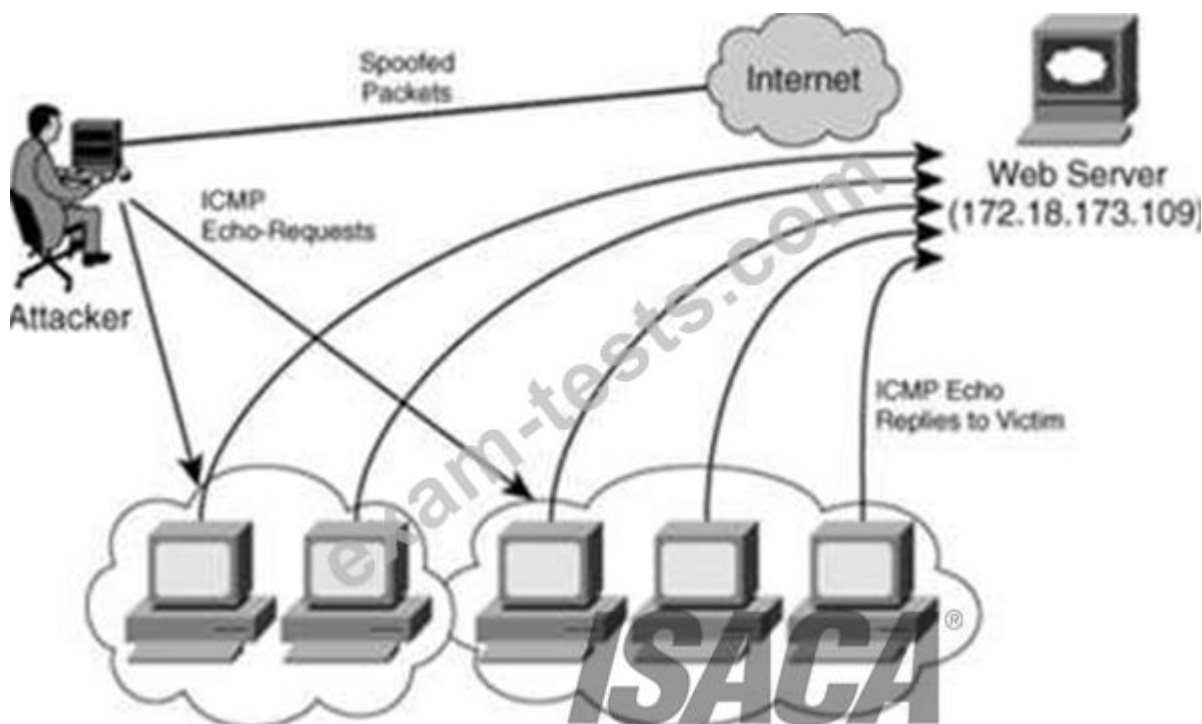
packet to the spoof address provided in the packets-which is the victim's address. All of these response

packets go to the victim system and overwhelm it because it is being bombarded with packets it does not

necessarily know how to process. The victim system may freeze, crash, or reboot. The Smurf attack is

illustrated in Figure below:

smurf-attack



The following answers are incorrect:

Brute force attack - Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES)

keys, through exhaustive effort (using brute force) rather than employing intellectual strategies.

Just as a

criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking

application proceeds through all possible combinations of legal characters in sequence. Brute force is

considered to be an infallible, although time-consuming, approach.

Buffer overflow - A buffer overflow occurs when a program or process tries to store more data in a buffer

(temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite

amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers,

corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Pulsing Zombie - A Dos attack in which a network is subjected to hostile pinging by different attacker

computer over an extended time period.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 322

NEW QUESTION: 124

The PRIMARY goal of a web site certificate is:

- A. authentication of the web site that will be surfed.
- B. authentication of the user who surfs through that site.
- C. preventing surfing of the web site by hackers.
- D. the same purpose as that of a digital certificate.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Authenticating the site to be surfed is the primary goal of a web certificate. Authentication of a user is achieved through passwords and not by a web site certificate. The site certificate does not prevent hacking nor does it authenticate a person.

NEW QUESTION: 125

Which of the following network components is PRIMARILY set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

- A. Firewalls
- B. Routers
- C. Layer 2 switches
- D. VLANs

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Firewall systems are the primary tool that enable an organization to prevent unauthorized access between networks. An organization may choose to deploy one or more systems that function as firewalls. Routers can filter packets based on parameters, such as source address, but are not primarily a security tool.

Based on Media Access Control (MAC) addresses, layer 2 switches separate traffic in a port as different segments and without determining if it is authorized or unauthorized traffic. A virtual LAN (VLAN) is a functionality of some switches that allows them to switch the traffic between different ports as if they are in the same LAN. Nevertheless, they do not deal with authorized vs. unauthorized traffic.

NEW QUESTION: 126

Which of the following presents the GREATEST concern when implementing data flow across borders?

- A. Software piracy laws
- B. National privacy laws
- C. Political unrest
- D. Equipment incompatibilities

Answer: B ([LEAVE A REPLY](#))

Section: Governance and Management of IT

NEW QUESTION: 127

Which of the following would be MOST helpful in ensuring security procedures are followed by employees in a multinational organization?

- A. Security architecture review
- B. Regular clean desk reviews
- C. Comprehensive end-user training
- D. Regular policy updates by management

Answer: C ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 128

Which of the following is the MOST significant impact to an organization that does not use an IT governance framework?

- A. adequate measurement of key risk indicators (KRIS)
- B. Inadequate alignment of IT plans and business objectives
- C. Inadequate business impact analysis (BIA) results and predictions
- D. Inadequate measurement of key performance indicators (KPIs)

Answer: B ([LEAVE A REPLY](#))

Explanation

The most significant impact to an organization that does not use an IT governance framework is inadequate alignment of IT plans and business objectives. IT governance is a framework for the governance and management of enterprise information and technology (I&T) that supports enterprise goal achievement¹. IT governance helps to ensure that IT investments and activities are aligned with the business strategy, vision, and values of the organization. IT governance also helps to optimize the value of IT, manage IT-related risks, and measure and monitor IT performance¹.

Without an IT governance framework, an organization may face challenges such as:

- Lack of clarity and direction for IT decision making
- Inconsistent or conflicting IT priorities and demands
- Inefficient or ineffective use of IT resources and capabilities
- Poor quality or delivery of IT services and products
- Increased exposure to IT-related threats and vulnerabilities
- Reduced customer satisfaction and trust in IT
- Missed opportunities for innovation and competitive advantage

Therefore, an organization that does not use an IT governance framework may fail to achieve its business objectives and may lose its competitive edge in the market.

References:

COBIT 2019 Framework Introduction and Methodology, Section 1.1: What Is Governance of Enterprise I&T?

IT Governance: Definitions, Frameworks and Planning, Section 1: What Is IT Governance?

NEW QUESTION: 129

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 ([LEAVE A REPLY](#))

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.

NEW QUESTION: 130

An IS audit manager is preparing the starting plan for an audit engagement of a cloud service provider. What should be the manager's PRIMARY concern when made aware that a new auditor in the department previously worked for this provider?

- A. Integrity
- B. Competency
- C. Independence
- D. Professional conduct

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 131

Which of the following is the BEST way to strengthen the security of smart devices to prevent data leakage?

- A. Enforce strong security settings on smart devices.
- B. Include usage restrictions in bring your own device (BYOD) security procedures.
- C. Require employees to formally acknowledge security procedures.
- D. Review access logs to the organization's sensitive data in a timely manner.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 132

Which of the following should an IS auditor expect to find in an organization's information security policies?

- A. Security configuration settings

- B. Asset provisioning lifecycle
- C. Authentication requirements
- D. Secure coding procedures

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 133

An IS auditor has completed a review of an outsourcing agreement and has identified IT governance issues. Which of the following is the MOST effective and efficient way of communicating the issues at a meeting with senior management?

- A. Present a completed report and discuss the details.
- B. Provide a detailed report in advance and open the floor to questions.
- C. Present an overview highlighting the key findings.
- D. Provide a plan of action and milestones.

Answer: ([SHOW ANSWER](#)**)**

Section: Governance and Management of IT

NEW QUESTION: 134

An IS auditor conducting an access control review in a client-server environment discovers that all printing

options are accessible by all users. In this situation, the IS auditor is MOST likely to conclude that:

- A. exposure is greater, since information is available to unauthorized users.
- B. operating efficiency is enhanced, since anyone can print any report at any time.
- C. operating procedures are more effective, since information is easily available.
- D. user friendliness and flexibility is facilitated, since there is a smooth flow of information among users.

Answer: ([SHOW ANSWER](#)**)**

Section: Protection of Information Assets

Explanation:

Information in all its forms needs to be protected from unauthorized access. Unrestricted access to the

report option results in an exposure. Efficiency and effectiveness are not relevant factors in this situation.

Greater control over reports will not be accomplished since reports need not be in a printed form only.

Information could be transmitted outside as electronic files, because print options allow for printing in an electronic form as well.

NEW QUESTION: 135

When auditing the closing stages of a system development project, which of the following should be the MOST important consideration?

- A. Control requirements
- B. Functional requirements documentation
- C. User acceptance test (UAT) results
- D. Rollback procedures

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 136

Which of the following is the PRIMARY basis on which audit objectives are established?

- A. Audit risk
- B. Consideration of risks
- C. Assessment of prior audits
- D. Business strategy

Answer: B ([LEAVE A REPLY](#))

Explanation

The primary basis on which audit objectives are established is the consideration of risks¹². This involves identifying and assessing the risks that could prevent the organization from achieving its objectives¹². The audit objectives are then designed to address these risks and provide assurance that the organization's controls are effective in managing them¹². While audit risk, assessment of prior audits, and business strategy are important factors in the audit process, they are secondary to the fundamental requirement of considering risks¹².

References:

Objectives of Auditing - Primary and Secondary Objectives of Auditing | Auditing Management Notes Audit Objectives | Primary and Subsidiary Audit Objectives - EDUCBA

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 137

IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

- A. desired result or purpose of implementing specific control procedures.
- B. best IT security control practices relevant to a specific entity.
- C. techniques for securing information.
- D. security policy.

Answer: A ([LEAVE A REPLY](#))

An IT control objective is defined as the statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. They provide the actual objectives for implementing controls and may or may not be the best practices. Techniques are the means of achieving an objective, and a security policy is a subset of IT control objectives.

NEW QUESTION: 138

Which of the following attack includes social engineering, link manipulation or web site forgery techniques?

- A.** surf attack
- B.** Traffic analysis
- C.** Phishing
- D.** Interrupt attack

Answer: C (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

Phishing technique include social engineering, link manipulation or web site forgery techniques.

For your exam you should know the information below:

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Spear phishing - Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success.

Link manipulation

Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization.

Misspelled URLs or the use of sub domains are common tricks used by phishes. In the following example URL, `http:// www.yourbank.example.com/`, it appears as though the URL will take you to the example section of the your bank website; actually this URL points to the "your bank" (i.e. phishing) section of the example website. Another common trick is to make the displayed text for a link (the text between the tags) suggest a reliable destination, when the link actually goes to the phishes' site. The following example link, `// en.wikipedia.org/wiki/Genuine`, appears to direct the user to an article entitled "Genuine"; clicking on it will in fact take the user to the article entitled

"Deception". In the lower left hand corner of most browsers users can preview and verify where the link is going to take them. Hovering your cursor over the link for a couple of seconds may do a similar thing, but this can still be set by the phishes through the HTML tooltip tag.

Website forgery

Once a victim visits the phishing website, the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original bar and opening up a new one with the legitimate URL.

An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge.

The following answers are incorrect:

Smurf Attack - Occurs when mis-configured network device allow packet to be sent to all hosts on a particular network via the broadcast address of the network
Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Interrupt attack- Interrupt attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call.

Reference:

CISA review manual 2014 Page number 323

Official ISC2 guide to CISSP CBK 3rd Edition Page number 493

<http://en.wikipedia.org/wiki/Phishing>

NEW QUESTION: 139

An accounting department uses a spreadsheet to calculate sensitive financial transactions. Which of the following is the MOST important control for maintaining the security of data in the spreadsheet?

- A. There is a reconciliation process between the spreadsheet and the finance system.
- B. The spreadsheet is locked down to avoid inadvertent changes.
- C. A separate copy of the spreadsheet is routinely backed up.
- D. Access to the spreadsheet is given only to those who require access.

Answer: A ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 140

Which of the following should an IS auditor verify when auditing the effectiveness of virus protection?

- A. Currency of software patch application
- B. Frequency of external Internet access
- C. Frequency of IDS log reviews
- D. Schedule for migration to production

Answer: (SHOW ANSWER)

NEW QUESTION: 141

Capacity management tools are PRIMARILY used to ensure that:

- A. available resources are used efficiently and effectively
- B. concurrent use by a large number of users is enabled
- C. proposed hardware acquisitions meet capacity requirements
- D. computer systems are used to their maximum capacity most of the time

Answer: A (LEAVE A REPLY)

NEW QUESTION: 142

The security level of a private key system depends on the number of:

- A. encryption key bits.
- B. messages sent.
- C. keys.
- D. channels used.

Answer: A (LEAVE A REPLY)

The security level of a private key system depends on the number of encryption key bits. The larger the number of bits, the more difficult it would be to understand or determine the algorithm. The security of the message will depend on the encryption key bits used. More than keys by themselves, the algorithm and its complexity make the content more secured. Channels, which could be open or secure, are the mode for sending the message.

NEW QUESTION: 143

.When should systems administrators first assess the impact of applications or systems patches?

- A. Within five business days following installation
- B. Prior to installation
- C. No sooner than five business days following installation
- D. Immediately following installation

Answer: B (LEAVE A REPLY)

Systems administrators should always assess the impact of patches before installation.

NEW QUESTION: 144

Input/output controls should be implemented for which applications in an integrated systems environment?

- A. The receiving application
- B. The sending application
- C. Both the sending and receiving applications
- D. Output on the sending application and input on the receiving application

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

Input/output controls should be implemented for both the sending and receiving applications in an integrated systems environment

NEW QUESTION: 145

Identify the correct sequence of Business Process Reengineering (BPR) application steps from the given choices below?

- A. Envision, Initiate, Diagnose, Redesign, Reconstruct and Evaluate
- B. Initiate, Envision, Diagnose, Redesign, Reconstruct and Evaluate
- C. Envision, Diagnose, Initiate, Redesign, Reconstruct and Evaluate
- D. Evaluate, Envision, Initiate, Diagnose, Redesign, Reconstruct

Answer: A ([LEAVE A REPLY](#))

Section: Information System Acquisition, Development and Implementation Explanation

Explanation:

The correct sequence of BRP application step is Envision, Initiate, Diagnose, Redesign, Reconstruct and Evaluate.

For your exam you should know the information below:

Overview of Business Process Reengineering

One of the principles in business that remains constant is the need to improve your processes and procedures. Most trade magazines today contain discussions of the detailed planning necessary for implementing change in an organization. The concept of change must be accepted as a fundamental principle. Terms such as business evolution and continuous improvement ricochet around the room in business meetings. It's a fact that organizations which fail to change are destined to perish.

As a CISA, you must be prepared to investigate whether process changes within the organization are accounted for with proper documentation. All internal control frameworks require that management be held responsible for safeguarding all the assets belonging to their organization. Management is also responsible for increasing revenue.

BPR Application Steps

ISACA cites six basic steps in their general approach to BPR. These six steps are simply an extension of Stewart's Plan-Do-Check-Act model for managing projects:

Envision -Visualize a need (envision). Develop an estimate of the ROI created by the proposed change.

Elaborate on the benefit with a preliminary project plan to gain sponsorship from the organization. The plan should define the areas to be reviewed and clarify the desired result at the end of the project (aka end state objective). The deliverables of the envision phase include the following: Project champion working with the steering committee to gain top management approval Brief description of project scope, goals, and objectives description of the specific deliverables from this project with a preliminary charter to evidence management's approval, the project may proceed into the initiation phase.

Initiate -This phase involves setting BPR goals with the sponsor. Focus on planning the collection of detailed evidence necessary to build the subsequent BPR plan for redesigning the process.

Deliverables in the initiation phase include the following:

Identifying internal and external requirements (project specifications) Business case explaining why this project makes sense (justification) and the estimated return on investment compared to the total cost (net ROI) Formal project plan with budget, schedule, staffing plan, procurement plan, deliverables, and project risk analysis Level of authority the BPR project manager will hold and the composition of any support committee or task force that will be required From the profit and loss (P&L) statement, identify the item line number that money will be debited from to pay for this project and identify the specific P&L line number that the financial return will later appear under (to provide strict monitoring of the ROI performance) Formal project charter signed by the sponsors It's important to realize that some BPR projects will proceed to their planned conclusion and others may be halted because of insufficient evidence. After a plan is formally approved, the BPR project may proceed to the diagnostic phase.

Diagnose Document existing processes. Now it's time to see what is working and identify the source of each requirement. Each process step is reviewed to calculate the value it creates. The goal of the diagnostic phase is to gain a better understanding of existing processes. The data collected in the diagnostic phase forms the basis of all planning decisions:

Detailed documentation of the existing process

Performance measurement of individual steps in the process

Evidence of specific process steps that add customer value

Identification of process steps that don't add value

Definition of attributes that create value and quality

Put in the extra effort to do a good job of collecting and analyzing the evidence. All future assumptions will be based on evidence from the diagnostic phase.

Redesign- Using the evidence from the diagnostic phase, it's time to develop the new process. This will take several planning iterations to ensure that the strategic objectives are met. The formal redesign plans will be reviewed by sponsors and stakeholders. A final plan will be presented to the steering committee for approval. Here's an example of deliverables from the redesign phase.

Comparison of the envisioned objective to actual specifications

Analysis of alternatives (AoA)

Prototyping and testing of the redesigned process

Formal documentation of the final design

The project will need formal approval to proceed into the reconstruction phase. Otherwise, the redesign is halted pending further scrutiny while comparing the proposed design with available evidence. Insufficient evidence warrants halting the project.

Reconstruct With formal approval received, it's time to begin the implementation phase.

The current processes are deconstructed and reassembled according to the plan. Reconstruction may be in the form of a parallel process, modular changes, or complete transition. Each method presents a unique risk and reward opportunity. Deliverables from this phase include the following:

Conversion plan with dependencies in time sequence

Change control management

Execution of conversion plan with progress monitoring

Training of users and support personnel

Pilot implementation to ensure a smooth migration

Formal approval by the sponsor.

The reconstructed process must be formally approved by management to witness their consent for fitness of use. IT governance dictates that executive management shall be held responsible for any failures and receive recognition for exceptional results. System performance will be evaluated again after entering production use.

Evaluate (post evaluation) The reconstructed process is monitored to ensure that it works and is producing the strategic value as forecast in the original justification.

Comparison of original forecast to actual performance Identification of lessons learned Total quality management plan to maintain the new process A method of continuous improvement is implemented to track the original goals against actual process performance. Annual reevaluation is needed to adapt new requirements or new opportunities.

Benchmarking as a BPR Tool

Benchmarking is the process of comparing performance data (aka metrics). It can be used to evaluate business processes that are under consideration for reengineering. Performance data may be obtained by using a self-assessment or by auditing for compliance against a standard (reference standard). Evidence captured during the diagnostic phase is considered the key to identifying areas for performance improvement and documenting obstacles. ISACA offers the following general guidelines for performing benchmarks:

Plan Identify the critical processes and create measurement techniques to grade the processes.

Research Use information about the process and collect regular data (samples) to build a baseline for comparison. Consider input from your customers and use analogous data from other industries.

Observe Gather internal data and external data from a benchmark partner to aid the comparison results.

Benchmark data can also be compared against published standards.

Analyze Look for root cause-effect relationships and other dependencies in the process. Use predefined tools and procedures to collate the data collected from all available sources.

Adapt Translate the findings into hypotheses of how these findings will help or hurt strategic business goals. Design a pilot test to prove or disprove the hypotheses.

Improve Implement a prototype of the new processes. Study the impact and note any unexpected results.

Revise the process by using controlled change management. Measure the process results again. Use reestablished procedures such as total quality management for continuous improvement.

The following answers are incorrect:

The other options specified does not represent the correct sequence of BRP application steps.

Reference:

CISA review manual 2014 page number 219 to 211

CISA certified information system auditor study guide Second Edition Page Number 154 to 158

NEW QUESTION: 146

Which of the following testing method examines the functionality of an application without peering into its internal structure or knowing the details of it's internals?

- A. Black-box testing
- B. Parallel Test
- C. Regression Testing
- D. Pilot Testing

Answer: ([SHOW ANSWER](#))

Section: Information System Acquisition, Development and Implementation Explanation:

Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings (see white-box testing). This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

For your exam you should know the information below:

Alpha and Beta Testing - An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically, software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests - usually over interim platform and with only basic functionalities.

White box testing - Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path.

However, testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing - An integrity based form of testing associated with testing components of an information system's "functional" operating effectiveness without regards to any specific internal program structure.

Applicable to integration and user acceptance testing.

Function/validation testing - It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Parallel Testing - This is the process of feeding test data into two systems - the modified system and an alternative system and comparing the result.

Sociability Testing -The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but, in a client server and web development, changes to the desktop environment. Multiple application may run on the user's desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs), making operating system registry or configuration file modification, and possibly extra memory utilization.

The following answers are incorrect:

Parallel Testing - This is the process of feeding test data into two systems - the modified system and an alternative system and comparing the result.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests - usually over interim platform and with only basic functionalities Reference:

CISA review manual 2014 Page number 167

Official ISC2 guide to CISSP CBK 3rd Edition Page number 176

NEW QUESTION: 147

A client reviewing a preliminary version of the audit report asks whether a finding in the report could be eliminated or have its risk rating lowered upon retest and audit validation. What would be the auditor's MOST appropriate response?

- A. The report can reflect that a finding was identified but immediately fixed.
- B. The risk rating could be reduced once the issue is resolved.
- C. The risk rating of the finding would need to be reassessed.
- D. The finding could be removed from the report after being remediated.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 148

Before implementing an IT balanced scorecard, an organization must:

- A. deliver effective and efficient services.
- B. define key performance indicators.
- C. provide business value to IT projects.
- D. control IT expenses.

Answer: B ([LEAVE A REPLY](#))

A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

NEW QUESTION: 149

A health care organization utilizes Internet of Things (IoT) devices to improve patient outcomes through real-time patient monitoring and advanced diagnostics. Which of the following would BEST assist in isolating these devices from corporate network traffic?

- A. Internal firewalls
- B. Blockchain technology
- C. Content filtering proxy
- D. Zero Trust architecture

Answer: A ([LEAVE A REPLY](#))

Internal firewalls are highly effective for isolating Internet of Things (IoT) devices from corporate network traffic. By segmenting the network and restricting communication between devices and the main corporate infrastructure, internal firewalls help mitigate the risk of lateral movement and data breaches caused by compromised IoT devices.

* Blockchain Technology (Option B): This is useful for ensuring data integrity but not for network isolation.

* Content Filtering Proxy (Option C): This is designed to manage web traffic and does not provide network segmentation.

* Zero Trust Architecture (Option D): While Zero Trust provides robust access controls, internal firewalls are more directly suited for traffic isolation.

Reference: ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 150

Which of the following control measures is the MOST effective against unauthorized access of confidential information on stolen or lost laptops?

- A. Remote wipe capabilities
- B. Disk encryption
- C. User awareness
- D. Password-protected files

Answer: B ([LEAVE A REPLY](#))

Comprehensive and Detailed Step-by-Step Explanation:

The best protection for a stolen laptop is full disk encryption, which prevents unauthorized access even if the device is lost.

* Option A (Incorrect): Remote wipe capabilities are useful, but they require an internet connection to function, which is not always available when a device is stolen.

* Option B (Correct): Full disk encryption (FDE) ensures that data remains unreadable without the correct decryption key, even if the hard drive is removed.

* Option C (Incorrect): User awareness is helpful, but it does not physically secure data on a lost device.

* Option D (Incorrect): Password-protected files can be bypassed by copying them to another system, making them an inadequate security measure.

Reference: ISACA CISA Review Manual - Domain 5: Protection of Information Assets - Covers encryption, data security, and endpoint protection.

NEW QUESTION: 151

A security administrator should have read-only access for which of the following?

- A. Security logs
- B. Router configuration
- C. Services/daemons configuration
- D. Password policy

Answer: A ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 152

Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

- A. System owners
- B. System users
- C. System designers
- D. System builders

Answer: A ([LEAVE A REPLY](#))

System owners are the information systems (project) sponsors or chief advocates. They normally are responsible for initiating and funding projects to develop, operate and maintain information systems. System users are the individuals who use or are affected by the information system.

Their requirements are crucial in the testing stage of a project. System designers translate business requirements and constraints into technical solutions. System builders construct the system based on the specifications from the systems designers. In most cases, the designers and builders are one and the same.

NEW QUESTION: 153

An organization currently using tape backups takes one full backup weekly and incremental backups daily.

They recently augmented their tape backup procedures with a backup-to-disk solution. This is appropriate because:

- A.** fast synthetic backups for offsite storage are supported.
- B.** backup to disk is always significantly faster than backup to tape.
- C.** tape libraries are no longer needed.
- D.** data storage on disks is more reliable than on tapes.

Answer: A (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

Disk-to-disk (D2D) backup should not be seen as a direct replacement for backup to tape; rather, it should

be viewed as part of a multitier backup architecture that takes advantage of the best features of both tape

and disk technologies. Backups to disks are not dramatically faster than backups to tapes in a balanced

environment. Most often than not there is hardly a difference, since the limiting components are not tape or

disk drives but the overall sustained bandwidth of the backup server's backplane. The advantage in terms

of speed is in restoring performance, since all data are on hand and can be accessed randomly, resulting in

a dramatic enhancement in throughput. This makes fast synthetic backups (making a full backup without

touching the host's data only by using the existing incremental backups) efficient and easy.

Although the

cost of disks has been reduced, tape-based backup can offer an overall cost advantage over disk-only

solutions. Even if RAID arrays are used for D2D storage, a failed drive must be swapped out and the RAID

set rebuilt before another disk drive fails, thus making this kind of backup more risky and not suitable as a

solution of last resort. In contrast, a single tape drive failure does not produce any data loss since the data resides on the tape media. In a multidrive library, the loss of the use of a single tape drive has no impact on the overall level of data protection. Conversely, the loss of a disk drive in an array can put all data at risk. This in itself reinforces the benefits of a disk-to-disk-to-any storage hierarchy, as data could be protected by a tertiary stage of disk storage and ultimately tape. Beyond the drive failure issue, tape has an inherent reliability advantage over any disk drive as it has no boot sector or file allocation table that can be infected or manipulated by a virus.

NEW QUESTION: 154

Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits vulnerability in a protocol?

- A. Install the vendor's security fix for the vulnerability.
- B. Block the protocol traffic in the perimeter firewall.
- C. Block the protocol traffic between internal network segments.
- D. Stop the service until an appropriate security fix is installed.

Answer: D ([LEAVE A REPLY](#))

Stopping the service and installing the security fix is the safest way to prevent the worm from spreading, if the service is not stopped, installing the fix is not the most effective method because the worm continues spreading until the fix becomes effective. Blocking the protocol on the perimeter does not stop the worm from spreading to the internal network(s). Blocking the protocol helps to slow down the spreading but also prohibits any software that utilizes it from working between segments.

NEW QUESTION: 155

In an environment where most IT services have been outsourced, continuity planning is BEST controlled by:

- A. outsourced service provider management
- B. continuity planning specialists.
- C. IT management,
- D. business management.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 156

Which of the following is the BEST way to mitigate risk to an organization's network associated with devices permitted under a bring your own device (BYOD) policy?

- A. Require personal devices to be reviewed by IT staff.
- B. Enable port security on all network switches.
- C. Implement a network access control system.
- D. Ensure the policy requires antivirus software on devices.

Answer: D ([LEAVE A REPLY](#))

The best way to mitigate risk to an organization's network associated with devices permitted under a BYOD policy is to implement a network access control system, as this will allow the organization to monitor, authenticate, and authorize the devices that connect to the network, and to enforce security policies and compliance requirements¹². A network access control system can help to prevent unauthorized or compromised devices from accessing sensitive data or resources, and to detect and isolate any potential threats or vulnerabilities³⁴.

References

1: Network Access Control (NAC) - ISACA 2: Network Access Control (NAC) - Cisco 3: BYOD Security Risks: 6 Ways to Protect Your Organization - ReliaQuest⁵ 4: How to Mitigate BYOD Risks and Challenges - CIOReview⁶

NEW QUESTION: 157

Which of the following is MOST important for an IS auditor to verify when evaluating an organization's data conversion and infrastructure migration plan?

- A. Strategic: goals have been considered.
- B. A rollback plan is included.
- C. A code check review is included.
- D. A migration steering committee has been formed.

Answer: ([SHOW ANSWER](#)**)**

Explanation

The most important thing for an IS auditor to verify when evaluating an organization's data conversion and infrastructure migration plan is that a rollback plan is included. A rollback plan is a contingency plan that describes the steps and actions to be taken in case the data conversion or infrastructure migration fails or causes unacceptable problems or risks. A rollback plan can help to restore the original data and infrastructure, minimize the impact on the business operations and functions, and ensure the continuity and availability of the IT services. The IS auditor should verify that the rollback plan is feasible, tested, documented, and approved, and that it covers all the possible scenarios and outcomes of the data conversion or infrastructure migration. The other options are not as important as verifying the rollback plan, because they either do not address the potential failure or disruption of the data conversion or infrastructure migration, or they are part of the normal planning and execution process rather than a contingency plan. References: CISA Review Manual (Digital Version)¹, Chapter 4, Section 4.2.3

NEW QUESTION: 158

Which of the following presents the GREATEST challenge to the alignment of business and IT?

- A. An IT steering committee chaired by the chief information officer (CIO)

- B. Insufficient IT budget to execute new business projects
- C. Lack of chief information officer (CIO) involvement in board meetings
- D. Lack of information security involvement in business strategy development

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 159

Depending on the complexity of an organization's business continuity plan (BCP), the plan may be

developed as a set of more than one plan to address various aspects of business continuity and disaster

recovery, in such an environment, it is essential that:

- A. each plan is consistent with one another.
- B. all plans are integrated into a single plan.
- C. each plan is dependent on one another.
- D. the sequence for implementation of all plans is defined.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Depending on the complexity of an organization, there could be more than one plan to address various

aspects of business continuity and disaster recovery. These do not necessarily have to be integrated into

one single plan. However, each plan has to be consistent with other plans to have a viable business

continuity planning strategy. It may not be possible to define a sequence in which plans have to be

implemented, as it may be dependent on the nature of disaster, criticality, recovery time, etc.

NEW QUESTION: 160

During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

- A. create the procedures document.
- B. terminate the audit.
- C. conduct compliance testing.
- D. identify and evaluate existing practices.

Answer: D ([LEAVE A REPLY](#))

One of the main objectives of an audit is to identify potential risks; therefore, the most proactive approach would be to identify and evaluate the existing security practices being followed by the organization. IS auditors should not prepare documentation, as doing so could jeopardize their independence. Terminating the audit may prevent achieving one of the basic audit objectives, i.e.,

identification of potential risks. Since there are no documented procedures, there is no basis against which to test compliance.

NEW QUESTION: 161

Which of the following is the GREATEST advantage of elliptic curve encryption over RSA encryption?

- A. Computation speed
- B. Ability to support digital signatures
- C. Simpler key distribution
- D. Greater strength for a given key length

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

The main advantage of elliptic curve encryption over RSA encryption is its computation speed. This method was first independently suggested by Neal Koblitz and Victor S. Miller. Both encryption methods support digital signatures and are used for public key encryption and distribution. However, a stronger key per se does not necessarily guarantee better performance, but rather the actual algorithm employed.

NEW QUESTION: 162

One advantage of monetary unit sampling is the fact that

- A. results are stated in terms of the frequency of items in error
- B. it can easily be applied manually when computer resources are not available
- C. large-value population items are segregated and audited separately
- D. it increases the likelihood of selecting material items from the population

Answer: D ([LEAVE A REPLY](#))

Explanation

Monetary unit sampling (MUS) is a statistical sampling method that is used to determine if the account balances or monetary amounts in a population contain any misstatements. MUS treats each individual dollar in the population as a separate sampling unit, so that larger balances or amounts have a higher probability of being selected than smaller ones. MUS then projects the results of testing the sample to the entire population in terms of dollar values, rather than error rates.

One advantage of MUS is that it increases the likelihood of selecting material items from the population.

Material items are those that have a significant impact on the financial statements and could influence the decisions of users. By giving more weight to larger items, MUS ensures that material misstatements are more likely to be detected and reported. MUS also reduces the sample size required to achieve a desired level of confidence and precision, as compared to other sampling methods that do not consider the value of items.

References:

- 4: Monetary unit sampling definition - AccountingTools
- 5: How Does Monetary Unit Sampling Work? - dummies
- 6: Audit sampling | ACCA Qualification | Students | ACCA Global

NEW QUESTION: 163

Which of the following BEST enables the effectiveness of an agile project for the rapid development of a new software application?

- A. Project segments are established.
- B. The work is separated into phases.
- C. The work is separated into sprints.
- D. Project milestones are created.

Answer: ([SHOW ANSWER](#))

Explanation

The best way to enable the effectiveness of an agile project for the rapid development of a new software application is to separate the work into sprints. Sprints are short, time-boxed iterations that deliver a potentially releasable product increment at the end of each sprint. Sprints allow agile teams to work in a flexible and adaptive manner, respond quickly to changing customer needs and feedback, and deliver value faster and more frequently. Sprints also help teams to plan, execute, review, and improve their work in a collaborative and transparent way. Project segments, phases, and milestones are not specific to agile projects and do not necessarily enable the effectiveness of an agile project. References: Agile Project Management [What is it & How to Start] - Atlassian, CISA Review Manual (Digital Version).

NEW QUESTION: 164

Which of the following is the BEST method to assess the adequacy of security awareness in an organization?

- A. Confirming a security awareness program exists
- B. Administering security survey questionnaires
- C. Observing employee security behaviors
- D. Interviewing employees about security responsibility

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 165

In an online application, which of the following would provide the MOST information about the transaction audit trail?

- A. System/process flowchart
- B. File layouts
- C. Data architecture
- D. Source code documentation

Answer: C ([LEAVE A REPLY](#))

Explanation

In an online application, data architecture provides the most information about the transaction audit trail, as it describes how data are created, stored, processed, accessed and exchanged among different components of the application. Data architecture includes data models, schemas, dictionaries, metadata, standards and policies that define the structure, quality, integrity, security and governance of data. Data architecture can help the IS auditor to trace the origin, flow, transformation and destination of data in an online transaction, and to identify the key data elements, attributes and relationships that are relevant for audit purposes. A system/process flowchart is a graphical representation of the sequence of steps or activities that are performed by a system or process. A system/process flowchart can provide some information about the transaction audit trail, but it is not as detailed or comprehensive as data architecture. A system/process flowchart shows the inputs, outputs, decisions and actions of a system or process, but it does not show the data elements, attributes and relationships that are involved in each step or activity. A file layout is a specification of the format and structure of a data file. A file layout can provide some information about the transaction audit trail, but it is not as detailed or comprehensive as data architecture. A file layout shows the fields, types, lengths and positions of data in a file, but it does not show the origin, flow, transformation and destination of data in an online transaction. Source code documentation is a description of the logic, functionality and purpose of a program or module written in a programming language. Source code documentation can provide some information about the transaction audit trail, but it is not as detailed or comprehensive as data architecture. Source code documentation shows the instructions, variables and parameters that are used to perform calculations and operations on data, but it does not show the data elements, attributes and relationships that are involved in each instruction or operation. References: CISA Review Manual (Digital Version) 1, Chapter 4: Information Systems Operations and Business Resilience, Section 4.2: Data Administration Practices.

NEW QUESTION: 166

An organization's plans to implement a virtualization strategy enabling multiple operating systems on a single host. Which of the following should be the GREATEST concern with this strategy?

- A.** Complexity of administration
- B.** Application performance
- C.** Network bandwidth
- D.** Adequate storage space

Answer: A ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

NEW QUESTION: 167

Which of the following term describes a failure of an electric utility company to supply power within acceptable range?

- A. Sag
- B. Blackout
- C. Brownout
- D. EMI

Answer: C (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

For CISA exam you should know below information about power failure

Total Failure (Blackout) - A complete loss of electric power, which may span from a single building to an entire geographical are and is often caused by weather conditions or inability of an electric utility company to meet user demands Severely reduced voltage (brownout) - The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

Sags, spike and surge - Temporary and rapid decreases (sag) or increases (spike and surges) in a voltage levels. These anomalies can cause loss of data, data corruption, network transmission errors or physical damage to hardware devices.

Electromagnetic interference (EMI) - The electromagnetic interference (EMI) caused by electrical storms or noisy electrical equipments. The interference may cause computer system to hang or crash as well as damages similar to those caused by sags, spike and surges.

The following were incorrect answers:

Sag - Temporarily rapid decrease in a voltage.

Total Failure (Blackout) - A complete loss of electric power, which may span from a single building to an entire geographical are and is often caused by weather conditions or inability of an electric utility company to meet user demands Severely reduced voltage (brownout) - The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

Reference:

CISA review manual 2014 Page number372

NEW QUESTION: 168

Which of the following should be an IS auditor's GREATEST concern when reviewing a reciprocal disaster recovery agreement between two organizations?

- A. Frequency of system testing
- B. Differences in IT policies and procedures
- C. Maintenance of hardware and software compatibility
- D. Right to terminate the agreement

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 169

Which of the following metrics is the BEST indicator of the performance of a web application

- A. HTTP server error rate
- B. Server thread count
- C. Average response time
- D. Server uptime

Answer: ([SHOW ANSWER](#))

Explanation

The best indicator of the performance of a web application is the average response time. This metric measures how long it takes for the web server to process and deliver a request from the client. It reflects the user's perception of how fast or slow the web application is, and it affects the user's satisfaction, engagement, and conversion. A low average response time means that the web application is responsive and efficient, while a high average response time means that the web application is sluggish and unreliable.

HTTP server error rate, server thread count, and server uptime are not as good indicators of the performance of a web application as the average response time. HTTP server error rate measures how often the web server fails to handle a request and returns an error code, such as 404 (Not Found) or 500 (Internal Server Error).

This metric indicates the reliability and availability of the web application, but it does not capture how fast or slow the web application is. Server thread count measures how many concurrent requests the web server can handle at a given time. This metric indicates the scalability and capacity of the web application, but it does not capture how long each request takes to process. Server uptime measures how long the web server has been running without interruption. This metric indicates the stability and resilience of the web application, but it does not capture how well the web application performs during that time.

References:

10 Key Application Performance Metrics & How to Measure Them - Stackify¹ Measuring performance - Learn web development | MDN² Understanding the Basics of Web Performance | BrowserStack³

14 Important Website Performance Metrics You Should Be Analyzing⁴

Top 8 Web Application Performance Metrics | MetricFire Blog⁵

Web Performance Monitoring: A How to Guide for Developers - Stackify⁶

NEW QUESTION: 170

Which of the following is MOST important to include in forensic data collection and preservation procedures?

- A. Determining tools to be used
- B. Preserving data integrity
- C. Assuring the physical security of devices
- D. Maintaining chain of custody

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 171

During a software acquisition review, an IS auditor should recommend that there be a software escrow agreement when:

- A. the estimated life for the product is less than 3 years.
- B. the product is new in the market
- C. the deliverables do not include the source code.
- D. there is no service level agreement (SLA).

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 172

The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

- A. financial results.
- B. customer satisfaction.
- C. internal process efficiency.
- D. innovation capacity.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Financial results have traditionally been the sole overall performance metric. The IT balanced scorecard (BSC) is an IT business governance tool aimed at monitoring IT performance evaluation indicators other than financial results. The IT BSC considers other key success factors, such as customer satisfaction, innovation capacity and processing.

NEW QUESTION: 173

A medium-sized organization, whose IT disaster recovery measures have been in place and regularly tested for years, has just developed a formal business continuity plan (BCP). A basic BCP tabletop exercise has been performed successfully. Which testing should an IS auditor recommend be performed NEXT to verify the adequacy of the new BCP?

- A. Full-scale test with relocation of all departments, including IT, to the contingency site
- B. Walk-through test of a series of predefined scenarios with all critical personnel involved
- C. IT disaster recovery test with business departments involved in testing the critical applications

D. Functional test of a scenario with limited IT involvement

Answer: D (LEAVE A REPLY)

After a tabletop exercise has been performed, the next step would be a functional test, which includes the mobilization of staff to exercise the administrative and organizational functions of a recovery. Since the IT part of the recovery has been tested for years, it would be more efficient to verify and optimize the business continuity plan (BCP) before actually involving IT in a full-scale test. The full-scale test would be the last step of the verification process before entering into a regular annual testing schedule. A full-scale test in the situation described might fail because it would be the first time that the plan is actually exercised, and a number of resources (including IT) and time would be wasted. The walk-through test is the most basic type of testing. Its intention is to make key staff familiar with the plan and discuss critical plan elements, rather than verifying its adequacy. The recovery of applications should always be verified and approved by the business instead of being purely IT-driven. A disaster recovery test would not help in verifying the administrative and organizational parts of the BCP which are not IT-related.

NEW QUESTION: 174

Which of the following statement INCORRECTLY describes the traditional audit approach in comparison to the Control self-assessment approach?

- A.** In traditional approach, Staffs at all level, in all functions, are the primary control analyst.
- B.** Traditional approach assigns duties/supervises staff
- C.** Traditional approach is a policy driven approach
- D.** Traditional approach requires limited employee participations.

Answer: A (LEAVE A REPLY)

Section: The process of Auditing Information System

Explanation:

The keyword INCORRECTLY is used in the question. You need to find out an option which incorrectly describes the traditional approach.

For your exam you should know the information below about control self-assessment and traditional approach:

The traditional approach can be summarized as any approach in which the primary responsibility for analyzing and reporting on internal control and risk is assigned to auditor and to lesser extent, controller department and outside consultants.

Control self-assessment is an assessment of controls made by the staff and management of the unit or units involved. It is a management technique that assures stakeholders, customers and other parties that the internal controls of the organization are reliable.

Benefits of CSA

Early detection of risk

More efficient and improved internal controls

Creation of cohesive teams through employee involvement

Developing a sense of ownership of the controls in the employees and process owners, and reducing their resistance to control improvement initiatives Increased employee awareness of

organizational objectives, and knowledge of risk and internal controls Highly motivated employees Improved audit training process Reduction in control cost Assurance provided to stakeholders and customers Traditional and CSA attributes Traditional Historical CSA Assign duties/supervises staff Empowered/accountable employees Policy/rule driven Continuous improvement/learning curve Limited employee participation Extensive employee participation and training Narrow stakeholders focus Broad stakeholders focus Auditors and other specialist Staff at all level, in all functions, are the primary control analysts The following answers are incorrect:
The other options specified are correctly describes about traditional approach.

Reference:

CISA review manual 2014 page number 61, 62 and 63

NEW QUESTION: 175

The following findings are the result of an IS auditor's post-implementation review of a newly implemented system. Which of the following findings is of GREATEST significance?

- A. A lessons learned session was never conducted.
- B. Monthly dashboards did not always contain deliverables.
- C. The project's 10% budget overrun was not reported to senior management.
- D. Measurable benefits were not defined.

Answer: D (LEAVE A REPLY)

Comprehensive and Detailed Step-by-Step Explanation:

If measurable benefits were not defined, the organization cannot assess whether the system achieved its intended goals, making it the most critical issue.

- * Measurable Benefits Not Defined (Correct Answer - D)
- * No clear KPIs or success metrics means no way to evaluate ROI.
- * Example: A company implements an ERP system but has no performance indicators to measure success.
- * No Lessons Learned (Incorrect - A)
- * Important but does not impact system effectiveness.
- * Missing Dashboard Deliverables (Incorrect - B)
- * A reporting issue, not a strategic failure.
- * Budget Overrun (Incorrect - C)
- * A financial concern but not as critical as system success measurement.

References:

- * ISACA CISA Review Manual
- * COBIT 2019 (Project Governance)

NEW QUESTION: 176

An IS auditor wants to inspect recent events in a system to observe failed authentications and password changes. Which of the following is the MOST appropriate method to use for this purpose?

- A. Penetration testing

- B. Change management records
- C. System log review
- D. Authenticated scanning

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 177

During a review, an IS auditor discovers that corporate users are able to access cloud-based applications and data from any Internet-connected web browser. Which of the following is the auditor's BEST recommendation to help prevent unauthorized access?

- A. Update security policies and procedures.
- B. Implement multi-factor authentication.
- C. Utilize strong anti-malware controls on all computing devices.
- D. Implement an intrusion detection system (IDS).

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 178

The practice of periodic secure code reviews is which type of control?

- A. Compensating
- B. Corrective
- C. Detective
- D. Preventive

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 179

Which of the following is the MOST important consideration when establishing vulnerability scanning on critical IT infrastructure?

- A. The scanning will not degrade system performance.
- B. The scanning will be followed by penetration testing.
- C. The scanning will be cost-effective.
- D. The scanning will be performed during non-peak hours.

Answer: D ([LEAVE A REPLY](#))

Section: Information System Acquisition, Development and Implementation Explanation

NEW QUESTION: 180

When determining which IS audits to conduct during the upcoming year, internal audit has received a request from management for multiple audits of the contract division due to fraud findings during the prior year. Which of the following is the BEST basis for selecting the audits to be performed?

- A. Select audits based on an organizational risk assessment.
- B. Select audits based on collusion risk.
- C. Select audits based on the skill sets of the IS auditors.

D. Select audits based on management's suggestion.

Answer: B ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

NEW QUESTION: 181

The maturity level of an organization's problem management support function is optimized when the function

- A. analyzes critical incidents to identify root cause.
- B. resolves requests in a timely manner
- C. has formally documented the escalation process.
- D. proactively provides solutions

Answer: D ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 182

An organization allows programmers to change production systems in emergency situations without seeking prior approval. Which of the following controls should an IS auditor consider MOST important?

- A. Programmers' subsequent reports
- B. Automated log of changes
- C. Limited number of super users
- D. Operator logs

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 183

Following the implementation of a data loss prevention (DLP) tool, administrators have been overwhelmed with a high number of false positives. Which of the following is the BEST way to address this issue?

- A. Educate staff about the risks of sharing sensitive information outside the organization.
- B. Amend policy rules to match approved and unapproved business information pathways.
- C. Ensure the latest signature files are present and configure regular updates.
- D. Enable monitoring-only mode to permit further tuning of the solution.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 184

During an audit of a data center, an IS auditor's BEST way to gain an understanding of physical security controls is to:

- A. take a tour of the facility and identify physical security controls.
- B. contact the alarm vendor and identify where alarms are installed in the data center
- C. review the data center's physical security procedures.
- D. obtain the engineering plans for the building and identify points of entry.

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 185

The role of the certificate authority (CA) as a third party is to:

- A. provide secured communication and networking services based on certificates.
- B. host a repository of certificates with the corresponding public and secret keys issued by that CA.
- C. act as a trusted intermediary between two communication partners.
- D. confirm the identity of the entity owning a certificate issued by that CA.

Answer: D [\(LEAVE A REPLY\)](#)

Section: Protection of Information Assets

Explanation:

The primary activity of a CA is to issue certificates. The primary role of the CA is to check the identity of the

entity owning a certificate and to confirm the integrity of any certificate it issued. Providing a communication

infrastructure is not a CA activity. The secret keys belonging to the certificates would not be archived at the

CA. The CA can contribute to authenticating the communicating partners to each other, but the CA is not

involved in the communication stream itself.

NEW QUESTION: 186

.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 [\(LEAVE A REPLY\)](#)

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 documented.

NEW QUESTION: 187

An IS auditor is reviewing a data conversion project. Which of the following is the auditor's BEST recommendation prior to go-live?

- A. Automate the test scripts
- B. Conduct a mock conversion test.
- C. Review test procedures and scenarios
- D. Establish a configuration baseline.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 188

An employee approaches an IS auditor and expresses concern about a critical security issue in a newly installed application. Which of the following would be the MOST appropriate action for the auditor to take?

- A. Discuss the concern with audit management.
- B. Recommend reverting to the previous application.
- C. Discuss the concern with additional end users.
- D. Immediately conduct a review of the application.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 189

Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures. True or false?

- A. True
- B. False

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

Fourth-generation languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures.

NEW QUESTION: 190

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

- A. Cold site
- B. Hot site
- C. Alternate site
- D. Warm site

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

A cold site is often an acceptable solution for preparing for recovery of noncritical systems and data.

NEW QUESTION: 191

When assessing whether an organization's IT performance measures are comparable to other organizations in the same industry, which of the following would be MOST helpful to review?

- A. IT governance frameworks
- B. Benchmarking surveys
- C. Utilization reports
- D. Balanced scorecard

Answer: B ([LEAVE A REPLY](#))

Benchmarking surveys are used to compare an organization's IT performance measures to those of other organizations in the same industry. The surveys provide data on a variety of IT performance metrics, including system availability, system reliability, cost effectiveness, and customer satisfaction. This data can then be used to assess whether an organization's IT performance measures are comparable to other organizations in the same industry.

NEW QUESTION: 192

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses which stream cipher for confidentiality?

- A. CRC-32
- B. CRC-64
- C. DES
- D. 3DES
- E. RC4
- F. RC5
- G. None of the choices.

Answer: E ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity.

NEW QUESTION: 193

A region where an organization conducts business has announced changes in privacy legislation. Which of the following should an IS auditor do FIRST to prepare for the changes?

- A. Provide suggested updates to the organization's privacy procedures.
- B. Perform a gap analysis with current privacy procedures.
- C. Communicate the changes in privacy legislation to the legal department.

D. Design compensating controls to be in compliance with new privacy legislation.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 194

Which of the following findings should be of MOST concern to an IS auditor when evaluating information security governance within an organization?

- A. The information security department has difficulty filling vacancies
- B. The information security oversight committee meets quarterly
- C. Information security policies were last updated two years ago
- D. The data center manager has final sign-off on security projects

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 195

Which of the following is an example of a passive attack initiated through the Internet?

- A. Traffic analysis
- B. Masquerading
- C. Denial of service
- D. E-mail spoofing

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Internet security threats/vulnerabilities are divided into passive and active attacks. Examples of passive attacks include network analysis, eavesdropping and traffic analysis. Active attacks include brute force attacks, masquerading, packet replay, message modification, unauthorized access through the Internet or web-based services, denial-of-service attacks, dial-in penetration attacks, e-mail bombing and spamming, and e-mail spoofing.

NEW QUESTION: 196

During a review of system access, an IS auditor notes that an employee who has recently changed roles within the organization still has previous access rights. The auditor's NEXT step should be to:

- A. recommend a control to automatically update access rights.
- B. determine the reason why access rights have not been revoked.
- C. direct management to revoke current access rights.
- D. determine if access rights are in violation of software licenses.

Answer: B ([LEAVE A REPLY](#))

Explanation

The NEXT step for the IS auditor after noting that an employee who has recently changed roles within the organization still has previous access rights should be to B. determine the reason why access rights have not been revoked. Identifying the cause of this situation is crucial for understanding whether it's due to oversight, process gaps, or other factors. Once the reason is

determined, appropriate corrective actions can be recommended to ensure that access rights are aligned with the employee's current role and responsibilities¹.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As

Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 197

An IS auditor reviewing an organization's data privacy controls observes that privacy notices do not clearly state how the organization uses customer data for its processing operations. Which of the following data protection principles **MUST** be implemented to address this gap?

- A. Maintenance of data integrity
- B. Access to collected data
- C. Retention of consent documentation
- D. Purpose for data collection

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 198

An IS auditor plans to review all access attempts to a video-monitored and proximity card-controlled communications room. Which of the following would be **MOST** useful to the auditor?

- A. Alarm system with CCTV
- B. Access control log
- C. Security incident log
- D. Access card allocation records

Answer: ([SHOW ANSWER](#)**)**

A system electronic log is the most useful source of information for an IS auditor to review all access attempts to a video-monitored and proximity card-controlled communications room. A system electronic log can provide accurate and detailed records of the date, time, card number, and status (success or failure) of each access attempt. A system electronic log can also be easily searched, filtered, and analyzed by the auditor to identify any unauthorized or suspicious access attempts.

A manual sign-in and sign-out log is not as reliable or useful as a system electronic log, because it depends on the honesty and compliance of the users. A manual log can be easily manipulated, forged, or omitted by the users or intruders. A manual log also does not capture the status of each access attempt, and it can be difficult to verify the identity of the users based on their signatures.

An alarm system with CCTV is not as useful as a system electronic log, because it only captures the events that trigger the alarm, such as unauthorized or forced entry. An alarm system with CCTV does not provide a complete record of all access attempts, and it can be affected by factors such as camera angle, lighting, and resolution. An alarm system with CCTV also requires more time and effort to review the video footage by the auditor.

A security incident log is not as useful as a system electronic log, because it only records the incidents that are reported by the users or detected by the security staff. A security incident log does not provide a comprehensive record of all access attempts, and it can be incomplete or inaccurate depending on the reporting and detection mechanisms. A security incident log also does not capture the details of each access attempt, such as the card number and status.

References:

* ISACA CISA Review Manual 27th Edition (2019), page 247

* ISACA CISA Certified Information Systems Auditor Exam ... - PUPUWEB

NEW QUESTION: 199

During an audit, an IT finding is agreed upon by all IT teams involved, but no team wants to be responsible for remediation or considers the finding within its area of responsibility. Which of the following is the IS auditor's BEST course of action?

- A. Escalate to IT management for resolution.
- B. Issue the finding without identifying an owner
- C. Assign shared responsibility to all IT teams.
- D. Determine the most appropriate team and assign accordingly.

Answer: A (LEAVE A REPLY)

The best course of action for the IS auditor is A. Escalate to IT management for resolution. This is because IT management is responsible for overseeing and coordinating the IT activities and functions within the organization, and ensuring that they comply with the audit findings and recommendations¹. IT management can help resolve the issue of finding ownership by:

- * Clarifying and communicating the roles and responsibilities of each IT team, and how they relate to the finding and its remediation².
- * Evaluating and assigning the finding to the most appropriate IT team, based on their expertise, authority, and availability².
- * Providing guidance and support to the assigned IT team, and monitoring their progress and performance in remediating the finding².

NEW QUESTION: 200

Who is ultimately responsible for providing requirement specifications to the software-development team?

- A. The project sponsor
- B. The project members
- C. The project leader
- D. The project steering committee

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

The project sponsor is ultimately responsible for providing requirement specifications to the software- development team.

NEW QUESTION: 201

When a data center is attempting to restore computing facilities at an alternative site following a disaster, which of the following should be restored FIRST?

- A. Data backups
- B. Decision support system
- C. Operating system
- D. Applications

Answer: C ([LEAVE A REPLY](#))

When a data center is attempting to restore computing facilities at an alternative site following a disaster, the operating system should be restored FIRST. Here's why:

* Operating System (OS):

* The OS is the foundation of any computing environment. It manages hardware resources, provides essential services, and allows applications to run.

* Restoring the OS ensures that the infrastructure is operational and ready for further recovery steps.

* Without a functional OS, applications cannot execute, and data backups cannot be effectively restored.

* Data Backups:

* While data backups are critical for recovery, they depend on a working infrastructure.

* If the OS is not operational, restoring data backups becomes challenging.

* Data backups should follow the OS restoration.

* Applications:

* Applications rely on the OS to function.

* Restoring applications before the OS may lead to compatibility issues or incomplete functionality.

* Applications should be restored after ensuring a stable OS environment.

* Decision Support System (DSS):

* DSS is an application category.

* It should follow the restoration of both the OS and critical applications.

In summary, prioritize restoring the operating system, which forms the basis for subsequent recovery steps¹².

Once the OS is functional, proceed with data backups, applications, and other systems as needed.

NEW QUESTION: 202

When evaluating information security governance within an organization, which of the following findings should be of MOST concern to an IS auditor?

- A. The information security department has difficulty filling vacancies
- B. An information security governance audit was not conducted within the past year
- C. The data center manager has final sign-off on security projects
- D. Information security policies are updated annually

Answer: C ([LEAVE A REPLY](#))

Explanation

The finding that should be of most concern to an IS auditor when evaluating information security governance within an organization is that the data center manager has final sign-off on security projects. This indicates a lack of segregation of duties and a potential conflict of interest between the operational and security roles. The data center manager may have access to sensitive information or systems that should be protected by security controls, or may influence or override security decisions that are not in the best interest of the organization.

This finding also suggests that there is no clear accountability or authority for information security governance at a higher level, such as senior management or board of directors. The other findings are not as concerning as this one, although they may indicate some areas for improvement or monitoring. References:

ISACA, CISA Review Manual, 27th Edition, chapter 5, section 5.11

ISACA, IT Governance Using COBIT and Val IT: Student Booklet - 2nd Edition4

NEW QUESTION: 203

An organization wants to reuse company-provided smartphones collected from staff leaving the organization. Which of the following would be the BEST recommendation?

- A. The memory cards of the smartphones should be replaced.
- B. Smartphones should not be reused, but physically destroyed.
- C. Data should be securely deleted from the smartphones.
- D. The SIM card and telephone number should be changed.

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 204

Which of the following types of firewalls provide the GREATEST degree of control against hacker intrusion?

- A. Circuit gateway
- B. Screening router
- C. Application level gateway
- D. Packet filtering router

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 205

Which of the following is the BEST control to detect errors in an accounts payable system?

- A. Quality control review of new payments
- B. Input validation
- C. Management approval of payments
- D. Alignment of the process to business objectives

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 206

An IS auditor plans to review all access attempts to a video-monitored and proximity-card controlled

communications room. Which of the following would be MOST useful to the auditor?

- A. System electronic log
- B. Security incident log
- C. Manual sign-in and sign-out log
- D. Alarm system with CCTV

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation/Reference: <https://www.slideshare.net/desmond.devendran/chap5-2007-cisa-review-course>

NEW QUESTION: 207

An organization has outsourced the maintenance of its customer database to an external vendor, and the vendor has requested live data to test the performance of the database. Which of the following is MOST important for the IS auditor to recommend?

- A. Ensure sensitive field data is anonymized by random characters.
- B. Ensure data transfer details are specified in the service engagement contract.
- C. Ensure the data is backed up before providing it to the vendor.
- D. Ensure both parties agree the data will be destroyed after the testing is complete.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 208

An IT department is unaware of spreadsheets and databases that have been created by business end users to support their respective operations Which of the following is the GREATEST risk in this situation?

- A. End-user solutions may not have proper documentation
- B. End-user developed systems may be inefficient
- C. End-user solutions may not be protected by IT general controls
- D. End-user developed systems may duplicate data

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 209

An IS auditor has been assigned to review IT structures and activities recently outsourced to various providers. Which of the following should the IS auditor determine FIRST?

- A. That an audit clause is present in all contracts
- B. That the SLA of each contract is substantiated by appropriate KPIs
- C. That the contractual warranties of the providers support the business needs of the organization
- D. That at contract termination, support is guaranteed by each outsourcer for new outsourcers

Answer: C ([LEAVE A REPLY](#))

The complexity of IT structures matched by the complexity and interplay of responsibilities and warranties may affect or void the effectiveness of those warranties and the reasonable certainty that the business needs will be met. All other choices are important, but not as potentially dangerous as the interplay of the diverse and critical areas of the contractual responsibilities of the outsourcers.

NEW QUESTION: 210

Which of the following is MOST important for an IS auditor to review when evaluating the effectiveness of an organization's incident response process?

- A. Past incident response actions
- B. Incident response staff experience and qualifications
- C. Results from management testing of incident response procedures
- D. Incident response roles and responsibilities

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 211

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

- A. Function point analysis (FPA)
- B. Feature point analysis (FPA)
- C. GANTT
- D. PERT

Answer: A ([LEAVE A REPLY](#))

A function point analysis (FPA) is a reliable technique for estimating the scope and cost of a software-development project.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

NEW QUESTION: 212

Which of the following is the BEST indication to an IS auditor that management's post-implementation review was effective?

- A. Lessons learned were documented and applied.
- B. Business and IT stakeholders participated in the post-implementation review.
- C. Post-implementation review is a formal phase in the system development life cycle (SDLC).
- D. Internal audit follow-up was completed without any findings.

Answer: A ([LEAVE A REPLY](#))

Explanation

The best indication to an IS auditor that management's post-implementation review was effective is that lessons learned were documented and applied, as this shows that the management has identified and addressed the issues and gaps that arose during the implementation, and has improved the processes and practices for future projects. Business and IT stakeholders participating in the post-implementation review is a good practice, but it does not guarantee that the review was effective or that the outcomes were implemented.

Post-implementation review being a formal phase in the system development life cycle (SDLC) is a requirement, but it does not ensure that the review was effective or that the outcomes were implemented. Internal audit follow-up being completed without any findings is a desirable result, but it does not indicate that the management's post-implementation review was effective or that the outcomes were implemented. References: CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development and Implementation, Section 3.2: Project Management Practices¹

NEW QUESTION: 213

Which of the following is an advantage of the top-down approach to software testing?

- A. Interface errors are identified early
- B. Testing can be started before all programs are complete
- C. it is more effective than other testing approaches
- D. Errors in critical modules are detected sooner

Answer: A ([LEAVE A REPLY](#))

The advantage of the top-down approach is that tests of major functions are conducted early, thus enabling the detection of interface errors sooner. The most effective testing approach is dependent on the environment being tested. Choices B and D are advantages of the bottom-up approach to system testing.

NEW QUESTION: 214

An IT governance framework provides an organization with:

- A. a basis for directing and controlling IT.

- B. assurance that there will be IT cost reductions.
- C. organizational structures to enlarge the market share through IT.
- D. assurance that there are surplus IT investments.

Answer: A (LEAVE A REPLY)

Section: Governance and Management of IT

Explanation/Reference:

NEW QUESTION: 215

Which of the following attack could be avoided by creating more security awareness in the organization and provide adequate security knowledge to all employees?

- A. surf attack
- B. Traffic analysis
- C. Phishing
- D. Interrupt attack

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Phishing techniques include social engineering, link manipulation, spear phishing, whaling, dishing, or web site forgery techniques.

For your exam you should know the information below:

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Spear phishing

Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success.

Link manipulation

Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization.

Misspelled URLs or the use of sub domains are common tricks used by phishes. In the following example URL, [http:// www.yourbank.example.com/](http://www.yourbank.example.com/), it appears as though the URL will take you to the example section of the your bank website; actually this URL points to the "your bank" (i.e. phishing) section of the example website. Another common trick is to make the displayed text for

a link (the text between the tags) suggest a reliable destination, when the link actually goes to the phishes' site. The following example link, // en.wikipedia.org/wiki/Genuine, appears to direct the user to an article entitled "Genuine"; clicking on it will in fact take the user to the article entitled "Deception". In the lower left hand corner of most browsers users can preview and verify where the link is going to take them. Hovering your cursor over the link for a couple of seconds may do a similar thing, but this can still be set by the phishes through the HTML tooltip tag.

Website forgery

Once a victim visits the phishing website, the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original bar and opening up a new one with the legitimate URL.

An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge.

The following answers are incorrect:

Smurf Attack - Occurs when mis-configured network device allow packet to be sent to all hosts on a particular network via the broadcast address of the network

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Interrupt attack- Interrupt attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 323

Official ISC2 guide to CISSP CBK 3rd Edition Page number 493

<http://en.wikipedia.org/wiki/Phishing>

NEW QUESTION: 216

IS management recently replaced its existing wired local area network (LAN) with a wireless infrastructure to accommodate the increased use of mobile devices within the organization. This will increase the risk of which of the following attacks?

- A. Port scanning
- B. Back door
- C. Man-in-the-middle
- D. War driving

Answer: D ([LEAVE A REPLY](#))

A war driving attack uses a wireless Ethernet card, set in promiscuous mode, and a powerful antenna to penetrate wireless systems from outside. Port scanning will often target the external firewall of the organization. A back door is an opening left in software that enables an unknown entry into a system. Man-in-the-middle attacks intercept a message and either replace or modify it.

NEW QUESTION: 217

What should an IS auditor do FIRST when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective?

- A. Determine the resources required to make the control effective.
- B. Ascertain the existence of other compensating controls.
- C. Verify the impact of the control no longer being effective.
- D. Validate the overall effectiveness of the internal control.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 218

An IS auditor is conducting a follow-up internal IS audit and determines that several recommendations from the prior year have not been implemented. Which of the following should be the auditor's FIRST course of action?

- A. Evaluate the recommendations in context of the current IT environment.
- B. Continue the audit and disregard prior audit recommendations.
- C. Request management implement recommendations from the prior year.
- D. Add unimplemented recommendations as findings for the new audit.

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 219

As part of a quality assurance initiative, an organization has engaged an external auditor to evaluate the internal IS audit function. Which of the following observations should be of MOST concern?

- A. Audit engagements are not risk-based.
- B. Audit reports do not state they are conducted in accordance with industry standards.
- C. The audit team is not sufficiently leveraging data analytics.
- D. Audit reports are not approved by the audit committee.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 220

An IS auditor discovers a box of hard drives in a secured location that are overdue for physical destruction.

The vendor responsible for this task was never made aware of these hard drives. Which of the following is the BEST course of action to address this issue?

- A. Evaluate the corporate asset handling policy for potential gaps.
- B. Recommend the drives be sent to the vendor for destruction.
- C. Examine the workflow to identify gaps in asset handling responsibilities.
- D. Escalate the finding to the asset owner for remediation

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 221

A database administrator (DBA) should be prevented from having end user responsibilities:

- A. having end user responsibilities
- B. accessing sensitive information
- C. having access to production files
- D. using an emergency user ID

Answer: A [\(LEAVE A REPLY\)](#)

Explanation

A database administrator (DBA) should be prevented from having end user responsibilities to avoid a conflict of interest and a violation of the principle of segregation of duties. End user responsibilities may include initiating transactions, authorizing transactions, recording transactions or reconciling transactions. A DBA who has end user responsibilities may compromise the integrity, confidentiality and availability of the data and the database systems. Accessing sensitive information, having access to production files and using an emergency user ID are not end user responsibilities, but rather potential risks or controls associated with the DBA role. References:

- 1: Database Administrator (DBA) Definition
- 2: Segregation of Duties | ISACA
- 3: [End User Definition]

NEW QUESTION: 222

Which of the following statements appearing in an organization's acceptable use policy BEST demonstrates alignment with data classification standards related to the protection of information assets?

- A. Any information assets transmitted over a public network must be approved by executive management.
- B. All information assets must be encrypted when stored on the organization's systems.
- C. Information assets should only be accessed by persons with a justified need.
- D. All information assets will be assigned a clearly defined level to facilitate proper employee handling.

Answer: D [\(LEAVE A REPLY\)](#)

The statement that BEST demonstrates alignment with data classification standards related to the protection of information assets is D. All information assets will be assigned a clearly defined level to facilitate proper employee handling. Data classification involves categorizing information assets based on their sensitivity, importance, and usage. Assigning clearly defined levels (such as public, internal, confidential, etc.) to information assets ensures that appropriate security controls are applied based on their classification. By doing so, organizations can manage access, encryption, and other protective measures effectively¹².

References:

* IFRC. "Information Security: Acceptable Use

Policy." 1(<https://www.ifrc.org/sites/default/files/2021-11/IFRC-Information-Security-Acceptable-Use-Po>

* UNSW Sydney. "Data Classification

Standard." 2(<https://www.unsw.edu.au/content/dam/pdfs/governance/policy/2022-01-policies/datastandard>

* Digital Guardian. "What is a Data Classification

Policy?" 3(<https://www.digitalguardian.com/blog/what-data-classification-policy>)

* Microsoft Service Trust Portal. "Data classification & sensitivity label taxonomy."

4(<https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-classification-and-la>

* Clark University ITS Policies. "Data Classification - Data Security

Policies." 5(https://www2.clarku.edu/offices/its/policies/data_classification.cfm)

NEW QUESTION: 223

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

A. Detective

B. Corrective

C. Preventative

D. Compensatory

Answer: ([SHOW ANSWER](#))

Batch control reconciliations is a compensatory control for mitigating risk of inadequate segregation of duties.

NEW QUESTION: 224

Which of the following findings should be of MOST concern to an IS auditor reviewing an organization's business continuity plan (BCP)?

A. The plan has not been signed by executive management.

B. End users have not been trained on the latest version of the plan.

C. The plan has not been updated in several years.

D. No tabletop exercises have been conducted for the plan.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 225

An information security manager is preparing an incident response plan. Which of the following is the MOST important consideration when responding to an incident involving sensitive customer data?

- A. The assignment of a forensics teams
- B. The ability to recover from the incident in a timely manner
- C. Following defined post-incident review procedures
- D. The ability to obtain incident information in a timely manner

Answer: (SHOW ANSWER)

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 226

Which of the following is the MOST important outcome of an information security program?

- A. Emerging security technologies are better understood and accepted.
- B. Operating system weaknesses are more easily identified.
- C. Organizational awareness of security responsibilities is improved.
- D. The cost to mitigate information security risk is reduced.

Answer: C (LEAVE A REPLY)

The most important outcome of an information security program is improved organizational awareness of security responsibilities. This is because an effective information security program requires an organization to be aware of the risks it is facing and its responsibilities to protect itself from these risks. Understanding the security responsibilities and the associated risks, and having a plan in place to mitigate them, is essential in order to ensure the security of an organization's data and systems

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As
Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 227

A source code repository should be designed to:

- A. prevent developers from accessing secure source code.
- B. prevent changes from being incorporated into existing code.
- C. provide automatic incorporation and distribution of modified code.
- D. provide secure versioning and backup capabilities for existing code.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 228

An IS auditor reviewing the implementation of an intrusion detection system (IDS) should be MOST concerned if:

- A. IDS sensors are placed outside of the firewall.
- B. a behavior-based IDS is causing many false alarms.
- C. a signature-based IDS is weak against new types of attacks.
- D. the IDS is used to detect encrypted traffic.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

An intrusion detection system (IDS) cannot detect attacks within encrypted traffic, and it would be a concern if someone was misinformed and thought that the IDS could detect attacks in encrypted traffic. An organization can place sensors outside of the firewall to detect attacks. These sensors are placed in highly sensitive areas and on extranets. Causing many false alarms is normal for a behavior-based IDS, and should not be a matter of concern. Being weak against new types of attacks is also expected from a signature-based IDS, because it can only recognize attacks that have been previously identified.

NEW QUESTION: 229

An IS auditor is assigned to audit a software development project which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

- A. Report that the organization does not have effective project management.
- B. Recommend the project manager be changed.
- C. Review the IT governance structure.
- D. Review the conduct of the project and the business case.

Answer: D ([LEAVE A REPLY](#))

Before making any recommendations, an IS auditor needs to understand the project and the factors that have contributed to making the project over budget and over schedule. The organization may have effective project management practices and sound IT governance and still be behind schedule or over budget. There is no indication that the project manager should be changed without looking into the reasons for the overrun.

NEW QUESTION: 230

Which of the following findings should be of GREATEST concern for an IS auditor when auditing the effectiveness of a phishing simulation test administered for staff members?

- A. Staff members who failed the test did not receive follow-up education
- B. Test results were not communicated to staff members.
- C. Staff members were not notified about the test beforehand.
- D. Security awareness training was not provided prior to the test.

Answer: A ([LEAVE A REPLY](#))

The IS auditor should be most concerned about the lack of follow-up education for staff members who failed the phishing simulation test. Phishing simulation tests are designed to assess the level of awareness and susceptibility of staff members to phishing attacks, and to provide feedback and training to improve their security behavior. If staff members who failed the test do not receive follow-up education, they will not learn from their mistakes and may continue to fall victim to real phishing attacks, which could compromise the security of the organization.

The other options are less concerning for the IS auditor:

- * Test results were not communicated to staff members. This is not ideal, as staff members should receive feedback on their performance and learn from the test results. However, this does not necessarily mean that they did not receive any training or education on how to avoid phishing attacks.
- * Staff members were not notified about the test beforehand. This is a common practice for phishing simulation tests, as it mimics the real-world scenario where staff members do not know when they will receive a phishing email. The purpose of the test is to measure their spontaneous reaction and awareness, not their preparedness or compliance.
- * Security awareness training was not provided prior to the test. This is not a major concern, as the test can serve as a baseline measurement of the current level of awareness and susceptibility of staff members, and as a starting point for providing tailored training and education based on the test results.

NEW QUESTION: 231

Sending a message and a message hash encrypted by the sender's private key will ensure:

- A.** authenticity and integrity.
- B.** authenticity and privacy.
- C.** integrity and privacy.
- D.** privacy and nonrepudiation.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

If the sender sends both a message and a message hash encrypted by its private key, then the receiver can apply the sender's public key to the hash and get the message hash. The receiver can apply the hashing algorithm to the message received and generate a hash. By matching the generated hash with the one received, the receiver is ensured that the message has been sent by the specific sender, i.e., authenticity, and that the message has not been changed enroute. Authenticity and privacy will be ensured by first using the sender's private key and then the receiver's public key to encrypt the message. Privacy and integrity can be ensured by using the receiver's public key to encrypt the message and sending a message hash/digest. Only nonrepudiation can be ensured by using the sender's private key to encrypt the message. The sender's public key, available to anyone, can decrypt a message; thus, it does not ensure privacy.

NEW QUESTION: 232

During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

- A. test data to validate data input.
- B. test data to determine system sort capabilities.
- C. generalized audit software to search for address field duplications.
- D. generalized audit software to search for account field duplications.

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Since the name is not the same {due to name variations}, one method to detect duplications would be to compare other common fields, such as addresses. A subsequent review to determine common customer names at these addresses could then be conducted. Searching for duplicate account numbers would not likely find duplications, since customers would most likely have different account numbers for each variation. Test data would not be useful to detect the extent of any data characteristic, but simply to determine how the data were processed.

NEW QUESTION: 233

Which of the following should be given GREATEST consideration when implementing the use of an open-source product?

- A. Support
- B. Performance
- C. Confidentiality
- D. Usability

Answer: A ([LEAVE A REPLY](#))

Explanation

Support should be given the greatest consideration when implementing the use of an open-source product, as open-source software may not have the same level of technical support, maintenance, and updates as proprietary software¹. Open-source software users may have to rely on the community of developers and users, online forums, or third-party vendors for support, which may not be timely, reliable, or consistent². Therefore, before implementing an open-source product, users should evaluate the availability and quality of support options, such as documentation, forums, mailing lists, bug trackers, chat channels, etc.³

NEW QUESTION: 234

An organization was recently notified by its regulatory body of significant discrepancies in its reporting data.

A preliminary investigation revealed that the discrepancies were caused by problems with the organization's data quality. Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be advisors to the process. To ensure that management concerns are addressed, which data set should internal audit recommend be reviewed FIRST?

- A. Data impacting business objectives
- B. Data supporting financial statements
- C. Data reported to the regulatory body
- D. Data with customer personal information

Answer: ([SHOW ANSWER](#))

Section: Governance and Management of IT

NEW QUESTION: 235

A CFO has requested an audit of IT capacity management due to a series of finance system slowdowns during month-end reporting. What would be MOST important to consider before including this audit in the program?

- A. Whether system delays result in more frequent use of manual processing
- B. Whether the system's performance poses a significant risk to the organization
- C. Whether stakeholders are committed to assisting with the audit
- D. Whether internal auditors have the required skills to perform the audit

Answer: B ([LEAVE A REPLY](#))

The most important thing to consider before including an audit of IT capacity management in the program is whether the system's performance poses a significant risk to the organization. IT capacity management is a process that ensures that IT resources are sufficient to meet current and future business needs, and that they are optimized for cost and performance. A poor IT capacity management can result in system slowdowns, outages, failures, or breaches, which can affect the availability, reliability, security, and efficiency of IT services and business processes. Therefore, before conducting an audit of IT capacity management, the auditor should assess the potential impact and likelihood of these risks on the organization's objectives, reputation, compliance, and customer satisfaction.

Whether system delays result in more frequent use of manual processing (option A) is not the most important thing to consider before including an audit of IT capacity management in the program, as it is only one possible consequence of poor IT capacity management. Manual processing can introduce errors, delays, inefficiencies, and inconsistencies in the data and reports, which can affect the quality and accuracy of financial information. However, manual processing is not the only or the worst outcome of poor IT capacity management; there may be other more severe or frequent risks that need to be considered.

Whether stakeholders are committed to assisting with the audit (option C) is also not the most important thing to consider before including an audit of IT capacity management in the program, as it is a factor that affects the feasibility and effectiveness of the audit, not the necessity or priority of it. Stakeholder commitment is important for ensuring that the auditor has access to relevant information, documents, data, and personnel, as well as for facilitating communication, collaboration, and feedback during the audit process. However, stakeholder commitment is not a sufficient reason to conduct an audit of IT capacity management; there must be a clear risk-based rationale for selecting this area for audit.

Whether internal auditors have the required skills to perform the audit (option D) is also not the most important thing to consider before including an audit of IT capacity management in the program, as it is a factor that affects the quality and credibility of the audit, not the urgency or importance of it. Internal auditors should have the appropriate knowledge, skills, and experience to perform an audit of IT capacity management, which may include technical, business, analytical, and communication skills. However, internal auditors can also acquire or supplement these skills through training, coaching, consulting, or outsourcing.

Therefore, internal auditors' skills are not a decisive factor for choosing this area for audit.

Therefore, option B is the correct answer.

References:

Guide to IT Capacity Management | Smartsheet

ISO 27001 capacity management: How to implement control A.12.1.3 - Advisera ISO 27002:2022
- Control 8.6 - Capacity Management

NEW QUESTION: 236

Which of the following is the BEST justification for deferring remediation testing until the next audit?

- A. Management's planned actions are sufficient given the relative importance of the observations
- B. The auditor who conducted the audit
- C. Auditee management has accepted all observations reported by the auditor.
- D. The audit environment has changed significantly

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 237

Which of the following is the MOST appropriate control to have in place after data migration?

- A. Mapping of transactions from source to receiving system
- B. Clearly defined and documented data migration roles
- C. Formal sign-off by senior management after completion
- D. Review of representative samples of migrated data

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 238

Which of the following should be of MOST concern to an IS auditor reviewing the information systems acquisition, development, and implementation process?

- A. A post-implementation lessons-learned exercise was not conducted.
- B. System deployment is routinely performed by contractors.
- C. There is no system documentation available for review.
- D. Data owners are not trained on the use of data conversion tools.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 239

Which of the following control provides an alternative measure of control?

- A. Deterrent
- B. Preventive
- C. Detective
- D. Compensating

Answer: D ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

Explanation:

For your exam you should know below information about different security controls Deterrent Controls Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process.

This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events. When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs. It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk. For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement. Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions.

Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations.

There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process.

This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers.

Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided.

For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access

controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions.

Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations.

There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Deterrent - Deterrent controls are intended to discourage a potential attacker Preventive -

Preventive controls are intended to avoid an incident from occurring Detective - Detective control helps identify an incident's activities and potentially an intruder Reference:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

NEW QUESTION: 240

Which of following is MOST important to determine when conducting a post-implementation review?

- A. Whether lessons learned have been documented
- B. Whether success criteria have been achieved
- C. Whether the project has been delivered within the approved budget
- D. Whether the solution architecture complies with IT standards

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 241

An IS auditor is reviewing an organization's sales and purchasing system due to ongoing data quality issues. An analysis of which of the following would provide the MOST useful information to determine the revenue loss?

- A. Correlation between data errors and loss in value of transaction
- B. Cost of implementing data validation controls within the system
- C. Comparison of the cost of data acquisition and loss in sales revenue
- D. Correlation between the number of issues and average downtime

Answer: A ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 242

Data Loss Prevention (DLP) tools provide the MOST protection against:

- A. The installation of unknown malware.
- B. Malicious programs running on organizational systems.
- C. The downloading of sensitive information to devices by employees.
- D. The sending of corrupt data files to external parties via email.

Answer: C ([LEAVE A REPLY](#))

Comprehensive and Detailed Step-by-Step Explanation:

DLP (Data Loss Prevention) tools are designed to prevent unauthorized access, transfer, or leakage of sensitive data, especially by insider threats or unauthorized downloads.

- * Preventing Unauthorized Downloads (Correct Answer - C)
- * DLP solutions block or log attempts to transfer sensitive files.
- * Example: A DLP tool detects and blocks an employee from copying confidential data to a USB drive.

- * Preventing Malware Installation (Incorrect - A, B)
- * Antivirus and endpoint protection tools, not DLP, handle malware threats.
- * Preventing Corrupt Data Transmission (Incorrect - D)
- * DLP focuses on data protection, not detecting corrupt files.

References:

- * ISACA CISA Review Manual
- * NIST 800-53 (Data Protection Controls)
- * CIS (Center for Internet Security) DLP Best Practices

NEW QUESTION: 243

.What supports data transmission through split cable facilities or duplicate cable facilities?

- A. Diverse routing
- B. Dual routing
- C. Alternate routing
- D. Redundant routing

Answer: A ([LEAVE A REPLY](#))

Diverse routing supports data transmission through split cable facilities, or duplicate cable facilities.

NEW QUESTION: 244

Which of the following is the MOST important control to implement when senior managers use smartphones to access sensitive company information?

- A. Mandatory virtual private network (VPN) connectivity
- B. Centralized device administration
- C. Strong passwords
- D. Anti-malware on the devices

Answer: D ([LEAVE A REPLY](#))

Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 245

Which of the following is a corrective control?

- A. Separating equipment development testing and production
- B. Verifying duplicate calculations in data processing
- C. Reviewing user access rights for segregation
- D. Executing emergency response plans

Answer: D ([LEAVE A REPLY](#))

A corrective control is a control that aims to restore normal operations after a disruption or incident has occurred. Executing emergency response plans is an example of a corrective control, as it helps to mitigate the impact of an incident and resume business functions.

Separating equipment development testing and production is a preventive control, as it helps to avoid errors or unauthorized changes in production systems.

Verifying duplicate calculations in data processing is a detective control, as it helps to identify errors or anomalies in data processing. Reviewing user access rights for segregation is also a detective control, as it helps to detect any violations of segregation of duties principles.

References: ISACA, CISA Review Manual,
27th Edition, 2018, page 64

NEW QUESTION: 246

Due to the small size of the payroll department, an organization is unable to segregate the employee setup and payroll processing functions. Which of the following would be the BEST compensating control for the lack of segregation of duties?

- A. A payroll variance report is reviewed for anomalies every pay period
- B. A review is conducted to verify that terminated employees, are removed from the employee master file.
- C. The system is configured to require secondary approval for changes to the employee master file
- D. An independent payroll disbursement review is conducted

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 247

Which of the following should be an IS auditor's GREATEST concern when reviewing an organization's security controls for policy compliance?

- A. Security policies are not applicable across all business units
- B. End users are not required to acknowledge security policy training
- C. The security policy has not been reviewed within the past year
- D. Security policy documents are available on a public domain website

Answer: D ([LEAVE A REPLY](#))

Explanation

The auditor should be most concerned about the security policy documents being available on a public domain website. This is because this exposes the organization's security posture and strategy to potential attackers, who can exploit the information to launch targeted attacks or bypass the security controls. The security policy documents should be classified as confidential and protected from unauthorized access or disclosure. The other options are less severe than exposing the security policy documents to the public, although they may also indicate some gaps or weaknesses in the security policy development, implementation, or maintenance process.

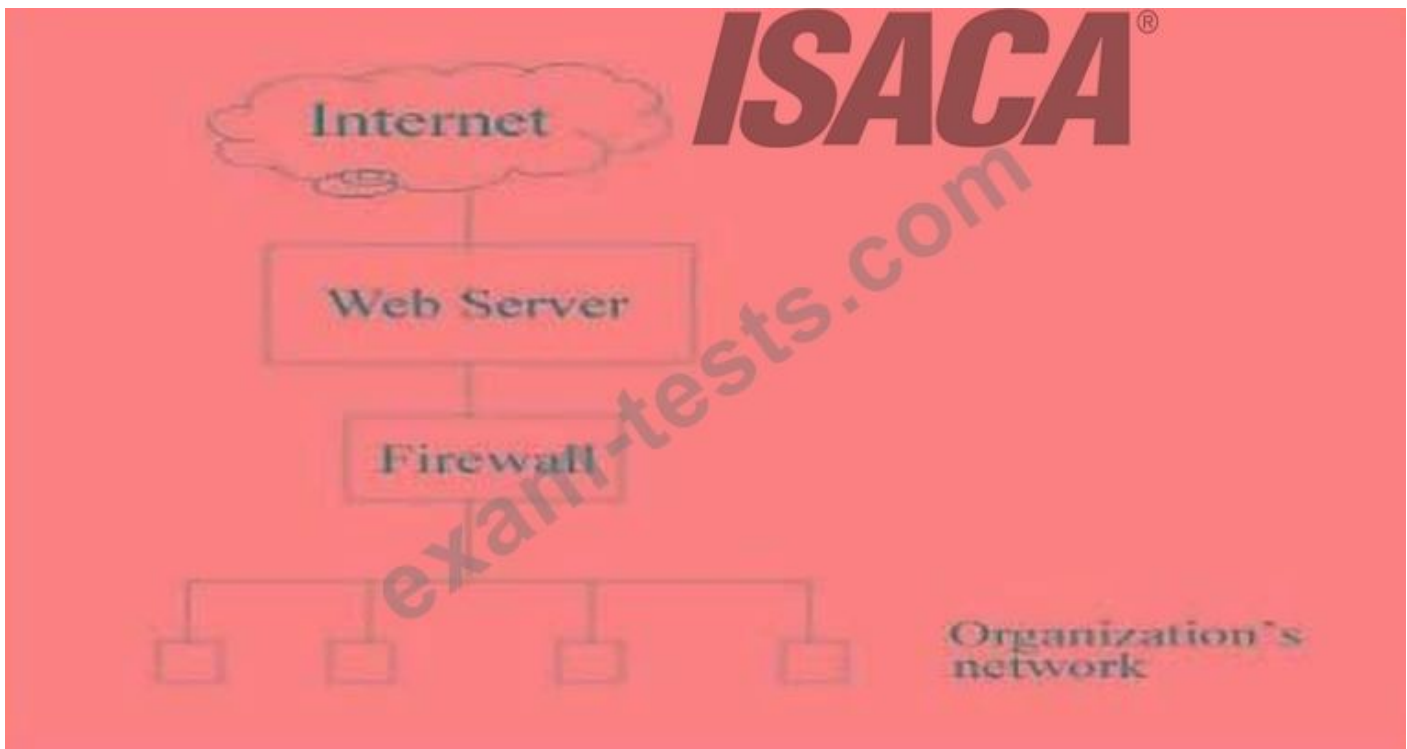
References:

CISA Review Manual (Digital Version), Chapter 5, Section 5.31
CISA Online Review Course, Domain 3, Module 1, Lesson 12

NEW QUESTION: 248

E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not

allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network.



The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

- A. alert the appropriate staff.
- B. create an entry in the log.
- C. close firewall-2.
- D. close firewall-1.

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Traffic for the internal network that did not originate from the mail gateway is a sign that firewall-1 is not functioning properly. This may have been caused by an attack from a hacker. Closing firewall-2 is the first thing that should be done, thus preventing damage to the internal network. After closing firewall-2, the malfunctioning of firewall-1 can be investigated. The IDS should trigger the closing of firewall-2 either automatically or by manual intervention. Between the detection by the IDS and a response from the system administrator valuable time can be lost, in which a hacker could also compromise firewall-2. An entry in the log is valuable for later analysis, but before that, the IDS should close firewall-2. If firewall-1 has already been compromised by a hacker, it might not be possible for the IDS to close it.

NEW QUESTION: 249

The activation of an enterprise's business continuity plan should be based on predetermined criteria that address the:

- A. duration of the outage.

- B. type of outage.
- C. probability of the outage.
- D. cause of the outage.

Answer: A ([LEAVE A REPLY](#))

The initiation of a business continuity plan (action) should primarily be based on the maximum period for which a business function can be disrupted before the disruption threatens the achievement of organizational objectives.

NEW QUESTION: 250

An IS auditor observes that a large number of departed employees have not been removed from the accounts payable system. Which of the following is MOST important to determine in order to assess the risk?

- A. The process for terminating access of departed employees
- B. The frequency of user access reviews performed by management
- C. The ability of departed employees to actually access the system
- D. The frequency of intrusion attempts associated with the accounts payable

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 251

At which stage of the software development life cycle should an organization identity privacy considerations?

- A. Testing
- B. Design
- C. Requirements
- D. Development

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 252

Which of the following issues associated with a data center's closed-circuit television (CCTV) surveillance cameras should be of MOST concern to an IS auditor?

- A. CCTV recordings are not regularly reviewed.
- B. CCTV cameras are not installed in break rooms
- C. CCTV records are deleted after one year.
- D. CCTV footage is not recorded 24 x 7.

Answer: A ([LEAVE A REPLY](#))

The most concerning issue associated with a data center's CCTV surveillance cameras is that the recordings are not regularly reviewed. This means that any unauthorized access, theft, vandalism, or other security incidents may go unnoticed and unreported. CCTV recordings are a valuable source of evidence and deterrence for data center security, and they should be monitored and audited periodically to ensure compliance with policies and regulations. If the

recordings are not reviewed, the data center may face legal, financial, or reputational risks in case of a security breach or an audit failure.

The other options are less concerning because they do not directly affect the security of the data center. CCTV cameras are not required to be installed in break rooms, as they are not critical areas for data protection. CCTV records can be deleted after one year, as long as they comply with the data retention policy of the organization and the applicable laws. CCTV footage does not need to be recorded 24 x 7, as long as there is sufficient coverage of the data center during operational hours and when access is granted to authorized personnel.

References:

- * ISACA Journal Article: Physical security of a data center¹
- * Data Center Security: Checklist and Best Practices | Kisi²
- * Video Surveillance Best Practices | Taylored Systems

NEW QUESTION: 253

Which of the following is the PRIMARY objective of a business impact analysis (BIA)?

- A. Define the recovery point objective (RPO).
- B. Analyze vulnerabilities.
- C. Confirm control effectiveness.
- D. Determine recovery priorities.

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 254

Following a discussion on the results of a recent audit engagement, the process owner of the audited area has provided an action plan addressing the gaps and recommendations. The auditor disagrees with some of the responses where the process owner is accepting a level of residual risk that is not within the organization's risk appetite. What is the auditor's BEST course of action?

- A. Escalate the situation to audit management.
- B. Accept the action plan proposed by the process owner.
- C. Inform executive management of the residual risk.
- D. Include the issue in the next report to the audit committee.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 255

The use of symmetric key encryption controls to protect sensitive data transmitted over a communications network requires that:

- A. primary keys for encrypting the data be stored in encrypted form.
- B. encryption keys be changed only when a compromise is detected at both ends.
- C. encryption keys at one end be changed on a regular basis.
- D. public keys be stored in encrypted form.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 256

In auditing a web server, an IS auditor should be concerned about the risk of individuals gaining unauthorized access to confidential information through:

- A. common gateway interface (CGI) scripts.
- B. enterprise Java beans (EJBs).
- C. applets.
- D. web services.

Answer: A ([LEAVE A REPLY](#))

Common gateway interface (CGI) scripts are executable machine independent software programs on the server that can be called and executed by a web server page. CGI performs specific tasks such as processing inputs received from clients. The use of CGI scripts needs to be evaluated, because as they run in the server, a bug in them may allow a user to gain unauthorized access to the server and from there gain access to the organization's network. Applets are programs downloaded from a web server and executed on web browsers on client machines to run any web-based applications. Enterprise java beans (EJBs) and web services have to be deployed by the web server administrator and are controlled by the application server. Their execution requires knowledge of the parameters and expected return values.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here: <https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 257

An IS auditor finds that the cost of developing an application is now projected to significantly exceed the budget. Which of the following is the GREATEST risk to communicate to senior management?

- A. Increased staff turnover
- B. Project abandonment
- C. Noncompliance with project methodology
- D. Inability to achieve expected benefits

Answer: B ([LEAVE A REPLY](#))

Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 258

Which of the following is MOST important for an effective control self-assessment (CSA) program?

- A. Determining the scope of the assessment
- B. Performing detailed test procedures
- C. Evaluating changes to the risk environment
- D. Understanding the business process

Answer: D ([LEAVE A REPLY](#))

Explanation

Understanding the business process is the most important factor for an effective control self-assessment (CSA) program. A CSA program is a technique that allows managers and work teams directly involved in business units, functions or processes to participate in assessing the organization's risk management and control processes¹. A CSA program can help identify risks and potential exposures to achieving strategic business objectives, evaluate the adequacy and effectiveness of controls, and implement remediation plans to address any gaps or weaknesses². To conduct a successful CSA, it is essential to have a clear and comprehensive understanding of the business process under review, including its objectives, inputs, outputs, activities, resources, dependencies, stakeholders, performance indicators, etc. This will help to identify the relevant risks and controls associated with the process, as well as to evaluate their impact and likelihood. Determining the scope of the assessment, performing detailed test procedures, and evaluating changes to the risk environment are also important factors for an effective CSA program, but not as important as understanding the business process. These factors are more related to the execution and monitoring phases of the CSA program, while understanding the business process is related to the planning and preparation phase. Without a solid understanding of the business process, the scope, testing, and evaluation of the CSA may not be accurate or complete.

References: ISACA CISA Review Manual 27th Edition, page 310

NEW QUESTION: 259

An organization performs both full and incremental database backups Which of the following will BEST enable full restoration in the event of the destruction of the data center?

- A. Transmit incremental backups to an offsite location daily.
- B. Rotate all backups to an offsite location daily
- C. Maintain full and incremental backups in a secure server room
- D. Move full backups to an offsite location weekly

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 260

Which of the following statements appearing in an organization's acceptable use policy BEST demonstrates alignment with data classification standards related to the protection of information assets?

- A. Any information assets transmitted over a public network must be approved by executive management.

- B.** All information assets must be encrypted when stored on the organization's systems.
- C.** Information assets should only be accessed by persons with a justified need.
- D.** All information assets will be assigned a clearly defined level to facilitate proper employee handling.

Answer: B (LEAVE A REPLY)

The statement that BEST demonstrates alignment with data classification standards related to the protection of information assets is D. All information assets will be assigned a clearly defined level to facilitate proper employee handling. Data classification involves categorizing information assets based on their sensitivity, importance, and usage. Assigning clearly defined levels (such as public, internal, confidential, etc.) to information assets ensures that appropriate security controls are applied based on their classification. By doing so, organizations can manage access, encryption, and other protective measures effectively¹².

References:

1. IFRC. "Information Security: Acceptable Use Policy."
1(<https://www.ifrc.org/sites/default/files/2021-11/IFRC-Information-Security-Acceptable-Use-Policy.pdf>)
2. UNSW Sydney. "Data Classification Standard."
2(<https://www.unsw.edu.au/content/dam/pdfs/governance/policy/2022-01-policies/datastandard.pdf>)
3. Digital Guardian. "What is a Data Classification Policy?"
3(<https://www.digitalguardian.com/blog/what-data-classification-policy>)
4. Microsoft Service Trust Portal. "Data classification & sensitivity label taxonomy."
4(<https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-classification-and-labels>)
5. Clark University ITS Policies. "Data Classification - Data Security Policies."
5(https://www2.clarku.edu/offices/its/policies/data_classification.cfm)

NEW QUESTION: 261

Which of the following PBX feature supports shared extensions among several devices, ensuring that only one device at a time can use an extension?

- A.** Call forwarding
- B.** Privacy release
- C.** Tenanting
- D.** Voice mail

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Privacy release supports shared extensions among several devices, ensuring that only one device at a time can use an extension.

For you exam you should know below mentioned PBX features and Risks:

System Features

Description

Risk

Automatic Call distribution

Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available Tapping and control of traffic Call forwarding Allow specifying an alternate number to which calls will be forwarded based on certain condition User tracking Account codes Used to:

Track calls made by certain people or for certain projects for appropriate billing Dial-In system access (user dials from outside and gain access to normal feature of the PBX) Changing the user class of service so a user can access a different set of features (i.e. the override feature) Fraud, user tracking, non authorized features Access Codes Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features

Silent Monitoring

Silently monitors other calls

Eavesdropping

Conferencing

Allows for conversation among several users

Eavesdropping, by adding unwanted/unknown parties to a conference
override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message

Eavesdropping Auto-answer Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off Gaining information not normally available, for various purpose Tenanting Limits system user access to only those users who belong to the same tenant group - useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc Illegal usage, fraud, eavesdropping Voice mail Stores messages centrally and - by using a password - allows for retrieval from inside or outside lines.

Disclosure or destruction of all messages of a user when that user's password is known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Privacy release

Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Eavesdropping

No busy extension

Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook Eavesdropping a conference in progress Diagnostics Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or

attendant diagnostics Fraud and illegal usage Camp-on or call waiting When activated, sends a visual audible warning to an off-hook instrument that is receiving another call.

Another option of this feature is to conference with the camped-on or call waiting Making the called individual a party to a conference without knowing it.

Dedicated connections

Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility Eavesdropping on a line

The following were incorrect answers:

Call forwarding - Allow specifying an alternate number to which calls will be forwarded based on certain condition Tenanting -Limits system user access to only those users who belong to the same tenant group - useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc Voice Mail -Stores messages centrally and - by using a password - allows for retrieval from inside or outside lines.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number358

NEW QUESTION: 262

Which of the following activities provides an IS auditor with the MOST insight regarding potential single person dependencies that might exist withing the organization?

- A. Reviewing vacation patterns
- B. Reviewing user activity logs
- C. Mapping IT processes to roles
- D. Interviewing senior IT management

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 263

The implementation of an IT governance framework requires that the board of directors of an organization:

- A. Approve the IT strategy.
- B. Be informed of all IT initiatives.
- C. Have an IT strategy committee.
- D. Address technical IT issues.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 264

An organization is migrating its HR application to an Infrastructure as a Service (IaaS) model in a private cloud. Who is PRIMARILY responsible for the security configurations of the deployed application's operating system?

- A. The cloud provider's external auditor
- B. The cloud provider

- C. The operating system vendor
- D. The organization

Answer: D ([LEAVE A REPLY](#))

The organization is primarily responsible for the security configurations of the deployed application's operating system when migrating its HR application to an Infrastructure as a Service (IaaS) model in a private cloud. This is because in an IaaS model, the cloud provider is responsible for the security of the underlying infrastructure that they lease to their customers, such as servers, storage, and networks, while the customer is responsible for the security of the areas of the cloud infrastructure over which they have control, such as operating systems, middleware, and applications. Therefore, the organization needs to ensure that the operating system is properly configured, patched, hardened, and monitored to protect the HR application from unauthorized access or malicious attacks.

The other options are not primarily responsible for the security configurations of the deployed application's operating system. The cloud provider's external auditor is not responsible for any security configurations, but rather for verifying and reporting on the cloud provider's compliance with relevant standards and regulations.

The cloud provider is responsible for the security of the underlying infrastructure, but not for the operating system or any software installed on it by the customer. The operating system vendor is responsible for providing updates and patches for the operating system, but not for configuring or securing it according to the customer's needs.

References:

- * 11: What Is IaaS (Infrastructure As A Service)? - Forbes
- * 12: What is Shared Responsibility Model? - Check Point Software
- * 13: Who Is Responsible for Cloud Security? - Security Intelligence

NEW QUESTION: 265

A government organization uses standard Wi-Fi Protected Access 2 (WPA2) to protect confidential information transmitted to a file server. Which of the following is the IS auditor's BEST recommendation to further strengthen security?

- A. Service set identifier (SSID) masking
- B. Certificate-based authentication
- C. Media access control (MAC) address filtering
- D. Network address translation (NAT)

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 266

Which of the following is an example of a control that is both detective and preventive at the same time?

- A. Detection of unauthorized activity in a database prevents further manipulation by the database administrator (DBA).

- B. A misconfiguration of an operating system is detected and future recurrence can successfully be prevented.
- C. A payment order to a sanctioned country is detected in the system before the payment is actually made.
- D. Detective fraud controls performed on past transactions prevent legal action being taken against the organization.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 267

When testing the adequacy of tape backup procedures, which step BEST verifies that regularly scheduled Backups are timely and run to completion?

- A. Observing the execution of a daily backup run
- B. Evaluating the backup policies and procedures
- C. Reviewing a sample of system-generated backup logs
- D. Interviewing key personnel evolved In the backup process

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 268

Which of the following provides the GREATEST assurance of message authenticity?

- A. Theprehash code is derived mathematically from the message being sent.
- B. Theprehash code is encrypted using the sender's private key.
- C. Theprehash code and the message are encrypted using the secret key.
- D. The sender attains the recipient's public key and verifies the authenticity of its digital certificate with a certificate authority.

Answer: B ([LEAVE A REPLY](#))

Encrypting the prehash code using the sender's private key provides assurance of the authenticity of the message. Mathematically deriving the prehash code provides integrity to the message. Encrypting the prehash code and the message using the secretkey provides confidentiality.

NEW QUESTION: 269

An IS audit reveals an IT application is experiencing poor performance including data inconsistency and integrity issues. What is the MOST likely cause?

- A. Database clustering
- B. Data caching
- C. Reindexing of the database table
- D. Load balancing

Answer: ([SHOW ANSWER](#))

Data caching is the most likely cause of poor performance, data inconsistency and integrity issues in an IT application, because it involves storing frequently accessed data in a temporary memory location (cache) to reduce the latency and bandwidth consumption of retrieving data from

the original source. However, data caching can also introduce problems such as stale data (when the cache is not updated with changes made to the original source), cache coherence (when multiple caches store copies of the same data and need to be synchronized), and cache corruption (when the cache is damaged or tampered with).

Database clustering is not a likely cause of poor performance, data inconsistency and integrity issues, because it involves distributing data across multiple servers or nodes to improve availability, scalability and load balancing of database operations. Database clustering can also enhance data consistency and integrity by using replication and synchronization mechanisms to ensure that all nodes have the same view of the data.

Reindexing of the database table is not a likely cause of poor performance, data inconsistency and integrity issues, because it involves rebuilding or reorganizing indexes on tables or views to improve query performance and reduce fragmentation of index pages. Reindexing can also improve data consistency and integrity by ensuring that indexes reflect the current state of the data in the tables or views.

Load balancing is not a likely cause of poor performance, data inconsistency and integrity issues, because it involves distributing workloads across multiple servers or resources to optimize resource utilization, throughput and response time of applications. Load balancing can also enhance data consistency and integrity by using algorithms and protocols to route requests to the most appropriate server or resource based on availability, capacity and performance.

References:

- * Data Caching
- * Database Clustering
- * Reindexing Database Tables in SQL Server
- * [Load Balancing]

NEW QUESTION: 270

When responding to an ongoing denial of service (DoS) attack, an organization's FIRST course of action should be to

- A.** analyze the attack path
- B.** restore service
- C.** investigate damage
- D.** minimize impact

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 271

An organization that has suffered a cyber-attack is performing a forensic analysis of the affected users' computers. Which of the following should be of GREATEST concern for the IS auditor reviewing this process?

- A.** An imaging process was used to obtain a copy of the data from each computer.
- B.** The legal department has not been engaged.
- C.** The chain of custody has not been documented.

D. Audit was only involved during extraction of the Information

Answer: C (LEAVE A REPLY)

The chain of custody has not been documented is a finding that should be of greatest concern for an IS auditor reviewing a forensic analysis process of an organization that has suffered a cyber attack. The chain of custody is a record of who handled, accessed, or modified the evidence during a forensic investigation.

Documenting the chain of custody is essential to preserve the integrity, authenticity, and admissibility of the evidence in a court of law. The other options are less concerning findings that may not affect the validity or reliability of the forensic analysis process. References:

* CISA Review Manual (Digital Version), Chapter 7, Section 7.51

* CISA Review Questions, Answers & Explanations Database, Question ID 220

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 272

planning an end-user computing (EUC) audit, it is MOST important for the IS auditor to

- A. evaluate EUC threats and vulnerabilities
- B. determine EUC materiality and complexity thresholds
- C. evaluate the organization's EUC policy
- D. obtains an inventory EUC applications

Answer: (SHOW ANSWER)

NEW QUESTION: 273

Which of the following should be an IS auditor's PRIMARY focus when evaluating the response process for cyber crimes?

- A. Notification to regulators
- B. Communication with law enforcement
- C. Evidence collection
- D. Root cause analysis

Answer: (SHOW ANSWER)

Section: The process of Auditing Information System

NEW QUESTION: 274

Which of the following will BEST ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure?

- A. Rotating backup copies of transaction files offsite
- B. Ensuring bisynchronous capabilities on all transmission lines
- C. Maintaining system console logs in electronic format
- D. Using a database management system (DBMS) to dynamically back-out partially processed transactions

Answer: D ([LEAVE A REPLY](#))

Using a DBMS to dynamically back-out partially processed transactions allows for the rollback of transactions that were only partially completed before the system failure. It ensures that the data remains consistent and eliminates any incomplete or inconsistent data that may have been created during the system failure.

NEW QUESTION: 275

Which of the following types of environmental equipment will MOST likely be deployed below the floor tiles of a data center?

- A. Temperature sensors
- B. Humidity sensors
- C. Water sensors
- D. Air pressure sensors

Answer: ([SHOW ANSWER](#)**)**

Water sensors are devices that can detect the presence of water or moisture in a given area.

They are often deployed below the floor tiles of a data center to monitor for any water leaks that may damage the equipment or cause electrical hazards. Water sensors can alert the data center staff or trigger an automatic response to prevent or mitigate the water leakage.

The other options are not likely to be deployed below the floor tiles of a data center. Temperature sensors and humidity sensors are usually deployed above the floor tiles to measure the ambient conditions of the data center and ensure optimal cooling and ventilation. Air pressure sensors are typically deployed at the air vents or ducts to monitor the airflow and pressure distribution in the data center.

References:

- * Data Center Environmental Monitoring
- * Water Detection in Data Centers

NEW QUESTION: 276

Which of the following is MOST important for an IS auditor to consider when performing the risk assessment prior to an audit engagement?

- A. The design of controls
- B. Industry standards and best practices
- C. The results of the previous audit
- D. The amount of time since the previous audit

Answer: C ([LEAVE A REPLY](#))

The results of the previous audit are an important source of information for an IS auditor to consider when performing the risk assessment prior to an audit engagement, as they can provide insights into the current state and performance of the auditee, identify any issues or gaps that need to be followed up or addressed, and highlight any areas that require special attention or focus. The design of controls is an important factor to evaluate during an audit engagement, but it is not the most important thing to consider when performing the risk assessment prior to an audit engagement, as it does not reflect the actual implementation or effectiveness of the controls. Industry standards and best practices are useful benchmarks or guidelines for an IS auditor to compare or measure against during an audit engagement, but they are not the most important thing to consider when performing the risk assessment prior to an audit engagement, as they may not be applicable or relevant to the specific context or objectives of the auditee. The amount of time since the previous audit is a relevant criterion to determine the frequency or timing of an audit engagement, but it is not the most important thing to consider when performing the risk assessment prior to an audit engagement, as it does not indicate the level or nature of risk associated with the auditee.

NEW QUESTION: 277

Which of the following BEST enables an organization to verify whether an encrypted message sent by a client has been altered?

- A. The digital signature
- B. The sender's private key
- C. The message header
- D. The date and time stamp of the received message

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 278

Validated digital signatures in an e-mail software application will:

- A. help detect spam.
- B. provide confidentiality.
- C. add to the workload of gateway servers.
- D. significantly reduce available bandwidth.

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

Validated electronic signatures are based on qualified certificates that are created by a certification authority (CA), with the technical standards required to ensure the key can neither be forced nor reproduced in a reasonable time. Such certificates are only delivered through a registration authority (RA) after a proof of identity has been passed. Using strong signatures in e-mail traffic, nonrepudiation can be assured and a sender can be tracked. The recipient can configure their e-mail server or client to automatically delete e-mails from specific senders. For

confidentiality issues, one must use encryption, not a signature, although both methods can be based on qualified certificates. Without any filters directly applied on mail gateway servers to block traffic without strong signatures, the workload will not increase.

Using filters directly on a gateway server will result in an overhead less than antivirus software imposes.

Digital signatures are only a few bytes in size and will not slash bandwidth. Even if gateway servers were to check CRLs, there is little overhead.

NEW QUESTION: 279

An IS auditor is evaluating an organization's IT strategy and plans. Which of the following would be of GREATEST concern?

- A. There is not a defined IT security policy.
- B. The business strategy meeting minutes are not distributed.
- C. IT is not engaged in business strategic planning.
- D. There is inadequate documentation of IT strategic planning.

Answer: C ([LEAVE A REPLY](#))

Explanation

The greatest concern for an IS auditor when evaluating an organization's IT strategy and plans is that IT is not engaged in business strategic planning, as this indicates a lack of alignment between IT and business objectives, which could result in inefficient and ineffective use of IT resources and capabilities. The absence of a defined IT security policy, the nondistribution of business strategy meeting minutes, and the inadequate documentation of IT strategic planning are also issues that should be addressed by an IS auditor, but they are not as significant as IT's noninvolvement in business strategic planning. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.1

NEW QUESTION: 280

Which of the following is the PRIMARY advantage of using virtualization technology for corporate applications?

- A. Stronger data security
- B. Improved disaster recovery
- C. Better utilization of resources
- D. Increased application performance

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 281

During a follow-up audit, an IS auditor finds that senior management has implemented a different remediation action plan than what was previously agreed upon. Which of the following is the auditor's BEST course of action?

- A. Evaluate the implemented control to ensure it mitigates the risk to an acceptable level.
- B. Request justification from management for not implementing the recommended control.

- C. Report the deviation by the control owner in the audit report.
- D. Cancel the follow-up audit and reschedule for the next audit period.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 282

Identify the WAN message switching technique being used from the description presented below:
"Data is routed in its entirety from the source node to the destination node, one hop at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, this WAN switching technology stores and delays the message until ample resources become available for effective transmission of the message. "

- A. Message Switching
- B. Packet switching
- C. Circuit switching
- D. Virtual Circuits

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

For your exam you should know below information about WAN message transmission technique:

Message Switching

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hop at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Message Switching

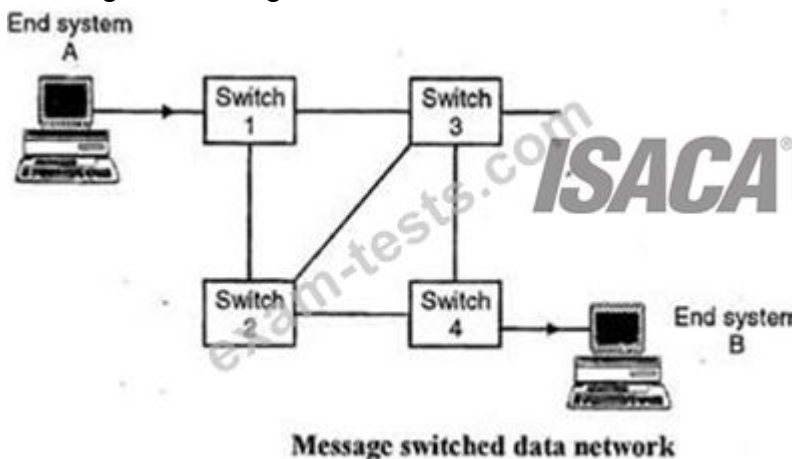


Image from: <http://ecomputernotes.com/images/Message-Switched-data-Network.jpg> Packet Switching

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.

Packet Switching

The original message is Green, Blue, Red.

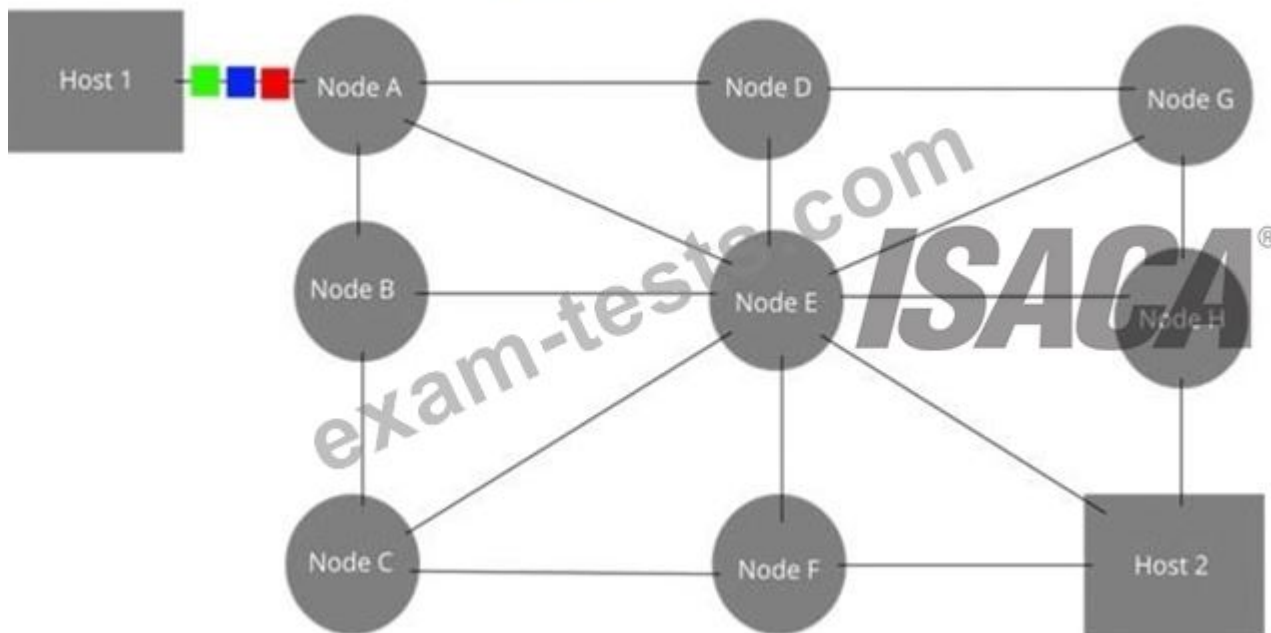


Image from: http://upload.wikimedia.org/wikipedia/commons/f/f6/Packet_Switching.gif Circuit Switching

Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays.

No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Circuit Switching

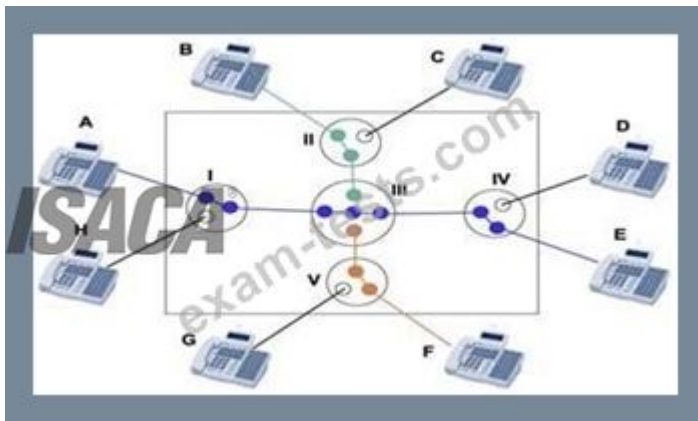


Image from: http://www.louiewong.com/wp-content/uploads/2010/09/Circuit_Switching.jpg See a table below comparing Circuit Switched versus Packet Switched networks:

Difference between Circuit and packet switching

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Image from: <http://www.hardware-one.com/reviews/network-guide-2/images/packet-vs-circuit.gif>

Virtual circuit

In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames. Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes,

varying bit rate generated by the application,

varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:

The other options presented are not valid choices.

The following reference(s) were/was used to create this question:

NEW QUESTION: 283

Which of the following is the MOST important consideration for an IS auditor when reviewing a vendor selection process?

- A. The lowest price possible was obtained for vendor services rendered
- B. Vendors were assessed and assigned a ranking during the selection process
- C. Responsible managers were assigned to monitor vendor performance
- D. Security and regulatory concerns were identified as part of the selection process

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 284

Due to a high volume of customer orders, an organization plans to implement a new application for customers to use for online ordering. Which type of testing is MOST important to ensure the security of the application prior to go-live?

- A. Stress testing
- B. User acceptance testing (UAT)
- C. Vulnerability testing
- D. Regression testing

Answer: A ([LEAVE A REPLY](#))

Stress testing is one of the most useful software testing procedures since it helps the team to assure the product's performance. Furthermore, it verifies the software's security, dependability, and error-handling capabilities, further enhancing its quality.

NEW QUESTION: 285

When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:

- A. allow changes, which will be completed using after-the-fact follow-up.
- B. allow undocumented changes directly to the production library.
- C. do not allow any emergency changes.
- D. allow programmers permanent access to production programs.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

There may be situations where emergency fixes are required to resolve system problems. This involves the use of special logon IDs that grant programmers temporary access to production programs during emergency situations. Emergency changes should be completed using after-the-fact follow-up procedures, which ensure that normal procedures are retroactively applied; otherwise, production may be impacted. Changes made in this fashion should be held in an emergency library from where they can be moved to the production library, following the normal

change management process. Programmers should not directly alter the production library nor should they be allowed permanent access to production programs.

NEW QUESTION: 286

Which of the following practices is MOST helpful in eliminating potential bias during the vendor proposal review process?

- A. A procurement professional is the point of contact for all vendors responding with proposals.
- B. The services of an internal or external auditor are available when vendor proposals are reviewed.
- C. The project sponsor is available to all vendors to explain proposal requirements.
- D. Internal software development teams are not permitted to provide proposals to the project.

Answer: ([SHOW ANSWER](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 287

In a client-server architecture, a domain name service (DNS) is MOST important because it provides the:

- A. address of the domain server.
- B. resolution service for the name/address.
- C. IP addresses for the internet.
- D. domain name system.

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

DNS is utilized primarily on the Internet for resolution of the name/address of the web site. It is an Internet service that translates domain names into IP addresses. As names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time a domain name is used, a DNS service must translate the name into the corresponding IP address. The DNS system has its own network, if one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

NEW QUESTION: 288

An employee who denies accusations of sending inappropriate images to other employees has been discharged. For evidential purposes, the mail database for the discharged employee's computer should be:

- A. deleted as it could subject the organization to further legal liability
- B. impounded by physically removing the disk drive
- C. backed up to the server, where its access can be tightly restricted
- D. copied to write-once, read-many media using the computer's OS tools

Answer: C ([LEAVE A REPLY](#))

Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 289

Which of the following is the MOST efficient solution for a multi-location healthcare organization that wants to be able to access patient data wherever patients present themselves for care?

- A. Network segmentation
- B. Infrastructure as a Service (IaaS) provider
- C. Software as a Service (SaaS) provider
- D. Dynamic localization

Answer: C ([LEAVE A REPLY](#))

The most efficient solution for a multi-location healthcare organization that wants to be able to access patient data wherever patients present themselves for care is B. Software as a Service (SaaS) provider. SaaS providers offer cloud-based services that allow organizations to access applications, data, and infrastructure on demand, making it easier to access patient data no matter where the patient is located. Reference: ISACA CISA Study Manual, section 5.3.3.1.

NEW QUESTION: 290

An organization is considering connecting a critical PC-based system to the Internet. Which of the following

would provide the BEST protection against hacking?

- A. An application-level gateway
- B. A remote access server
- C. A proxy server
- D. Port scanning

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

An application-level gateway is the best way to protect against hacking because it can define with detail

rules that describe the type of user or connection that is or is not permitted, it analyzes in detail each

package, not only in layers one through four of the OSI model but also layers five through seven, which

means that it reviews the commands of each higher-level protocol (HTTP, FTP, SNMP, etc.). For a remote access server, there is a device (server) that asks for a username and password before entering the network. This is good when accessing private networks, but it can be mapped or scanned from the Internet creating security exposure. Proxy servers can provide protection based on the IP address and ports. However, an individual is needed who really knows how to do this, and applications can use different ports for the different sections of the program. Port scanning works when there is a very specific task to complete, but not when trying to control what comes from the Internet, or when all the ports available need to be controlled. For example, the port for Ping (echo request) could be blocked and the IP addresses would be available for the application and browsing, but would not respond to Ping.

NEW QUESTION: 291

When should systems administrators first assess the impact of applications or systems patches?

- A.** Within five business days following installation
- B.** Prior to installation
- C.** No sooner than five business days following installation
- D.** Immediately following installation

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Systems administrators should always assess the impact of patches before installation.

NEW QUESTION: 292

During the walk-through procedures for an upcoming audit, an IS auditor notes that the key application in scope is part of a Software as a Service (SaaS) agreement. What should the auditor do NEXT?

- A.** Verify whether IT management monitors the effectiveness of the environment.
- B.** Verify whether a right-to-audit clause exists.
- C.** Verify whether a third-party security attestation exists.
- D.** Verify whether service level agreements (SLAs) are defined and monitored.

Answer: B ([LEAVE A REPLY](#))

The auditor should verify whether a right-to-audit clause exists (B) next, because it is a contractual provision that grants the auditor the right to access and examine the records, systems, and processes of the SaaS provider. A right-to-audit clause is important for ensuring transparency, accountability, and compliance of the SaaS provider with the customer's

requirements and expectations. A right-to-audit clause can also help the auditor to identify and mitigate any risks or issues related to the SaaS agreement¹².

Verifying whether IT management monitors the effectiveness of the environment (A) is not the next step, because it is a part of the ongoing monitoring and evaluation process, not the initial walk-through procedures.

The auditor should first establish the scope, objectives, and criteria of the audit before assessing the performance and controls of the SaaS provider.

Verifying whether a third-party security attestation exists © is not the next step, because it is not a mandatory requirement for a SaaS agreement. A third-party security attestation is a report or certificate issued by an independent auditor that evaluates and validates the security controls and practices of the SaaS provider. A third-party security attestation can provide assurance and confidence to the customer, but it does not replace or eliminate the need for a right-to-audit clause³.

Verifying whether service level agreements (SLAs) are defined and monitored (D) is not the next step, because it is not directly related to the audit process. SLAs are contractual agreements that specify the quality, availability, and performance standards of the SaaS provider. SLAs are important for measuring and managing the service delivery and customer satisfaction, but they do not grant or guarantee the right to audit⁴.

NEW QUESTION: 293

Which of the following BEST helps data loss prevention (DLP) tools detect movement of sensitive data in transit?

- A. Network traffic logs
- B. Deep packet inspection
- C. Data inventory
- D. Proprietary encryption

Answer: B (LEAVE A REPLY)

Deep packet inspection (DPI) is a core capability of data loss prevention (DLP) tools that allows the analysis of the content of data packets in transit. This helps detect the unauthorized movement of sensitive data by examining packet-level details.

* Network Traffic Logs (Option A): These provide historical data but do not actively detect data in transit.

* Data Inventory (Option C): Useful for identifying where sensitive data resides but not for monitoring its movement.

* Proprietary Encryption (Option D): Protects data but does not detect unauthorized transmission.

Reference: ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 294

Which of the following findings should be of GREATEST concern to an IS auditor performing a review of IT operations?

- A. The job scheduler application has not been designed to display pop-up error messages.

- B.** Access to the job scheduler application has not been restricted to a maximum of two staff members
- C.** Operations shift turnover logs are not utilized to coordinate and control the processing environment
- D.** Changes to the job scheduler application's parameters are not approved and reviewed by an operations supervisor

Answer: D ([LEAVE A REPLY](#))

Changes to the job scheduler application's parameters are not approved and reviewed by an operations supervisor. This is a serious control weakness that could compromise the integrity, availability, and security of the IT operations. An IS auditor should be concerned about the lack of oversight and accountability for such changes, which could result in unauthorized, erroneous, or malicious modifications that affect the processing environment. The other options are less critical issues that may not have a significant impact on the IT operations. References:

* CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3.11

* CISA Review Questions, Answers & Explanations Database, Question ID 202

NEW QUESTION: 295

Identify the payment model from description presented below:

A users write an electronic check, which is digitally signed with instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

- A.** Electronic Money Model
- B.** Electronics Checks model
- C.** Electronic transfer model
- D.** Electronic withdraw model

Answer: B ([LEAVE A REPLY](#))

Section: Information System Acquisition, Development and Implementation Explanation:

Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

For CISA exam you should know below information about payment systems

There are two types of parties involved in all payment systems - the issuer and the user. An issuer is an entity that operates the payment service. An issuer holds the items that the payment represents. The user of the payment service performs two main functions- making payments and receiving payments - and therefore can be described as a payer or payee receptively.

Electronic Money Model - The objective of electronic money systems is emulating physical cash. An issuer attempts to do this by creating digital certificates, which are then purchased by users who redeem them with the issuer at a later date. In the interim, certificates can be transferred

among users to trade for goods or services. For the certificate to take on some of the attributes of physical cash, certain techniques are used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the certificate. This provides an electronic certificate with unconditional uncertainty.

Electronic Check Model - Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

Electronic Transfer Model - Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

The following were incorrect answers:

Electronic Money Model - The objective of electronic money systems is emulating physical cash. An issuer attempts to do this by creating digital certificates, which are then purchased by users who redeem them with the issuer at a later date. In the interim, certificates can be transferred among users to trade for goods or services. For the certificate to take on some of the attributes of physical cash, certain techniques are used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the certificate. This provides an electronic certificate with unconditional uncertainty.

Electronic Transfer Model - Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

Electronic Withdraw Model - Not a valid type of payment system.

Reference:

CISA review manual 2014 Page number 183

NEW QUESTION: 296

Which of the following IT resource management practices is MOST Important for an IS auditor to verify when evaluating third-party outsourcing relationships?

- A. Service level agreements (SLAs) in external contracts are monitored.
- B. Operational level agreements (OLAs) for departments and projects are monitored
- C. Management regularly meets with the service provider
- D. An IT strategy for dividing activities among multiple suppliers is in place.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 297

Which of the following would BEST help prioritize various projects in an organization's IT portfolio?

- A. Total cost of ownership (TCO)
- B. Enterprise architecture (EA)
- C. Industry trends
- D. Business cases

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 298

An IS auditor identifies that a legacy application to be decommissioned in three months cannot meet the security requirements established by the current policy.

What is the BEST way for the auditor to address this issue?

- A. Verify management has approved a policy exception to accept the risk.
- B. Take no action since the application will be decommissioned in three months.
- C. Inform the IT director of the policy noncompliance.
- D. Recommend the application be patched to meet requirements.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 299

Which of the following should an IS auditor review FIRST when evaluating incident management procedures?

- A. Command center monitoring
- B. Root cause analysis steps
- C. Prioritization criteria
- D. Peer review requirements

Answer: C ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

NEW QUESTION: 300

Which of the following BEST indicates that the effectiveness of an organization's security awareness program has improved?

- A. A decrease in the number of information security audit findings
- B. An increase in the number of staff who complete awareness training
- C. An increase in the number of phishing emails reported by employees
- D. A decrease in the number of malware outbreaks

Answer: C ([LEAVE A REPLY](#))

The effectiveness of an organization's security awareness program can be measured by capturing data on changes in the way people react to threats, such as the ability to recognize and avoid social engineering attacks¹. An increase in the number of phishing emails reported by employees indicates that they are more aware of the signs and risks of phishing, and are more likely to take appropriate actions to prevent or mitigate the impact of such attacks²³.

References

1: The Importance Of Measuring Security Awareness 2: Measuring the effectiveness of your security awareness program 3: How effective is security awareness training?

The effectiveness of an organization's security awareness program can be measured by capturing data on changes in the way people react to threats, such as the ability to recognize and avoid social engineering attacks¹. An increase in the number of phishing emails reported by employees indicates that they are more aware of the signs and risks of phishing, and are more likely to take appropriate actions to prevent or mitigate the impact of such attacks²³.

References

1: The Importance Of Measuring Security Awareness 2: Measuring the effectiveness of your security awareness program 3: How effective is security awareness training?

NEW QUESTION: 301

Following a recent internal data breach, an IS auditor was asked to evaluate information security practices within the organization. Which of the following findings would be MOST important to report to senior management?

- A. Users lack technical knowledge related to security and data protection
- B. Desktop passwords do not require special characters
- C. Security education and awareness workshops have not been completed
- D. Employees are not required to sign a non-compete agreement.

Answer: D ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 302

Which of the following provides the BEST assurance that a new process for purging transactions does not have a detrimental impact on the integrity of the database?

- A. Assessing the design of triggers
- B. Analyzing the database structure
- C. Reviewing results of the process in a test environment
- D. Reviewing the entity relationship diagram of the database

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 303

An organization has implemented application whitelisting in response to the discovery of a large amount of unapproved software. Which type of control has been deployed?

- A. Directive
- B. Preventive
- C. Detective
- D. Corrective

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 304

An IS auditor should be concerned when a telecommunication analyst:

- A. monitors systems performance and tracks problems resulting from program changes.
- B. reviews network load requirements in terms of current and future transaction volumes.
- C. assesses the impact of the network load on terminal response times and network data transfer rates.
- D. recommends network balancing procedures and improvements.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

The responsibilities of a telecommunications analyst include reviewing network load requirements in terms of current and future transaction volumes {choice B}, assessing the impact of network load or terminal response times and network data transferrates (choice C), and recommending network balancing procedures and improvements (choice D). Monitoring systems performance and tracking problems as a result of program changes {choice A} would put the analyst in a self-monitoring role.

NEW QUESTION: 305

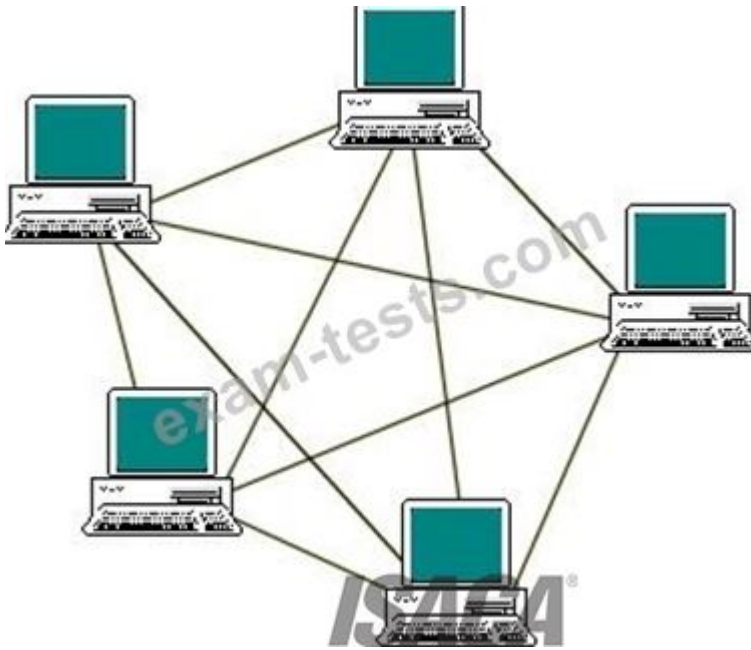
Several unattended laptops containing sensitive customer data were stolen from personnel offices Which of the following would be an IS auditor's BEST recommendation to protect data in case of recurrence?

- A. Require the use of cable locks
- B. Encrypt the disk drive
- C. Require two-factor authentication
- D. Enhance physical security

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 306

Identify the network topology from below diagram presented below:



Network Topology

- A. Bus
- B. Star
- C. Ring
- D. Mesh

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

For your exam you should know the information below related to LAN topologies:

LAN Topologies

Network topology is the physical arrangement of the various elements (links, nodes, etc.) of a computer network.

Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design.

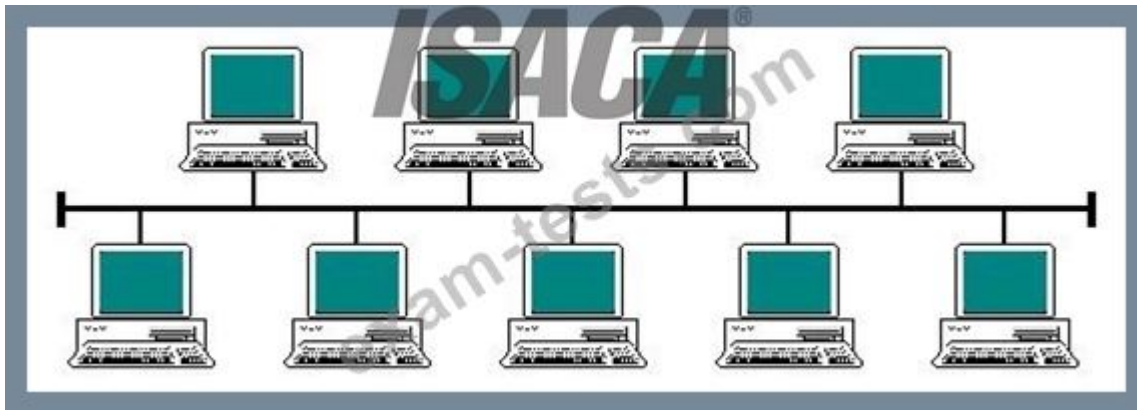
Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Bus

In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of

failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down.

Bus topology



Graphic from:

http://www.technologyuk.net/telecommunications/networks/images/bus_topology.gif Linear bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) - all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium - the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

Star

In local area networks with a star topology, each network host is connected to a central point with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device.

All traffic that traverses the network passes through the central point. The central point acts as a signal repeater.

The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the central point represents a single point of failure.

Star Topology

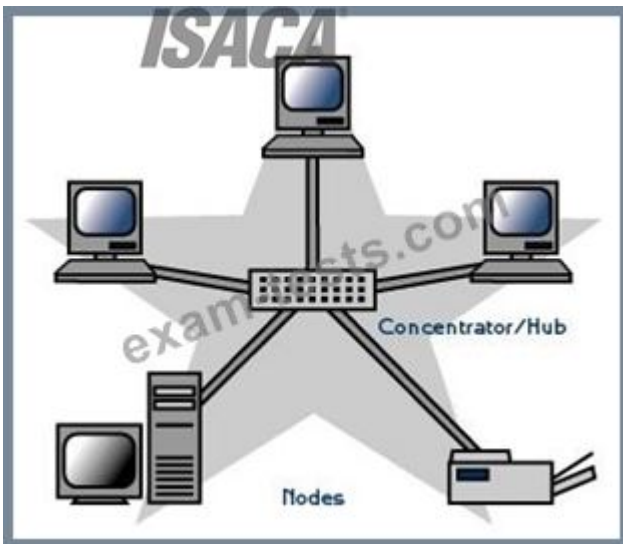


Image from: <http://fcit.usf.edu/network/chap5/pics/star.gif>

Ring

A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring.

The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link. If one node goes down the whole link would be affected.

Ring Topology

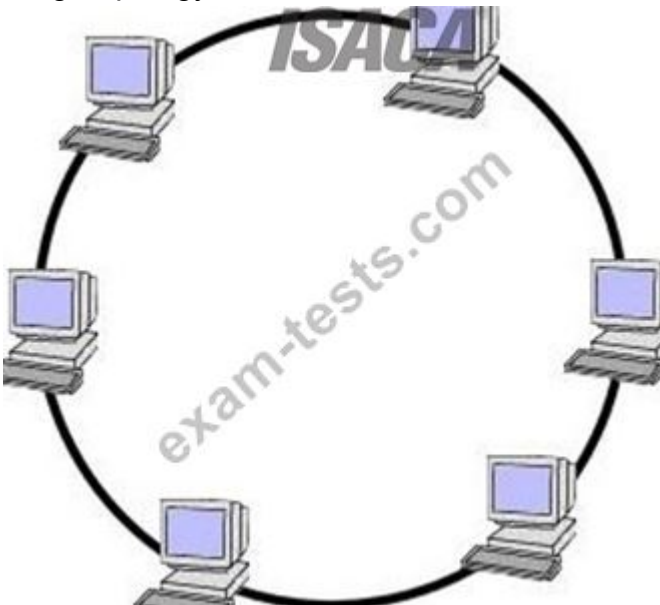


Image from: <https://forrester-infosystems.wikispaces.com/>

Mesh

The value of a fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

A mesh network provides for high availability and redundancy. However, the cost of such network could be very expensive if dozens of devices are in the mesh.

Mesh Topology

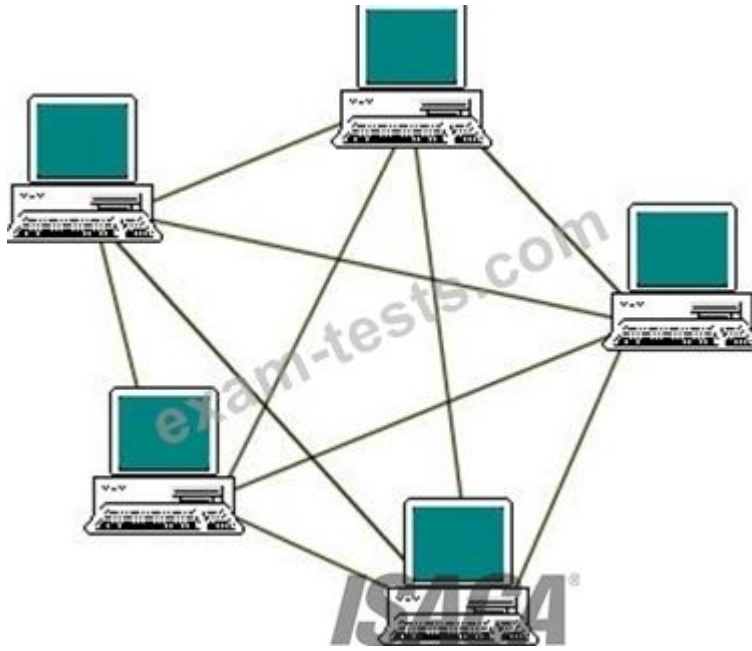


Image from:

http://www.technologyuk.net/telecommunications/networks/images/mesh_topology.gif Fully connected mesh topology

A fully connected network is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network doesn't need to use switching nor broadcasting. However, its major disadvantage is that the number of connections grows quadratic ally with the number of nodes, so it is extremely impractical for large networks. A two-node network is technically a fully connected network.

Partially connected mesh topology

The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link - this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.

The following answers are incorrect:

The other options presented are not valid.

The following reference(s) were/was used to create this question:

CISA review manual 2014, Page number 262

NEW QUESTION: 307

The MOST effective biometric control system is the one:

- A. which has the highest equal-error rate (EER).
- B. which has the lowest EER.
- C. for which the false-rejection rate (FRR) is equal to the false-acceptance rate (FAR).
- D. for which the FRR is equal to the failure-to-enroll rate (FER).

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

The equal-error rate (EER) of a biometric system denotes the percent at which the false-acceptance rate

(FAR) is equal to the false-rejection rate (FRR). The biometric that has the lowest EER is the most

effective. The biometric that has the highest EER is the most ineffective. For any biometric, there will be a

measure at which the FRR will be equal to the FAR. This is the EER. FER is an aggregate measure of

FRR.

NEW QUESTION: 308

The PRIMARY purpose of running a new system in parallel s to:

- A. provide the basis for comprehensive unit and system testing.
- B. resolve any errors in the program and file interfaces.
- C. determine which of the two systems is more efficient and effective.
- D. validate the operation of the new system against its predecessor.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 309

Which of the following attack techniques will succeed because of an inherent security weakness in an Internet firewall?

- A. Phishing
- B. Using a dictionary attack of encrypted passwords
- C. Intercepting packets and viewing passwords
- D. Flooding the site with an excessive number of packets

Answer: ([SHOW ANSWER](#)**)**

Explanation

Flooding the site with an excessive number of packets is an attack technique that will succeed because of an inherent security weakness in an Internet firewall. This type of attack is also known as a denial-of-service (DoS) attack or a distributed denial-of-service (DDoS) attack if it involves multiple sources. The aim of this attack is to overwhelm the network bandwidth or the processing capacity of the firewall or the target system, rendering it unable to respond to legitimate requests or perform its normal functions. An Internet firewall is a device or software that monitors and controls incoming and outgoing network traffic based on predefined rules. A firewall can block or allow traffic based on various criteria, such as source address, destination address, port number, protocol type, application type, etc. However, a firewall cannot prevent traffic from reaching its interface or distinguish between legitimate and malicious traffic based on its content or behavior. Therefore, a firewall is vulnerable to flooding attacks that exploit its limited resources. Phishing is an attack technique that involves sending fraudulent emails or messages that appear to come

from legitimate sources, such as banks, government agencies, online services, etc., in order to trick recipients into revealing their personal or financial information, such as passwords, credit card numbers, bank account details, etc., or into clicking on malicious links or attachments that can infect their systems with malware or ransomware.

Phishing does not exploit an inherent security weakness in an Internet firewall, but rather exploits human psychology and social engineering techniques. A firewall cannot prevent phishing emails or messages from reaching their intended targets, unless they contain some identifiable features that can be filtered out by the firewall rules. However, a firewall cannot detect or prevent users from responding to phishing emails or messages or from opening malicious links or attachments. Using a dictionary attack of encrypted passwords is an attack technique that involves trying to guess or crack passwords by using a list of common or likely passwords or by using a brute-force method that tries all possible combinations of characters. This type of attack does not exploit an inherent security weakness in an Internet firewall, but rather exploits weak or poorly chosen passwords or weak encryption algorithms. A firewall cannot prevent a dictionary attack of encrypted passwords, unless it has some mechanisms to detect and block repeated or suspicious login attempts or to enforce strong password policies. However, a firewall cannot protect passwords from being stolen or intercepted by other means, such as phishing, malware, keylogging, etc. Intercepting packets and viewing passwords is an attack technique that involves capturing and analyzing network traffic that contains sensitive information, such as passwords, credit card numbers, bank account details, etc., in order to use them for malicious purposes. This type of attack does not exploit an inherent security weakness in an Internet firewall, but rather exploits insecure or unencrypted network communication protocols or channels. A firewall cannot prevent packets from being intercepted and viewed by unauthorized parties, unless it has some mechanisms to encrypt or obfuscate the network traffic or to authenticate the source and destination of the traffic. However, a firewall cannot protect packets from being modified or tampered with by other means, such as man-in-the-middle attacks, replay attacks, etc.

References: ISACA CISA Review Manual 27th Edition, page 300

NEW QUESTION: 310

Which of the following application input controls would MOST likely detect data input errors in the customer account number field during the processing of an accounts receivable transaction?

- A. Validity check
- B. Reasonableness check
- C. Parity check
- D. Limit check

Answer: A ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 311

Which of the following provides the MOST assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system?

- A. Comparing code between old and new systems
- B. Loading balance and transaction data to the new system
- C. Running historical transactions through the new system
- D. Reviewing quality assurance (QA) procedures

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 312

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

- A. User management
- B. Project steering committee
- C. IT management
- D. Systems developers

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

User management assumes ownership of a systems-development project and the resulting system.

NEW QUESTION: 313

What type of fire-suppression system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities?

- A. A dry-pipe sprinkler system
- B. A deluge sprinkler system
- C. A wet-pipe system
- D. A halon sprinkler system

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

A dry-pipe sprinkler system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities.

NEW QUESTION: 314

When developing a business continuity plan (BCP), which of the following steps should be completed FIRST?

- A. Ensure that offsite backups can be efficiently restored.
- B. Identify alternatives to critical applications.
- C. Review the business continuity insurance policy.
- D. Carry out a risk assessment.

Answer: (SHOW ANSWER)

Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 315

Which of the following would provide the BEST evidence of the adequacy of firewall rules?

- A. Performing penetration tests
- B. Reviewing intrusion detection system (IDS) logs
- C. Reviewing network logs
- D. Verifying firewall configuration

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 316

An IS auditor reviewing an organization's IT strategic plan should FIRST review:

- A. the existing IT environment.
- B. the business plan.
- C. the present IT budget.
- D. current technology trends.

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, an IS auditor would first need to familiarize themselves with the business plan.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 317

Which of the following is the MOST important factor when determining the frequency of information security risk reassessment?

- A. Audit findings
- B. Risk priority
- C. Mitigating controls
- D. Risk metrics

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

NEW QUESTION: 318

Which of the following is the MOST important reason to periodically review data that has already been classified?

- A. Older data may need to be archived on removable media.
- B. The classification nomenclature has changed.
- C. The associated risk may change over time.
- D. Additional data may have been added to the inventory.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 319

An IS auditor learns of a new regulation which imposes penalties based on the number of individuals whose personally identifiable information (PII) is exposed by a security breach. What would be the BEST recommendation to help the organization limit the liability associated with a breach to its customer information database?

- A. Database optimization
- B. Database harmonization
- C. Database normalization
- D. Database segmentation

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 320

Which of the following is the BEST way to ensure that an application is performing according to its specifications?

- A. Unit testing
- B. Pilot testing
- C. System testing
- D. Integration testing

Answer: ([SHOW ANSWER](#)**)**

Explanation

Integration testing is the best way to ensure that an application is performing according to its specifications, because it tests the interaction and compatibility of different modules or components of the application. Unit testing, pilot testing and system testing are also important, but they do not cover the whole functionality and integration of the application as well as integration testing does. References: CISA Review Manual (Digital Version)¹, Chapter 4, Section 4.2.3

NEW QUESTION: 321

In a typical system development life cycle (SDLC), which group is PRIMARILY responsible for confirming compliance with requirements?

- A. Internal audit
- B. Quality assurance (QA)
- C. Steering committee

D. Risk management

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 322

Which of the following is the GREATEST threat to Voice-over Internet Protocol (VoIP) related to privacy release?

A. Incorrect routing

B. Eavesdropping

C. Call recording

D. Denial of service

Answer: B ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 323

Disaster recovery planning (DRP) for a company's computer system usually focuses on:

A. operations turnover procedures.

B. strategic long-range planning.

C. the probability that a disaster will occur.

D. alternative procedures to process transactions.

Answer: D ([LEAVE A REPLY](#))

It is important that disaster recovery identifies alternative processes that can be put in place while the system is not available.

NEW QUESTION: 324

Which of the following layer of an enterprise data flow architecture represents subsets of information from the core data warehouse?

A. Presentation layer

B. Desktop Access Layer

C. Data Mart layer

D. Data access layer

Answer: (SHOW ANSWER)

Section: Information System Acquisition, Development and Implementation

Explanation/Reference:

Data Mart layer - Data mart represents subset of information from the core DW selected and organized to

meet the needs of a particular business unit or business line. Data mart can be relational databases or

some form on-line analytical processing (OLAP) data structure.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to

assist decision making and assess organizational performance. To deliver effective BI, organizations need

to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer - This is where end users directly deal with information. This layer

includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits

offered by vendors such as Congas and business objects, and purpose built application such as balanced

source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data - Data captured and maintained by an organization's existing systems, and usually held in

system-specific database or flat files.

External Data - Data provided to an organization by external sources. This could include data such as

customer demographic and market share information.

Nonoperational data - Information needed by end user that is not currently maintained in a computer

accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to

assist reporting and analysis. DWs are normally instituted as large relational databases. A property

constituted DW should support three basic form of an inquiry.

Drilling up and drilling down - Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can

also be used to refine the analysis.

Drill across - Use common attributes to access a cross section of information in the warehouse such as

sum sales across all product lines by customer and group of customers according to length of association

with the company.

Historical Analysis - The warehouse should support this by holding historical, time variant data.

An

example of historical analysis would be to report monthly store sales and then repeat the analysis using

only customer who were preexisting at the start of the year in order to separate the effective new customer

from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to

meet the needs of a particular business unit or business line. Data mart can be relational databases or

some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format

and quality control. It is particularly important that only reliable data into core DW. This layer needs to be

able to deal with problems periodically thrown by operational systems such as change to account number

format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the

data source layer and, in the process, avoiding the need to know to know exactly how these data stores are

organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into

data marts. The usual practice is to pre-calculate the values that are loaded into OLAP data repositories to

increase access speed. Data mining is concern with exploring large volume of data to determine patterns

and trends of information. Data mining often identifies patterns that are counterintuitive due to number and

complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to

extend beyond data structure names and formats to provide detail on business purpose and context. The

metadata layer should be comprehensive in scope, covering data as they flow between the various layers,

including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build

and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various

layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer - This layer is concerned with basic data communication. Included here are browser

based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram - De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods

obviously play an important part in developing an enterprise data model. However, it is also crucial that

knowledgeable business operative is involved in the process. This way proper understanding can be

obtained of the business purpose and context of the data. This also mitigates the risk of replication of

suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer

includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits

offered by vendors such as Congas and business objects, and purpose built application such as balanced

source cards and digital dashboards.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the

data source layer and, in the process, avoiding the need to know to know exactly how these data stores are

organized. Technology now permits SQL access to data even if it is not stored in a relational database.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

NEW QUESTION: 325

Which of the following would be an indicator of the effectiveness of a computer security incident response team?

- A. Financial impact per security incident
- B. Number of security vulnerabilities that were patched
- C. Percentage of business applications that are being protected
- D. Number of successful penetration tests

Answer: [\(SHOW ANSWER\)](#)

Explanation/Reference:

Explanation:

The most important indicator is the financial impact per security incident. Choices B, C and D could be measures of effectiveness of security, but would not be a measure of the effectiveness of a response team.

NEW QUESTION: 326

Which of the following provides the best evidence of the adequacy of a security awareness program?

- A. The number of stakeholders including employees trained at various levels
- B. Coverage of training at all locations across the enterprise
- C. The implementation of security devices from different vendors
- D. Periodic reviews and comparison with best practices

Answer: [D \(LEAVE A REPLY\)](#)

The adequacy of security awareness content can best be assessed by determining whether it is periodically reviewed and compared to industry best practices. Choices A, B and C provide metrics for measuring various aspects of a security awareness program, but do not help assess the content.

NEW QUESTION: 327

When reviewing a project to replace multiple manual data entry systems with an artificial intelligence (AI) system, the IS auditor should be MOST concerned with the impact AI will have on

- A. employee retention
- B. enterprise architecture (EA)
- C. future task updates
- D. task capacity output

Answer: [B \(LEAVE A REPLY\)](#)

Explanation

The auditor should be most concerned with the impact AI will have on enterprise architecture (EA) when reviewing a project to replace multiple manual data entry systems with an AI system. EA is a comprehensive framework that defines the structure, components, relationships, and principles of an organization's IT environment. EA can help to align the IT strategy with the business strategy and ensure the coherence, consistency, and integration of the IT systems and services. Replacing manual data entry systems with an AI system may have significant implications for the

EA, such as changing the business processes, data flows, security requirements, performance standards, or governance models. The auditor should assess whether the project has considered the impact of AI on EA and whether the EA has been updated accordingly. References:
CISA Review Manual (Digital Version), Chapter 1, Section 1.41
CISA Online Review Course, Domain 5, Module 1, Lesson 22

NEW QUESTION: 328

Which of the following conditions would be of MOST concern to an IS auditor assessing the risk of a successful brute force attack encrypted data at rest?

- A. Use of symmetric encryption
- B. Use of asymmetric encryption
- C. Random key generation
- D. Short key length

Answer: [\(SHOW ANSWER\)](#)

Section: The process of Auditing Information System

NEW QUESTION: 329

In the review of a feasibility study for an IS acquisition, the MOST important step is to:

- A. determine whether the cost-benefits are achievable.
- B. determine whether security and control requirements have been specified.
- C. ensure that a contingency plan is in place should the project fail.
- D. ensure that the right to audit the vendor has been considered.

Answer: D [\(LEAVE A REPLY\)](#)

NEW QUESTION: 330

Which of the following documents would be MOST useful in detecting a weakness in segregation of duties?

- A. Process flowchart
- B. Data flow diagram
- C. Systems flowchart
- D. Entity-relationship diagram

Answer: A [\(LEAVE A REPLY\)](#)

NEW QUESTION: 331

An IS auditor conducts a review of a third-party vendor's reporting of key performance indicators (KPIs) Which of the following findings should be of MOST concern to the auditor?

- A. KPI data is not being analyzed
- B. KPIs are not clearly defined
- C. Some KPIs are not documented
- D. KPIs have never been updated

Answer: B ([LEAVE A REPLY](#))

Explanation

KPIs are not clearly defined is the most concerning finding for an IS auditor, because it implies that the third-party vendor does not have a clear understanding of what constitutes success or failure in their performance. This can lead to inaccurate or misleading reporting, poor decision making, and lack of accountability. KPIs should be SMART (specific, measurable, achievable, relevant, and time-bound) and aligned with the business objectives and expectations of the stakeholders¹². References: 1: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2
2: CISA Online Review Course, Module 5, Lesson 3

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As
Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 332

During an audit, an IS auditor notices that the IT department of a medium-sized organization has no separate risk management function, and the organization's operational risk documentation only contains a few broadly described IT risks. What is the MOST appropriate recommendation in this situation?

- A.** Create an IT risk management department and establish an IT risk framework with the aid of external risk management experts.
- B.** Use common industry standard aids to divide the existing risk documentation into several individual risks which will be easier to handle.
- C.** No recommendation is necessary since the current approach is appropriate for a medium-sized organization.
- D.** Establish regular IT risk management meetings to identify and assess risks, and create a mitigation plan as input to the organization's risk management.

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Establishing regular meetings is the best way to identify and assess risks in a medium-sized organization, to address responsibilities to the respective management and to keep the risk list and mitigation plans up to date. A medium-sized organization would normally not have a separate IT risk management department.

Moreover, the risks are usually manageable enough so that external help would not be needed. While common risks may be covered by common industry standards, they cannot address the

specific situation of an organization. Individual risks will not be discovered without a detailed assessment from within the organization. Splitting the one risk position into several is not sufficient.

NEW QUESTION: 333

In order for a firewall to effectively protect a network against external attacks, what fundamental practice must be followed?

- A. Filters for external information must be defined.
- B. All external communication must be via the firewall.
- C. The firewall must be placed in the demilitarized zone (DMZ).
- D. Only essential external services should be permitted.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 334

When should application controls be considered within the system-development process?

- A. After application unit testing
- B. After application module testing
- C. After applications systems testing
- D. As early as possible, even in the development of the project's functional specifications

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Application controls should be considered as early as possible in the system-development process, even in the development of the project's functional specifications.

NEW QUESTION: 335

Which of the following is the PRIMARY advantage of parallel processing for a new system implementation?

- A. Assurance that the new system meets functional requirements
- B. More time for users to complete training for the new system
- C. Significant cost savings over other system implemental or approaches
- D. Assurance that the new system meets performance requirements

Answer: D ([LEAVE A REPLY](#))

Explanation

Parallel processing is a system implementation approach that involves running the new system and the old system simultaneously for a period of time until the new system is verified and accepted. The primary advantage of parallel processing is that it provides assurance that the new system meets performance requirements and produces the same or better results as the old system. Parallel processing also minimizes the risk of system failure and data loss, as the old system can be used as a backup or fallback option in case of any problems with the new system.

NEW QUESTION: 336

An IS auditor has discovered that a software system still in regular use is years out of date and no longer supported. The auditee has stated that it will take six months until the software is running on the current version. Which of the following is the BEST way to reduce the immediate risk associated with using an unsupported version of the software?

- A. Verify all patches have been applied to the software system's outdated version.
- B. Close all unused ports on the outdated software system.
- C. Monitor network traffic attempting to reach the outdated software system.
- D. Segregate the outdated software system from the main network.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 337

Which of the following would be MOST important for an IS auditor to verify when conducting a business continuity audit?

- A. Data backups are performed on a timely basis
- B. A recovery site is contracted for and available as needed
- C. Human safety procedures are in place
- D. insurance coverage is adequate and premiums are current

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

The most important element in any business continuity process is the protection of human life. This takes precedence over all other aspects of the plan.

NEW QUESTION: 338

What is the purpose of using a write blocker during the acquisition phase of a digital forensics investigation?

- A. To preserve chain of custody
- B. To protect against self-destruct utilities
- C. To prevent the activation of installed malware
- D. To prevent evidence alteration

Answer: D ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 339

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

- A. User management
- B. Project steering committee
- C. IT management
- D. Systems developers

Answer: A ([LEAVE A REPLY](#))

User management assumes ownership of a systems-development project and the resulting system.

NEW QUESTION: 340

An organization's IT risk assessment should include the identification of:

- A. business process owners
- B. compensating controls
- C. vulnerabilities
- D. business needs

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 341

Which of the following is the BEST approach to verify that internal help desk procedures are executed in compliance with policies?

- A. Benchmark help desk procedures.
- B. Interview end users.
- C. Test a sample of closed tickets.
- D. Evaluate help desk call metrics.

Answer: C ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 342

Which of the following type of computer has highest processing speed?

- A. Supercomputers
- B. Midrange servers
- C. Personal computers
- D. Thin client computers

Answer: A ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

Explanation

Explanation/Reference:

Supercomputers are very large and expensive computers with the highest processing speed, designed to

be used for specialized purpose or fields that require extensive processing power.

A supercomputer is focused on performing tasks involving intense numerical calculations such as weather

forecasting, fluid dynamics, nuclear simulations, theoretical astrophysics, and complex scientific computations.

A supercomputer is a computer that is at the frontline of current processing capacity, particularly speed of

calculation. The term supercomputer itself is rather fluid, and the speed of today's supercomputers tends to become typical of tomorrow's ordinary computer. Supercomputer processing speeds are measured in floating point operations per second, or FLOPS. An example of a floating point operation is the calculation of mathematical equations in real numbers. In terms of computational capability, memory size and speed, I/O technology, and topological issues such as bandwidth and latency, supercomputers are the most powerful, are very expensive, and not cost-effective just to perform batch or transaction processing. Transaction processing is handled by less powerful computers such as server computers or mainframes.

For your exam you should know the information below:

Common Types of computers

Supercomputers

A supercomputer is focused on performing tasks involving intense numerical calculations such as weather forecasting, fluid dynamics, nuclear simulations, theoretical astrophysics, and complex scientific computations. A supercomputer is a computer that is at the frontline of current processing capacity, particularly speed of calculation. The term supercomputer itself is rather fluid, and the speed of today's supercomputers tends to become typical of tomorrow's ordinary computer. Supercomputer processing speeds are measured in floating point operations per second, or FLOPS. An example of a floating point operation is the calculation of mathematical equations in real numbers. In terms of computational capability, memory size and speed, I/O technology, and topological issues such as bandwidth and latency, supercomputers are the most powerful, are very expensive, and not cost-effective just to perform batch or transaction processing. Transaction processing is handled by less powerful computers such as server computers or mainframes.

Mainframes

The term mainframe computer was created to distinguish the traditional, large, institutional computer intended to service multiple users from the smaller, single user machines. These computers are capable of

handling and processing very large amounts of data quickly. Mainframe computers are used in large

institutions such as government, banks and large corporations. They are measured in MIPS (million

instructions per second) and respond to up to 100s of millions of users at a time.

Mid-range servers

Midrange systems are primarily high-end network servers and other types of servers that can handle the

large-scale processing of many business applications. Although not as powerful as mainframe computers,

they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing

needs of many organizations. Midrange systems have become popular as powerful network servers to help

manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange

systems include servers used in industrial process-control and manufacturing plants and play major roles in

computer-aided manufacturing (CAM). They can also take the form of powerful technical workstations for

computer-aided design (CAD) and other computation and graphics-intensive applications.

Midrange system

are also used as front-end servers to assist mainframe computers in telecommunications processing and

network management.

Personal computers

A personal computer (PC) is a general-purpose computer, whose size, capabilities and original sale price

makes it useful for individuals, and which is intended to be operated directly by an end-user with no

intervening computer operator. This contrasted with the batch processing or time-sharing models which

allowed larger, more expensive minicomputer and mainframe systems to be used by many people, usually

at the same time. Large data processing systems require a full-time staff to operate efficiently.

Laptop computers

A laptop is a portable personal computer with a clamshell form factor, suitable for mobile use.[1]

They are

also sometimes called notebook computers or notebooks. Laptops are commonly used in a variety of

settings, including work, education, and personal multimedia.

A laptop combines the components and inputs as a desktop computer; including display, speakers, keyboard, and pointing device (such as a touchpad), into a single device. Most modern-day laptop computers also have a webcam and a microphone pre-installed. [citation needed] A laptop can be powered either from a rechargeable battery, or by mains electricity via an AC adapter. Laptops are a diverse category of devices, and other more specific terms, such as ultra-books or net books, refer to specialist types of laptop which have been optimized for certain uses. Hardware specifications change vastly between these classifications, forgoing greater and greater degrees of processing power to reduce heat emissions.

Smartphone, tablets and other handheld devices

A mobile device (also known as a handheld computer or simply handheld) is a small, handheld computing

device, typically having a display screen with touch input and/or a miniature keyboard.

A handheld computing device has an operating system (OS), and can run various types of application

software, known as apps. Most handheld devices can also be equipped with Wi-Fi, Bluetooth, and GPS

capabilities that can allow connections to the Internet and other Bluetooth-capable devices, such as an

automobile or a microphone headset. A camera or media player feature for video or music files can also be

typically found on these devices along with a stable battery power source such as a lithium battery.

Early pocket-sized devices were joined in the late 2000s by larger but otherwise similar tablet computers.

Much like in a personal digital assistant (PDA), the input and output of modern mobile devices are often

combined into a touch-screen interface.

Smartphone's and PDAs are popular amongst those who wish to use some of the powers of a conventional

computer in environments where carrying one would not be practical. Enterprise digital assistants can

further extend the available functionality for the business user by offering integrated data capture devices

like barcode, RFID and smart card readers.

Thin Client computers

A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

The following answers are incorrect:

Mid-range servers- Midrange systems are primarily high-end network servers and other types of servers that can handle the large-scale processing of many business applications. Although not as powerful as mainframe computers, they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing needs of many organizations. Midrange systems have become popular as powerful network servers to help manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange systems include servers used in industrial process-control and manufacturing plants and play major roles in computer-aided manufacturing (CAM).

Personal computers - A personal computer (PC) is a general-purpose computer, whose size, capabilities and original sale price makes it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator. This contrasted with the batch processing or time-sharing models which allowed larger, more expensive minicomputer and mainframe systems to be used by many people, usually at the same time. Large data processing systems require a full-time staff to operate efficiently.

Thin Client computers- A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by

itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for

diskless nodes) to actual information processing on the client's behalf.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 246

http://en.wikipedia.org/wiki/Thin_client

http://en.wikipedia.org/wiki/Mobile_device

http://en.wikipedia.org/wiki/Personal_computer

http://en.wikipedia.org/wiki/Classes_of_computers

<http://en.wikipedia.org/wiki/Laptop>

NEW QUESTION: 343

Which of the following term in business continuity determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity?

A. RPO

B. RTO

C. WRT

D. MTD

Answer: (SHOW ANSWER)

Explanation/Reference:

The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual

Business as usual



Image Reference - <http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png> At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

Disaster Occurs

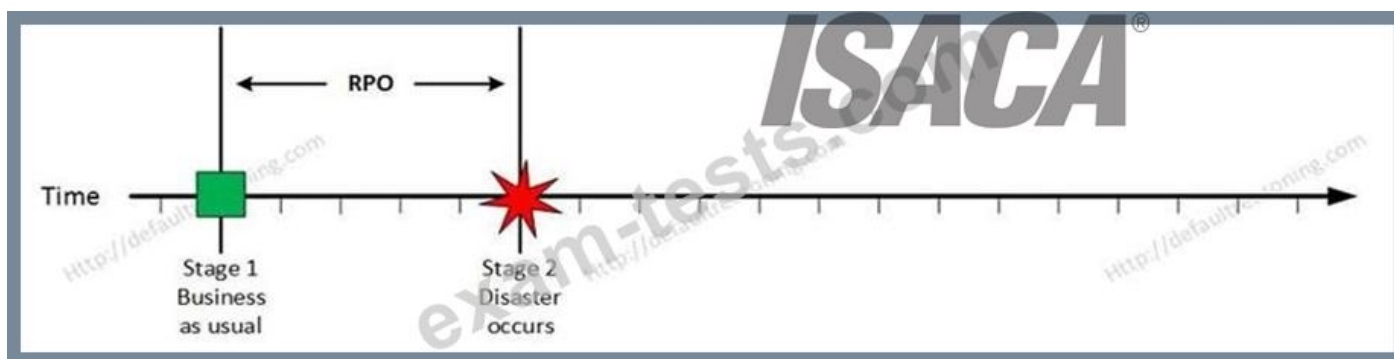


Image Reference - <http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png> On a given point in time, disaster occurs and systems need to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

Recovery

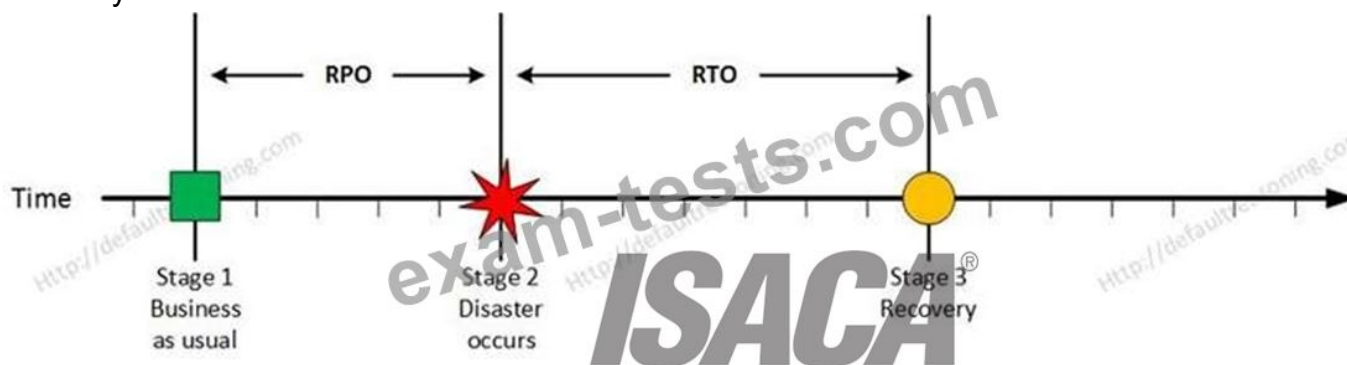


Image Reference - <http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png> At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production

Resume Production

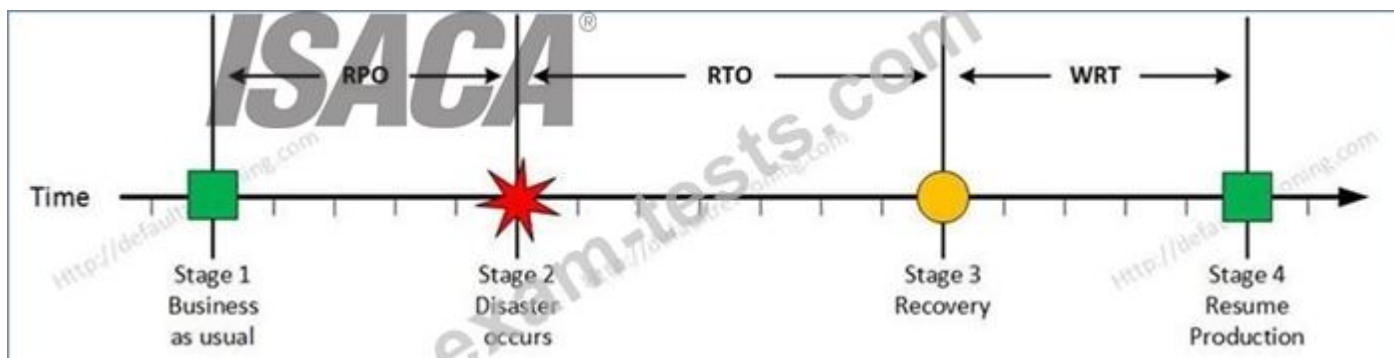


Image Reference - <http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png> At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for

example, checking the databases and logs, making sure the applications or services are running and are available.

In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD

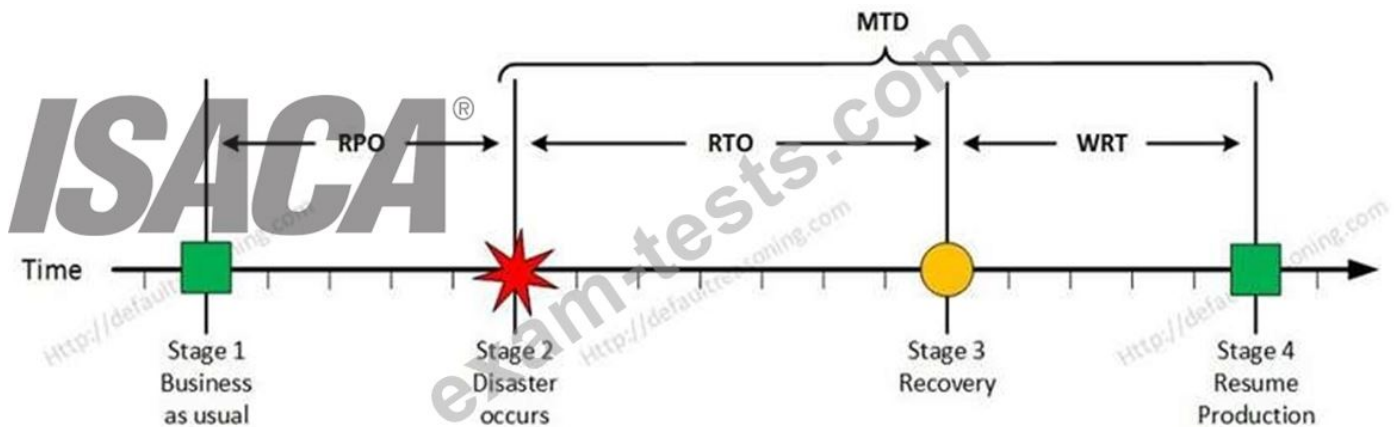


Image Reference - <http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png> The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure.

In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 284

<http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/>

NEW QUESTION: 344

A system administrator recently informed the IS auditor about the occurrence of several unsuccessful intrusion attempts from outside the organization. Which of the following is MOST effective in detecting such an intrusion?

A. Using smart cards with one-time passwords

- B. Periodically reviewing log files
- C. Configuring the router as a firewall
- D. Installing biometrics-based authentication

Answer: B ([LEAVE A REPLY](#))

Periodically reviewing log files is the most effective way to detect intrusion attempts from outside the organization, as they can provide evidence of unauthorized access attempts, source IP addresses, timestamps and other relevant information. Using smart cards with one-time passwords or installing biometrics-based authentication can prevent unauthorized access, but not detect it. Configuring the router as a firewall can block unwanted traffic, but not log it. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 361

NEW QUESTION: 345

Which of the following should be identified FIRST during the risk assessment process?

- A. Information assets
- B. Legal requirements
- C. Vulnerability
- D. Existing controls

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 346

Involvement of senior management is MOST important in the development of:

- A. strategic plans.
- B. IS policies.
- C. IS procedures.
- D. standards and guidelines.

Answer: A ([LEAVE A REPLY](#))

Strategic plans provide the basis for ensuring that the enterprise meets its goals and objectives. Involvement of senior management is critical to ensuring that the plan adequately addresses the established goals and objectives. IS policies, procedures, standards and guidelines are all structured to support the overall strategic plan.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 347

Which of the following should be of GREATEST concern to an IS auditor reviewing an organization's IT process performance reports over the last quarter?

- A. Metrics are not aligned with industry benchmarks.
- B. Metrics were defined without stakeholder review.
- C. Key performance indicators (KPIs) were met in only one month.
- D. Performance reporting includes too many technical terms.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 348

Which of the following is MOST directly affected by network performance monitoring tools?

- A. Integrity
- B. Availability
- C. Completeness
- D. Confidentiality

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

In case of a disruption in service, one of the key functions of network performance monitoring tools is to ensure that the information has remained unaltered. It is a function of security monitoring to assure confidentiality by using such tools as encryption. However, the most important aspect of network performance is assuring the ongoing dependence on connectivity to run the business. Therefore, the characteristic that benefits the most from network monitoring is availability.

NEW QUESTION: 349

Which of the following would help to ensure the portability of an application connected to a database?

- A. Verification of database import and export procedures
- B. Usage of a structured query language (SQL)
- C. Analysis of stored procedures/triggers
- D. Synchronization of the entity-relation model with the database physical schema

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

The use of SQL facilitates portability. Verification of import and export procedures with other systems

ensures better interfacing with other systems, analyzing stored procedures/triggers ensures proper access/

performance, and reviewing the design entity- relation model will be helpful, but none of these contribute to

the portability of an application connecting to a database.

NEW QUESTION: 350

Which type of review is MOST important to conduct when an IS auditor is informed that a recent internal exploitation of a bug has been discovered in a business application?

- A. Penetration testing
- B. Server security audit
- C. Application security testing
- D. Forensic audit

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 351

In which of the following sampling methods is the entire sample considered to be irregular if a single error is found?

- A. Discovery sampling
- B. Variable sampling
- C. Stop-or-go sampling
- D. Judgmental sampling

Answer: ([SHOW ANSWER](#)**)**

The sampling method in which the entire sample is considered to be irregular if a single error is found is discovery sampling. Discovery sampling is a type of statistical sampling that is used to test for the existence of at least one occurrence of a specific characteristic or condition in a population. Discovery sampling is often used when the auditor expects the characteristic or condition to be very rare or nonexistent, and when any occurrence would have a significant impact on the audit objective. For example, discovery sampling can be used to test for fraud, noncompliance, or material misstatement.

Discovery sampling works by setting a very low tolerable error rate (the maximum rate of occurrence of the characteristic or condition that the auditor is willing to accept) and a high confidence level (the degree of assurance that the auditor wants to obtain). The auditor then selects a sample from the population using a random or systematic method, and examines each item in the sample for the presence or absence of the characteristic or condition. If no error is found in the sample, the auditor can conclude with a high level of confidence that the characteristic or condition does not exist or is very rare in the population. However, if one or more errors are found in the sample, the auditor cannot draw any conclusion about the population and must either expand the sample size or perform alternative procedures.

Discovery sampling differs from other sampling methods in that it does not allow for any errors in the sample.

Other sampling methods, such as variable sampling, stop-or-go sampling, or judgmental sampling, can tolerate some errors in the sample and use them to estimate the error rate or amount in the population.

However, discovery sampling is designed to test for zero-tolerance situations, where any error would be unacceptable or material. Therefore, discovery sampling considers the entire sample to be irregular if a single error is found.

References:

Audit Sampling - Overview, Purpose, Importance, and Types¹

Audit Sampling - What Is It, Methods, Example, Advantage, Reason²

ISA 530: Audit sampling | ICAEW³

Audit Sampling - AICPA⁴

NEW QUESTION: 352

A security review reveals an organization b struggling with a large number of findings from vulnerability scans. What should the IS auditor recommend be done FIRST.

- A. Remediate issues that are rated as most critical
- B. Address gaps for all internally developed applications
- C. Conduct penetration tests to confirm critical findings.
- D. Remediate vulnerabilities for the most critical systems

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 353

A third-party service provider has proposed a data loss prevention (DLP) solution. Which of the following MUST be in place for this solution to be relevant to the organization?

- A. An adequate data testing environment
- B. Senior management support
- C. A business case
- D. A data classification

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 354

Which of the following is MOST important to the effectiveness of smoke detectors installed in a data processing facility?

- A. Detectors trigger audible alarms when activated.
- B. Detectors are linked to wet pipe fire suppression systems.
- C. Detectors are linked to dry pipe fire suppression systems.
- D. Detectors have the correct industry certification.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 355

What is the recommended minimum length of a good password?

- A. 6 characters
- B. 8 characters

- C. 12 characters
- D. 18 characters
- E. 22 characters
- F. None of the choices.

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password. A good password has mixed-case alphabetic characters, numbers, and symbols. Do use a password that is at least eight or more characters.

NEW QUESTION: 356

Functionality is a characteristic associated with evaluating the quality of software products throughout their life cycle, and is BEST described as the set of attributes that bear on the:

- A. existence of a set of functions and their specified properties.
- B. ability of the software to be transferred from one environment to another.
- C. capability of software to maintain its level of performance under stated conditions.
- D. relationship between the performance of the software and the amount of resources used.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Functionality is the set of attributes that bears on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs. Choice B refers to portability, choice C refers to reliability and choice D refers to efficiency.

NEW QUESTION: 357

The FIRST course of action an investigator should take when a computer is being attacked is to:

- A. disconnect the power source.
- B. terminate all active processes
- C. copy the contents of the hard drive.
- D. disconnect it from the network.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 358

An IS auditor reviewing the threat assessment for a data center would be MOST concerned if:

- A. some of the identified threats are unlikely to occur.
- B. all identified threats relate to external entities.
- C. the exercise was completed by local management.
- D. neighboring organizations' operations have been included.

Answer: B ([LEAVE A REPLY](#))

An IS auditor reviewing the threat assessment for a data center would be most concerned if all identified threats relate to external entities. This indicates that the threat assessment is incomplete and biased, as it ignores the potential threats from internal sources, such as employees, contractors, vendors, or authorized visitors. Internal threats can pose significant risks to the data center, as they may have access to sensitive information, systems, or facilities, and may exploit their privileges for malicious or fraudulent purposes. According to a study by IBM, 60% of cyberattacks in 2015 were carried out by insiders¹. Some of the identified threats are unlikely to occur is not a cause for concern, as it shows that the threat assessment is comprehensive and realistic, and considers all possible scenarios, regardless of their probability. A threat assessment should not exclude any potential threats based on subjective judgments or assumptions, as they may still have a high impact if they materialize.

The exercise was completed by local management is not a cause for concern, as it shows that the threat assessment is conducted by the people who are most familiar with the data center's operations, environment, and risks. Local management may have more relevant and accurate information and insights than external parties, and may be more invested in the outcome of the threat assessment.

Neighboring organizations' operations have been included is not a cause for concern, as it shows that the threat assessment is holistic and contextual, and considers the interdependencies and influences of external factors on the data center's security. Neighboring organizations' operations may pose direct or indirect threats to the data center, such as physical damage, network interference, or shared vulnerabilities.

References:

* IBM Security Services 2016 Cyber Security Intelligence Index 1

NEW QUESTION: 359

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: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

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

NEW QUESTION: 360

An organization is migrating its HR application to an Infrastructure as a Service (IaaS) model in a private cloud. Who is PRIMARILY responsible for the security configurations of the deployed application's operating system?

- A. The cloud provider
- B. The organization
- C. The operating system vendor
- D. The cloud provider's external auditor

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 361

Which risk response has been adopted by a risk owner postponing the implementation of proper controls due to budget constraints?

- A. Acceptance
- B. Transfer
- C. Avoidance
- D. Mitigation

Answer: A ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 362

During the planning phase of a data loss prevention (DLP) audit, management expresses a concern about mobile computing. Which of the following should the IS auditor identify as the associated risk?

- A. The use of the cloud negatively impacting IT availability
- B. Increased need for user awareness training
- C. Increased vulnerability due to anytime, anywhere accessibility
- D. Lack of governance and oversight for IT infrastructure and applications

Answer: C ([LEAVE A REPLY](#))

The associated risk of mobile computing that an IS auditor should identify during the planning phase of a data loss prevention (DLP) audit is increased vulnerability due to anytime, anywhere accessibility. Mobile computing refers to the use of portable devices, such as laptops, tablets, smartphones, or wearable devices, that can access data and applications over wireless networks from any location⁶. Mobile computing enables greater flexibility, productivity, and convenience for

users, but also poses significant security challenges for organizations. One of these challenges is increased vulnerability due to anytime, anywhere accessibility. This means that mobile devices are exposed to a higher risk of loss, theft, damage, or unauthorized access than stationary devices⁷. If mobile devices contain or access sensitive data without proper protection, such as encryption or authentication, they could result in data leakage or breach in case of compromise⁸. Therefore, an IS auditor should identify this risk as part of a DLP audit. The other options are less relevant or incorrect because:

* A. The use of cloud negatively impacting IT availability is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more related to cloud computing than mobile computing. Cloud computing refers to the delivery of computing services, such as data storage or processing, over the Internet from remote servers. Cloud computing may enable or support mobile computing by providing access to data and applications from any device or location, but it does not necessarily imply mobile computing. The use of cloud may negatively impact IT availability if there are disruptions or outages in the cloud service provider's network or infrastructure, but this is not a direct consequence of mobile computing.

* B. Increased need for user awareness training is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more of a control or mitigation measure than a risk. User awareness training refers to educating users about security policies, procedures, and best practices for using mobile devices and protecting data. User awareness training may help to reduce the risk of data loss or breach due to mobile computing by increasing user knowledge and responsibility, but it does not eliminate or prevent the risk.

* D. Lack of governance and oversight for IT infrastructure and applications is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more of a general or organizational risk than a specific or technical risk. Governance and oversight refer to the establishment and implementation of policies, standards, and procedures for managing IT resources and aligning them with business objectives. Lack of governance and oversight for IT infrastructure and applications may affect the security and performance of mobile devices and data, but it is not a direct or inherent result of mobile computing. References: Mobile Computing - ISACA, Mobile Computing Device Threats, Vulnerabilities and Risk Factors Are Ubiquitous - ISACA, Data Loss Prevention-Next Steps - ISACA, [Cloud Computing - ISACA], [Cloud Computing Risk Assessment - ISACA], [User Awareness Training - ISACA], [Governance and Oversight - ISACA]

NEW QUESTION: 363

An IS auditor is concerned that unauthorized access to a highly sensitive data center might be gained by piggybacking or tailgating. Which of the following is the BEST recommendation? (Choose Correct answer and give explanation from CISA Certification - Information Systems Auditor official book)

A. Biometrics

B. Procedures for escorting visitors

C. Airlock entrance

D. Intruder alarms

Answer: C ([LEAVE A REPLY](#))

The best recommendation to prevent unauthorized access to a highly sensitive data center by piggybacking or tailgating is to use an airlock entrance. An airlock entrance is a type of access control system that consists of two doors that are interlocked, so that only one door can be opened at a time. This prevents an unauthorized person from following an authorized person into the data center without being detected. An airlock entrance can also be integrated with other security measures, such as biometrics, card readers, or PIN pads, to verify the identity and authorization of each person entering the data center.

Biometrics (option A) is a method of verifying the identity of a person based on their physical or behavioral characteristics, such as fingerprints, iris scans, or voice recognition. Biometrics can provide a high level of security, but they are not sufficient to prevent piggybacking or tailgating, as an unauthorized person can still follow an authorized person who has been authenticated by the biometric system.

Procedures for escorting visitors (option B) is a policy that requires all visitors to the data center to be accompanied by an authorized employee at all times. This can help prevent unauthorized access by visitors, but it does not address the risk of piggybacking or tailgating by other employees or contractors who may have legitimate access to the building but not to the data center.

Intruder alarms (option D) are devices that detect and alert when an unauthorized person enters a restricted area. Intruder alarms can provide a deterrent and a response mechanism for unauthorized access, but they are not effective in preventing piggybacking or tailgating, as they rely on the detection of the intruder after they have already entered the data center.

References: 1: CISA Certification | Certified Information Systems Auditor | ISACA 2: CISA Certified Information Systems Auditor Study Guide, 4th Edition 3: CISA - Certified Information Systems Auditor Study Guide [Book]

NEW QUESTION: 364

A mission-critical application utilizes a one-node database server. On multiple occasions, the database service has been stopped to perform routine patching, causing application outages. Which of the following should be the IS auditor's GREATEST concern?

A. Revenue lost due to application outages

B. A large number of scheduled database changes

C. The presence of a single point of failure

D. Patching performed by the vendor

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 365

What is the Most critical finding when reviewing an organization's information security management?

- A. No dedicated security officer
- B. No official charter for the information security management system
- C. No periodic assessments to identify threats and vulnerabilities
- D. No employee awareness training and education program

Answer: ([SHOW ANSWER](#))

The most critical finding when reviewing an organization's information security management is no periodic assessments to identify threats and vulnerabilities. Periodic assessments are essential for ensuring that the organization's information security policies, procedures, standards, and controls are aligned with the current and emerging risks and threats that may affect its information assets. Without periodic assessments, the organization may not be aware of its actual security posture, gaps, or weaknesses, and may not be able to take appropriate measures to mitigate or prevent potential security incidents. No dedicated security officer, no official charter for the information security management system, and no employee awareness training and education program are also findings that may indicate some deficiencies in the organization's information security management, but they are not as critical as no periodic assessments to identify threats and vulnerabilities. References: ISACA CISA Review Manual 27th Edition, page 343.

NEW QUESTION: 366

Which of the following is the GREATEST risk of using a reciprocal site for disaster recovery?

- A. Inability to utilize the site when required
- B. Inability to test the recovery plans onsite
- C. Equipment compatibility issues at the site
- D. Mismatched organizational security policies

Answer: A ([LEAVE A REPLY](#))

Explanation

The greatest risk of using a reciprocal site for disaster recovery is the inability to utilize the site when required. A reciprocal site is an agreement between two organizations to provide backup facilities for each other in case of a disaster. However, this arrangement may not be reliable or enforceable, especially if both organizations are affected by the same disaster or have conflicting priorities. Therefore, the IS auditor should recommend that management consider alternative options for disaster recovery, such as dedicated sites or cloud services¹². References:

CISA Review Manual, 27th Edition, page 3381

CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION: 367

Which of the following is the PRIMARY reason to follow a configuration management process to maintain application?

- A. To optimize system resources
- B. To follow system hardening standards
- C. To optimize asset management workflows
- D. To ensure proper change control

Answer: D ([LEAVE A REPLY](#))

Explanation

Following a configuration management process to maintain applications is the primary reason for ensuring proper change control. Configuration management is a process of identifying, documenting, controlling, and verifying the configuration items and their interrelationships within an IT system or environment. Following a configuration management process can help to ensure that any changes to the applications are authorized, tested, documented, and tracked throughout their lifecycle. This will help to prevent unauthorized or improper changes that could affect the functionality, performance, or security of the applications. The other options are not the primary reasons for following a configuration management process, but rather possible benefits or outcomes of doing so. References:

CISA Review Manual (Digital Version), Chapter 4, Section 4.3.31

CISA Review Questions, Answers & Explanations Database, Question ID 225

NEW QUESTION: 368

The use of residual biometric information to gain unauthorized access is an example of which of the following attacks?

- A. Replay
- B. Brute force
- C. Cryptographic
- D. Mimic

Answer: ([SHOW ANSWER](#))

Residual biometric characteristics, such as fingerprints left on a biometric capture device, may be reused by an attacker to gain unauthorized access. A brute force attack involves feeding the biometric capture device numerous different biometric samples. A cryptographic attack targets the algorithm or the encrypted data, in a mimic attack, the attacker reproduces characteristics similar to those of the enrolled user, such as forging a signature or imitating a voice.

NEW QUESTION: 369

Which of the following activities would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA)?

- A. Implementing the remediation plan
- B. Developing the CSA questionnaire
- C. Developing the remediation plan
- D. Partially completing the CSA

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 370

What is the BEST approach to mitigate the risk of a phishing attack?

- A. implement an intrusion detection system (IDS)
- B. Assess web site security

C. Strong authentication

D. User education

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Phishing attacks can be mounted in various ways; intrusion detection systems (IDSs) and strong authentication cannot mitigate most types of phishing attacks. Assessing web site security does not

mitigate the risk. Phishing uses a server masquerading as a legitimate server. The best way to mitigate the

risk of phishing is to educate users to take caution with suspicious internet communications and not to trust

them until verified. Users require adequate training to recognize suspicious web pages and e-mail.

NEW QUESTION: 371

A digital signature contains a message digest to:

A. show if the message has been altered after transmission.

B. define the encryption algorithm.

C. confirm the identity of the originator.

D. enable message transmission in a digital format.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

The message digest is calculated and included in a digital signature to prove that the message has not been altered. It should be the same value as a recalculation performed upon receipt. It does not define the algorithm or enable the transmission in digital format and has no effect on the identity of the user; it is there to ensure integrity rather than identity.

NEW QUESTION: 372

Which of the following is the BEST method to prevent wire transfer fraud by bank employees?

A. Independent reconciliation

B. Re-keying of wire dollar amounts

C. Two-factor authentication control

D. System-enforced dual control

Answer: D ([LEAVE A REPLY](#))

The best method to prevent wire transfer fraud by bank employees is system-enforced dual control. System-enforced dual control is a segregation of duties control that requires two or more individuals to perform or authorize a transaction or activity using a system that enforces this requirement. System-enforced dual control can prevent wire transfer fraud by requiring independent verification and approval of payment requests, amounts, and recipients by different

bank employees using a system that does not allow any single employee to complete the transaction alone. The other options are not as effective as system-enforced dual control in preventing wire transfer fraud, as they do not involve independent checks or approvals using a system.

Independent reconciliation is a detective control that can help compare and confirm payment records with bank statements, but it does not prevent wire transfer fraud from occurring. Re-keying of wire dollar amounts is an input control that can help detect any errors or discrepancies in payment amounts, but it does not prevent wire transfer fraud from occurring. Two-factor authentication control is an access control that can help verify the identity and authorization of bank employees, but it does not prevent wire transfer fraud from occurring. References: CISA Review Manual (DigitalVersion), Chapter 3, Section 3.2

NEW QUESTION: 373

Which of the following conditions would be of MOST concern to an IS auditor assessing the risk of a successful brute force attack against encrypted data at rest?

- A. Short key length
- B. Random key generation
- C. Use of symmetric encryption
- D. Use of asymmetric encryption

Answer: (SHOW ANSWER)

The condition that would be of most concern to an IS auditor assessing the risk of a successful brute force attack against encrypted data at rest is short key length. A brute force attack is a method of breaking encryption by trying all possible combinations of keys until finding the correct one. The shorter the key length, the easier it is for an attacker to guess or crack the encryption. Random key generation, use of symmetric encryption, and use of asymmetric encryption are not conditions that would increase the risk of a successful brute force attack. In fact, random key generation can enhance security by preventing predictable patterns in key selection. Symmetric encryption and asymmetric encryption are different types of encryption that have their own advantages and disadvantages, but neither is inherently more vulnerable to brute force attacks than the other. References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

NEW QUESTION: 374

When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

- A. establishment of a review board.
- B. creation of a security unit.
- C. effective support of an executive sponsor.
- D. selection of a security process owner.

Answer: C (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

The executive sponsor would be in charge of supporting the organization's strategic security program, and would aid in directing the organization's overall security management activities. Therefore, support by the executive level of management is the most critical success factor (CSF). None of the other choices are effective without visible sponsorship of top management.

NEW QUESTION: 375

Which of the following roles is responsible for validating compliance with the agreed-upon systems development methodology during the development of a new system?

- A. Information security officer
- B. Quality assurance (QA) function.
- C. Project management office (PMO)
- D. Systems development management

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 376

Which of the following is the MOST important reason for an IS auditor to examine the results of a post-incident review performed after a security incident?

- A. To evaluate the effectiveness of continuous improvement efforts
- B. To compare incident response metrics with industry benchmarks
- C. To re-analyze the incident to identify any hidden backdoors planted by the attacker
- D. To evaluate the effectiveness of the network firewall against future security breaches

Answer: A ([LEAVE A REPLY](#))

A post-incident review (PIR) is a process to review the incident information from occurrence to closure and to identify potential findings and recommendations for improvement¹. The most important reason for an IS auditor to examine the results of a PIR is to evaluate the effectiveness of continuous improvement efforts and to ensure that the lessons learned from the incident are implemented and followed up². A PIR can help an organization to eliminate or reduce the risk of the incident to re-occur, improve the initial incident detection time, identify improvements needed to diagnose and repair the incident, and update the incident management best practices¹. Therefore, a PIR is a valuable source of information for an IS auditor to assess the maturity and performance of the organization's incident management process.

CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As
Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 377

Which of the following is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality?

- A. Function point analysis
- B. Critical path methodology
- C. Rapid application development
- D. Program evaluation review technique

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Rapid application development is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality. The program evaluation review technique (PERT) and critical path methodology (CPM) are both planning and control techniques, while function point analysis is used for estimating the complexity of developing business applications.

NEW QUESTION: 378

An IS auditor is reviewing a software-based configuration. Which of the following represents the GREATEST vulnerability? The firewall software:

- A. is configured with an implicit deny rule as the last rule in the rule base.
- B. is installed on an operating system with default settings.
- C. has been configured with rules permitting or denying access to systems or networks.
- D. is configured as a virtual private network (VPN) endpoint.

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Default settings are often published and provide an intruder with predictable configuration information, which allows easier system compromise. To mitigate this risk, firewall software should be installed on a system using a hardened operating system that has limited functionality, providing only the services necessary to support the firewall software. Choices A, C and D are normal or best practices for firewall configurations.

NEW QUESTION: 379

When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:

- A. allow changes, which will be completed using after-the-fact follow-up.

- B. allow undocumented changes directly to the production library.
- C. do not allow any emergency changes.
- D. allow programmers permanent access to production programs.

Answer: A (LEAVE A REPLY)

There may be situations where emergency fixes are required to resolve system problems. This involves the use of special logon IDs that grant programmers temporary access to production programs during emergency situations. Emergency changes should be completed using after-the-fact follow-up procedures, which ensure that normal procedures are retroactively applied; otherwise, production may be impacted. Changes made in this fashion should be held in an emergency library from where they can be moved to the production library, following the normal change management process. Programmers should not directly alter the production library nor should they be allowed permanent access to production programs.

NEW QUESTION: 380

An IS auditor is reviewing the security of a web-based customer relationship management (CRM) system that is directly accessed by customers via the Internet, which of the following should be a concern for the auditor?

- A. The system is hosted on an external third-party service provider's server.
- B. The system is hosted in a hybrid-cloud platform managed by a service provider.
- C. The system is hosted within a demilitarized zone (DMZ) of a corporate network.
- D. The system is hosted within an internal segment of a corporate network.

Answer: D (LEAVE A REPLY)

A web-based CRM system that is directly accessed by customers via the Internet should be hosted in a secure and isolated environment to protect it from external threats and unauthorized access. A web-based CRM system should also be reliable, trusted, and backed up regularly¹. Hosting the system on an external third-party service provider's servers (A) or a hybrid-cloud platform managed by a service provider (B) may not be a concern for the auditor if the service provider has adequate security measures and service level agreements in place. The auditor should verify the security controls and contractual terms of the service provider before trusting them with the CRM data²³.

Hosting the system within a demilitarized zone (DMZ) of a corporate network is a common practice to provide an extra layer of security to the CRM system from untrusted networks, such as the Internet. A DMZ is a perimeter network that isolates the CRM system from the internal network and filters the incoming traffic from the external network using a security gateway⁴⁵⁶⁷. Hosting the system within an internal segment of a corporate network (D) is a concern for the auditor because it exposes the CRM system and the internal network to potential attacks from the Internet. The CRM system should not be directly accessible from the Internet without a DMZ or a firewall to protect it. This could compromise the confidentiality, integrity, and availability of the CRM data and the internal network⁷⁸.

NEW QUESTION: 381

Which of the following should be the IS auditor's PRIMARY focus when evaluating an organization's offsite storage facility?

- A. Retention policy and period
- B. Shared facilities
- C. Results of business continuity plan (BCP) tests
- D. Adequacy of physical and environmental controls

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 382

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 ([LEAVE A REPLY](#))

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.

NEW QUESTION: 383

Capacity management enables organizations to:

- A. forecast technology trends
- B. establish the capacity of network communication links
- C. identify the extent to which components need to be upgraded
- D. determine business transaction volumes.

Answer: ([SHOW ANSWER](#)**)**

Capacity management is a process that ensures that the IT resources of an organization are sufficient to meet the current and future demands of the business. Capacity management enables organizations to identify the extent to which components need to be upgraded, by monitoring and analyzing the performance, utilization, and availability of the IT components, such as servers, networks, storage, applications, etc., and identifying any bottlenecks, gaps, or risks that may affect the service level agreements (SLAs) or quality of service (QoS).

Capacity management also helps organizations to plan and optimize the use of IT resources, by forecasting the future demand and growth of the business, and aligning the IT capacity with the business needs and objectives.

Forecasting technology trends is a possible outcome of capacity management, but it is not its main purpose.

Establishing the capacity of network communication links is a part of capacity management, but it is not its main goal. Determining business transaction volumes is an input for capacity management, but it is not its main objective.

NEW QUESTION: 384

The BEST method for assessing the effectiveness of a business continuity plan is to review the:

- A. plans and compare them to appropriate standards.
- B. results from previous tests.
- C. emergency procedures and employee training.
- D. offsite storage and environmental controls.

Answer: ([SHOW ANSWER](#))

Previous test results will provide evidence of the effectiveness of the business continuity plan. Comparisons to standards will give some assurance that the plan addresses the critical aspects of a business continuity plan but will not reveal anything about its effectiveness. Reviewing emergency procedures, offsite storage and environmental controls would provide insight into some aspects of the plan but would fall short of providing assurance of the plan's overall effectiveness.

NEW QUESTION: 385

Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management?

- A. Governing
- B. Culture
- C. Enabling and support
- D. Emergence

Answer: ([SHOW ANSWER](#))

Section: Governance and Management of IT

Explanation:

Emergence - which connotes surfacing, developing, growing and evolving - refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

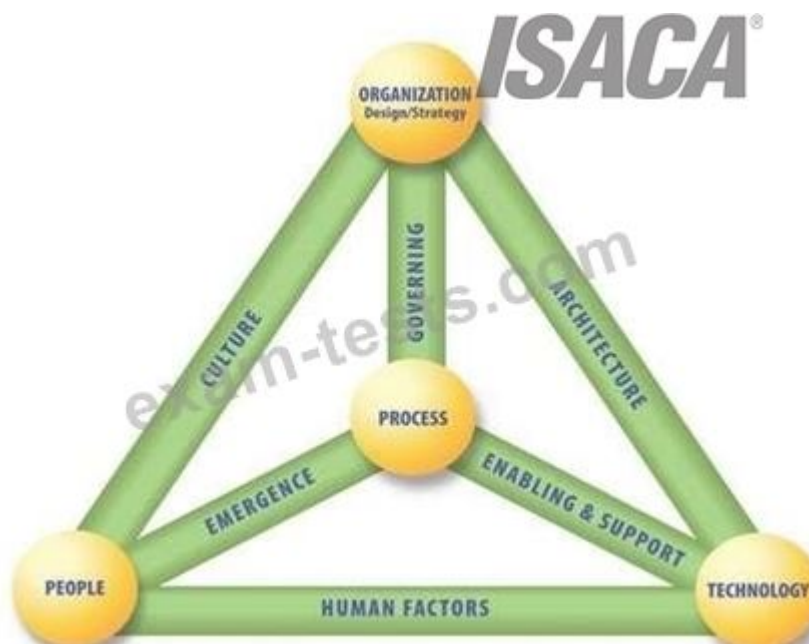
For your exam you should know the information below.

Business Model for Information Security

The Business Model for Information Security (BMIS) originated at the Institute for Critical Information Infrastructure Protection at the Marshall School of Business at the University of Southern California in the USA. ISACA has undertaken the development of the Systemic Security Management Model. The BMIS takes a business-oriented approach to managing information security, building on the foundational concepts developed by the Institute. The model utilizes systems thinking to clarify complex relationships within the enterprise, and thus to more effectively manage security. The elements and dynamic interconnections that form the basis of the model establish the boundaries of an information security program and model how the program functions and reacts to internal and external change. The BMIS provides the context for frameworks such as Cubit.

The essence of systems theory is that a system needs to be viewed holistically - not merely as a sum of its parts - to be accurately understood. A holistic approach examines the system as a complete functioning unit. Another tenet of systems theory is that one part of the system enables understanding of other parts of the system. "Systems thinking" is a widely recognized term that refers to the examination of how systems interact, how complex systems work and why "the whole is more than the sum of its parts." Systems theory is most accurately described as a complex network of events, relationships, reactions, consequences, technologies, processes and people that interact in often unseen and unexpected ways. Studying the behaviors and results of the interactions can assist the manager to better understand the organizational system and the way it functions. While management of any discipline within the enterprise can be enhanced by approaching it from a systems thinking perspective, its implementation will certainly help with managing risk.

The success that the systems approach has achieved in other fields bodes well for the benefits it can bring to security. The often dramatic failures of enterprises to adequately address security issues in recent years are due, to a significant extent, to their inability to define security and present it in a way that is comprehensible and relevant to all stakeholders. Utilizing a systems approach to information security management will help information security managers address complex and dynamic environments, and will generate a beneficial effect on collaboration within the enterprise, adaptation to operational change, navigation of strategic uncertainty and tolerance of the impact of external factors. The model is represented below.



As illustrated in above, the model is best viewed as a flexible, three-dimensional, pyramid-shaped structure made up of four elements linked together by six dynamic interconnections.

All aspects of the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, the equilibrium of the model is potentially at risk. The dynamic interconnections act as tensions, exerting a push/pull force in reaction to changes in the enterprise, allowing the model to adapt as needed.

The four elements of the model are:

1. Organization Design and Strategy - organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal.

An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued. It is the enterprise's formula for success and sets its basic direction. The strategy should adapt to external and internal factors. Resources are the primary material to design the strategy and can be of different types (people, equipment, know-how). Design defines how the organization implements its strategy. Processes, culture and architecture are important in determining the design.

2. People - The human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors and biases. Internally, it is critical for the information security manager to work with the human resources and legal departments to address issues such as: Recruitment strategies (access, background checks, interviews, roles and responsibilities) Employment issues (location of office, access to tools and data, training and awareness, movement within the enterprise) Termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees). Externally, customers, suppliers, media, stakeholders and others can have a strong influence on the enterprise and need to be considered within the security posture.

3. Process - Includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections.

Processes identify, measure, manage and control risk, availability, integrity and confidentiality, and they also ensure accountability. They derive from the strategy and implement the operational part of the organization element.

To be advantageous to the enterprise, processes must:

Meet business requirements and align with policy

Consider emergence and be adaptable to changing requirements

Be well documented and communicated to appropriate human resources

Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness

4. Technology - Composed of all of the tools, applications and infrastructure that make processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risk. Given the typical enterprise's dependence on technology, technology constitutes a core part of the enterprise's infrastructure and a critical component in accomplishing its mission.

Technology is often seen by the enterprise's management team as a way to resolve security threats and risk. While technical controls are helpful in mitigating some types of risk, technology should not be viewed as an information security solution.

Technology is greatly impacted by users and by organizational culture. Some individuals still mistrust technology; some have not learned to use it; and others feel it slows them down.

Regardless of the reason, information security managers must be aware that many people will try to sidestep technical controls.

Dynamic Interconnections

The dynamic interconnections are what link the elements together and exert a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium.

The six dynamic interconnections are:

1. Governing - Governing is the steering of the enterprise and demands strategic leadership.

Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

2. Culture - Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/ regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

3. Enabling and support - The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

4. Emergence - Emergence - which connotes surfacing, developing, growing and evolving - refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

5. Human factors - The human factors dynamic interconnection represents the interaction and gap between technology and people and, as such, is critical to an information security program. If people do not understand how to use the technology, do not embrace the technology or will not follow pertinent policies, serious security problems can evolve. Internal threats such as data leakage, data theft and misuse of data can occur within this dynamic interconnection. Human factors may arise because of age, experience level and/or cultural experiences. Because human factors are critical components in maintaining balance within the model, it is important to train all of the enterprise's human resources on pertinent skills.

6. Architecture - A security architecture is a comprehensive and formal encapsulation of the people, processes, policies and technology that comprise an enterprise's security practices. A robust business information architecture is essential to understanding the need for security and designing the security architecture. It is within the architecture dynamic interconnection that the enterprise can ensure defense in depth. The design describes how the security controls are positioned and how they relate to the overall IT architecture. An enterprise security architecture facilitates security capabilities across lines of businesses in a consistent and a cost-effective manner and enables enterprises to be proactive with their security investment decisions.

The following answers are incorrect:

Governing - Governing is the steering of the enterprise and demands strategic leadership.

Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions.

Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

Enabling and support - The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with

technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

Culture - Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/ regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

Reference:

CISA review manual 2014 page number 37 and 38

<http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf>

NEW QUESTION: 386

Which of the following is the BEST way for an organization to mitigate the risk associated with third-party application performance?

- A.** Ensure the third party allocates adequate resources to meet requirements.
- B.** Use analytics within the internal audit function
- C.** Conduct a capacity planning exercise
- D.** Utilize performance monitoring tools to verify service level agreements (SLAs)

Answer: D ([LEAVE A REPLY](#))

Explanation

The best way for an organization to mitigate the risk associated with third-party application performance is to utilize performance monitoring tools to verify service level agreements (SLAs). Performance monitoring tools are software or hardware devices that measure and report the performance of an application or system, such as speed, availability, reliability, etc. Performance monitoring tools can help mitigate the risk associated with third-party application performance, by allowing the organization to verify whether the third-party provider is meeting the SLAs, which are contracts or agreements that define the expected level and quality of service for an application or system. Performance monitoring tools can also help identify and resolve any performance issues or problems that may arise from the third-party application. Ensuring the third party allocates adequate resources to meet requirements is a possible way to mitigate the risk associated with

third-party application performance, but it is not the best one, as it may not be feasible or effective depending on the availability, cost, and suitability of the resources. Using analytics within the internal audit function is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be timely or relevant depending on the frequency, scope, and quality of the analytics. Conducting a capacity planning exercise is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be accurate or reliable depending on the assumptions, methods, and data used for the capacity planning.

NEW QUESTION: 387

Which of the following is MOST important for an IS auditor to verify when reviewing the planned use of Benford's law as a data analytics technique to detect fraud in a set of credit card transactions?

- A.** The transactions are in double integer format.
- B.** The transaction amounts are selected randomly without restriction.
- C.** The transaction analysis is limited to transactions within standard deviation.
- D.** The transactions are all in the same currency.

Answer: D ([LEAVE A REPLY](#))

Benford's Law analyzes numerical data to detect anomalies based on the frequency distribution of leading digits. For it to be effective, the dataset must follow specific criteria, including consistency in measurement units. If transactions are in different currencies, the leading digits can vary due to currency conversion rates, invalidating the analysis.

* Double Integer Format (Option A): Benford's Law applies to any set of numerical data, not specifically double integers.

* Random Selection of Transactions (Option B): The data set must represent the entire population, not a random selection.

* Limiting Analysis to Standard Deviations (Option C): This is irrelevant to the application of Benford's Law.

Reference: ISACA CISA Review Manual, Job Practice Area 2: Information Systems Audit and Assurance.

NEW QUESTION: 388

A system was recently promoted to the production environment. An IS auditor has been asked by senior management to update the annual IT audit plan. Which of the following should be the auditor's NEXT course of action?

- A.** Update the risk assessment to include the new system.
- B.** Update the audit plan to include the new system
- C.** Maintain the plan with no changes and perform a separate review of the new system
- D.** Contract with a third party to conduct an audit of the new system.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 389

An organization is concerned about duplicate vendor payments on a complex system with a high volume of transactions. Which of the following would be MOST helpful to an IS auditor to determine whether duplicate vendor payments exist?

- A. Computer-assisted technique
- B. Stratified sampling
- C. Statistical sampling
- D. Process walk-through

Answer: A ([LEAVE A REPLY](#))

The most helpful technique for an IS auditor to determine whether duplicate vendor payments exist is Computer-assisted technique, which is discussed in ISACA's CISA Study Manual. According to the manual, computer-assisted techniques use computerized techniques to identify potential errors and irregularities in a system. These techniques can be used to detect errors such as duplicate payments, which can be easily missed in manual systems. In addition, these techniques can be used to analyze data to detect patterns or trends that may indicate fraud or misappropriation of funds.

NEW QUESTION: 390

Which of the following BEST contributes to the quality of an audit of a business-critical application?

- A. Reviewing previous findings reported by the application owner
- B. Assigning the audit to independent external auditors
- C. Identifying common coding errors made by the development team
- D. Involving the application owner early in the audit planning process

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 391

Which of the following Confidentiality, Integrity, Availability (CIA) attribute supports the principle of least privilege by providing access to information only to authorized and intended users?

- A. Confidentiality
- B. Integrity
- C. Availability
- D. Accuracy

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Confidentiality supports the principle of "least privilege" by providing that only authorized individuals, processes, or systems should have access to information on a need-to-know basis. The level of access that an authorized individual should have is at the level necessary for them to do their job. In recent years, much press has been dedicated to the privacy of information and the need to protect it from individuals, who may be able to commit crimes by viewing the information.

Identity theft is the act of assuming one's identity through knowledge of confidential information obtained from various sources.

An important measure to ensure confidentiality of information is data classification. This helps to determine who should have access to the information (public, internal use only, or confidential). Identification, authentication, and authorization through access controls are practices that support maintaining the confidentiality of information.

A sample control for protecting confidentiality is to encrypt information. Encryption of information limits the usability of the information in the event it is accessible to an unauthorized person.

For your exam you should know the information below:

Integrity

Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes.

Information stored in files, databases, systems, and networks must be relied upon to accurately process transactions and provide accurate information for business decision making. Controls are put in place to ensure that information is modified through accepted practices.

Sample controls include management controls such as segregation of duties, approval checkpoints in the systems development life cycle, and implementation of testing practices that assist in providing information integrity. Well-formed transactions and security of the update programs provide consistent methods of applying changes to systems. Limiting update access to those individuals with a need to access limits the exposure to intentional and unintentional modification.

Availability

Availability is the principle that ensures that information is available and accessible to users when needed.

The two primary areas affecting the availability of systems are:

1. Denial-of-Service attacks and
2. Loss of service due to a disaster, which could be man-made (e.g., poor capacity planning resulting in system crash, outdated hardware, and poor testing resulting in system crash after upgrade) or natural (e.g., earthquake, tornado, blackout, hurricane, fire, and flood).

In either case, the end user does not have access to information needed to conduct business.

The criticality of the system to the user and its importance to the survival of the organization will determine how significant the impact of the extended downtime becomes. The lack of appropriate security controls can increase the risk of viruses, destruction of data, external penetrations, or denial-of-service (DOS) attacks.

Such events can prevent the system from being used by normal users.

CIA

The following answers are incorrect:

Integrity- Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes.

Availability - Availability is the principle that ensures that information is available and accessible to users when needed.

Accuracy - Accuracy is not a valid CIA attribute.



Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 314

Official ISC2 guide to CISSP CBK 3rd Edition Page number 350

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 392

Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?

- A. Halon gas
- B. Wet-pipe sprinklers
- C. Dry-pipe sprinklers
- D. Carbon dioxide gas

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: Water sprinklers, with an automatic power shutoff system, are accepted as efficient because they can be set to automatic release without threat to life, and water is environmentally friendly.

Sprinklers must be dry-pipe to prevent the risk of leakage. Halon is efficient and effective as it does not threaten human life and, therefore, can be set to automatic release, but it is environmentally damaging and very expensive. Water is an acceptable medium but the pipes should be empty to avoid leakage, so a full system is not a viable option. Carbon dioxide is accepted as an environmentally acceptable gas, but it is less efficient because it cannot be set to automatic release in a staffed site since it threatens life.

NEW QUESTION: 393

The waterfall life cycle model of software development is most appropriately used when:

A. requirements are well understood and are expected to remain stable, as is the business environment in

which the system will operate.

B. requirements are well understood and the project is subject to time pressures.

C. the project intends to apply an object-oriented design and programming approach.

D. the project will involve the use of new technology.

Answer: A (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

Historically, the waterfall model has been best suited to the stable conditions described in choice A. When the degree of uncertainty of the system to be delivered and the conditions in which it will be used

rises, the waterfall model has not been successful, in these circumstances, the various forms of iterative

development life cycle gives the advantage of breaking down the scope of the overall system to be

delivered, making the requirements gathering and design activities more manageable. The ability to deliver

working software earlier also acts to alleviate uncertainty and may allow an earlier realization of benefits.

The choice of a design and programming approach is not itself a determining factor of the type of software

development life cycle that is appropriate. The use of new technology in a project introduces a significant

element of risk. An iterative form of development, particularly one of the agile methods that focuses on

early development of actual working software, is likely to be the better option to manage this uncertainty.

NEW QUESTION: 394

A new information security manager is charged with reviewing and revising the information security

strategy. The information security manager's FIRST course of action should be to gain an understanding of

the organization's:

A. security architecture

B. risk register

C. internal control framework

D. business strategy

Answer: D (LEAVE A REPLY)

NEW QUESTION: 395

Fault-tolerance is a feature particularly sought-after in which of the following kinds of computer systems (choose all that apply):

- A. desktop systems
- B. laptop systems
- C. handheld PDAs
- D. business-critical systems
- E. None of the choices.

Answer: D (LEAVE A REPLY)

Fault-tolerance enables a system to continue operating properly in the event of the failure of some parts of it. It avoids total breakdown, and is particularly sought-after in high-availability environment full of businesscritical systems.

NEW QUESTION: 396

When planning a follow-up, the IS auditor is informed by operational management that recent organizational changes have addressed the previously identified risk and implementing the action plan is no longer necessary. What should the auditor do NEXT?

- A. Report that the changes make it impractical to determine whether the risks have been addressed.
- B. Accept management's assertion and report that the risks have been addressed.
- C. Determine whether the changes have introduced new risks that need to be addressed.
- D. Review the changes and determine whether the risks have been addressed.

Answer: (SHOW ANSWER)

When operational management informs the IS auditor that recent organizational changes have addressed previously identified risks and implementing the action plan is no longer necessary, the IS auditor should accept management's assertion and report that the risks have been addressed. However, it is essential to document this communication and ensure that there is evidence supporting management's claim. If there are any doubts or concerns, further investigation may be necessary. The auditor should not assume new risks without proper assessment or evidence¹.

References: 1(<https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/enhancing-the-audit-follow-up-process-using-cobit-5>)

NEW QUESTION: 397

A third-party service provider has proposed a data loss prevention (DLP) solution. Which of the following

MUST be in place for this solution to be relevant to the organization?

- A. An adequate data testing environment
- B. Senior management support
- C. A business case

D. A data classification

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 398

Which of the following is the MOST effective control to reduce the risk of information leakage through social media?

- A. Security awareness training
- B. Use of keystroke loggers
- C. Periodic review of the data classification policy
- D. Limited access to social media sites in the workplace

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 399

A programmer maliciously modified a production program to change data and then restored the original code. Which of the following would MOST effectively detect the malicious activity?

- A. Comparing source code
- B. Reviewing system log files
- C. Comparing object code
- D. Reviewing executable and source code integrity

Answer: B ([LEAVE A REPLY](#))

Reviewing system log files is the only trail that may provide information about the unauthorized activities in the production library. Source and object code comparisons are ineffective, because the original programs were restored and do not exist. Reviewing executable and source code integrity is an ineffective control, because integrity between the executable and source code is automatically maintained.

NEW QUESTION: 400

An IS auditor who is reviewing incident reports discovers that, in one instance, an important document left on an employee's desk was removed and put in the garbage by the outsourced cleaning staff. Which of the following should the IS auditor recommend to management?

- A. Stricter controls should be implemented by both the organization and the cleaning agency.
- B. No action is required since such incidents have not occurred in the past.
- C. A clear desk policy should be implemented and strictly enforced in the organization.
- D. A sound backup policy for all important office documents should be implemented.

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

Explanation:

An employee leaving an important document on a desk and the cleaning staff removing it may result in a serious impact on the business. Therefore, the IS auditor should recommend that strict

controls be implemented by both the organization and the outsourced cleaning agency. That such incidents have not occurred in the past does not reduce the seriousness of their impact. Implementing and monitoring a clear desk policy addresses only one part of the issue. Appropriate confidentiality agreements with the cleaning agency, along with ensuring that the cleaning staff has been educated on the dos and don'ts of the cleaning process, are also controls that should be implemented. The risk here is not a loss of data, but leakage of data to unauthorized sources. A backup policy does not address the issue of unauthorized leakage of information.

NEW QUESTION: 401

Organizations should use off-site storage facilities to maintain _____ (fill in the blank) of current and critical information within backup files.

- A. Confidentiality
- B. Integrity
- C. Redundancy
- D. Concurrency

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation: Redundancy is the best answer because it provides both integrity and availability. Organizations should use off-site storage facilities to maintain redundancy of current and critical information within backup files.

NEW QUESTION: 402

Which of the following is MOST important for an IS auditor to validate when reviewing the controls for an organization's quality management system (QMS)?

- A. Whether there is a process to monitor continuous improvement areas and necessary targets
- B. Whether root cause analysis is performed on all failed and rejected changes
- C. Whether critical services are delivered in a timely and sustainable manner
- D. Whether the organization follows an industry-recognized service management framework

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 403

An IS Auditor is performing a business continuity plan (BCP) audit and identifies that the plan has not been tested for five years, however, the plan was successfully activated during a recent extended power outage. Which of the following is the 15 auditor's BEST count of action?

- A. Determine if a follow-up BCP audit is required to identify future gaps
- B. Determine if the business impact analysis (BIA) is still accurate.
- C. Determine if the annual BCP training program is in need of review
- D. Determine if lessons learned from the activation were incorporated into the plan

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 404

As part of a payroll department IS audit, which of the following is the PRIMARY reason an IS auditor would recommend that a supervisor review exception reports before authorizing payments?

- A. To evaluate gaps between employee performance and salary adjustments
- B. To identify unusual fluctuations or changes in any employee's monthly pay
- C. To verify the accuracy of bank account information for payroll deposit
- D. To collect statistical information in preparation for future pay scale reviews

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 405

Which of the following insurance types provide for a loss arising from fraudulent acts by employees?

- A. Business interruption
- B. Fidelity coverage
- C. Errors and omissions
- D. Extra expense

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

Fidelity insurance covers the loss arising from dishonest or fraudulent acts by employees.

Business interruption insurance covers the loss of profit due to the disruption in the operations of an organization.

Errors and omissions insurance provides legal liability protection in the event that the professional practitioner commits an act that results in financial loss to a client. Extra expense insurance is designed to cover the extra costs of continuing operations following a disaster/disruption within an organization.

NEW QUESTION: 406

Which type of risk would MOST influence the selection of a sampling methodology?

- A. Inherent
- B. Residual
- C. Control
- D. Detection

Answer: D ([LEAVE A REPLY](#))

The type of risk that would most influence the selection of a sampling methodology is detection risk (option D). This is because:

Detection risk is the risk that the auditor will not detect a material misstatement that exists in an assertion¹. Detection risk depends on the effectiveness of the audit procedures and how well they are applied by the auditor¹.

The selection of a sampling methodology is part of the design of audit procedures, which aims to reduce detection risk to an acceptable level¹. The auditor should consider the following factors when selecting a sampling methodology²³:

The objectives of the audit procedure and the related assertions.

The characteristics of the population from which the sample will be drawn, such as its size, homogeneity, and structure.

The sampling technique to be used, such as random, systematic, haphazard, or judgmental.

The sample size and the method of selecting sample items.

The evaluation of the sample results and the projection of errors to the population.

The auditor should also consider the advantages and disadvantages of different sampling methodologies, such as statistical and non-statistical sampling²³. Statistical sampling is a sampling technique that uses random selection and probability theory to evaluate sample results. Non-statistical sampling is a sampling technique that does not use random selection or probability theory to evaluate sample results. Some of the advantages and disadvantages are as follows²³: Statistical sampling allows the auditor to measure and control sampling risk, which is the risk that the sample is not representative of the population. Statistical sampling also allows the auditor to quantify the precision and reliability of the sample results. However, statistical sampling requires more technical knowledge and skills, as well as more time and cost, than non-statistical sampling. Non-statistical sampling relies on the auditor's professional judgment and experience to select and evaluate sample items. Non-statistical sampling is more flexible and less complex than statistical sampling. However, non-statistical sampling does not provide an objective basis for measuring and controlling sampling risk, nor does it allow the auditor to quantify the precision and reliability of the sample results.

Therefore, the type of risk that would most influence the selection of a sampling methodology is detection risk (option D), as it determines how effective and efficient the audit procedures should be in order to provide sufficient appropriate audit evidence.

References: 1: Audit Sampling - Overview, Purpose, Importance, and Types 2: Audit Sampling | Auditing and Attestation | CPA Exam FAR 3: Audit Sampling | ACCA Qualification | Students | ACCA Global

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

NEW QUESTION: 407

An organization is choosing key performance indicators (KPIs) for its information security management. Which of the following KPIs would provide stakeholders with the MOST useful information about whether information security risk is being managed?

- A. The number of security incidents during the past quarter
- B. Time from identifying a security threat to implementing a solution
- C. The number of security controls implemented
- D. Time from initial reporting of an incident to appropriate escalation

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 408

Which of the following is the BEST way for an organization that is using a Software as a Service (SaaS) application to reduce its risk associated with the collection and protection of personal information?

- A. Limit the amount of personal information collected to industry standards.
- B. Limit the amount of personal information collected to the minimum required.
- C. Encrypt personal information held by the organization.
- D. Only allow remote access to personal information from an alternate site.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 409

Which of the following would BEST manage the risk of changes in requirements after the analysis phase of a business application development project?

- A. Sign-off from the IT team
- B. Expected deliverables meeting project deadlines
- C. Quality assurance (QA) review
- D. Ongoing participation by relevant stakeholders

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 410

When auditing the security architecture of an online application, an IS auditor should FIRST review the:

- A. firmware version of the firewall
- B. configuration of the firewall
- C. firewall standards.
- D. location of the firewall within the network

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 411

Disaster recovery planning (DRP) addresses the:

- A. technological aspect of business continuity planning.
- B. operational piece of business continuity planning.
- C. functional aspect of business continuity planning.
- D. overall coordination of business continuity planning.

Answer: A ([LEAVE A REPLY](#))

Disaster recovery planning (DRP) is the technological aspect of business continuity planning. Business resumption planning addresses the operational part of business continuity planning.

NEW QUESTION: 412

An IS auditor finds that the access-controlled doors to a work area are kept unlocked during power outages. Which of the following is the auditor's BEST course of action?

- A. Recommend keeping the doors locked at all times.
- B. Confirm whether the practice complies with the security policy.
- C. Report the finding to management as high-risk.
- D. Determine whether there are compensating controls.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 413

An IS auditor is evaluating the progress of a web-based customer service application development project.

Which of the following would be MOST helpful for this evaluation?

- A. Backlog consumption reports
- B. Critical path analysis reports
- C. Developer status reports
- D. Change management logs

Answer: A ([LEAVE A REPLY](#))

Explanation

A backlog consumption report is a report that shows the amount of work that has been completed and the amount of work that remains to be done in a project. It is a useful tool for measuring the progress and performance of a web-based customer service application development project, as it can indicate whether the project is on track, ahead or behind schedule, and how much effort is required to finish the project. A backlog consumption report can also help identify any issues or risks that may affect the project delivery. Critical path analysis reports, developer status reports and change management logs are also helpful for evaluating a project, but they are not as helpful as a backlog consumption report, as they do not provide a clear picture of the overall project status and completion rate. References:

- 1: [Backlog Consumption Report Definition]
- 2: Backlog Consumption Report | ISACA

NEW QUESTION: 414

Which of the following is the MAIN purpose of an information security management system?

- A. To identify and eliminate the root causes of information security incidents
- B. To enhance the impact of reports used to monitor information security incidents
- C. To keep information security policies and procedures up-to-date
- D. To reduce the frequency and impact of information security incidents

Answer: D ([LEAVE A REPLY](#))

The main purpose of an information security management system (ISMS) is to reduce the frequency and impact of information security incidents. An ISMS is a systematic approach to managing information security risks, policies, procedures, and controls within an organization. An ISMS aims to ensure the confidentiality, integrity, and availability of information assets, as well as to comply with relevant laws and regulations. The other options are not the main purpose of an ISMS, but rather some of its possible benefits or components.

References:

* CISA Review Manual (Digital Version), Chapter 7, Section 7.11

* CISA Review Questions, Answers & Explanations Database, Question ID 205

NEW QUESTION: 415

Which of the following is the BEST indicator to measure service quality of change and incident management processes outsourced to an external provider?

- A. Percentage of requests resolved within the service level agreement (SLA)
- B. Total number of reopened service requests
- C. Total number of resolved service requests
- D. Average wait time for service request resolution

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 416

In which of the following sampling methods is the entire sample considered to be irregular if a single error is found?

- A. Stop-or-go sampling
- B. Variable sampling
- C. Judgmental sampling
- D. Discovery sampling

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 417

An online retailer is receiving customer complaints about receiving different items from what they ordered on the organization's website. The root cause has been traced to poor data quality. Despite efforts to clean erroneous data from the system, multiple data quality issues continue to occur. Which of the following recommendations would be the BEST way to reduce the likelihood of future occurrences?

- A. Implement business rules to validate employee data entry.
- B. Assign responsibility for improving data quality.
- C. Outsource data cleansing activities to reliable third parties.
- D. Invest in additional employee training for data entry.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 418

During a project assessment, an IS auditor finds that business owners have been removed from the project initiation phase. Which of the following should be the auditor's GREATEST concern with this situation?

- A. Unrealistic milestones
- B. Inadequate deliverables
- C. Unclear benefits
- D. Incomplete requirements

Answer: D ([LEAVE A REPLY](#))

According to the ISACA CISA Study Manual (2020), it is important that business owners are involved in the project initiation phase in order to ensure that the project is aligned with the organization's objectives and that the necessary requirements have been identified (p. 183). Therefore, the IS auditor's greatest concern should be that incomplete requirements may have been identified due to the lack of business owner involvement in the project initiation phase.

NEW QUESTION: 419

During a review of a business continuity plan, an IS auditor noticed that the point at which a situation is declared to be a crisis has not been defined. The MAJOR risk associated with this is that:

- A. assessment of the situation may be delayed.
- B. execution of the disaster recovery plan could be impacted.
- C. notification of the teams might not occur.
- D. potential crisis recognition might be ineffective.

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation: Execution of the business continuity plan would be impacted if the organization does not know when to declare a crisis. Choices A, C and D are steps that must be performed to know whether to declare a crisis. Problem and severity assessment would provide information necessary in declaring a disaster.

Once a potential crisis is recognized, the teams responsible for crisis management need to be notified.

Delaying this step until a disaster has been declared would negate the effect of having response teams.

Potential crisis recognition is the first step in responding to a disaster.

NEW QUESTION: 420

Which of the following is the BEST way to determine if IT is delivering value to the business?

- A. Distribute surveys to various end users of IT services.
- B. Interview key IT managers and service providers.
- C. Review IT service level agreement (SLA) metrics.
- D. Analyze downtime frequency and duration.

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

A service level agreement (SLA) is a written document, which officially describe the details of services, in non-technical terms, provided by the IT department (internal or external) to its customers. The aim of SLA is to maintain and improve the customer satisfaction to an agreed level.

NEW QUESTION: 421

An audit identified that a computer system is not assigning sequential purchase order numbers to order requests. The IS auditor is conducting an audit follow-up to determine if management has reserved this finding. Which of two following is the MOST reliable follow-up procedure?

- A. Inspect the system settings and transaction logs to determine if sequential order numbers are generated.
- B. Examine a sample of system generated purchase orders obtained from management
- C. Inquire with management if the system has been configured and tested to generate sequential order numbers.
- D. Review the documentation of recant changes to implement sequential order numbering.

Answer: ([SHOW ANSWER](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As

Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 422

When performing an audit of a client relationship management (CRM) system migration project, which of the following should be of GREATEST concern to an IS auditor?

- A. The technical migration is planned for a Friday preceding a long weekend, and the time window is too short for completing all tasks.

- B.** Employees pilot-testing the system are concerned that the data representation in the new system is completely different from the old system.
- C.** A single implementation is planned, immediately decommissioning the legacy system.
- D.** Five weeks prior to the target date, there are still numerous defects in the printing functionality of the new system's software.

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Major system migrations should include a phase of parallel operation or a phased cut-over to reduce implementation risks. Decommissioning or disposing of the old hardware would complicate any fallback strategy, should the new system not operate correctly. A weekend can be used as a time buffer so that the new system will have a better chance of being up and running after the weekend. A different data representation does not mean different data presentation at the front end. Even when this is the case, this issue can be solved by adequate training and user support. The printing functionality is commonly one of the last functions to be tested in a new system because it is usually the last step performed in any business event. Thus, meaningful testing and the respective error fixing are only possible after all other parts of the software have been successfully tested.

NEW QUESTION: 423

Which of the following is a form of Hybrid Cryptography where the sender encrypts the bulk of the data using Symmetric Key cryptography and then communicates securely a copy of the session key to the receiver?

- A.** Digital Envelope
- B.** Digital Signature
- C.** Symmetric key encryption
- D.** Asymmetric

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

A Digital Envelope is used to send encrypted information using symmetric keys, and the relevant session key along with it. It is a secure method to send electronic document without compromising the data integrity, authentication and non-repudiation, which were obtained with the use of symmetric keys.

A Digital envelope mechanism works as follows:

The symmetric key, which is used to encrypt the bulk of the data or message can be referred to as session key. It is simply a symmetric key picked randomly in the key space.

In order for the receiver to have the ability to decrypt the message, the session key must be sent to the receiver.

This session key cannot be sent in clear text to the receiver, it must be protected while in transit, else anyone who have access to the network could have access to the key and confidentiality can easily be compromised.

Therefore, it is critical to encrypt and protect the session key before sending it to the receiver. The session key is encrypted using receiver's public key. Thus providing confidentiality of the key. The encrypted message and the encrypted session key are bundled together and then sent to the receiver who, in turn opens the session key with the receiver matching private key.

The session key is then applied to the message to get it in plain text.

The process of encrypting bulk data using symmetric key cryptography and encrypting the session key with a public key algorithm is referred as a digital envelope. Sometimes people refer to it as Hybrid Cryptography as well.

The following were incorrect answers:

Digital-signature - A digital signature is an electronic identification of a person or entity created by using public key algorithm and intended to verify to recipient the integrity of the data and the identity of the sender. Applying a digital signature consist of two simple steps, first you create a message digest, then you encrypt the message digest with the sender's private key. Encrypting the message digest with the private key is the act of signing the message.

Symmetric Key Encryption - Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Asymmetric Key Encryption - The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other - as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both. Public-key algorithms are based on mathematical problems which currently admit no efficient solution that are inherent in certain integer factorization, discrete logarithm, and elliptic curve relationships. It is computationally easy for a user to generate their own public and private key-pair and to use them for encryption and decryption. The strength lies in the fact that it is "impossible" (computationally unfeasible) for a properly generated private key to be determined from its corresponding public key. Thus the public key may be published without compromising security, whereas the private key must not be revealed to anyone not authorized to read messages or perform digital signatures. Public key algorithms, unlike symmetric key algorithms, do not require a secure initial exchange of one (or more) secret keys between the parties.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 350 and 351

http://en.wikipedia.org/wiki/Public-key_cryptography

NEW QUESTION: 424

Which of the following activities should occur after a business impact analysis (BIA)?

- A.** Identify threats to the IT environment
- B.** Identify critical applications
- C.** Analyze recovery options
- D.** Review the computing and user environment

Answer: (SHOW ANSWER)

Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 425

A fire alarm system has been installed in the computer room. The MOST effective location for the fire alarm control panel would be inside the

- A. computer room closest to the uninterruptible power supply (UPS) module
- B. computer room closest to the server computers
- C. system administrators' office
- D. booth used by the building security personnel

Answer: (SHOW ANSWER)

Explanation

A fire alarm system is a device that detects and alerts people of the presence of fire or smoke in a building. A fire alarm control panel is the central unit that monitors and controls the fire alarm system. The most effective location for the fire alarm control panel would be inside the booth used by the building security personnel.

This is because:

The security personnel can quickly and easily access the fire alarm control panel in case of an emergency, and take appropriate actions such as notifying the fire department, evacuating the building, or resetting the system.

The fire alarm control panel can be protected from unauthorized access, tampering, or damage by the security personnel, who can also monitor its status and performance regularly.

The fire alarm control panel can be isolated from the computer room, which may be exposed to higher risks of fire or smoke due to the presence of electrical equipment, such as uninterruptible power supply (UPS) modules or server computers.

The fire alarm control panel can be connected to the computer room through a dedicated communication line, which can ensure reliable and timely transmission of signals and information between the two locations.

References:

[1]: Fire Alarm Control Panel - an overview | ScienceDirect Topics

[2]: Fire Alarm Control Panel - What is it and how does it work? | Fire Protection Online

[3]: Fire Alarm Control Panel Installation Guide - XLS3000 - Honeywell

NEW QUESTION: 426

Which of the following is MOST important for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA) to automate routine business tasks?

- A. The end-to-end process is understood and documented.
- B. Roles and responsibilities are defined for the business processes in scope.
- C. A request for proposal (RFP) has been issued to qualified vendors.
- D. A benchmarking exercise of industry peers who use RPA has been completed.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 427

Which of the following is the MOST important consideration when evaluating the data retention policy for a global organization with regional offices in multiple countries?

- A. The policy aligns with corporate policies and practices.
- B. The policy aligns with global best practices.
- C. The policy aligns with business goals and objectives.
- D. The policy aligns with local laws and regulations.

Answer: D ([LEAVE A REPLY](#))

The data retention policy for a global organization with regional offices in multiple countries should align with local laws and regulations, as they may vary significantly from one country to another and may impose different requirements and penalties for non-compliance. The policy should also consider the corporate policies and practices, the global best practices, and the business goals and objectives, but these are secondary to the legal compliance. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.3: Data Classification and Protection

NEW QUESTION: 428

An information security manager has identified and implemented migrating controls according to industry

best practices. Which of the following is the GREATEST risk associated with this approach?

- A. Important security controls may be missed without senior management input.
- B. The cost of control implementation may be too high.
- C. The migration measures may not be updated in a timely manner.
- D. The security program may not be aligned with organizational objectives.

Answer: ([SHOW ANSWER](#))

Section: Governance and Management of IT

NEW QUESTION: 429

An IS auditor is reviewing a bank's service level agreement (SLA) with a third-party provider that hosts the bank's secondary data center, which of the following findings should be of GREATEST concern to the auditor?

- A. The recovery time objective (RTO) has a longer duration than documented in the disaster recovery plan (ORP).
- B. The SLA has not been reviewed in more than a year.
- C. Backup data is hosted online only.
- D. The recovery point objective (RPO) has a shorter duration than documented in the disaster recovery plan (DRP).

Answer: A ([LEAVE A REPLY](#))

The recovery time objective (RTO) has a longer duration than documented in the disaster recovery plan (DRP) should be of greatest concern to the auditor when reviewing a bank's SLA with a third-party provider that hosts the bank's secondary data center. This is because the RTO is the maximum acceptable time for restoring a system or an application after a disaster or a disruption. A longer RTO than the DRP means that the bank may not be able to resume its critical business operations within the expected time frame, which may result in significant financial losses, reputational damage, customer dissatisfaction, or regulatory non-compliance¹².

The SLA has not been reviewed in more than a year is not the greatest concern, although it is a good practice to review and update the SLA periodically to ensure that it reflects the current business needs and expectations, as well as any changes in the service provider's capabilities or performance. However, a lack of review does not necessarily imply a lack of compliance or quality of service, as long as the SLA is still valid and enforceable³⁴.

Backup data is hosted online only is not the greatest concern, although it may pose some security risks if the backup data is not encrypted or protected by adequate access controls. Online backup data means that the backup data is stored on a remote server that can be accessed via the Internet, which may offer some advantages such as faster recovery, lower cost, and higher availability than offline backup data that is stored on physical media such as tapes or disks. However, online backup data also requires reliable network connectivity and bandwidth, as well as proper security measures to prevent unauthorized access or tampering⁵⁶.

The recovery point objective (RPO) has a shorter duration than documented in the DRP is not the greatest concern, although it may indicate some inconsistency or misalignment between the SLA and the DRP. The RPO is the maximum acceptable amount of data loss measured in time from a disaster or a disruption. A shorter RPO than the DRP means that the bank may lose less data than expected, which may be beneficial for its business continuity and recovery. However, a shorter RPO may also imply more frequent backups, which may increase the cost and complexity of the backup process

NEW QUESTION: 430

An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

- A.** variable sampling.
- B.** substantive testing.
- C.** compliance testing.
- D.** stop-or-go sampling.

Answer: C ([LEAVE A REPLY](#))

Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized. Variable sampling is used to estimate numerical values, such as dollar values. Substantive testing substantiates the integrity of actual processing, such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be

minimized. Stop-or-go sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.

NEW QUESTION: 431

A system administrator recently informed the IS auditor about the occurrence of several unsuccessful intrusion attempts from outside the organization. Which of the following is MOST effective in detecting such an intrusion?

- A. Using smart cards with one-time password
- B. Installing Biometrics-based authentication
- C. Periodically reviewing log files
- D. Configuring the router as a firewall

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 432

Which of the following would be of GREATEST concern to an IS auditor when a multi-function printer device is sent offsite for maintenance?

- A. Business impact during the maintenance period.
- B. The printout has to be redirected to another department.
- C. Internal memory does not automatically clear.
- D. Maintenance costs exceed the value of the device.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 433

Which of the following is the MOST effective way to detect as many abnormalities as possible during an IS audit?

- A. Conduct a walk-through of the process.
- B. Perform substantive testing on sampled records.
- C. Perform judgmental sampling of key processes.
- D. Use a data analytics tool to identify trends.

Answer: D ([LEAVE A REPLY](#))

A data analytics tool is the most effective way to detect as many abnormalities as possible during an IS audit, as it can process large volumes of data, perform complex calculations, and generate visualizations that reveal patterns, outliers, anomalies, or deviations from expected results. A data analytics tool can also help the auditor to test the entire population of data, rather than a sample, and to perform continuous auditing and monitoring.

References

ISACA CISA Review Manual, 27th Edition, page 256

What is Problem Solving? Steps, Process & Techniques | ASQ

Data Analytics for Auditors - IIA

NEW QUESTION: 434

The drives of a file server are backed up at a hot site. Which of the following is the BEST way to duplicate the files stored on the server for forensic analysis?

- A. Capture a bit-by-bit image of the file server's drives.
- B. Run forensic analysis software on the backup drive.
- C. Create a logical copy of the file server's drives.
- D. Replicate the server's volatile data to another drive.

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

NEW QUESTION: 435

Which of the following biometric access controls has the HIGHEST rate of false negatives?

- A. Iris recognition
- B. Fingerprint scanning
- C. Face recognition
- D. Retina scanning

Answer: B ([LEAVE A REPLY](#))

Among the options provided, fingerprint scanning has the highest rate of false negatives. False negatives occur when a biometric system fails to recognize an authentic individual. Factors such as skin conditions (wet, dry, greasy), finger injuries, and inadequate scanning can contribute to false negatives in fingerprint scanning¹. In comparison, iris recognition²³, face recognition⁴⁵, and retina scanning⁶⁷ generally have lower rates of false negatives.

References:

How Accurate are today's Fingerprint Scanners? - Biometric

25 Advantages and Disadvantages of Iris Recognition - Biometric Today

Iris Recognition Technology (or, Musings While Going through Airport ...

The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist | ITIF NIST Launches Studies into Masks' Effect on Face Recognition Software

Retinal scan - Wikipedia How accurate are retinal security scans - Smart Eye Technology

NEW QUESTION: 436

An outsourced recruitment vendor processes personally identifiable information (PII) related to an organization's new hires. Which of the following would be the GREATEST concern to an IS auditor reviewing the third-party risk management process?

- A. The vendor collects data using an external-facing web service.
- B. The vendor lacks a team of dedicated privacy professionals.
- C. The vendor uses a fourth party to host client data.
- D. The vendor is excluded from the third-party due diligence process.

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation:

The greatest concern is if the vendor is excluded from the organization's third-party due diligence process.

Without proper due diligence, the organization has no assurance that the vendor meets minimum security and privacy requirements, exposing PII to significant risk.

- * Option A: External-facing services carry risk but can be mitigated by proper controls.
- * Option B: Lack of dedicated privacy staff may increase risk, but controls may still exist.
- * Option C: Fourth-party hosting adds risk but is acceptable if included in due diligence.
- * Option D: Correct - exclusion from due diligence represents a fundamental breakdown in vendor risk management.

ISACA Reference: CISA Review Manual 27th Edition, Domain 5, section on third-party/vendor risk management and data privacy.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 437

What kind of testing should programmers perform following any changes to an application or system?

- A. Unit, module, and full regression testing
- B. Module testing
- C. Unit testing
- D. Regression testing

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

Programmers should perform unit, module, and full regression testing following any changes to an application or system.

NEW QUESTION: 438

In which phase of penetration testing would host detection and domain name system (DNS) interrogation be performed?

- A. Discovery
- B. Attacks
- C. Planning
- D. Reporting

Answer: A ([LEAVE A REPLY](#))

Penetration testing is a method of evaluating the security of a system or network by simulating an attack from a malicious source. Penetration testing typically consists of four phases: planning, discovery, attacks, and reporting. In the discovery phase, penetration testers gather information about the target system or network, such as host detection, domain name system (DNS) interrogation, port scanning, service identification, operating system fingerprinting, vulnerability scanning, etc. This information can help to identify potential entry points, weaknesses, or vulnerabilities that can be exploited in the subsequent attack phase. Host detection and DNS interrogation are techniques that can be used in the discovery phase to determine the active hosts and their IP addresses and hostnames on the target network. References: [ISACA CISA Review Manual 27th Edition], page 368.

NEW QUESTION: 439

Which of the following controls MOST efficiently ensures that orders transmitted from a sales office to a production warehouse are received accurately and completely?

- A. Transaction totals and record counts should be sent and reconciled before transaction processing.
- B. Parity checking should be incorporated into all data transmissions.
- C. Data should be sent back to the originating site and compared to what was sent to production.
- D. Continuity of numerical sequences for all sales orders should be checked.

Answer: B ([LEAVE A REPLY](#))

Section: Governance and Management of IT

NEW QUESTION: 440

Which of the following is MOST important for the improvement of an organization's incident response processes

- A. Post-event reviews by the incident response team
- B. Ongoing incident response training for users
- C. Periodic walk-through of incident response procedures
- D. Regular upgrades to incident management software

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 441

In which of the following sampling methods is the entire sample considered to be irregular if a single error is found?

- A. Discovery sampling
- B. Variable sampling
- C. Stop-or-go sampling
- D. Judgmental sampling

Answer: ([SHOW ANSWER](#)**)**

The sampling method in which the entire sample is considered to be irregular if a single error is found is discovery sampling. Discovery sampling is a type of statistical sampling that is used to

test for the existence of at least one occurrence of a specific characteristic or condition in a population. Discovery sampling is often used when the auditor expects the characteristic or condition to be very rare or nonexistent, and when any occurrence would have a significant impact on the audit objective. For example, discovery sampling can be used to test for fraud, noncompliance, or material misstatement.

Discovery sampling works by setting a very low tolerable error rate (the maximum rate of occurrence of the characteristic or condition that the auditor is willing to accept) and a high confidence level (the degree of assurance that the auditor wants to obtain). The auditor then selects a sample from the population using a random or systematic method, and examines each item in the sample for the presence or absence of the characteristic or condition. If no error is found in the sample, the auditor can conclude with a high level of confidence that the characteristic or condition does not exist or is very rare in the population. However, if one or more errors are found in the sample, the auditor cannot draw any conclusion about the population and must either expand the sample size or perform alternative procedures.

Discovery sampling differs from other sampling methods in that it does not allow for any errors in the sample.

Other sampling methods, such as variable sampling, stop-or-go sampling, or judgmental sampling, can tolerate some errors in the sample and use them to estimate the error rate or amount in the population. However, discovery sampling is designed to test for zero-tolerance situations, where any error would be unacceptable or material. Therefore, discovery sampling considers the entire sample to be irregular if a single error is found.

References:

- * Audit Sampling - Overview, Purpose, Importance, and Types¹
- * Audit Sampling - What Is It, Methods, Example, Advantage, Reason²
- * ISA 530: Audit sampling | ICAEW³
- * Audit Sampling - AICPA⁴

NEW QUESTION: 442

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

A. True

B. False

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

With the objective of mitigating the risk and impact of a major business interruption, a disaster recovery plan should endeavor to reduce the length of recovery time necessary and the costs associated with recovery. Although DRP results in an increase of pre-and post-incident

operational costs, the extra costs are more than offset by reduced recovery and business impact costs.

NEW QUESTION: 443

Cisco IOS based routers perform basic traffic filtering via which of the following mechanisms?

- A. datagram scanning
- B. access lists
- C. stateful inspection
- D. state checking
- E. link progressing
- F. None of the choices.

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

In addition to deploying stateful firewall, you may setup basic traffic filtering on a more sophisticated router.

As an example, on a Cisco IOS based router you may use ip access lists (ACL) to perform basic filtering on the network edge. Note that if they have denied too much traffic, something is obviously being too restrictive and you may want to reconfigure them.

NEW QUESTION: 444

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

- A. Cold site
- B. Hot site
- C. Alternate site
- D. Warm site

Answer: (SHOW ANSWER)

A cold site is often an acceptable solution for preparing for recovery of noncritical systems and data .

NEW QUESTION: 445

Which of the following IS functions can be performed by the same group or individual while still providing the proper segregation of duties?

- A. Computer operations and application Multiple versions of the same operating system programming
- B. Security administration and application programming
- C. Database administration and computer operations
- D. Application programming and systems analysis

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 446

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

- A. FAR
- B. EER
- C. ERR
- D. FRR

Answer: B ([LEAVE A REPLY](#))

When evaluating biometric access controls, a low equal error rate (EER) is preferred. EER is also called the crossover error rate (CER).

NEW QUESTION: 447

An IS auditor suspects an organization's computer may have been used to commit a crime Which of the following is the auditor's BEST course of action?

- A. Advise management of the ante after the investigation.
- B. Notify local law enforcement of the potential crime before further investigation
- C. Examine the computer to search for evidence supporting the suspicions
- D. Contact the modem response team to conduct an investigation

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 448

When evaluating whether the expected benefits of a project have been achieved, it is MOST important for an IS auditor to review:

- A. post-implementation issues.
- B. quality assurance results.
- C. the project schedule.
- D. the business case.

Answer: ([SHOW ANSWER](#)**)**

Section: The process of Auditing Information System

NEW QUESTION: 449

When conducting a penetration test of an organization's internal network, which of the following approaches would BEST enable the conductor of the test to remain undetected on the network?

- A. Use the IP address of an existing file server or domain controller.
- B. Pause the scanning every few minutes to allow thresholds to reset.
- C. Conduct the scans during evening hours when no one is logged-in.
- D. Use multiple scanning tools since each tool has different characteristics.

Answer: ([SHOW ANSWER](#)**)**

Section: Protection of Information Assets

Explanation:

Pausing the scanning every few minutes avoids overtaxing the network as well as exceeding thresholds that may trigger alert messages to the network administrator. Using the IP address of a server would result in an address contention that would attract attention. Conducting scans after hours would increase the chance of detection, since there would be less traffic to conceal ones activities. Using different tools could increase the likelihood that one of them would be detected by an intrusion detection system.

NEW QUESTION: 450

The PRIMARY purpose of an incident response plan is to:

- A.** reduce the impact of an adverse event on information assets.
- B.** increase the effectiveness of preventive controls.
- C.** reduce the maximum tolerable downtime (MTD) of impacted systems.
- D.** increase awareness of impacts from adverse events to IT systems.

Answer: A ([LEAVE A REPLY](#))

Explanation

The primary purpose of an incident response plan is to reduce the impact of an adverse event on information assets. An incident response plan is a set of instructions and procedures that guide the organization's actions in the event of a security breach, cyberattack, or other disruption that affects its information systems and data. An incident response plan aims to:

Detect and identify the incident as soon as possible.

Contain and isolate the incident to prevent further damage or spread.

Analyze and investigate the incident to determine its cause, scope, and impact.

Eradicate and eliminate the incident and its root causes from the affected systems and data.

Recover and restore the normal operations and functionality of the systems and data.

Learn and improve from the incident by documenting the lessons learned, best practices, and recommendations for future prevention and mitigation.

By following an incident response plan, the organization can minimize the negative consequences of an adverse event on its information assets, such as:

Loss or corruption of data or information.

Disclosure or theft of confidential or sensitive data or information.

Interruption or degradation of system or service availability or performance.

Legal or regulatory noncompliance or liability.

Financial or reputational loss or damage.

An incident response plan also helps the organization to demonstrate its due diligence and accountability in protecting its information assets and complying with its legal and contractual obligations.

The other options are not the primary purpose of an incident response plan, although they may be secondary benefits or outcomes of having one.

Increasing the effectiveness of preventive controls is not the primary purpose of an incident response plan.

Preventive controls are controls that aim to prevent or deter incidents from occurring in the first place, such as firewalls, antivirus software, encryption, authentication, etc. An incident response plan is a reactive control that deals with incidents after they have occurred. However, an incident response plan may help to improve the effectiveness of preventive controls by identifying and addressing their weaknesses or gaps.

Reducing the maximum tolerable downtime (MTD) of impacted systems is not the primary purpose of an incident response plan. MTD is a measure of how long an organization can tolerate a system or service outage before it causes unacceptable harm or loss to its business operations or objectives. An incident response plan may help to reduce the MTD of impacted systems by facilitating a faster and smoother recovery process.

However, reducing the MTD is not the main goal of an incident response plan, but rather a desired outcome.

Increasing awareness of impacts from adverse events to IT systems is not the primary purpose of an incident response plan. Awareness is a state of being informed or conscious of something. An incident response plan may help to increase awareness of impacts from adverse events to IT systems by providing information and communication channels for stakeholders, such as management, employees, customers, regulators, etc.

However, increasing awareness is not the main objective of an incident response plan, but rather a means to achieve other objectives, such as reducing impact, ensuring compliance, or maintaining trust.

NEW QUESTION: 451

An organization has recently moved to an agile model for deploying custom code to its in-house accounting software system. When reviewing the procedures in place for production code deployment, which of the following is the MOST significant security concern to address?

- A. Software vulnerability scanning is done on an ad hoc basis.
- B. Current DevSecOps processes have not been independently verified.
- C. Production code deployment is not automated.
- D. Change control does not include testing and approval from quality assurance (QA).

Answer: ([SHOW ANSWER](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 452

Which of the following provides the BEST evidence of an organization's disaster recovery readiness?

- A. A disaster recovery plan
- B. Customer references for the alternate site provider
- C. Processes for maintaining the disaster recovery plan
- D. Results of tests and drills

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Plans are important, but mere plans do not provide reasonable assurance unless tested.

References for the alternate site provider and the existence and maintenance of a disaster recovery plan are important, but only tests and drills demonstrate the adequacy of the plans and provide reasonable assurance of an organization's disaster recovery readiness.

NEW QUESTION: 453

An organization's information security policies should be developed PRIMARILY on the basis of:

- A. industry best practices.
- B. past information security incidents.
- C. a risk management process.
- D. enterprise architecture (EA).

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 454

Which of the following provides the MOST assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system?

- A. Loading balance and transaction data to the new system
- B. Running historical transactions through the new system
- C. Reviewing quality assurance (QA) procedures
- D. Comparing code between old and new systems

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 455

Which of the following is an IS auditor's BEST approach when preparing to evaluate whether the IT strategy supports the organization's vision and mission?

- A. Review strategic projects for return on investments (ROIs)
- B. Solicit feedback from other departments to gauge the organization's maturity
- C. Meet with senior management to understand business goals
- D. Review the organization's key performance indicators (KPIs)

Answer: (SHOW ANSWER)

The best approach for an IS auditor when preparing to evaluate whether the IT strategy supports the Organization's vision and mission is C. Meet with senior management to understand business

goals. According to the ISACA Certified Information Systems Auditor (CISA) Study Guide [1], IS auditors should meet with senior management to understand the organization's vision and mission, and the related business goals, objectives and strategies. This will help the auditor to assess whether the proposed IT strategy is aligned with the organization's overall objectives, and whether the information systems are providing the expected returns. Additionally, the IS auditor should understand the organization's risk appetite and risk management approach, as these will affect the design and implementation of the IT strategy.

NEW QUESTION: 456

Which of the following is MOST important when an incident may lead to prosecution?

- A. Right to perform e-discovery
- B. Adherence to incident response procedures
- C. Preservation of evidence
- D. Advice from legal counsel

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 457

Compared to developing a system in-house, acquiring a software package means that the need for testing by end users is:

- A. eliminated
- B. unchanged
- C. increased
- D. reduced

Answer: B ([LEAVE A REPLY](#))

Compared to developing a system in-house, acquiring a software package means that the need for testing by end users is unchanged. This is because end users are still the ultimate customers and beneficiaries of the system, and they need to ensure that the software package meets their requirements, expectations, and satisfaction. End user testing, also known as user acceptance testing (UAT) or beta testing, is the final stage of testing performed by the user or client to determine whether the software can be accepted or not¹. End user testing is important for both in-house developed and acquired software packages, as it helps to verify the functionality, usability, performance, and reliability of the system². End user testing also helps to identify and resolve any defects, errors, or issues that may not have been detected by the developers or vendors³.

Therefore, option B is the correct answer.

Option A is not correct because end user testing is not eliminated by acquiring a software package. Even though the software package may have been tested by the vendor or supplier, it may still have bugs, compatibility issues, or configuration problems that need to be fixed before deployment⁴. Option C is not correct because end user testing is not increased by acquiring a software package. The scope and extent of end user testing depend on various factors, such as the complexity, criticality, and customization of the system, and not on whether it is developed in-

house or acquired. Option D is not correct because end user testing is not reduced by acquiring a software package. The software package may still require modifications or integrations to suit the specific needs and environment of the organization, and these changes need to be tested by the end users.

References:

Chapter 4 Methods of Software Acquisition⁵

What is User Acceptance Testing (UAT): A Complete Guide¹

What Is End-to-End Testing? (With How-To and Example)³

How to Evaluate New Software in 5 Steps⁴

User Acceptance Testing (UAT) in ERP Projects

User Acceptance Testing for Packaged Software

NEW QUESTION: 458

What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

- A. An organizational certificate
- B. A user certificate
- C. A website certificate
- D. Authenticode

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

A website certificate is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption.

NEW QUESTION: 459

An IS auditor is evaluating the risks and controls associated with a virtualized environment. Which of the following observations should be of GREATEST concern?

- A. Offline and dormant virtual machine Images are not patched on the same cycle as online ones.
- B. The change management process has not been updated to include virtualized environments.
- C. The hypervisor's partitioning resources have not been modified from its default settings.
- D. The hypervisor's security settings are not reviewed on a regular basis.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 460

Which of the following should be the PRIMARY basis for prioritizing follow-up audits?

- A. Audit cycle defined in the audit plan
- B. Complexity of management's action plans
- C. Recommendation from executive management
- D. Residual risk from the findings of previous audits

Answer: D ([LEAVE A REPLY](#))

Residual risk from the findings of previous audits should be the primary basis for prioritizing follow-up audits, because it reflects the level of exposure and potential impact that remains after management has implemented corrective actions or accepted the risk. Follow-up audits should focus on verifying whether the residual risk is within acceptable levels and whether the corrective actions are effective and sustainable. Audit cycle defined in the audit plan, complexity of management's action plans, and recommendation from executive management are not valid criteria for prioritizing follow-up audits, because they do not consider the residual risk from previous audits. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4.3

NEW QUESTION: 461

An IS auditor is reviewing an industrial control system (ICS) that uses older unsupported technology in the scope of an upcoming audit. What should the auditor consider the MOST significant concern?

- A.** Attack vectors are evolving for industrial control systems.
- B.** There is a greater risk of system exploitation.
- C.** Disaster recovery plans (DRPs) are not in place.
- D.** Technical specifications are not documented.

Answer: ([SHOW ANSWER](#))

Explanation

The most significant concern for an IS auditor when reviewing an industrial control system (ICS) that uses older unsupported technology in the scope of an upcoming audit is that there is a greater risk of system exploitation. System exploitation is an attack that occurs when an unauthorized entity or individual takes advantage of a vulnerability or weakness in a system to compromise its security or functionality. System exploitation can cause harm or damage to the system or its users, such as data loss, corruption, theft, manipulation, denial of service (DoS), etc. An ICS that uses older unsupported technology poses a high risk of system exploitation, as older technology may have known or unknown vulnerabilities or defects that have not been patched or fixed by the vendor or manufacturer, and unsupported technology may not receive any updates or support from the vendor or manufacturer in case of issues or incidents. Attack vectors are evolving for industrial control systems is a possible concern for an IS auditor when reviewing an ICS that uses older unsupported technology in the scope of an upcoming audit, but it is not the most significant one. Attack vectors are methods or pathways that attackers use to gain access to or attack a system. Attack vectors are evolving for industrial control systems, as attackers are developing new techniques or tools to target ICSs that are increasingly connected and complex. However, this concern may not be specific to older unsupported technology, as it may affect any ICS regardless of its technology level. Disaster recovery plans (DRPs) are not in place is a possible concern for an IS auditor when reviewing an ICS that uses older unsupported technology in the scope of an upcoming audit, but it is not the most significant one. DRPs are documents that outline the technical and operational steps for restoring the IT systems and infrastructure that support critical functions or processes in the event of a disruption or disaster. DRPs are not in place, as they may affect the availability and continuity of the ICS and its functions or processes

in case of a failure or incident. However, this concern may not be related to older unsupported technology, as it may apply to any ICS regardless of its technology level.

Technical specifications are not documented is a possible concern for an IS auditor when reviewing an ICS that uses older unsupported technology in the scope of an upcoming audit, but it is not the most significant one. Technical specifications are documents that describe the technical characteristics or requirements of a system or component, such as functionality, performance, design, etc. Technical specifications are not documented, as they may affect the understanding, maintenance, and improvement of the ICS and its components. However, this concern may not be associated with older unsupported technology, as it may affect any ICS regardless of its technology level.

NEW QUESTION: 462

Which of the following findings would be of GREATEST concern to an IS auditor reviewing the security architecture of an organization that has just implemented a Zero Trust solution?

- A. A noticeable drop in the performance of IT systems
- B. An increase in user identification errors
- C. User complaints about the new mode of working
- D. An increase in security-related costs

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 463

Which of the following is the PRIMARY benefit of using a SIEM tool to collate high amounts of data collected across various security tools?

- A. Reducing the number of isolated events noted as incidents
- B. Correlating many isolated events to create a single source of record
- C. Reducing the number of false positive incidents
- D. Decreasing the effort needed to monitor security events

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 464

Which of the following activities is MOST important in determining whether a test of a disaster recovery plan (DRP) has been successful?

Analyzing whether predetermined test objectives were met

- A. Evaluating participation by key personnel
- B. Testing with offsite backup files
- C. Testing at the backup data center

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 465

Which of the following is a concern when data are transmitted through Secure Sockets Layer (SSL) encryption, implemented on a trading partner's server?

- A. The organization does not have control over encryption.
- B. Messages are subjected to wire tapping.
- C. Data might not reach the intended recipient.
- D. The communication may not be secure.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

The SSL security protocol provides data encryption, server authentication, message integrity and optional client authentication. Because SSL is built into all major browsers and web servers, simply installing a digital certificate turns on the SSL capabilities. SSL encrypts the datum while it is being transmitted over the internet. The encryption is done in the background, without any interaction from the user; consequently, there is no password to remember. The other choices are incorrect. Since the communication between client and server is encrypted, the confidentiality of information is not affected by wire tapping. Since SSL does the client authentication, only the intended recipient will receive the decrypted data. All data sent over an encrypted SSL connection are protected with a mechanism to detect tampering, i.e., automatically determining whether data has been altered in transit.

NEW QUESTION: 466

Which of the following is MOST important for an IS auditor to review when assessing the integrity of encryption controls for data at rest?

- A. Encryption of test data
- B. Protection of encryption keys
- C. Frequency of encryption key changes
- D. Length of encryption keys

Answer: ([SHOW ANSWER](#)**)**

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As

Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 467

Which of the following device in Frame Relay WAN technique is a service provider device that does the actual data transmission and switching in the frame relay cloud?

- A. DTE
- B. DCE

C. DME

D. DLE

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Data Circuit Terminal Equipment (DCE) is a service provider device that does the actual data transmission and switching in the frame relay cloud.

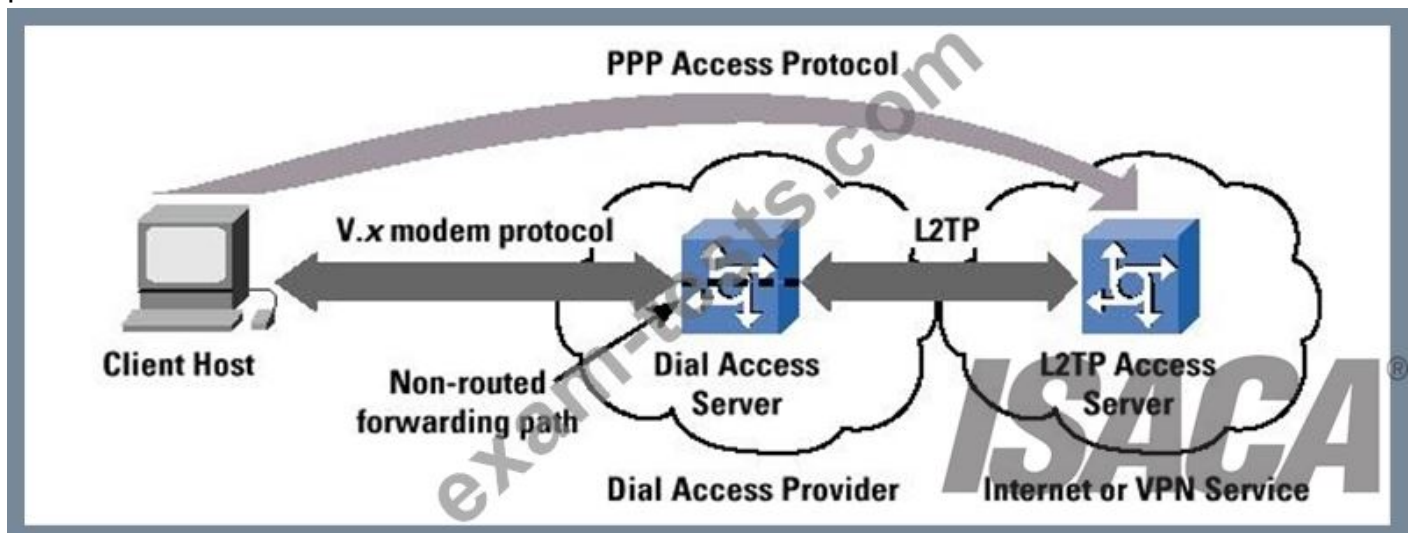
For your exam you should know below information about WAN Technologies:

Point-to-point protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.



Point-to-point protocol

X.25

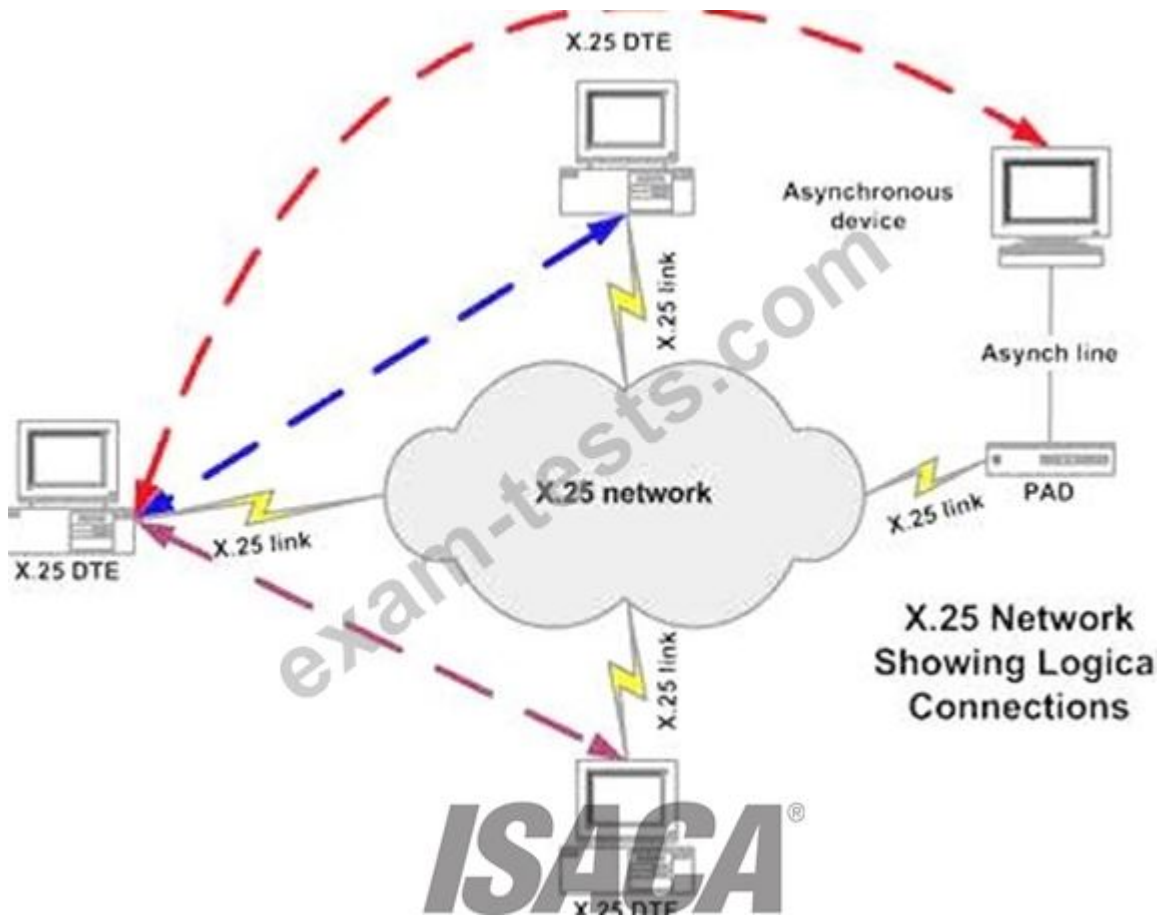
X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Subscribers are charged based on amount of bandwidth they use. Data are divided into 128 bytes and encapsulated in High Level Data Link Control (HDLC).

X.25 works at network and data link layer of an OSI model.

X.25



Frame Relay

Works on a packet switching

Operates at data link layer of an OSI model

Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

Two main types of equipments are used in Frame Relay

1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.
2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.

Frame Relay

Integrated Service Digital Network

Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

Same copper telephone wire is used.

Provide digital point-to-point circuit switching medium

ISDN



Asynchronous Transfer Mode (ATM)

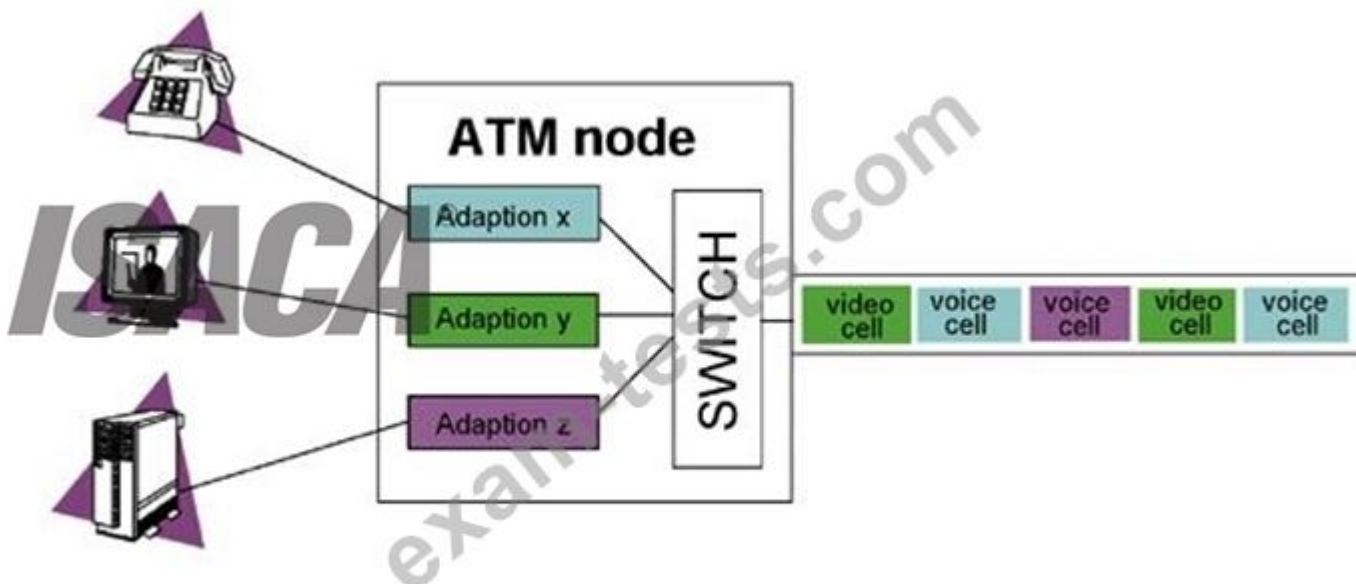
Uses Cell switching method

High speed network technology used for LAN, MAN and WAN

Like a frame relay it is connection oriented technology which creates and uses fixed channel Data are segmented into fixed size cell of 53 bytes

Some companies have replaces FDDI back-end with ATM

Asynchronous Transfer Mode



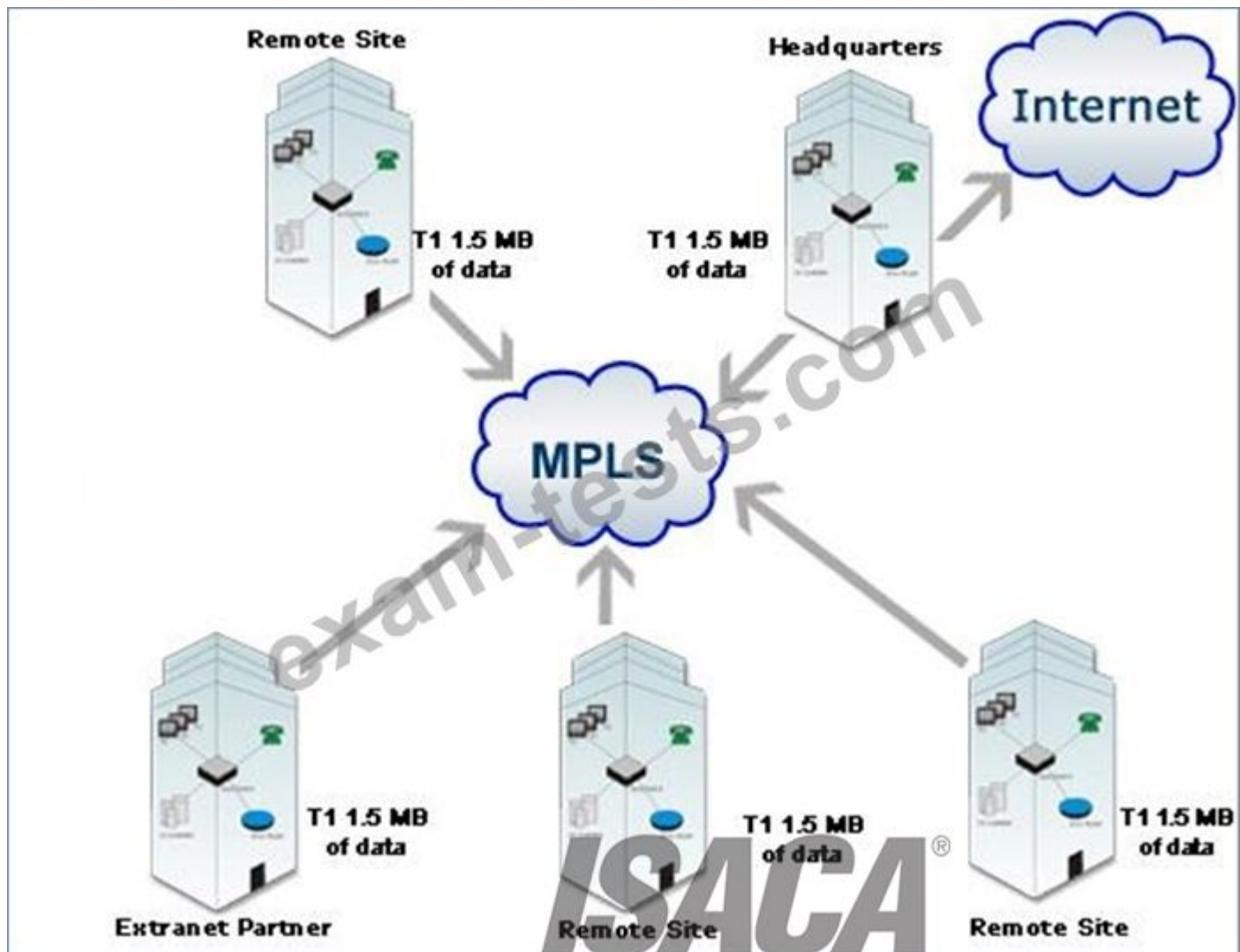
Services	Adaptation layer	ATM layer	Physical Layer
----------	------------------	-----------	----------------

Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called

multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS



The following answers are incorrect:

DTE - Data Terminal Equipment (DTE) is usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.

DME - Not a valid frame relay technique

DLE - Not a valid frame relay technique

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 266

NEW QUESTION: 468

The PRIMARY objective of IT service level management is to.

- A. improve IT cost control
- B. manage computer operations activities.
- C. increase awareness of IT services
- D. satisfy customer requirements.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 469

Which of the following is an attribute of the control self-assessment (CSA) approach?

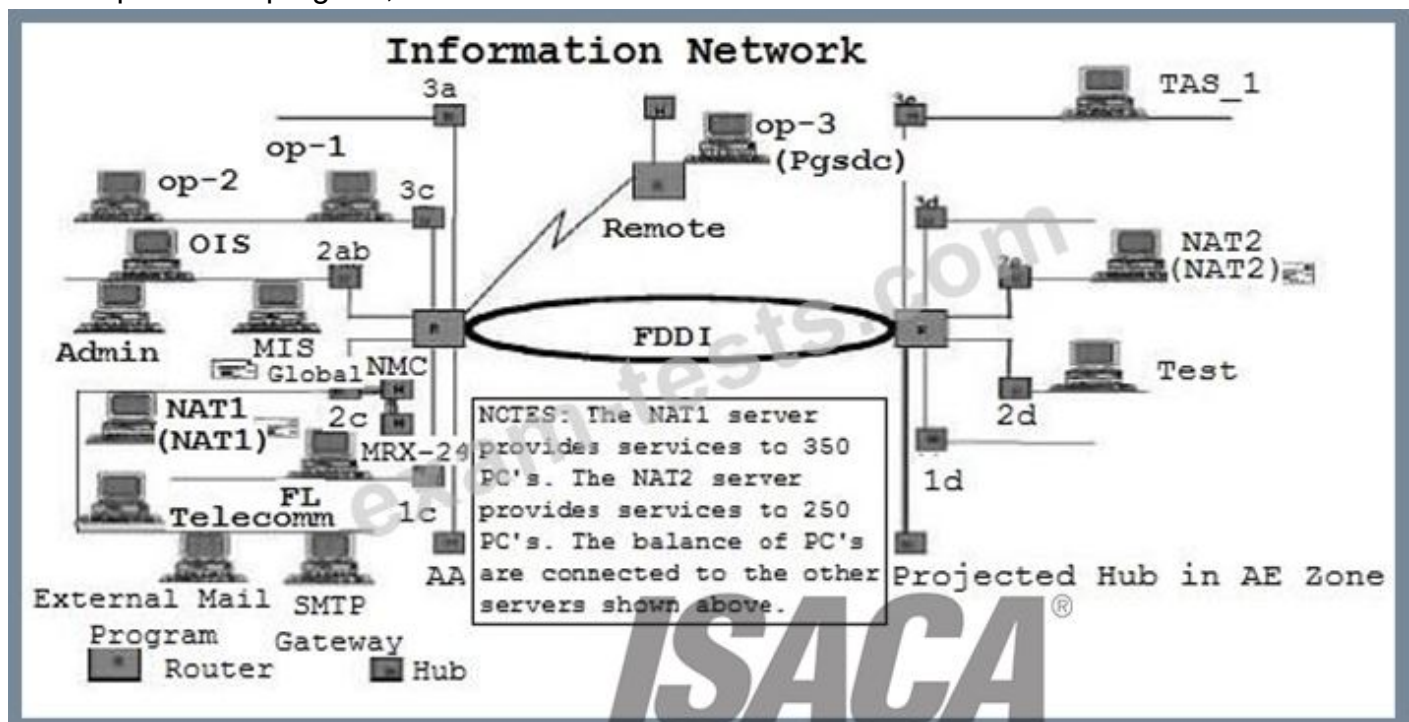
- A. Broad stakeholder involvement
- B. Auditors are the primary control analysts
- C. Limited employee participation
- D. Policy driven

Answer: A ([LEAVE A REPLY](#))

The control self-assessment (CSA) approach emphasizes management of and accountability for developing and monitoring the controls of an organization's business processes. The attributes of CSA include empowered employees, continuous improvement, extensive employee participation and training, all of which are representations of broad stakeholder involvement. Choices B, C and D are attributes of a traditional audit approach.

NEW QUESTION: 470

Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?



- A. No firewalls are needed
- B. Op-3 location only
- C. MIS (Global) and NAT2
- D. SMTP Gateway and op-3

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

The objective of a firewall is to protect a trusted network from an untrusted network; therefore, locations needing firewall implementations would be at the existence of the external connections. All other answers are incomplete or represent internal connections.

NEW QUESTION: 471

Which of the following methods would BEST help detect unauthorized disclosure of confidential documents sent over corporate email?

- A. Requiring all users to encrypt documents before sending
- B. Installing firewalls on the corporate network
- C. Reporting all outgoing emails that are marked as confidential
- D. Monitoring all emails based on pre-defined criteria

Answer: D (LEAVE A REPLY)

To detect unauthorized disclosure of confidential documents sent over corporate email, monitoring all emails based on pre-defined criteria is the best approach. This involves setting up automated monitoring systems that analyze email content, attachments, and metadata to identify any potential unauthorized disclosures. By defining specific criteria (such as keywords related to confidential information), organizations can proactively detect and prevent leaks. Requiring encryption before sending documents (option A) is important but does not address monitoring for unauthorized disclosures. Firewalls (option B) protect the network but do not specifically focus on email content. Reporting outgoing emails marked as confidential (option C) relies on user self-reporting and may not catch all incidents¹². References: 1(<https://www.isaca.org/resources/isaca-journal/past-issues/2010/data-governance-for-p>

NEW QUESTION: 472

When reviewing a database supported by a third-party service provider, an IS auditor found minor control deficiencies. The auditor should FIRST discuss recommendations with the:

- A. service provider support team manager
- B. organization's service level manager
- C. organization's chief information officer (CIO)
- D. service provider contract liaison

Answer: (SHOW ANSWER)

Section: The process of Auditing Information System

NEW QUESTION: 473

Which of the following is MOST likely to be detected by an IS auditor applying data analytic techniques?

- A. Potentially fraudulent invoice payments originating within the accounts payable department
- B. Unauthorized salary or benefit changes to the payroll system generated by authorized users

- C. Issues resulting from an unsecured application automatically uploading transactions to the general ledger
- D. Completion of inappropriate cross-border transmission of personally identifiable information (PII)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 474

Which of the following would BEST help to support an auditor's conclusion about the effectiveness of an implemented data classification program?

- A. Purchase of information management tools
- B. Business use cases and scenarios
- C. Access rights provisioned according to scheme
- D. Detailed data classification scheme

Answer: C ([LEAVE A REPLY](#))

Access rights provisioned according to scheme would best help to support an auditor's conclusion about the effectiveness of an implemented data classification program. This would indicate that the data classification program has been properly implemented and enforced, and that the data is protected according to its sensitivity and value. The other options are not sufficient to demonstrate the effectiveness of a data classification program, as they do not show how the data is actually accessed and used by authorized users.

References:

- * CISA Review Manual (Digital Version), Chapter 6, Section 6.2.31
- * CISA Review Questions, Answers & Explanations Database, Question ID 2042

NEW QUESTION: 475

In a controlled application development environment, the MOST important segregation of duties should be between the person who implements changes into the production environment and the:

- A. application programmer.
- B. quality assurance (QA) personnel.
- C. computer operator.
- D. systems programmer.

Answer: A ([LEAVE A REPLY](#))

Developer and deployment personnel should be segregated its main must, nothing else matters.

NEW QUESTION: 476

Which of the following is a mechanism for mitigating risks?

- A. Security and control practices
- B. Property and liability insurance
- C. Audit and certification
- D. Contracts and service level agreements (SLAs)

Answer: A ([LEAVE A REPLY](#))

Risks are mitigated by implementing appropriate security and control practices. Insurance is a mechanism for transferring risk. Audit and certification are mechanisms of risk assurance, while contracts and SLAs are mechanisms of risk allocation.

NEW QUESTION: 477

Which of the following methods BEST enforces data leakage prevention in a multi-tenant cloud environment?

- A.** Monitoring tools are configured to alert in case of downtime
- B.** A comprehensive security review is performed every quarter.
- C.** Data for different tenants is segregated by database schema
- D.** Tenants are required to implement data classification policies

Answer: ([SHOW ANSWER](#))

Data leakage prevention (DLP) is the process of preventing unauthorized access, disclosure, or transfer of sensitive data. In a multi-tenant cloud environment, where multiple customers share the same infrastructure and resources, DLP is a critical challenge. One of the best methods to enforce DLP in such an environment is to require tenants to implement data classification policies. Data classification policies define the types and levels of sensitivity of data, and the corresponding security controls and measures to protect them. By implementing data classification policies, tenants can ensure that their data is properly labeled, encrypted, segregated, and monitored according to their specific requirements and compliance standards. This can help prevent data leakage from accidental or malicious actions by other tenants, cloud service providers, or external parties.

References:

- * 2: How Do I Secure my Data in a Multi-Tenant Cloud Environment? | Thales
- * 3: Protecting Sensitive Customer Data in a Cloud-Based Multi-Tenant Environment | Saturn Cloud
- * 4: Microsoft 365 isolation controls - Microsoft Service Assurance

NEW QUESTION: 478

In RFID technology which of the following risk could represent a threat to non-RFID networked or collocated systems, assets, and people?

- A.** Business Process Risk
- B.** Business Intelligence Risk
- C.** Privacy Risk
- D.** Externality Risk

Answer: **D** ([LEAVE A REPLY](#))

Explanation/Reference:

RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

RFID systems typically are not isolated from other systems and assets in the enterprise. Every connection point between the RFID system and something outside the RFID system represents a

potential vulnerability for the entity on the other side of the connection, whether that is an application process, a valued asset, or a person.

Externality risks are present for both the RF and enterprise subsystems of an RFID system. The main externality risk for the RF subsystem is hazards resulting from electromagnetic radiation, which could possibly range from adverse human health effects to ignition of combustible material, such as fuel or ordnance.

The main externality risk for the enterprise subsystem is successful computer network attacks on networked devices and applications. Computer network attacks can involve malware (e.g., worms and viruses) or attack tools that exploit software vulnerabilities and configuration weaknesses to gain access to systems, perform a denial of service, or cause other damage.

The impact of computer network attacks can range from performance degradation to complete compromise of a mission-critical application. Because the externality risk by definition involves risks outside of the RFID system, it is distinct from both the business process and business intelligence risks; externality risks can be realized without having any effect on RFID-supported business processes or without revealing any information to adversaries.

For your exam you should know the information below:

Radio-frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects.

The tags contain electronically stored information. Some tags are powered by and read at short ranges (a few meters) via magnetic fields (electromagnetic induction). Others use a local power source such as a battery, or else have no battery but collect energy from the interrogating EM field, and then act as a passive transponder to emit microwaves or UHF radio waves (i.e., electromagnetic radiation at high frequencies). Battery powered tags may operate at hundreds of meters. Unlike a barcode, the tag does not necessarily need to be within line of sight of the reader, and may be embedded in the tracked object.

RFID tags are used in many industries. An RFID tag attached to an automobile during production can be used to track its progress through the assembly line. Pharmaceuticals can be tracked through warehouses.

Livestock and pets may have tags injected, allowing positive identification of the animal.

RFID RISKS

RFID technology enables an organization to significantly change its business processes to: Increase its efficiency, which results in lower costs, Increase its effectiveness, which improves mission performance and makes the implementing organization more resilient and better able to assign accountability, and Respond to customer requirements to use RFID technology to support supply chains and other applications.

The RFID technology itself is complex, combining a number of different computing and communications technologies to achieve the desired objectives. Unfortunately, both change and complexity generate risk.

For RFID implementations to be successful, organizations need to effectively manage that risk, which requires an understanding of its sources and its potential characteristics. This section

reviews the major high-level business risks associated with RFID systems so that organizations planning or operating these systems can better identify, characterize, and manage the risk in their environments.

The risks are as follows:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood.

The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

Externality Risk -RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people. An important characteristic of RFID that impacts all of these risks is that RF communication is invisible to operators and users.

The following answers are incorrect:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood.

The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 248

NIST SP 800-98 RFID 2007 -

http://www.csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf

NEW QUESTION: 479

What would an IS auditor expect to find in the console log?

- A. Evidence of password spoofing
- B. System errors
- C. Evidence of data copy activities
- D. Evidence of password sharing

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation:

An IS auditor can expect to find system errors to be detailed in the console log.

NEW QUESTION: 480

An organization that has suffered a cyber attack is performing a forensic analysis of the affected users' computers. Which of the following should be of GREATEST concern for the IS auditor reviewing this process?

- A. Audit was only involved during extraction of the Information
- B. The legal department has not been engaged.
- C. An imaging process was used to obtain a copy of the data from each computer.
- D. The chain of custody has not been documented.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 481

Which of the following is the BEST way to increase the effectiveness of security incident detection?

- A. Determining containment activities based on the type of incident
- B. Establishing service level agreements (SLAs) with appropriate forensic service providers
- C. Educating end users on identifying suspicious activity
- D. Documenting root cause analysis procedures

Answer: D ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 482

The editing/validation of data entered at a remote site would be performed MOST effectively at the:

- A. central processing site after running the application system.
- B. central processing site during the running of the application system.
- C. remote processing site after transmission of the data to the central processing site.
- D. remote processing site prior to transmission of the data to the central processing site.

Answer: ([SHOW ANSWER](#))

It is important that the data entered from a remote site is edited and validated prior to transmission to the central processing site.

NEW QUESTION: 483

A project manager of a project that is scheduled to take 18 months to complete announces that the project

is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The

IS auditor should FIRST determine:

- A.** what amount of progress against schedule has been achieved.
- B.** if the project budget can be reduced.
- C.** if the project could be brought in ahead of schedule.
- D.** if the budget savings can be applied to increase the project scope.

Answer: A (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

Cost performance of a project cannot be properly assessed in isolation of schedule performance.

Cost

cannot be assessed simply in terms of elapsed time on a project. To properly assess the project budget

position, it is necessary to know how much progress has actually been made and, given this, what level of

expenditure would be expected. It is possible that project expenditure appears to be low because actual

progress has been slow. Until the analysis of project against schedule has been completed, it is impossible

to know whether there is any reason to reduce budget, if the project has slipped behind schedule, then not

only may there be no spare budget but it is possible that extra expenditure may be needed to retrieve the

slippage. The low expenditure could actually be representative of a situation where the project is likely to

miss deadlines rather than potentially come in ahead of time. If the project is found to be ahead of budget

after adjusting for actual progress, this is not necessarily a good outcome because it points to flaws in the

original budgeting process; and, as said above, until further analysis is undertaken, it cannot be determined

whether any spare funds actually exist. Further, if the project is behind schedule, then adding scope may

be the wrong thing to do.

NEW QUESTION: 484

When auditing the security architecture of an online application, an IS auditor should FIRST review the:

- A. firewall standards.
- B. configuration of the firewall
- C. firmware version of the firewall
- D. location of the firewall within the network

Answer: D ([LEAVE A REPLY](#))

Explanation

The security architecture of an online application is a design that describes how various security components and controls are integrated and configured to protect the application from internal and external threats. When auditing the security architecture of an online application, an IS auditor should first review the location of the firewall within the network, as this determines how effectively the firewall can filter and monitor the traffic between different network segments and zones. The firewall standards, configuration, and firmware version are also important aspects to review, but they are secondary to the location of the firewall.

NEW QUESTION: 485

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

- A. End-user involvement
- B. Senior management involvement
- C. Security administration involvement
- D. IS auditing involvement

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

End-user involvement is critical during the business impact assessment phase of business continuity planning.

NEW QUESTION: 486

Which of the following term related to network performance refers to the number of corrupted bits expressed as a percentage or fraction of the total sent?

- A. Bandwidth
- B. Throughput
- C. Latency
- D. Error Rate

Answer: D ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

Explanation/Reference:

Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sent
For your exam you should know below information about Network performance:
Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sent

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of

the signals travel time, and processing time at any nodes the information traverses

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 275

NEW QUESTION: 487

Which of the following audit procedures would BEST assist an IS auditor in determining the effectiveness of a business continuity plan (BCP)?

- A. Performing an assessment of BCP test documentation
- B. Participating in BCP meetings held with user department managers
- C. Performing a maturity assessment of BCP methodology against industry standards
- D. Observing tests of the BCP performed at the alternate processing site

Answer: ([SHOW ANSWER](#))

Section: The process of Auditing Information System

NEW QUESTION: 488

Which of the following issues identified during a formal review of an organization's information security policies presents the GREATEST potential risk to the organization?

- A. The policies are not aligned with the information security risk appetite.
- B. The policies have not been reviewed by the risk management committee.
- C. The policies are not based on industry best practices for information security.
- D. The policies are not available to key risk stakeholders.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 489

Which of the following intrusion detection systems (IDSs) monitors the general patterns of activity and traffic on a network and creates a database?

- A. Signature-based
- B. Neural networks-based
- C. Statistical-based
- D. Host-based

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

The neural networks-based IDS monitors the general patterns of activity and traffic on the network and creates a database. This is similar to the statistical model but has the added function of self-learning.

Signature-based systems are a type of IDS in which the intrusive patterns identified are stored in the form of signatures. These IDS systems protect against detected intrusion patterns. Statistical-based systems need a comprehensive definition of the known and expected behavior of systems. Host-based systems are not a type of IDS, but a category of IDS, and are configured for a specific environment. They will monitor various internal resources of the operating system to warn of a possible attack.

NEW QUESTION: 490

An organization has outsourced the development of a core application. However, the organization plans to bring the support and future maintenance of the application back in-house. Which of the following findings should be the IS auditor's GREATEST concern?

- A.** The cost of outsourcing is lower than in-house development.
- B.** The vendor development team is located overseas.
- C.** A training plan for business users has not been developed.
- D.** The data model is not clearly documented.

Answer: D ([LEAVE A REPLY](#))

The finding that should be the IS auditor's greatest concern is that the data model is not clearly documented.

A data model is a representation of the structure, relationships, and constraints of the data used by an application. It is a vital component of the software development process, as it helps to ensure the accuracy, consistency, and quality of the data¹. A clear and comprehensive documentation of the data model is essential for the maintenance and support of the application, as it facilitates the understanding, modification, and troubleshooting of the data and the application logic².

If the organization plans to bring the support and future maintenance of the application back in-house, it will need to have access to the data model documentation from the vendor. Without it, the organization may face difficulties in transferring the knowledge and skills from the vendor to the in-house team, as well as in adapting and enhancing the application to meet changing business needs and requirements³. The lack of data model documentation may also increase the risk of errors, inconsistencies, and inefficiencies in the data and the application performance².

The other findings are not as concerning as the lack of data model documentation, because they do not directly affect the quality and maintainability of the application. The cost of outsourcing is lower than in-house development is a benefit rather than a risk for the organization, as it implies that outsourcing has helped to save time and money for the organization⁴. The vendor development team is located overseas is a common practice in outsourcing, and it does not necessarily imply a lower quality or a higher risk of the application. However, it may pose some challenges in terms of communication, coordination, and cultural differences, which can be managed by establishing clear expectations, roles, and responsibilities, as well as using effective

tools and methods for communication and collaboration⁵. A training plan for business users has not been developed is a gap that should be addressed by the organization before deploying the application, as it may affect the user acceptance and satisfaction of the application. However, it does not directly impact the quality or maintainability of the application itself. References:

- * What is Data Modeling? Definition & Types | Informatica¹
- * Data Modeling Best Practices: Documentation | erwin²
- * Data Model Documentation - an overview | ScienceDirect Topics³
- * Outsourcing App Development Pros and Cons - Droids On Roids⁴
- * 8 Risks of Software Development Outsourcing & Their Solutions - Acropolium⁵
- * Software Training Plan: How to Create One for Your Business - Elinext

NEW QUESTION: 491

An advantage of object-oriented system development is that it:

- A.** partitions systems into a client/server architecture.
- B.** decreases the need for system documentation.
- C.** is easier to code than procedural languages.
- D.** is suited to data with complex relationships.

Answer: ([SHOW ANSWER](#))

Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 492

Which of the following should be the FIRST step in managing the impact of a recently discovered zero-day attack?

- A.** Evaluating the likelihood of attack
- B.** Estimating potential damage
- C.** Identifying vulnerable assets
- D.** Assessing the Impact of vulnerabilities

Answer: ([SHOW ANSWER](#))

The first step in managing the impact of a recently discovered zero-day attack is to identify vulnerable assets.

A zero-day attack is a cyberattack that exploits a previously unknown or unpatched vulnerability in a software or system, before the vendor or developer has had time to fix it. Identifying vulnerable assets is crucial for managing the impact of a zero-day attack, because it helps to determine the scope and severity of the attack, prioritize the protection and mitigation measures, and isolate or quarantine the affected assets from further damage or compromise. The other options are not the first steps in managing the impact of a zero-day attack, because they either require more information about the vulnerable assets, or they are part of the subsequent steps of assessing, responding, or recovering from the attack. References: CISA Review Manual (Digital Version)¹, Chapter 5, Section 5.2.4

NEW QUESTION: 493

Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

- A. Apply single sign-on for access control
- B. Implement segregation of duties.
- C. Enforce an internal data access policy.
- D. Enforce the use of digital signatures.

Answer: C ([LEAVE A REPLY](#))

Explanation

The most appropriate control to prevent unauthorized retrieval of confidential information stored in a business application system is to enforce an internal data access policy. A data access policy defines who can access what data, under what conditions and for what purposes. It also specifies the roles and responsibilities of data owners, custodians and users, as well as the security measures and controls to protect data confidentiality, integrity and availability. By enforcing a data access policy, the organization can ensure that only authorized personnel can retrieve confidential information from the business application system. Applying single sign-on for access control, implementing segregation of duties and enforcing the use of digital signatures are also useful controls, but they are not sufficient to prevent unauthorized data retrieval without a clear and comprehensive data access policy. References:

CISA Review Manual, 27th Edition, page 2301

CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2

NEW QUESTION: 494

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

- A. Identify high-risk areas that might need a detailed review later
- B. Reduce audit costs
- C. Reduce audit time
- D. Increase audit accuracy

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

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.

NEW QUESTION: 495

In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

- A. Diskless workstations
- B. Data encryption techniques
- C. Network monitoring devices
- D. Authentication systems

Answer: C (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

Network monitoring devices may be used to inspect activities from known or unknown users and can

identify client addresses, which may assist in finding evidence of unauthorized access. This serves as a

detective control. Diskless workstations prevent access control software from being bypassed.

Data

encryption techniques can help protect sensitive or propriety data from unauthorized access, thereby

serving as a preventive control. Authentication systems may provide environment wide, logical facilities that

can differentiate among users, before providing access to systems.

NEW QUESTION: 496

Which of the following would a digital signature MOST likely prevent?

- A. Repudiation
- B. Unauthorized change
- C. Corruption
- D. Disclosure

Answer: (SHOW ANSWER)

A digital signature is a cryptographic technique that uses the sender's private key to generate a unique code for a message or document. The receiver can use the sender's public key to verify the authenticity and integrity of the message or document. A digital signature can prevent unauthorized change, as any modification to the message or document will invalidate the signature and alert the receiver of tampering.

References

What is a digital signature?

Digital Signature - an overview | ScienceDirect Topics

ISACA CISA Review Manual, 27th Edition, page 253

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 497

Which of the following is a rewrite of ipfwadm?

- A. ipchains
- B. iptables
- C. Netfilter
- D. ipcook
- E. None of the choices.

Answer: A ([LEAVE A REPLY](#))

ipchains is a free software based firewall running on earlier Linux. It is a rewrite of ipfwadm but is superseded by iptables in Linux 2.4 and above. Iptables controls the packet filtering and NAT components within the Linux kernel. It is based on Netfilter, a framework which provides a set of hooks within the Linux kernel for intercepting and manipulating network packets.

NEW QUESTION: 498

Which of the following BEST ensures the confidentiality of sensitive data during transmission?

- A. Sending data through proxy servers
- B. Restricting the recipient through destination IP addresses
- C. Password protecting data over virtual local area networks (VLAN)
- D. Sending data over public networks using Transport Layer Security (TLS)

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 499

An organization is concerned about duplicate vendor payments on a complex system with a high volume of transactions. Which of the following would be MOST helpful to an IS auditor to determine whether duplicate vendor payments exist?

- A. Computer-assisted audit technique (CAAT)
- B. Stratified sampling
- C. Statistical sampling
- D. Process walk-through

Answer: (SHOW ANSWER)

Comprehensive and Detailed Step-by-Step Explanation:

To efficiently detect duplicate payments, data analytics and automated checks are required due to the high volume of transactions.

* Option A (Correct): Computer-Assisted Audit Techniques (CAATs) allow auditors to automatically scan large datasets for duplicate payments based on invoice numbers, vendor names, and payment amounts.

* Option B (Incorrect): Stratified sampling groups data into categories, which helps in analysis but does not directly detect duplicates.

* Option C (Incorrect): Statistical sampling is useful for extrapolating results, but it does not systematically find duplicate transactions.

* Option D (Incorrect): Process walk-throughs review procedures but do not analyze transactions at scale.

Reference: ISACA CISA Review Manual - Domain 2: Governance and Management of IT - Covers CAATs, data analytics, and fraud detection techniques.

NEW QUESTION: 500

If a database is restored from information backed up before the last system image, which of the following is recommended?

- A. The system should be restarted after the last transaction.
- B. The system should be restarted before the last transaction.
- C. The system should be restarted at the first transaction.
- D. The system should be restarted on the last transaction.

Answer: B ([LEAVE A REPLY](#))

If a database is restored from information backed up before the last system image, the system should be restarted before the last transaction because the final transaction must be reprocessed.

NEW QUESTION: 501

An organization is disposing of a system containing sensitive data and has deleted all files from the hard disk. An IS auditor should be concerned because:

- A. deleting the files logically does not overwrite the files' physical data.
- B. deleted data cannot easily be retrieved.
- C. deleting all files separately is not as efficient as formatting the hard disk.
- D. backup copies of files were not deleted as well.

Answer: (SHOW ANSWER)

NEW QUESTION: 502

Which of the following should be PRIMARILY included in a security training program for business process owners?

- A. Application vulnerabilities
- B. List of security incidents reported
- C. Application recovery time
- D. Impact of security risks

Answer: D ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 503

Which of the following should an IS auditor use when verifying a three-way match has occurred in an enterprise resource planning (ERP) system?

- A. Goods delivery notification
- B. Purchase requisition

- C. Bank confirmation
- D. Purchase order

Answer: ([SHOW ANSWER](#))

Section: Governance and Management of IT

NEW QUESTION: 504

What should an IS auditor do when informed that some recommendations cannot be implemented due to financial constraints?

- A. Suggest management identify cost-effective alternatives.
- B. Document management's response in the working papers.
- C. Agree to waive the recommendations.
- D. Insist the recommendations be implemented.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 505

Which of the following is the MOST important factor when an organization is developing information security policies and procedures?

- A. Consultation with security staff
- B. Inclusion of mission and objectives
- C. Compliance with relevant regulations
- D. Alignment with an information security framework

Answer: D ([LEAVE A REPLY](#))

Explanation

Information security policies and procedures are the foundation of an organization's information security program. They define the roles, responsibilities, rules, and standards for protecting information assets from unauthorized access, use, disclosure, modification, or destruction. The most important factor when developing information security policies and procedures is to align them with an information security framework that provides a comprehensive and consistent approach to managing information security risks. An information security framework can also help ensure compliance with relevant regulations, inclusion of mission and objectives, and consultation with security staff. However, these factors are secondary to alignment with an information security framework. References: CISA Certification | Certified Information Systems Auditor | ISACA, CISA Review Manual (Digital Version)

NEW QUESTION: 506

Which of the following is MOST important for an IS auditor to do during an exit meeting with an auditee?

- A. Communicate the recommendations to senior management
- B. Request input in determining corrective action.
- C. Ensure that the facts presented in the report are correct
- D. Specify implementation dates for the recommendations.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 507

Which of the following should an IS auditor review when verifying the integrity of a relational database management system (RDBMS)?

- A. Database size value
- B. Secret key algorithm used
- C. Cyclic redundancy check value
- D. Foreign key attributes

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 508

Which of the following key performance indicators (KPIs) provides stakeholders with the MOST useful information about whether information security risk is being managed?

- A. Time from security log capture to log analysis
- B. Time from identifying security threats to implementing solutions
- C. The number of entries in the security risk register
- D. The number of security controls implemented

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 509

Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a place

to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management?

- A. Governing
- B. Culture
- C. Enabling and support
- D. Emergence

Answer: ([SHOW ANSWER](#))

Section: Governance and Management of IT

Explanation:

Emergence-which connotes surfacing, developing, growing and evolving-refers to patterns that arise in

the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to

predict and control. The emergence dynamic interconnection (between people and processes) is a place to

introduce possible solutions such as feedback loops; alignment with process improvement; and

consideration of emergent issues in system design life cycle, change control, and risk management.

For your exam you should know the information below.

Business Model for Information Security

The Business Model for Information Security (BMIS) originated at the Institute for Critical Information

Infrastructure Protection at the Marshall School of Business at the University of Southern California in the

USA. ISACA has undertaken the development of the Systemic Security Management Model. The BMIS

takes a business-oriented approach to managing information security, building on the foundational

concepts developed by the Institute. The model utilizes systems thinking to clarify complex relationships

within the enterprise, and thus to more effectively manage security. The elements and dynamic interconnections that form the basis of the model establish the boundaries of an information security

program and model how the program functions and reacts to internal and external change. The BMIS

provides the context for frameworks such as Cubit.

The essence of systems theory is that a system needs to be viewed holistically-not merely as a sum of its

parts-to be accurately understood. A holistic approach examines the system as a complete functioning

unit. Another tenet of systems theory is that one part of the system enables understanding of other parts of

the system. "Systems thinking" is a widely recognized term that refers to the examination of how systems

interact, how complex systems work and why "the whole is more than the sum of its parts."

Systems theory

is most accurately described as a complex network of events, relationships, reactions, consequences,

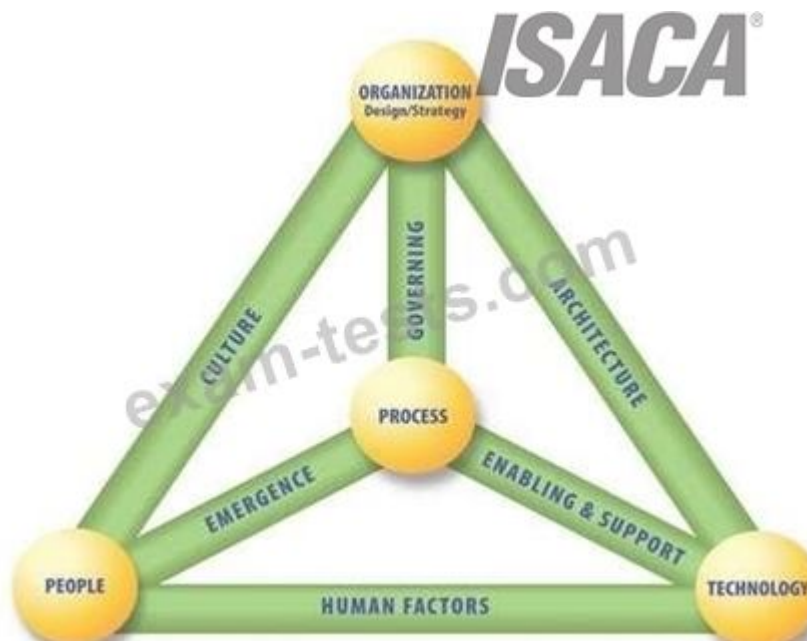
technologies, processes and people that interact in often unseen and unexpected ways. Studying the

behaviors and results of the interactions can assist the manager to better understand the organizational

system and the way it functions. While management of any discipline within the enterprise can be enhanced by approaching it from a systems thinking perspective, its implementation will certainly help with

managing risk.

The success that the systems approach has achieved in other fields bodes well for the benefits it can bring to security. The often dramatic failures of enterprises to adequately address security issues in recent years are due, to a significant extent, to their inability to define security and present it in a way that is comprehensible and relevant to all stakeholders. Utilizing a systems approach to information security management will help information security managers address complex and dynamic environments, and will generate a beneficial effect on collaboration within the enterprise, adaptation to operational change, navigation of strategic uncertainty and tolerance of the impact of external factors. The model is represented below.



As illustrated in above, the model is best viewed as a flexible, three-dimensional, pyramid-shaped structure made up of four elements linked together by six dynamic interconnections. All aspects of the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, the equilibrium of the model is potentially at risk. The dynamic interconnections act as tensions, exerting a push/pull force in reaction to changes in the enterprise, allowing the model to adapt as needed.

The four elements of the model are:

1. Organization Design and Strategy-An organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal.

An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values

and missions to be pursued. It is the enterprise's formula for success and sets its basic direction.

The

strategy should adapt to external and internal factors. Resources are the primary material to design the

strategy and can be of different types (people, equipment, know-how). Design defines how the organization

implements its strategy. Processes, culture and architecture are important in determining the design.

2. People-The human resources and the security issues that surround them. It defines who implements

(through design) each part of the strategy. It represents a human collective and must take into account

values, behaviors and biases. Internally, it is critical for the information security manager to work with the

human resources and legal departments to address issues such as:

Recruitment strategies (access, background checks, interviews, roles and responsibilities)

Employment issues (location of office, access to tools and data, training and awareness, movement within

the enterprise)

Termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to

other employees). Externally, customers, suppliers, media, stakeholders and others can have a strong

influence on the enterprise and need to be considered within the security posture.

3. Process-Includes formal and informal mechanisms (large and small, simple and complex) to get things

done and provides a vital link to all of the dynamic interconnections.

Processes identify, measure, manage and control risk, availability, integrity and confidentiality, and they

also ensure accountability. They derive from the strategy and implement the operational part of the

organization element.

To be advantageous to the enterprise, processes must:

Meet business requirements and align with policy

Consider emergence and be adaptable to changing requirements

Be well documented and communicated to appropriate human resources

Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness

4. Technology-Composed of all of the tools, applications and infrastructure that make processes more

efficient. As an evolving element that experiences frequent changes, it has its own dynamic risk.

Given the

typical enterprise's dependence on technology, technology constitutes a core part of the enterprise's

infrastructure and a critical component in accomplishing its mission.

Technology is often seen by the enterprise's management team as a way to resolve security threats and

risk. While technical controls are helpful in mitigating some types of risk, technology should not be viewed

as an information security solution.

Technology is greatly impacted by users and by organizational culture. Some individuals still mistrust

technology; some have not learned to use it; and others feel it slows them down. Regardless of the reason,

information security managers must be aware that many people will try to sidestep technical controls.

Dynamic Interconnections

The dynamic interconnections are what link the elements together and exert a multidirectional force that

pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can

force the model out of balance or bring it back to equilibrium.

The six dynamic interconnections are:

1. Governing-Governing is the steering of the enterprise and demands strategic leadership.

Governing

sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent

conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that

risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

2. Culture-Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is

emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a

group goes through a set of common experiences. Those similar experiences cause certain responses,

which become a set of expected and shared behaviors. These behaviors become unwritten rules, which

become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

3. Enabling and support-The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

4. Emergence-Emergence-which connotes surfacing, developing, growing and evolving-refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

5. Human factors-The human factors dynamic interconnection represents the interaction and gap between technology and people and, as such, is critical to an information security program. If people do not understand how to use the technology, do not embrace the technology or will not follow pertinent policies,

serious security problems can evolve. Internal threats such as data leakage, data theft and misuse of data

can occur within this dynamic interconnection. Human factors may arise because of age, experience level

and/or cultural experiences. Because human factors are critical components in maintaining balance within

the model, it is important to train all of the enterprise's human resources on pertinent skills.

6. Architecture-A security architecture is a comprehensive and formal encapsulation of the people,

processes, policies and technology that comprise an enterprise's security practices. A robust business

information architecture is essential to understanding the need for security and designing the security

architecture. It is within the architecture dynamic interconnection that the enterprise can ensure defense in

depth. The design describes how the security controls are positioned and how they relate to the overall IT

architecture. An enterprise security architecture facilitates security capabilities across lines of businesses in

a consistent and a cost-effective manner and enables enterprises to be proactive with their security

investment decisions.

The following answers are incorrect:

Governing - Governing is the steering of the enterprise and demands strategic leadership.

Governing sets

limits within which an enterprise operates and is implemented within processes to monitor performance,

describe activities and achieve compliance while also providing adaptability to emergent conditions.

Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are

managed appropriately, and verifying that the enterprise's resources are used responsibly.

Enabling and support - The enabling and support dynamic interconnection connects the technology

element to the process element. One way to help ensure that people comply with technical security

measures, policies and procedures is to make processes usable and easy. Transparency can help

generate acceptance for security controls by assuring users that security will not inhibit their ability to work

effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

Culture - Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/ regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 37 and 38

<http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf>

NEW QUESTION: 510

Who is responsible for authorizing access level of a data user?

- A. Data Owner
- B. Data User
- C. Data Custodian
- D. Security Administrator

Answer: (SHOW ANSWER)

Explanation/Reference:

Data owners are responsible for authorizing access level of a data user. These peoples are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are

updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

For your exam you should know below roles in an organization

Data Owners - Data Owners are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

Data Custodian or Data Steward -are responsible for storing and safeguarding the data, and include IS personnel such as system analysis and computer operators.

Security Administrator -Security administrator is responsible for providing adequate physical and logical security for IS programs, data and equipment.

Data Users - Data users, including internal and external user community, are the actual user of computerized data. Their level of access into the computer should be authorized by data owners, and restricted and monitor by security administrator.

The following were incorrect answers:

Security Administrator -Security administrator is responsible for providing adequate and logical security for IS programs, data and equipment.

Data Users - Data users, including internal and external user community, are the actual user of computerized data.

Data custodian is responsible for storing and safeguarding the data, and include IS personnel such as system analyst and computer operators.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 361

NEW QUESTION: 511

An IS audit team is planning to rely on a system-generated report to reduce the substantive procedures they will need to perform. Which of the following procedures should the IS auditor perform to verify the completeness of the report?

- A.** Trace a sample of transactions to the internal transactions.
- B.** Validate the report query.
- C.** Test data for appropriateness.
- D.** Establish some criteria for expected results and compare to actual results.

Answer: C ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

NEW QUESTION: 512

In reviewing the IT strategic plan, the IS auditor should consider whether it identifies the:

- A. allocation of IT staff.
- B. project management methodologies used.
- C. major IT initiatives.
- D. links to operational tactical plans.

Answer: (SHOW ANSWER)

In reviewing the IT strategic plan, the IS auditor should consider whether it identifies the major IT initiatives that are aligned with the organization's vision, mission, and objectives, and that support the business strategy and priorities¹². The major IT initiatives should also be realistic, measurable, and achievable, and should have clear timelines, budgets, and responsibilities³⁴.

References

1: IT Strategy Template for a Successful Strategic Plan | Gartner² 2: IT Strategy Template for a Successful Strategic Plan | Gartner⁴ 3: Conduct a Strategic Plan Review & Assessment - Governance³ 4: Time To Conduct A Strategy Review? Here's How To Get Started¹

NEW QUESTION: 513

Regarding a disaster recovery plan, the role of an IS auditor should include:

- A. identifying critical applications.
- B. determining the external service providers involved in a recovery test.
- C. observing the tests of the disaster recovery plan. determining the criteria for
- D. establishing a recovery time objective (RTO).

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

The IS auditor should be present when disaster recovery plans are tested, to ensure that the test meets the targets for restoration, and the recovery procedures are effective and efficient. As appropriate, the auditor should provide a report of the test results. All other choices are a responsibility of management.

NEW QUESTION: 514

Effective IT governance requires organizational structures and processes to ensure that:

- A. the organization's strategies and objectives extend the IT strategy.
- B. the business strategy is derived from an IT strategy.
- C. IT governance is separate and distinct from the overall governance.
- D. the IT strategy extends the organization's strategies and objectives.

Answer: (SHOW ANSWER)

Effective IT governance requires that board and executive management extend governance to IT and provide the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives, and that the strategy is aligned with business strategy. Choice A is incorrect because it is the IT strategy that extends the organizational objectives, not the opposite. IT governance is not an isolated discipline; it must become an integral part of the overall enterprise governance.

NEW QUESTION: 515

An IS auditor has completed an audit on the organization's IT strategic planning process. Which of the

following findings should be given the HIGHEST priority?

- A. The IT strategic plan was completed prior to the formulation of the business strategic plan
- B. Assumptions in the IT strategic plan have not been communicated to business stakeholders
- C. The IT strategic plan was formulated based on the current IT capabilities
- D. The IT strategic plan does not include resource requirements for implementation

Answer: A ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

NEW QUESTION: 516

The optimum business continuity strategy for an entity is determined by the:

- A. lowest downtime cost and highest recovery cost.
- B. lowest sum of downtime cost and recovery cost.
- C. lowest recovery cost and highest downtime cost.
- D. average of the combined downtime and recovery cost.

Answer: ([SHOW ANSWER](#)**)**

Section: Protection of Information Assets

Explanation:

Both costs have to be minimized, and the strategy for which the costs are lowest is the optimum strategy.

The strategy with the highest recovery cost cannot be the optimum strategy. The strategy with the highest

downtime cost cannot be the optimum strategy. The average of the combined downtime and recovery cost

will be higher than the lowest combined cost of downtime and recovery.

NEW QUESTION: 517

Which of the following is MOST important to ensure when developing an effective security awareness program?

- A. Training personnel are information security professionals.
- B. Outcome metrics for the program are established.
- C. Security threat scenarios are included in the program content.

D. Phishing exercises are conducted post-training

Answer: ([SHOW ANSWER](#))

Explanation

The most important factor to ensure when developing an effective security awareness program is B. Outcome metrics for the program are established. This is because outcome metrics are measures that evaluate the impact and results of the security awareness program on the behavior and performance of the users, and the security posture and objectives of the organization¹.

Outcome metrics can help ensure the effectiveness of the security awareness program by:

Providing feedback and evidence on whether the security awareness program is achieving its goals and expectations, such as reducing the number of incidents, improving the compliance rate, or increasing the reporting rate¹.

Identifying and quantifying the strengths and weaknesses of the security awareness program, and enabling continuous improvement and optimization of the program content, delivery, and frequency¹.

Demonstrating and communicating the value and return on investment of the security awareness program to the stakeholders and management, and securing their support and commitment for the program¹.

NEW QUESTION: 518

An IS auditor discovers from patch logs that some in-scope systems are not compliant with the regular patching schedule. What should the auditor do NEXT?

- A. Report this finding to senior management.
- B. Request a plan of action to be established as a follow-up item.
- C. Review the organization's patch management policy.
- D. Interview IT management to clarify the current procedure.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 519

Nowadays, computer security comprises mainly "preventive" measures.

- A. True
- B. True only for trusted networks
- C. True only for untrusted networks
- D. False
- E. None of the choices.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

"Nowadays, computer security comprises mainly "preventive" measures, like firewalls or an Exit Procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network and is normally implemented as software running on the machine or as physical integrated hardware."

NEW QUESTION: 520

Wi-Fi Protected Access implements the majority of which IEEE standard?

- A. 802.11i
- B. 802.11g
- C. 802.11x
- D. 802.11v
- E. None of the choices.

Answer: ([SHOW ANSWER](#))

Wi-Fi Protected Access (WPA / WPA2) is a class of systems to secure wireless computer networks. It implements the majority of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards (but not necessarily with first generation wireless access points). One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used.

NEW QUESTION: 521

Who is responsible for implementing cost-effective controls in an automated system?

- A. Security policy administrators
- B. Business unit management
- C. Senior management
- D. Board of directors

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Business unit management is responsible for implementing cost-effective controls in an automated system.

NEW QUESTION: 522

An IS auditor is providing input to an RFP to acquire a financial application system. Which of the following is MOST important for the auditor to recommend?

- A. The application should meet the organization's requirements.
- B. Audit trails should be included in the design.
- C. Potential suppliers should have experience in the relevant area.
- D. Vendor employee background checks should be conducted regularly.

Answer: ([SHOW ANSWER](#))

This is because audit trails are records of system activity and user actions that can provide evidence of the validity and integrity of transactions and data in a financial application system. Audit trails can help to ensure compliance with laws, regulations, policies, and standards, as well as to detect and prevent fraud, errors, or misuse of information. Audit trails can also facilitate auditing, monitoring, and evaluation of the financial application system's performance and controls¹.

The application should meet the organization's requirements (A) is not the best answer, because it is a general and obvious criterion that applies to any application system acquisition, not a specific and important recommendation for a financial application system. The organization's requirements should be clearly defined and documented in the RFP, but they may not necessarily include audit trails as a design feature.

Potential suppliers should have experience in the relevant area is not the best answer, because it is a factor that affects the selection of the supplier, not the design of the financial application system. The experience and reputation of potential suppliers should be evaluated and verified during the RFP process, but they may not guarantee that the supplier will include audit trails in the design.

Vendor employee background checks should be conducted regularly (D) is not the best answer, because it is a measure that affects the security and trustworthiness of the vendor, not the design of the financial application system. Vendor employee background checks should be performed as part of the vendor management and due diligence process, but they may not ensure that the vendor will include audit trails in the design.

NEW QUESTION: 523

Data flow diagrams are used by IS auditors to:

- A. order data hierarchically.
- B. highlight high-level data definitions.
- C. graphically summarize data paths and storage.
- D. portray step-by-step details of data generation.

Answer: (SHOW ANSWER)

Section: Protection of Information Assets

Explanation:

Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its

origination to destination, highlighting the paths and storage of data. They do not order data in any

hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

NEW QUESTION: 524

Facilitating telecommunications continuity by providing redundant combinations of local carrier T-1 lines, microwaves and/or coaxial cables to access the local communication loop:

- A. last-mile circuit protection.
- B. long-haul network diversity.
- C. diverse routing.
- D. alternative routing.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

The method of providing telecommunication continuity through the use of many recovery facilities, providing redundant combinations of local carrier T-Is, microwave and/or coaxial cable to access the local communication loop in the event of a disaster, is called last-mile circuit protection. Providing diverse long-distance network availability utilizing T-I circuits among major long-distance carriers is called long-haul network diversity. This ensures long-distance access should any one carrier experience a network failure. The method of routing traffic through split-cable facilities or duplicate-cable facilities is called diverse routing. Alternative routing is the method of routing information via an alternative medium, such as copper cable or fiber optics.

NEW QUESTION: 525

Which of the following incident management practices would BEST facilitate rapid resolution and reduce downtime from unplanned interruptions?

- A. Ensuring IT systems are monitored on a continual basis
- B. Ensuring the service desk is trained on issue resolution
- C. Ensuring the service desk has access to catalogs of known errors
- D. Ensuring incidents with unknown root causes are escalated

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 526

An IS auditor finds that a DBA has read and write access to production data. The IS auditor should:

- A. accept the DBA access as a common practice.
- B. assess the controls relevant to the DBA function.
- C. recommend the immediate revocation of the DBA access to production data.
- D. review user access authorizations approved by the DBA.

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

It is good practice when finding a potential exposure to look for the best controls. Though granting the database administrator (DBA) access to production data might be a common practice, the IS auditor should evaluate the relevant controls. The DBA should have access based on a need-to-know and need-to-do basis; therefore, revocation may remove the access required. The DBA, typically, may need to have access to some production data. Granting user authorizations is the responsibility of the data owner and not the DBA.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

NEW QUESTION: 527

The computer security incident response team (CSIRT) of an organization disseminates detailed descriptions of recent threats. An IS auditor's GREATEST concern should be that the users might:

- A. use this information to launch attacks.
- B. forward the security alert.
- C. implement individual solutions.
- D. fail to understand the threat.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: An organization's computer security incident response team (CSIRT) should disseminate recent threats, security guidelines and security updates to the users to assist them in understanding the security risk of errors and omissions. However, this introduces the risk that the users may use this information to launch attacks, directly or indirectly. An IS auditor should ensure that the CSIRT is actively involved with users to assist them in mitigation of risks arising from security failures and to prevent additional security incidents resulting from the same threat. Forwarding the security alert is not harmful to the organization, implementing individual solutions is unlikely and users failing to understand the threat would not be a serious concern.

NEW QUESTION: 528

The PRIMARY purpose of running a new system in parallel is to:

- A. resolve any errors in the program and file interfaces.
- B. validate the operation of the new system against its predecessor.
- C. provide the basis for comprehensive unit and system testing.
- D. determine which of the two systems is more efficient and effective.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 529

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: (SHOW ANSWER)

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.

NEW QUESTION: 530

A computer forensic audit is MOST relevant in which of the following situations?

- A. Inadequate controls in the IT environment
- B. Mismatches in transaction data
- C. Missing server patches
- D. Data loss due to hacking of servers

Answer: ([SHOW ANSWER](#))

Explanation

A computer forensic audit is a process of collecting, preserving, analyzing, and presenting digital evidence from electronic devices in a legally admissible manner. It is most relevant in situations where data loss due to hacking of servers occurs, as it can help to identify the source, method, and extent of the attack, as well as recover the lost or damaged data. The other options are not as suitable for a computer forensic audit, as they relate to internal control issues, data quality issues, or system maintenance issues, which can be addressed by other types of audits or reviews. References: CISA Review Manual (Digital Version), Domain 4: Information Systems Operations and Business Resilience, Section 4.5 Computer Forensics1

NEW QUESTION: 531

When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

- A. whose sum of activity time is the shortest.
- B. that have zero slack time.
- C. that give the longest possible completion time.
- D. whose sum of slack time is the shortest.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

A critical path's activity time is longer than that for any other path through the network. This path is important because if everything goes as scheduled, its length gives the shortest possible completion time for the overall project. Activities on the critical path become candidates for crashing, i.e., for reduction in their time by payment of a premium for early completion. Activities on the critical path have zero slack time and conversely, activities with zero slack time are on a critical path. By successively relaxing activities on a critical path, a curve showing total project costs vs. time can be obtained.

NEW QUESTION: 532

An IS auditor learns that an organization's business continuity plan (BCP) has not been updated in the last 18 months and that the organization recently closed a production plant. Which of the following is the auditor's BEST course of action?

- A. Determine the types of technologies used at the plant and how they may affect the BCP.
- B. Determine whether the business impact analysis (BIA) is current with the organization's structure and context.
- C. Perform testing to determine the impact to the recovery time objective (RTO).
- D. Assess the risk to operations from the closing of the plant.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 533

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: ([SHOW ANSWER](#)**)**

Section: Protection of Information Assets

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.

NEW QUESTION: 534

An organization is permanently transitioning from onsite to fully remote business operations. When should the existing business impact analysis (BIA) be reviewed?

- A. During the next scheduled review
- B. As soon as the decision about the transition is announced
- C. At least one year after the transition
- D. As soon as the new operating model is in place

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 535

Which of the following is MOST important for an IS auditor to understand when planning an IS audit?

- A. Inherent risk of auditable areas
- B. Management focus on particular operations
- C. Availability of IS audit resources
- D. Number of high-risk auditable processes

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 536

Which of the following should be done FIRST to develop an effective business continuity plan (BCP)?

- A. Create a disaster recovery plan (DRP).
- B. Perform a business impact analysis (BIA).
- C. Create a business unit communications plan.
- D. Secure an alternate processing site

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 537

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

- A. A star network topology
- B. A mesh network topology with packet forwarding enabled at each host
- C. A bus network topology
- D. A ring network topology

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

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.

NEW QUESTION: 538

When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

- A. analysis.
- B. evaluation.
- C. preservation.
- D. disclosure.

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Preservation and documentation of evidence for review by law enforcement and judicial authorities are of primary concern when conducting an investigation. Failure to properly preserve the evidence could jeopardize the acceptance of the evidence in legal proceedings. Analysis, evaluation and disclosure are important but not of primary concern in a forensic investigation.

NEW QUESTION: 539

While performing a risk-based audit, which of the following would BEST enable an IS auditor to identify and categorize risk?

- A. Understanding the control framework
- B. Developing a comprehensive risk model
- C. Understanding the business environment
- D. Adopting qualitative risk analysis

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 540

Which of the following statement INCORRECTLY describes packet switching technique?

- A. Packet uses many different dynamic paths to get the same destination
- B. Traffic is usually burst in nature
- C. Fixed delays to reach each packet to destination
- D. Usually carries data-oriented data

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

The word INCORRECTLY is the keyword used in the question. You need to find out a statement which is not valid about packet switching. As in the network switching, packet traverse different path, there will be always variable delay for each packet to reach to destination.

For your exam you should know below information about WAN message transmission technique:

Message Switching

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hop at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Message Switching

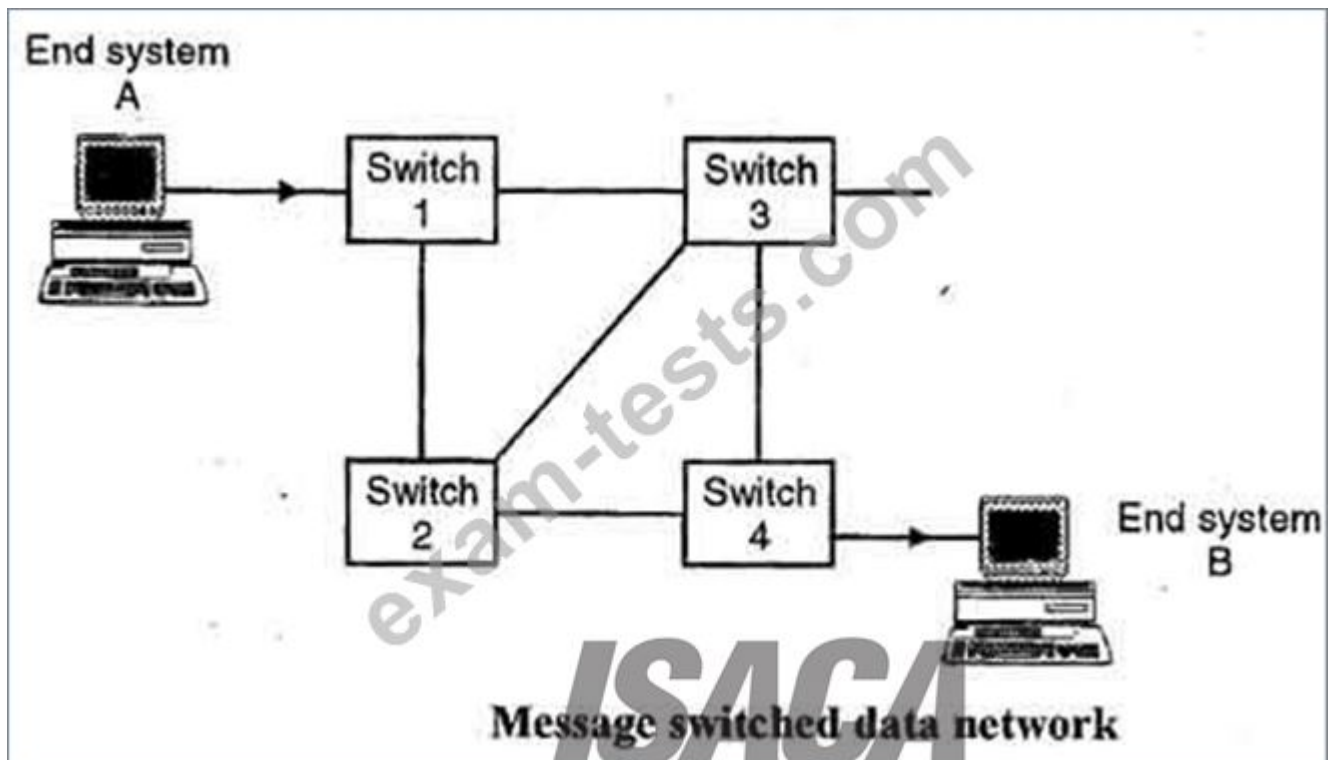


Image from: <http://ecomputernotes.com/images/Message-Switched-data-Network.jpg> Packet Switching

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.

Packet Switching

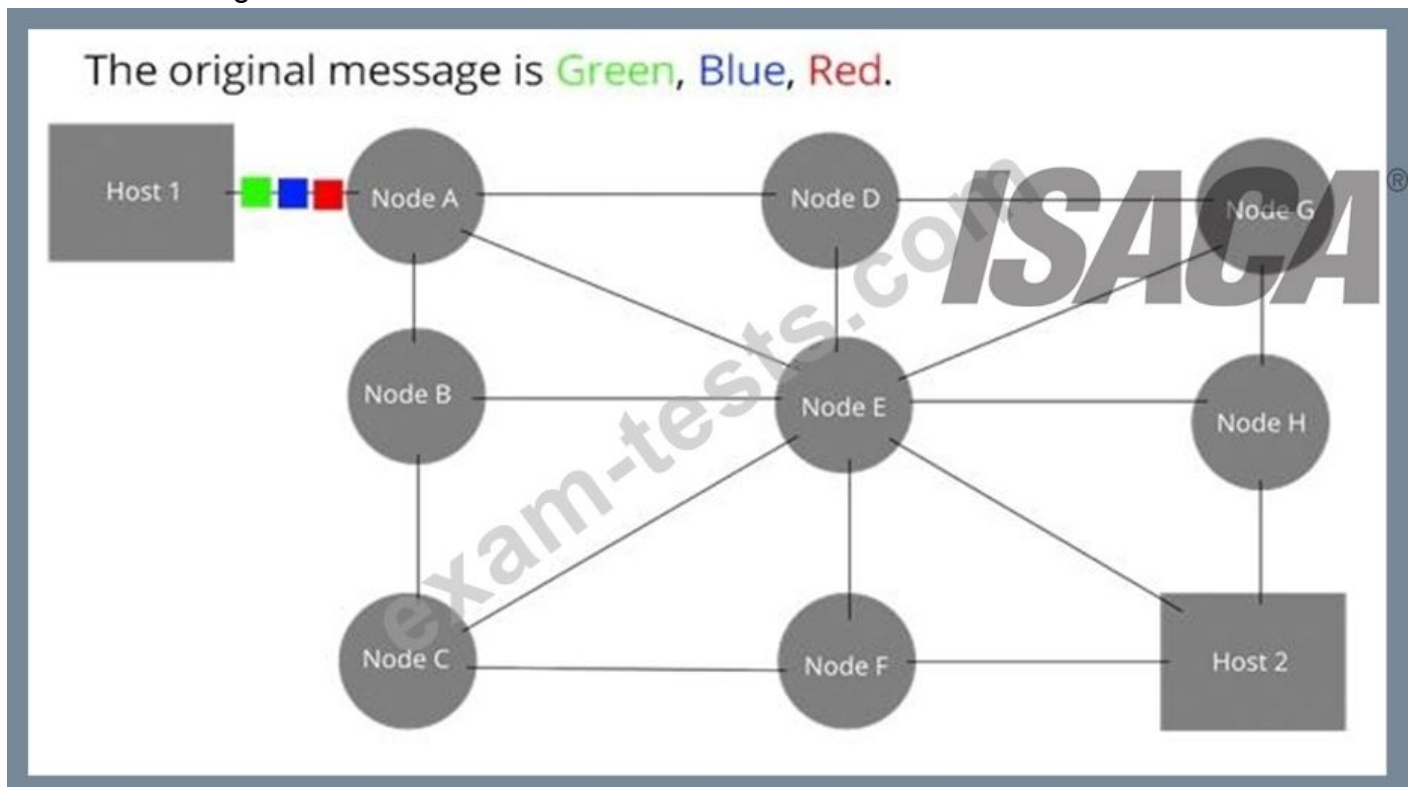


Image from: http://upload.wikimedia.org/wikipedia/commons/f/f6/Packet_Switching.gif Circuit Switching

Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays.

No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Circuit Switching

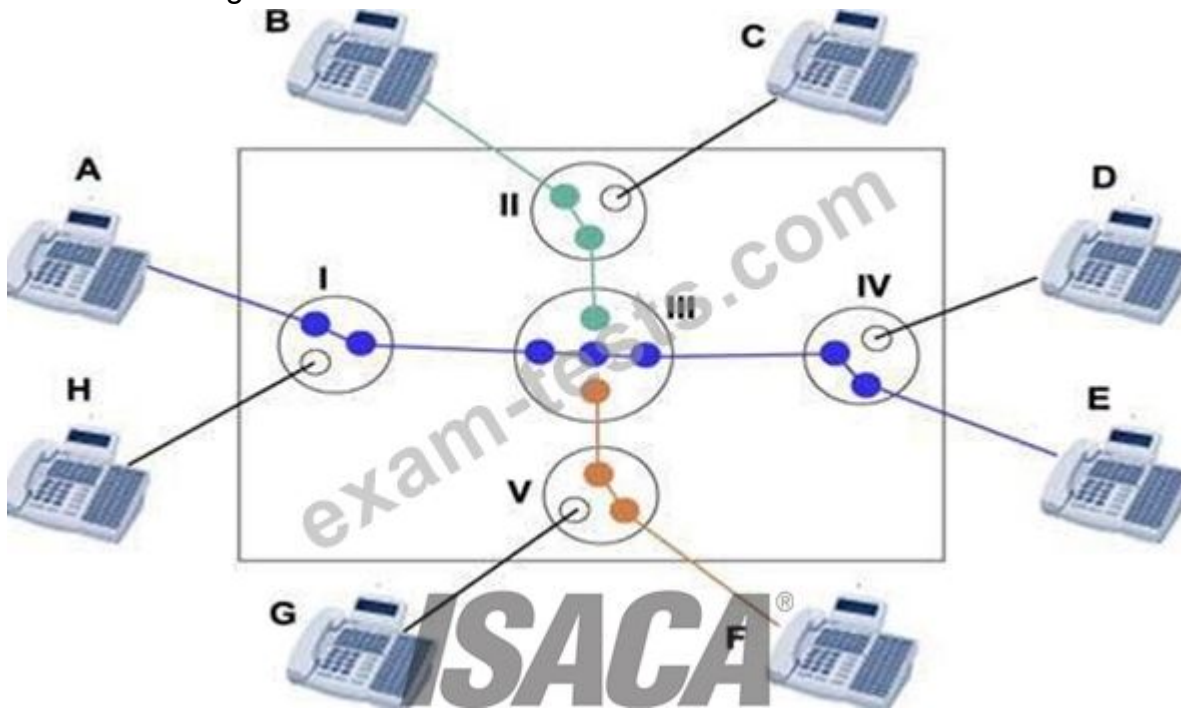


Image from: http://www.louiewong.com/wp-content/uploads/2010/09/Circuit_Switching.jpg See a table below comparing Circuit Switched versus Packet Switched networks:

Difference between Circuit and packet switching

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Image from: <http://www.hardware-one.com/reviews/network-guide-2/images/packet-vs-circuit.gif>

Virtual circuit

In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames. Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes,

varying bit rate generated by the application,

varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:

The other options presented correctly describes about packet switching.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 265

NEW QUESTION: 541

How is the risk of improper file access affected upon implementing a database system?

- A. Risk varies.
- B. Risk is reduced.
- C. Risk is not affected.
- D. Risk is increased.

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Improper file access becomes a greater risk when implementing a database system.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 542

What is the FIRST step an auditor should take when beginning a follow-up audit?

- A. Review workpapers from the previous audit.
- B. Gather evidence of remediation to conduct tests of controls.
- C. Review previous findings and action plans.
- D. Meet with the auditee to discuss remediation progress.

Answer: C ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

NEW QUESTION: 543

Which of the following would be the BEST criteria for monitoring an IT vendor's service levels?

- A. Service auditor's report
- B. Performance metrics
- C. Surprise visit to vendor
- D. Interview with vendor

Answer: ([SHOW ANSWER](#)**)**

Explanation

The best criteria for monitoring an IT vendor's service levels are the performance metrics, as they provide quantifiable and measurable indicators of how well the vendor is delivering the agreed-upon services, such as availability, reliability, quality, timeliness, and customer satisfaction. A service auditor's report is a document that provides an independent opinion on the vendor's controls and processes, but it may not reflect the actual service levels or performance. A surprise visit to the vendor may help to verify the vendor's compliance and operations, but it may not be feasible or effective for monitoring the service levels on a regular basis. An interview with the vendor may help to obtain feedback and insights from the vendor's perspective, but it may not be objective or reliable for monitoring the service levels. References: CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.4: IT Service Delivery and Support

NEW QUESTION: 544

Which of the following must be in place before an IS auditor initiates audit follow-up activities?

- A. Available resources for the activities included in the action plan

- B.** A management response in the final report with a committed implementation date
- C.** A heat map with the gaps and recommendations displayed in terms of risk
- D.** Supporting evidence for the gaps and recommendations mentioned in the audit report

Answer: ([SHOW ANSWER](#))

This must be in place before an IS auditor initiates audit follow-up activities, because it indicates that management has acknowledged and accepted the audit findings and recommendations, and has agreed to take corrective actions within a specified timeframe. Audit follow-up activities are the processes and procedures that the IS auditor performs to verify that management has implemented the agreed-upon actions effectively and in a timely manner, and that the audit findings have been resolved or mitigated.

The other options are not required to be in place before an IS auditor initiates audit follow-up activities:

* Available resources for the activities included in the action plan. This is a factor that may affect the feasibility and success of the action plan, but it is not a prerequisite for the audit follow-up activities.

The IS auditor should assess the availability and adequacy of the resources for the action plan during the audit planning and execution phases, and provide recommendations accordingly. However, the IS auditor does not need to wait for the resources to be available before initiating the audit follow-up activities.

* A heat map with the gaps and recommendations displayed in terms of risk. This is a tool that may help the IS auditor prioritize and communicate the gaps and recommendations, but it is not a requirement for the audit follow-up activities. A heat map is a graphical representation of data that uses colors to indicate the level of risk or impact of each gap or recommendation. The IS auditor may use a heat map to support the audit report or presentation, but it does not replace the need for a management response with a committed implementation date.

* Supporting evidence for the gaps and recommendations mentioned in the audit report. This is a component that should be included in the audit report, but it is not a condition for the audit follow-up activities. Supporting evidence is the information or data that supports or substantiates the audit findings and recommendations. The IS auditor should collect and document sufficient, reliable, relevant, and useful evidence during the audit execution phase, and present it in the audit report. However, the IS auditor does not need to have supporting evidence in place before initiating the audit follow-up activities.

NEW QUESTION: 545

Which of the following is the BEST way to help ensure new IT implementations align with enterprise architecture (EA) principles and requirements?

- A.** Consider stakeholder concerns when defining the EA
- B.** Perform mandatory post-implementation reviews of IT implementations
- C.** Conduct EA reviews as part of the change advisory board
- D.** Document the security view as part of the EA

Answer: **A** ([LEAVE A REPLY](#))

NEW QUESTION: 546

Which of the following is the BEST way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster?

- A. Prepare detailed plans for each business function.
- B. Involve staff at all levels in periodic paper walk-through exercises.
- C. Regularly update business impact assessments.
- D. Make senior managers responsible for their plan sections.

Answer: B ([LEAVE A REPLY](#))

The best way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster is to involve staff at all levels in periodic paper walk-through exercises. This means that the BCPs are tested and validated by the people who will execute them in a real situation, and any gaps, errors, or inconsistencies can be identified and corrected. Paper walk-through exercises are also a good way to raise awareness and train staff on their roles and responsibilities in a BCP scenario, as well as to evaluate the feasibility and effectiveness of the recovery strategies¹.

The other options are not the best ways to ensure that BCPs will work effectively, because they do not involve testing or validating the plans. Preparing detailed plans for each business function is important, but it does not guarantee that the plans are realistic, practical, or aligned with the overall business objectives and priorities². Regularly updating business impact assessments is also essential, but it does not ensure that the BCPs are aligned with the current business environment and risks². Making senior managers responsible for their plan sections is a good way to assign accountability and authority, but it does not ensure that the plan sections are coordinated and integrated with each other². References:

- * Best Practice Guide: Business Continuity Planning (BCP)³
- * Best Practices for Creating a Business Continuity Plan¹
- * Business Continuity Plan Best Practices

NEW QUESTION: 547

When protecting an organization's IT systems, which of the following is normally the next line of defense after the network firewall has been compromised?

- A. Personal firewall
- B. Antivirus programs
- C. Intrusion detection system (IDS)
- D. Virtual local area network (VLAN) configuration

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

Explanation:

An intrusion detection system (IDS) would be the next line of defense after the firewall. It would detect anomalies in the network/server activity and try to detect the perpetrator. Antivirus programs, personal firewalls and VLAN configurations would be later in the line of defense.

NEW QUESTION: 548

To prevent unauthorized entry to the data maintained in a dial-up, fast response system, an IS auditor

should recommend:

- A. online terminals are placed in restricted areas.
- B. online terminals are equipped with key locks.
- C. ID cards are required to gain access to online terminals.
- D. online access is terminated after a specified number of unsuccessful attempts.

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

The most appropriate control to prevent unauthorized entry is to terminate connection after a specified

number of attempts. This will deter access through the guessing of IDs and passwords. The other choices

are physical controls, which are not effective in deterring unauthorized accesses via telephone lines.

NEW QUESTION: 549

When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. The IS auditor should recommend that the:

- A. project be discontinued.
- B. business case be updated and possible corrective actions be identified.
- C. project be returned to the project sponsor for reapproval.
- D. project be completed and the business case be updated later.

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: An IS auditor should not recommend discontinuing or completing the project before reviewing an updated business case. The IS auditor should recommend that the business case be kept current throughout the project since it is a key input to decisions made throughout the life of any project.

NEW QUESTION: 550

A trojan horse simply cannot operate autonomously.

- A. true
- B. false

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

As a common type of Trojan horses, a legitimate software might have been corrupted with malicious code which runs when the program is used. The key is that the user has to invoke the program in order to trigger the malicious code.

In other words, a trojan horse simply cannot operate autonomously. You would also want to know that most but not all trojan horse payloads are harmful - a few of them are harmless.

NEW QUESTION: 551

Segregation of duties would be compromised if:

- A. database administrators (DBAs) modified the structure of user tables.
- B. application programmers accessed test data.
- C. application programmers moved programs into production.
- D. operations staff modified batch schedules.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 552

In a relational database with referential integrity, the use of which of the following keys would prevent deletion of a row from a customer table as long as the customer number of that row is stored with live orders on the orders table?

- A. Foreign key
- B. Primary key
- C. Secondary key
- D. Public key

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

In a relational database with referential integrity, the use of foreign keys would prevent events such as primary key changes and record deletions, resulting in orphaned relations within the database. It should not be possible to delete a row from a customer table when the customer number (primary key) of that row is stored with live orders on the orders table (the foreign key to the customer table). A primary key works in one table, so it is not able to provide/ensure referential integrity by itself. Secondary keys that are not foreign keys are not subject to referential integrity checks. Public key is related to encryption and not linked in any way to referential integrity.

NEW QUESTION: 553

Which of the following provides the BE ST method for maintaining the security of corporate applications pushed to employee-owned mobile devices?

- A. Enabling remote data destruction capabilities
- B. Implementing mobile device management (MDM)
- C. Disabling unnecessary network connectivity options
- D. Requiring security awareness training for mobile users

Answer: B ([LEAVE A REPLY](#))

Explanation

The best method for maintaining the security of corporate applications pushed to employee-owned mobile devices is implementing mobile device management (MDM). MDM is a software solution that allows an organization to remotely manage, configure, and secure the mobile devices that access its network and data.

MDM can help protect corporate applications on employee-owned devices by:

Enforcing security policies and settings, such as encryption, password, firewall, antivirus, and VPN.

Controlling the installation, update, and removal of corporate applications and data.

Separating corporate and personal data and applications on the device using containers or profiles.

Monitoring and auditing the device's compliance status, activity, and location.

Performing remote actions, such as lock, wipe, backup, or restore, in case of loss, theft, or compromise.

MDM can provide a comprehensive and centralized approach to maintain the security of corporate applications on employee-owned devices, regardless of the device type, platform, or ownership. MDM can also help the organization comply with regulatory and industry standards for data protection and privacy.

Enabling remote data destruction capabilities is a useful feature for maintaining the security of corporate applications on employee-owned devices, but it is not the best method by itself.

Remote data destruction allows the organization to erase the corporate data and applications from the device in case of loss, theft, or compromise. However, this feature does not prevent unauthorized access or misuse of the corporate data and applications before they are destroyed. Remote data destruction is usually part of an MDM solution.

Disabling unnecessary network connectivity options is a good practice for maintaining the security of corporate applications on employee-owned devices, but it is not the best method by itself.

Network connectivity options, such as Wi-Fi, Bluetooth, NFC, or USB, can expose the device to potential attacks or data leakage. Disabling these options when they are not needed can reduce the attack surface and improve battery life. However, this practice does not address other security risks or requirements for the corporate applications on the device. Disabling network connectivity options can also be part of an MDM solution.

Requiring security awareness training for mobile users is an important measure for maintaining the security of corporate applications on employee-owned devices, but it is not the best method by itself. Security awareness training can educate the users about the potential threats and best practices for using their devices securely. It can also help foster a culture of security and responsibility among the users. However, security awareness training cannot guarantee that the users will follow the security policies and guidelines consistently and correctly. Security awareness training should be complemented by technical controls, such as MDM.

References:

Protecting Corporate Data on Mobile Devices for All Companies¹

NEW QUESTION: 554

An IS auditor is reviewing a machine learning algorithm-based system for loan approvals and is preparing a data set to test the algorithm for bias. Which of the following is MOST important for the auditor's test data set to include?

- A. Incomplete records and incorrectly formatted data
- B. Duplicate records
- C. Applicants from a range of geographic areas and income levels
- D. Applicants of all ages

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 555

A healthcare facility offers patients health tracking devices that can be monitored remotely by healthcare professionals. Which of the following is the BEST way to protect patient personal information from unauthorized exfiltration?

- A. Restrict the devices to using Internet Protocol (IP) version 6 only.
- B. Add a digital certificate to the devices that limits communication to specific servers.
- C. Configure the devices to reboot automatically every 7 days.
- D. Provide the patients with Internet security training and education programs.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 556

An organization with high availability resource requirements is selecting a provider for cloud computing.

Which of the following would cause the GREATEST concern to an IS auditor? The provider:

- A. hosts systems for the organization's competitor.
- B. deploys patches automatically without testing.
- C. does not store backup media offsite.
- D. is not internationally certified for high availability.

Answer: B ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 557

Which of the following is MOST important to determine during the planning phase of a cloud-based messaging and collaboration platform acquisition?

- A. Role-based access control policies
- B. Types of data that can be uploaded to the platform
- C. Processes for on-boarding and off-boarding users to the platform
- D. Processes for reviewing administrator activity

Answer: ([SHOW ANSWER](#))

Explanation

The most important thing to determine during the planning phase of a cloud-based messaging and collaboration platform acquisition is the types of data that can be uploaded to the platform. This is because different types of data may have different security, privacy, and compliance requirements, depending on the nature, sensitivity, and value of the data. For example, personal data, financial data, health data, or intellectual property data may be subject to various laws and regulations that govern how they can be collected, stored, processed, and shared in the cloud. Therefore, it is essential to identify and classify the types of data that will be uploaded to the platform, and ensure that the platform meets the organization's policies and standards for data protection¹.

The other options are not as important as the types of data that can be uploaded to the platform during the planning phase of a cloud-based messaging and collaboration platform acquisition. Option A, role-based access control policies, is a mechanism that defines who can access what data and resources on the platform based on their roles and responsibilities. Role-based access control policies are important for ensuring data security and accountability, but they can be designed and implemented after the platform is acquired². Option C, processes for on-boarding and off-boarding users to the platform, are procedures that enable or disable user accounts and access rights on the platform. Processes for on-boarding and off-boarding users are important for managing user identities and lifecycles, but they can be developed and executed after the platform is acquired³. Option D, processes for reviewing administrator activity, are methods that monitor and audit the actions and events performed by administrators on the platform. Processes for reviewing administrator activity are important for detecting and preventing unauthorized or malicious activities, but they can be established and performed after the platform is acquired⁴.

References:

Cloud Messaging and Collaboration Services - Maryland.gov DoIT⁴

MessageBird acquires real-time notifications and in-app messaging platform Pusher for \$35M | TechCrunch² Symphony to lead financial market communications with the acquisition of Cloud9 Technologies³ Cloud messaging and collaboration | Sumo Logic

NEW QUESTION: 558

Failing to prevent or detect a material error would represent which type of risk?

- A. Overall audit risk
- B. Detection risk

- C. Inherent risk
- D. Control risk

Answer: ([SHOW ANSWER](#))

A detection risk is that you would fail to detect that a material error has occurred.

NEW QUESTION: 559

The PRIMARY responsibility of a project steering committee is to:

- A. sign off on the final build document.
- B. ensure that each project deadline is met.
- C. ensure that developed systems meet business needs.
- D. provide regular project updates and oversight.

Answer: D ([LEAVE A REPLY](#))

The primary responsibility of a project steering committee is to provide regular project updates and oversight.

A project steering committee is an advisory group that consists of senior stakeholders and experts who offer guidance and support to a project manager and their team. The steering committee is mainly concerned with the direction, scope, budget, timeline, and methods used to realize a given project¹.

One of the key roles of a steering committee is to monitor the progress and performance of the project and ensure that it aligns with the business objectives and stakeholder expectations. The steering committee also provides feedback, advice, and recommendations to the project manager and helps them resolve any issues or challenges that may arise during the project lifecycle. The steering committee communicates regularly with the project manager and other stakeholders through meetings, reports, and presentations²³.

Therefore, providing regular project updates and oversight is the primary responsibility of a project steering committee.

References:

Steering Committee: Definition, Roles & Meeting Tips - ProjectManager

Project Steering Committee: Roles, Best Practices, Challenges - ProjectPractical

Steering Committee: Complete Guide with Examples & Templates - Status.net

NEW QUESTION: 560

During a logical access controls review, an IS auditor observes that user accounts are shared. The

GREATEST risk resulting from this situation is that:

- A. an unauthorized user may use the ID to gain access.
- B. user access management is time consuming.
- C. passwords are easily guessed.
- D. user accountability may not be established.

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

The use of a single user ID by more than one individual precludes knowing who in fact used that ID to access a system; therefore, it is literally impossible to hold anyone accountable. All user IDs, not just shared IDs, can be used by unauthorized individuals. Access management would not be any different with shared IDs, and shared user IDs do not necessarily have easily guessed passwords.

NEW QUESTION: 561

An IS auditor finds multiple situations where the help desk resolved security incidents without notifying IT security as required by policy. Which of the following is the BEST audit recommendation?

- A. Display the incident response hotline in common areas.
- B. Have IT security review problem management policy.
- C. Reinforce the incident escalation process.
- D. Redesign the help desk reporting process.

Answer: (SHOW ANSWER)

Section: Protection of Information Assets

NEW QUESTION: 562

Which of the following is MOST important to include in forensic data collection and preservation procedures?

- A. Assuring the physical security of devices
- B. Preserving data integrity
- C. Maintaining chain of custody
- D. Determining tools to be used

Answer: (SHOW ANSWER)

Explanation

The most important thing to include in forensic data collection and preservation procedures is preserving data integrity. Data integrity is the property that ensures that data is accurate, complete, and consistent throughout its lifecycle. Preserving data integrity is essential for forensic data collection and preservation procedures because it ensures that the data can be used as valid and reliable evidence in legal proceedings or investigations. Preserving data integrity can be achieved by using methods such as hashing, checksums, digital signatures, write blockers, tamper-evident seals, or timestamps. The other options are not as important as preserving data integrity in forensic data collection and preservation procedures, as they do not affect the validity or reliability of the data. Assuring the physical security of devices is a security measure that protects devices from unauthorized access, theft, damage, or destruction, but it does not ensure that the data on the devices is accurate, complete, and consistent. Maintaining chain of custody is a documentation technique that records and tracks the handling and transfer of devices or data

among different parties involved in forensic activities, but it does not ensure that the data on the devices is accurate, complete, and consistent. Determining tools to be used is a planning activity that selects and prepares the appropriate tools for forensic data collection and preservation procedures, but it does not ensure that the data collected and preserved by the tools is accurate, complete, and consistent. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4

NEW QUESTION: 563

Which of the following would be of GREATEST concern to an IS auditor reviewing a critical spreadsheet during a financial audit?

- A. Changes to the file are not always documented.
- B. Periodic access reviews are manually performed.
- C. Access requests are manually processed.
- D. A copy of the current validated file is not available.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 564

Which of the following is NOT a disadvantage of Single Sign On (SSO)?

- A. Support for all major operating system environment is difficult
- B. The cost associated with SSO development can be significant
- C. SSO could be single point of failure and total compromise of an organization asset
- D. SSO improves an administrator's ability to manage user's account and authorization to all associated system

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Single sign-on (SSO) is a Session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

SSO Advantages include

Multiple passwords are no longer required

It improves an administrator's ability to manage user's accounts and authorization to all associated systems

It reduces administrative overhead in resetting forgotten password over multiple platforms and applications It reduces time taken by users to logon into multiple application and platform SSO

Disadvantages include

Support for all major operating system is difficult

The cost associated with SSO development can be significant when considering the nature and extent of interface development and maintenance that may be necessary

The centralized nature of SSO presents the possibility of a single point of failure and total compromise of an organization's information asset.

The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 332

NEW QUESTION: 565

Which of the following is the BEST indicator of a mature quality management system (QMS)?

- A. Most IT projects have been completed on time and within budget.
- B. Projects are showing continuous improvement
- C. End users are satisfied with the outcome of IT projects.
- D. Continuous improvement has been integrated into business processes.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 566

An organization is using an enterprise resource management (ERP) application. Which of the following

would be an effective access control?

- A. User-level permissions
- B. Role-based
- C. Fine-grained
- D. Discretionary

Answer: ([SHOW ANSWER](#)**)**

Section: Protection of Information Assets

Explanation:

Role-based access controls the system access by defining roles for a group of users. Users are assigned to the various roles and the access is granted based on the user's role. User-level permissions for an ERP system would create a larger administrative overhead. Fine-grained access control is very difficult to implement and maintain in the context of a large enterprise. Discretionary access control may be configured or modified by the users or data owners, and therefore may create inconsistencies in the access control management.

NEW QUESTION: 567

Which of the following audit procedures would be MOST conclusive in evaluating the effectiveness of an e-commerce application system's edit routine?

- A. Review of program documentation
- B. Use of test transactions
- C. Interviews with knowledgeable users
- D. Review of source code

Answer: ([SHOW ANSWER](#)**)**

The most conclusive audit procedure for evaluating the effectiveness of an e-commerce application system's edit routine is to use test transactions. A test transaction is a simulated input that is processed by the system to verify its output and performance¹. By using test transactions, an auditor can directly observe how the edit routine checks the validity, accuracy, and completeness of data entered by users, and how it handles incorrect or invalid data. A test transaction can also help measure the efficiency, reliability, and security of the edit routine, as well as identify any errors or weaknesses in the system.

The other options are not as conclusive as using test transactions, as they rely on indirect or secondary sources of information. Reviewing program documentation is an audit procedure that involves examining the written description of the system's design, specifications, and functionality². However, program documentation may not reflect the actual implementation or operation of the system, and it may not reveal any discrepancies or defects in the edit routine. Interviews with knowledgeable users is an audit procedure that involves asking questions to the people who use or manage the system³. However, interviews with knowledgeable users may not provide sufficient or objective evidence of the edit routine's effectiveness, and they may be influenced by personal opinions or biases. Reviewing source code is an audit procedure that involves analyzing the programming language and logic of the system⁴. However, reviewing source code may not be feasible or practical for complex or large systems, and it may not demonstrate how the edit routine performs in real scenarios.

NEW QUESTION: 568

An IS audit manager finds that data manipulation logic developed by the audit analytics team leads to incorrect conclusions. This inaccurate logic is MOST likely an indication of which of the following?

- A. Poor security controls that grant inappropriate access to analysis produced
- B. The team's poor understanding of the business process being analyzed
- C. Incompatibility between data volume and analytics processing capacity
- D. Poor change controls over data sets collected from the business

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 569

An IS auditor is reviewing an artificial intelligence (AI) and expert system application. The system has produced several critical errors with severe impact. Which of the following should the IS auditor do NEXT to understand the cause of the errors?

- A. Interview the system owner.
- B. Review the decision-making logic built into the system.
- C. Understand the purpose and functionality of the system.
- D. Verify system adherence to corporate policy.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 570

Which of the following would have the HIGHEST priority in a business continuity plan (BCP)?

- A. Resuming critical processes
- B. Recovering sensitive processes
- C. Restoring the site
- D. Relocating operations to an alternative site

Answer: A (LEAVE A REPLY)

The resumption of critical processes has the highest priority as it enables business processes to begin immediately after the interruption and not later than the declared mean time between failure (MTBF). Recovery of sensitive processes refers to recovering the vital and sensitive processes that can be performed manually at a tolerable cost for an extended period of time and those that are not marked as high priority. Repairing and restoring the site to original status and resuming the business operations are time consuming operations and are not the highest priority. Relocating operations to an alternative site, either temporarily or permanently depending on the interruption, is a time consuming process; moreover, relocation may not be required.

NEW QUESTION: 571

.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 (LEAVE A REPLY)

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.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 572

Which of the following ACID property ensures that transaction will bring the database from one valid state to another?

- A. Atomicity
- B. Consistency
- C. Isolation
- D. Durability

Answer: B ([LEAVE A REPLY](#))

Section: Information System Acquisition, Development and Implementation

Explanation/Reference:

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

For CISA exam you should know below information about ACID properties in DBMS:

Atomicity - Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged. An atomic system must guarantee atomicity in each and every situation, including power failures, errors, and crashes. To the outside world, a committed transaction appears (by its effects on the database) to be indivisible ("atomic"), and an aborted transaction does not happen.

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system

state that would be obtained if transactions were executed serially, i.e. one after the other.

Providing

isolation is the main goal of concurrency control. Depending on concurrency control method, the effects of

an incomplete transaction might not even be visible to another transaction.[citation needed]

Durability - Durability means that once a transaction has been committed, it will remain so, even in the

event of power loss, crashes, or errors. In a relational database, for instance, once a group of SQL

statements execute, the results need to be stored permanently (even if the database crashes immediately

thereafter). To defend against power loss, transactions (or their effects) must be recorded in a non-volatile

memory.

The following were incorrect answers:

Atomicity - Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the

entire transaction fails, and the database state is left unchanged.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system

state that would be obtained if transactions were executed serially, i.e. one after the other.

Durability - Durability means that once a transaction has been committed, it will remain so, even in the

event of power loss, crashes, or errors.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 218

NEW QUESTION: 573

An IS audit reveals that an organization operating in business continuity mode during a pandemic situation has not performed a simulation test of the business continuity plan (BCP). Which of the following is the auditor's BEST course of action?

- A.** Confirm the BCP has been recently updated.
- B.** Review the effectiveness of the business response.
- C.** Raise an audit issue for the lack of simulated testing.
- D.** Interview staff members to obtain commentary on the BCP's effectiveness.

Answer: B ([LEAVE A REPLY](#))

Explanation

This is because the auditor's primary objective is to evaluate the adequacy and performance of the business continuity plan (BCP) in ensuring the continuity and resilience of the organization's critical functions and processes during a disruption. The auditor should review the actual results and outcomes of the business response, such as the recovery time, recovery point, service level,

customer satisfaction, and incident management, and compare them with the predefined objectives and criteria of the BCP. The auditor should also identify and analyze any gaps, issues, or lessons learned from the business response, and provide recommendations for improvement¹².

Answer A. Confirm the BCP has been recently updated. is not the best answer, because it is not directly related to the auditor's course of action. Confirming the BCP has been recently updated is a part of the audit planning and scoping process, not the audit execution or reporting process. The auditor should confirm the BCP has been recently updated before conducting the audit, not after revealing that a simulation test has not been performed. Moreover, confirming the BCP has been recently updated does not provide sufficient evidence of the effectiveness of the business response¹².

Answer C. Raise an audit issue for the lack of simulated testing. is not the best answer, because it is not relevant to the auditor's course of action. Raising an audit issue for the lack of simulated testing is a part of the audit reporting and follow-up process, not the audit execution or evaluation process. The auditor should raise an audit issue for the lack of simulated testing after reviewing the effectiveness of the business response, not before or instead of doing so. Furthermore, raising an audit issue for the lack of simulated testing does not address the root cause or impact of the problem, nor does it provide any constructive feedback or guidance for improvement¹².

Answer D. Interview staff members to obtain commentary on the BCP's effectiveness. is not the best answer, because it is not sufficient to guide the auditor's course of action. Interviewing staff members to obtain commentary on the BCP's effectiveness is a part of the audit evidence collection and analysis process, not the audit evaluation or conclusion process. The auditor should interview staff members to obtain commentary on the BCP's effectiveness as one of the sources of information, not as the only or main source of information. Additionally, interviewing staff members to obtain commentary on the BCP's effectiveness may be subjective, biased, or incomplete, and may not reflect the actual performance or outcomes of the business response¹².

References:

Business Continuity Management Audit/Assurance Program

Business Continuity Plan Testing: Types and Best Practices

NEW QUESTION: 574

When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

- A.** sufficient evidence will be collected.
- B.** all significant deficiencies identified will be corrected within a reasonable period.
- C.** all material weaknesses will be identified.
- D.** audit costs will be kept at a minimum level.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Procedures are processes an IS auditor may follow in an audit engagement. In determining the appropriateness of any specific procedure, an IS auditor should use professional judgment

appropriate to the specific circumstances. Professional judgment involves a subjective and often qualitative evaluation of conditions arising in the course of an audit. Judgment addresses a grey area where binary (yes/no) decisions are not appropriate and the auditor's past experience plays a key role in making a judgment.

ISACA's guidelines provide information on how to meet the standards when performing IS audit work.

Identifying material weaknesses is the result of appropriate competence, experience and thoroughness in planning and executing the audit and not of professional judgment. Professional judgment is not a primary input to the financial aspects of the audit.

NEW QUESTION: 575

Which of the following function in traditional EDI translate data between the standard format and trading partner's propriety format?

- A.** Communication handler
- B.** Application Interface
- C.** Application System
- D.** EDI Translator

Answer: (SHOW ANSWER)

Section: Information System Acquisition, Development and Implementation

Explanation/Reference:

EDI Translator translates data between standard format (ANSI X12) and trading partner's propriety information.

For CISA Exam you should know below information about Traditional EDI functions.

Moving data in a batch transmission process through the traditional EDI process generally involves three

functions within each trading partner's computer system

Communication handler - Process for transmitting and receiving electronic documents between trading

partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network

(VAN). VAN use computerized message switching and storage capabilities to provide electronic mailbox

services similar to post offices. The VAN receives all the outbound transactions from an organization, sort

them by destination and passes them to precipitants when they log on to check their mailbox and receive transmission.

EDI Interface -Interface function that manipulates and routes data between the application system and the

communication handler. The interface consists of two components

EDI Translator - The device translates data between standard format (ANSI X12) and trading partner's propriety information.

Application Interface - This interface moves electronic transactions to or from the application systems and

perform data mapping. Data mapping is the process by which data are extracted from EDI translation

process and integrated with the data or process of receiving company.

3. Application System -The program that process the data sent to, or received from, the trading partner.

Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

The following were incorrect answers:

Communication handler - Process for transmitting and receiving electronic documents between trading

partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network

(VAN).

Application System -The program that process the data sent to, or received from, the trading partner.

Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

Application Interface - This interface moves electronic transactions to or from the application systems and

perform data mapping.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 178

NEW QUESTION: 576

Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

A. Traffic analysis

B. SYN flood

C. Denial of service (DoS)

D. Distributed denial of service (DoS)

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

Traffic analysis is a passive attack method used by intruders to determine potential network vulnerabilities.

All others are active attacks.

NEW QUESTION: 577

Which of the following should be the FIRST step when developing a business continuity plan (BCP)?

- A. Conduct a risk assessment
- B. Discuss recovery time and recovery process objectives with the business owner
- C. Develop a business continuity strategy
- D. Choose appropriate controls and measures for recovering IT components.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 578

Which of the following is the MOST reliable network connection medium in an environment where there is

strong electromagnetic interference?

- A. Coaxial cable
- B. Fiber optic cable
- C. Shielded twisted-pair cable
- D. Wireless link

Answer: B ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 579

An IS auditor observes that a bank's web page address is prefixed "https://". The auditor would be correct to conclude that:

- A. transactions are encrypted
- B. the customer is connected to the bank's intranet
- C. the bank has a restricted Internet protocol (IP) address
- D. the bank has established a virtual private network (VPN).

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 580

Which of the following observations should be of GREATEST concern to an IS auditor performing an audit of change and release management controls for a new complex system developed by a small in-house IT team?

- A. Access to change testing strategy and results is not restricted to staff outside the IT team.
- B. Some user acceptance testing (IJAT) was completed by members of the IT team.
- C. IT administrators have access to the production and development environment
- D. Post-implementation testing is not conducted for all system releases.

Answer: D ([LEAVE A REPLY](#))

Post-implementation testing is the process of verifying and validating the functionality, performance, and security of a system after it has been deployed to the production environment¹. Post-implementation testing is important for ensuring that the system meets the user requirements and expectations, as well as the operational and business objectives. Post-implementation testing also helps to identify and resolve any defects, errors, or issues that may have occurred during the deployment process or that may have been missed during the previous testing stages².

Therefore, the observation that post-implementation testing is not conducted for all system releases should be of greatest concern to an IS auditor performing an audit of change and release management controls for a new complex system developed by a small in-house IT team. This observation indicates that the system may have quality, reliability, or security problems that could affect the user satisfaction, system performance, or data integrity. This observation also suggests that the change and release management controls are not adequate or effective, as they do not ensure that all system releases are properly tested and validated before and after deployment.

Option A is not correct because access to change testing strategy and results is not restricted to staff outside the IT team is not a major concern for an IS auditor. While it is good practice to limit access to sensitive or confidential information, such as test data or test cases, to authorized personnel only, access to change testing strategy and results may not pose a significant risk to the system or the organization. Moreover, access to change testing strategy and results may be beneficial for some stakeholders outside the IT team, such as business users, project managers, or auditors, who may need to review or evaluate the testing process or outcomes.

Option B is not correct because some user acceptance testing (UAT) was completed by members of the IT team is not a major concern for an IS auditor. User acceptance testing is the process of verifying and validating that the system meets the user requirements and expectations by involving actual or representative users in the testing process³. While it is preferable to have independent and unbiased users perform UAT, it may not be feasible or practical for some organizations, especially those with small or limited resources.

Therefore, some UAT may be completed by members of the IT team, as long as they have sufficient knowledge and experience of the user needs and expectations, and as long as they follow the UAT plan and criteria.

Option C is not correct because IT administrators have access to the production and development environment is not a major concern for an IS auditor. IT administrators are responsible for managing and maintaining the IT infrastructure, including the production and development environments⁴. Therefore, it is reasonable and necessary for them to have access to both environments, as long as they follow the appropriate policies and procedures for accessing, using, and securing them. Moreover, IT administrators may need to perform tasks such as backup, restore, patching, or troubleshooting in both environments.

References:

What Is Post Implementation Testing?¹

Post Implementation Review (PIR) - Definition & Process²

User Acceptance Testing (UAT): Definition & Examples³

What Is an IT Administrator? Definition & Examples⁴

NEW QUESTION: 581

When an IS auditor evaluates key performance indicators (KPIs) (or IT initiatives, it is MOST important that the KPIs indicate.

- A. IT solutions are within budget
- B. IT objectives are measured
- C. IT deliverables are process driven.
- D. IT resources are fully utilized

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 582

When replacing a critical software application, which of the following provides for the LOWEST risk of interruption to business processes?

- A. Incremental implementation
- B. Pilot implementation
- C. Parallel implementation
- D. Big-bang implementation

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 583

An organization has implemented an automated match between purchase orders, goods receipts, and invoices. Which of the following risks will this control BEST mitigate?

- A. Customer discounts not being applied
- B. Delay of purchase orders
- C. A legitimate transaction being paid multiple times
- D. Invalid payments being processed by the system

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 584

When reviewing hard disk utilization reports, an IS auditor observes that utilization is routinely above 95%. Which of the following should be the GREATEST concern to the IS auditor?

- A. Denial of service (DoS) attacks
- B. Consistency
- C. Availability
- D. Data security

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 585

The reliability of an application system's audit trail may be questionable if:

- A. user IDs are recorded in the audit trail.
- B. the security administrator has read-only rights to the audit file.
- C. date and time stamps are recorded when an action occurs.
- D. users can amend audit trail records when correcting system errors.

Answer: D (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

An audit trail is not effective if the details in it can be amended.

NEW QUESTION: 586

Reviewing which of the following would provide the BEST indication that a project is progressing as planned?

- A. Identification of the critical path
- B. Earned value analysis (EVA) results
- C. Work breakdown structure
- D. Traceability matrix

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed Explanation:

Earned Value Analysis (EVA) provides a quantitative measure of project progress by comparing planned value, earned value, and actual costs. This gives insight into schedule and budget performance, making it the best tool to assess whether the project is on track.

* Critical path (A): Helps in identifying dependencies but not progress.

* Work breakdown structure (C): Defines scope but does not measure progress.

* Traceability matrix (D): Ensures requirements coverage, not schedule/cost progress.

ISACA Reference: CISA Review Manual 27th Edition, Domain 3 (Information Systems Acquisition, Development, and Implementation), section on project management metrics and monitoring techniques.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 587

A small business unit is implementing a control self-assessment (CSA) program and leveraging the internal audit function to test its internal controls annually. Which of the following is the MOST significant benefit of this approach?

- A. Business owners can focus more on their core roles.
- B. Compliance costs are reduced.
- C. Risks are detected earlier.
- D. Line management is more motivated to avoid control exceptions.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 588

An IS auditor learns the organization has experienced several server failures in its distributed environment.

Which of the following is the BEST recommendation to limit the potential impact of server failures in the future?

- A. Redundant pathways
- B. Clustering
- C. Failover power
- D. Parallel testing

Answer: B ([LEAVE A REPLY](#))

Explanation

Clustering is a technique that allows multiple servers to work together as a single system, providing high availability, load balancing, and fault tolerance. Clustering can limit the potential impact of server failures in a distributed environment, as it can automatically switch the workload to another server in the cluster if one server fails, without interrupting the service. Redundant pathways, failover power, and parallel testing are also useful for improving the reliability and availability of servers, but they do not directly address the issue of server failures.

NEW QUESTION: 589

Which of the following should be the FIRST step in managing the impact of a recently discovered zero-day attack?

- A. Estimating potential damage
- B. Identifying vulnerable assets
- C. Assessing the impact of vulnerabilities
- D. Evaluating the likelihood of attack

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 590

When using digital signatures, a sender transmits an encrypted message digest. This ensures that the:

- A. message is not intercepted during transmission
- B. message is not altered during transmission

- C. message sender obtains acknowledgement of delivery
- D. message remains confidential during transmission

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 591

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: ([SHOW ANSWER](#)**)**

Explanation/Reference:

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 proposed development contract should 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.

NEW QUESTION: 592

During a review, an IS auditor discovers that corporate users are able to access cloud-based applications and data any Internet-connected web browser. Which Of the following is the auditor's BEST recommendation to prevent unauthorized access?

- A. Implement an intrusion detection system (IDS),
- B. Update security policies and procedures.
- C. Implement multi-factor authentication.
- D. Utilize strong anti-malware controls on all computing devices.

Answer: C ([LEAVE A REPLY](#))

The best recommendation to prevent unauthorized access to cloud-based applications and data is to implement multi-factor authentication (MFA). MFA is a method of verifying the identity of a user by requiring two or more pieces of evidence, such as a password, a code sent to a phone, or a biometric factor. MFA adds an extra layer of security to prevent unauthorized access, even if the user's password is compromised or stolen. MFA can also help comply with data privacy and security regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).

The other options are not as effective as MFA in preventing unauthorized access. An intrusion detection system (IDS) is a tool that monitors network traffic and alerts administrators of suspicious or malicious activity, but it does not prevent access by itself. Updating security policies and procedures is a good practice, but it does not ensure that users follow them or that they are enforced. Utilizing strong anti-malware controls on all computing devices can help protect against malware infections, but it does not prevent users from accessing cloud-based applications and data from any Internet-connected web browser.

References:

ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471

ISACA, CISAR Review Questions, Answers & Explanations Database - 12 Month Subscription²

What Is Cloud Security? | Google Cloud³

5 Cloud Application Security Best Practices | Snyk⁴

NEW QUESTION: 593

Which of the following would an IS auditor consider a weakness when performing an audit of an organization that uses a public key infrastructure with digital certificates for its business-to-consumer transactions via the internet?

- A.** Customers are widely dispersed geographically, but the certificate authorities are not.
- B.** Customers can make their transactions from any computer or mobile device.
- C.** The certificate authority has several data processing subcenters to administer certificates.
- D.** The organization is the owner of the certificate authority.

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation: If the certificate authority belongs to the same organization, this would generate a conflict of

interest. That is, if a customer wanted to repudiate a transaction, they could allege that because of the

shared interests, an unlawful agreement exists between the parties generating the certificates, if a customer wanted to repudiate a transaction, they could argue that there exists a bribery between the

parties to generate the certificates, as shared interests exist. The other options are not weaknesses.

NEW QUESTION: 594

TEMPEST is a hardware for which of the following purposes?

- A.** Eavedropping
- B.** Social engineering
- C.** Virus scanning
- D.** Firewalling
- E.** None of the choices.

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Any data that is transmitted over a network is at some risk of being eavesdropped, or even modified by a malicious person. Even machines that operate as a closed system can be eavesdropped upon via monitoring the faint electromagnetic transmissions generated by the hardware such as TEMPEST.

NEW QUESTION: 595

An IS auditor evaluating the change management process must select a sample from the change log. What is the BEST way to the auditor to confirm the change log is complete?

- A.** Interview change management personnel about completeness.
- B.** Take an item from the log and trace it back to the system.
- C.** Obtain management attestation of completeness.
- D.** Take the last change from the system and trace it back to the log.

Answer: D (LEAVE A REPLY)

The answer D is correct because the best way for the auditor to confirm the change log is complete is to take the last change from the system and trace it back to the log. A change log is a record of all the changes that have been made to a system, such as software updates, bug fixes, configuration modifications, etc. A change log should contain information such as the date and time of the change, the description and purpose of the change, the person or service who made the change, and the approval status of the change. A complete change log helps to ensure that the system is secure, reliable, and compliant with the relevant standards and regulations.

An IS auditor evaluating the change management process must select a sample from the change log to verify that the changes are properly authorized, documented, tested, and implemented. However, before selecting a sample, the auditor must ensure that the change log is complete and accurate, meaning that it contains all the changes that have been made to the system and that there are no missing, duplicated, or falsified entries. To do this, the auditor can use a technique called backward tracing, which involves taking the last change from the system and tracing it back to the log. This way, the auditor can check if the change is recorded in the log with all the relevant details and if there are any gaps or inconsistencies in the log. If the last change from the system is not found in the log or does not match with the log entry, it indicates that the change log is incomplete or inaccurate.

The other options are not as good as option D. Interviewing change management personnel about completeness (option A) is not a reliable way to confirm the change log is complete because it relies on subjective opinions and self-reported information, which may not be truthful or accurate. Taking an item from the log and tracing it back to the system (option B) is a technique called forward tracing, which can be used to verify that a specific change in the log has been implemented in the system. However, this technique does not confirm that all changes in the system are recorded in the log. Obtaining management attestation of completeness (option C) is not a sufficient way to confirm the change log is complete because it does not provide any

evidence or verification of completeness. Management attestation may also be biased or influenced by conflicts of interest.

References:

- * IS Audit Basics: Auditing Data Privacy
- * Audit Logging: What It Is & How It Works | Datadog
- * Change Management for SOC: Risks, Controls, Audits, Guidance
- * Turn auditing on or off | Microsoft Learn
- * #118 | ITGC- System Change (Audit) Log Review - A2Q2

NEW QUESTION: 596

Due to changes in IT, the disaster recovery plan of a large organization has been changed. What is the

PRIMARY risk if the new plan is not tested?

- A. Catastrophic service interruption
- B. High consumption of resources
- C. Total cost of the recovery may not be minimized
- D. Users and recovery teams may face severe difficulties when activating the plan

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

Choices B, C and D are all possible problems that might occur, and would cause difficulties and financial

losses or waste of resources. However, if a new disaster recovery plan is not tested, the possibility of a

catastrophic service interruption is the most critical of all risks.

NEW QUESTION: 597

Which of the following would prevent accountability for an action performed, thus allowing nonrepudiation?

- A. Proper authentication
- B. Proper identification AND authentication
- C. Proper identification
- D. Proper identification, authentication, AND authorization

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

If proper identification and authentication are not performed during access control, no accountability can exist for any action performed.

NEW QUESTION: 598

The purpose of a mainframe audit is to provide assurance that (choose all that apply):

- A. processes are being implemented as required

- B. the mainframe is operating as it should
- C. security is strong
- D. procedures in place are working
- E. procedures in place are updated as needed
- F. the OS applications are secured
- G. None of the choices.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

The purpose of a mainframe audit is to provide assurance that processes are being implemented as required, the mainframe is operating as it should, security is strong, and that procedures in place are working and are updated as needed. The auditor may accordingly make recommendations for improvement.

NEW QUESTION: 599

An IT balanced scorecard is PRIMARILY used for:

- A. allocating IT budget and resources.
- B. evaluating the IT project portfolio.
- C. monitoring risk in IT-related processes.
- D. measuring IT strategic performance.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 600

The PRIMARY reason for using digital signatures is to ensure data:

- A. confidentiality.
- B. integrity.
- C. availability.
- D. timeliness.

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Digital signatures provide integrity because the digital signature of a signed message (file, mail, document, etc.) changes every time a single bit of the document changes; thus, a signed document cannot be altered.

Depending on the mechanism chosen to implement a digital signature, the mechanism might be able to ensure data confidentiality or even timeliness, but this is not assured. Availability is not related to digital signatures.

NEW QUESTION: 601

The responsibility for authorizing access to application data should be with the:

- A. data custodian.

- B. database administrator (DBA).
- C. data owner.
- D. security administrator.

Answer: C ([LEAVE A REPLY](#))

Data owners should have the authority and responsibility for granting access to the data and applications for which they are responsible. Data custodians are responsible only for storing and safeguarding the data. The database administrator (DBA) is responsible for managing the database and the security administrator is responsible for implementing and maintaining IS security. The ultimate responsibility for data resides with the data owner.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 602

A CIO has asked an IS auditor to implement several security controls for an organization's IT processes and systems. The auditor should:

- A. perform the assignment and future audits with due professional care.
- B. refuse due to independence issues.
- C. communicate the conflict of interest to audit management
- D. obtain approval from executive management for the implementation

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 603

During the implementation of an upgraded enterprise resource planning (ERP) system, which of the following is the MOST important consideration for a go-live decision?

- A. Test cases
- B. Post-implementation review objectives
- C. Rollback strategy
- D. Business case

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 604

Which of the following audit procedures would be MOST conclusive in evaluating the effectiveness of an e-commerce application system's edit routine?

- A. Review of source code

- B. Use of test transactions
- C. Interviews with knowledgeable users
- D. Review of program documentation

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 605

An IS auditor has been asked to audit the proposed acquisition of new computer hardware. The auditor's PRIMARY concern is that:

- A. a clear business case has been established.
- B. the new hardware meets established security standards.
- C. a full, visible audit trail will be included.
- D. the implementation plan meets user requirements.

Answer: A ([LEAVE A REPLY](#))

The first concern of an IS auditor should be to establish that the proposal meets the needs of the business, and this should be established by a clear business case. Although compliance with security standards is essential, as is meeting the needs of the users and having users involved in the implementation process, it is too early in the procurement process for these to be an IS auditors first concern.

NEW QUESTION: 606

The use of which of the following would BEST enhance a process improvement program?

- A. Balanced scorecard
- B. Capability maturity models
- C. Project management methodologies
- D. Model-based design notations

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 607

Which of the following is a benefit of requiring management to issue a report to stakeholders regarding the internal controls over IT?

- A. Transparency of IT costs
- B. Improved portfolio management
- C. Improved cost management
- D. Focus on IT governance

Answer: D ([LEAVE A REPLY](#))

Section: Governance and Management of IT

NEW QUESTION: 608

Which of the following is the MOST appropriate document for granting authority to an external IS auditor in an audit engagement with a client organization?

- A. Approved statement of work

- B. Formally approved audit charter
- C. An internal memo to all concerned parties
- D. Request for proposal for audit services

Answer: ([SHOW ANSWER](#))

Section: The process of Auditing Information System

NEW QUESTION: 609

Which of the following is the GREATEST advantage of implementing an IT enterprise architecture framework within an organization?

- A. It helps to identify security issues in systems across the organization.
- B. It better equips an organization to adopt innovative and emerging technologies.
- C. It reduces the overlap of infrastructure technologies within the organization.
- D. It improves the organization's ability to meet service level agreements (SLAs).

Answer: A ([LEAVE A REPLY](#))

Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 610

In wireless communication, which of the following controls allows the device receiving the communications to verify that the received communications have not been altered in transit?

- A. Device authentication and data origin authentication
- B. Wireless intrusion detection (IDS) and prevention systems (IPS)
- C. The use of cryptographic hashes
- D. Packet headers and trailers

Answer: ([SHOW ANSWER](#))

Calculating cryptographic hashes for wireless communications allows the device receiving the communications to verify that the received communications have not been altered in transit. This prevents masquerading and message modification attacks. Device authentication and data origin authentication is not the correct answer since authenticating wireless endpoints to each other prevents man-in-the-middle attacks and masquerading. Wireless IDS / IPSs is not the correct answer since wireless IDS/ IPSs have the ability to detect misconfigured devices and rogue devices, and detect and possibly stop certain types of attacks. Packet headers and trailers alone do not ensure that the content has not been altered.

NEW QUESTION: 611

Which of the following issues associated with a data center's closed-circuit television (CCTV) surveillance cameras should be of MOST concern to an IS auditor?

- A. CCTV recordings are not regularly reviewed.
- B. CCTV cameras are not installed in break rooms
- C. CCTV records are deleted after one year.
- D. CCTV footage is not recorded 24 x 7.

Answer: A ([LEAVE A REPLY](#))

The most concerning issue associated with a data center's CCTV surveillance cameras is that the recordings are not regularly reviewed. This means that any unauthorized access, theft, vandalism, or other security incidents may go unnoticed and unreported. CCTV recordings are a valuable source of evidence and deterrence for data center security, and they should be monitored and audited periodically to ensure compliance with policies and regulations. If the recordings are not reviewed, the data center may face legal, financial, or reputational risks in case of a security breach or an audit failure.

The other options are less concerning because they do not directly affect the security of the data center. CCTV cameras are not required to be installed in break rooms, as they are not critical areas for data protection.

CCTV records can be deleted after one year, as long as they comply with the data retention policy of the organization and the applicable laws. CCTV footage does not need to be recorded 24 x 7, as long as there is sufficient coverage of the data center during operational hours and when access is granted to authorized personnel. References:

* ISACA Journal Article: Physical security of a data center¹

* Data Center Security: Checklist and Best Practices | Kisi²

* Video Surveillance Best Practices | Taylored Systems

NEW QUESTION: 612

Management has requested a post-implementation review of a newly implemented purchasing package to determine the extent that business requirements are being met. Which of the following is MOST likely to be assessed?

- A. Acceptance testing results
- B. Implementation methodology
- C. Results of live processing
- D. Purchasing guidelines and policies

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 613

The waterfall life cycle model of software development is BEST suited for which of the following situations?

- A. The project will involve the use of new technology
- B. The project requirements are well understood
- C. The project is subject to time pressures.
- D. The project intends to apply an object-oriented design approach.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 614

Which of the following is the MOST important consideration for patching mission critical business application servers against known vulnerabilities?

- A. Vulnerability assessments are periodically conducted according to defined schedules.

- B. Patches are implemented in a test environment prior to rollout into production.
- C. Network vulnerability scans are conducted after patches are implemented.
- D. Roles and responsibilities for implementing patches are defined.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 615

Identify the correct sequence which needs to be followed as a chain of event in regards to evidence handling in computer forensics?

- A. Identify, Analyze, preserve and Present
- B. Analyze, Identify, preserve and present
- C. Preserve, Identify, Analyze and Present
- D. Identify, Preserve, Analyze and Present

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

There are 4 major considerations in the chain of event in regards to evidence in computer forensics:

Identify -Refers to identification of information that is available and might form evidence of an accident
Preserve -Refers to the practice of retrieving identified information and preserving it as evidence. The practice generally includes the imaging of original media in presence of an independent third party. The process also requires being able to document chain-of-custody so that it can be established in a court law.

Analyze - Involves extracting, processing and interpreting the evidence. Extracted data could be unintelligible binary data after it has been processed and converted into human readable format. Interpreting the data requires an in-depth knowledge of how different pieces of evidences may fit together.

The analysis should be performed using an image of media and not the original.

Present -Involves a presentation of the various audiences such as management, attorneys, court, etc. Acceptance of evidence depends upon the manner of presentation, qualification of the presenter, and credibility of the process used to preserve and analyze the evidence.

The following were incorrect answers:

The other options presented are not a valid sequence which needs to be followed in the chain of events in regards to evidence in computer forensic.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number367

NEW QUESTION: 616

Which of the following would provide the BEST evidence for use in a forensic investigation of an employee's hard drive?

- A. A file level copy of the hard drive
- B. Bit-stream copy of the hard drive
- C. Memory dump to an external hard drive

D. Prior backups

Answer: B (LEAVE A REPLY)

Section: Protection of Information Assets

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 617

An organization has outsourced the development of a core application. However, the organization plans to bring the support and future maintenance of the application back in-house. Which of the following findings should be the IS auditor's GREATEST concern?

- A. A training plan for business users has not been developed.
- B. The cost of outsourcing is lower than in-house development.
- C. The vendor development team is located overseas.
- D. The data model is not clearly documented.

Answer: (SHOW ANSWER)

Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 618

In the development of a new financial application, the IS auditor's FIRST involvement should be in the:

- A. control design.
- B. feasibility study.
- C. application design.
- D. system test.

Answer: B (LEAVE A REPLY)

In the development of a new financial application, the IS auditor's first involvement should be in the feasibility study. A feasibility study is a preliminary analysis that evaluates the technical, operational, economic, and legal aspects of a proposed project or system. A feasibility study helps determine whether the project or system is viable, feasible, and desirable for the organization and its stakeholders.

The IS auditor's role in the feasibility study is to provide an independent and objective assessment of the project or system's risks, benefits, costs, and impacts. The IS auditor should also ensure that the feasibility study follows a structured and systematic approach, considers all relevant factors and alternatives, and complies with the organization's policies and standards.

The IS auditor should also verify that the feasibility study is documented and communicated to the appropriate decision-makers.

The IS auditor's involvement in the feasibility study is important because it can help:

- * Identify and mitigate potential risks and issues that could affect the project or system's success
- * Evaluate and justify the project or system's alignment with the organization's strategy, goals, and value proposition
- * Estimate and optimize the project or system's resources, budget, schedule, and quality
- * Assess and enhance the project or system's security, reliability, performance, and usability
- * Ensure that the project or system meets the expectations and requirements of the users and other stakeholders

The other three options are not the first involvement of the IS auditor in the development of a new financial application, although they may be part of the subsequent stages of the development process. Control design is the process of defining and implementing controls that ensure the security, integrity, availability, and efficiency of the system. Application design is the process of specifying the functional and technical features of the system. System test is the process of verifying that the system meets the specifications and requirements.

Therefore, feasibility study is the best answer.

References:

- * [Feasibility Study - ISACA]
- * [IS Auditing Guideline G13 Performing an IS Audit Engagement - ISACA]

NEW QUESTION: 619

Software is considered malware based on:

- A.** the intent of the creator.
- B.** its particular features.
- C.** its location.
- D.** its compatibility.
- E.** None of the choices.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation

Explanation:

Malware is software designed to infiltrate or damage a computer system without the owner's informed

consent. Software is considered malware based on the intent of the creator rather than any particular

features. It includes computer viruses, worms, trojan horses, spyware, adware, and other malicious and unwanted software.

NEW QUESTION: 620

Which of the following is the MOST important requirement for an IS auditor to evaluate when reviewing a transmission of personally identifiable information (PII) between two organizations?

- A. Completeness
- B. Timeliness
- C. Necessity
- D. Accuracy

Answer: C ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

NEW QUESTION: 621

The responsibility for authorizing access to a business application system belongs to the:

- A. data owner.
- B. security administrator.
- C. IT security manager.
- D. requestor's immediate supervisor.

Answer: ([SHOW ANSWER](#)**)**

Section: Protection of Information Assets

Explanation:

When a business application is developed, the best practice is to assign an information or data owner to the application. The Information owner should be responsible for authorizing access to the application itself or to back-end databases for queries. Choices B and C are not correct because the security administrator and manager normally do not have responsibility for authorizing access to business applications. The requestor's immediate supervisor may share the responsibility for approving user access to a business application system; however, the final responsibility should go to the information owner.

NEW QUESTION: 622

Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?

- A. Allocating resources
- B. Keeping current with technology advances
- C. Conducting control self-assessment
- D. Evaluating hardware needs

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

The IS department should specifically consider the manner in which resources are allocated in the short term. Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake. Conducting control self-assessments and evaluating hardware needs are not as critical as allocating resources during short-term planning for the IS department.

NEW QUESTION: 623

The MOST effective method for an IS auditor to determine which controls are functioning in an operating system is to:

- A. Compare the current configuration to the corporate standard
- B. Compare the current configuration to the default configuration
- C. Consult with the systems programmer
- D. Consult with the vendor of the system

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 624

After the merger of two organizations, which of the following is the MOST important task for an IS auditor to perform?

- A. Updating the security policy
- B. Updating the continuity plan for critical resources
- C. Investigating access rights for expiration dates
- D. Verifying that access privileges have been reviewed

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 625

An IS auditor finds that a DBA has read and write access to production data. The IS auditor should:

- A. accept the DBA access as a common practice.
- B. assess the controls relevant to the DBA function.
- C. recommend the immediate revocation of the DBA access to production data.
- D. review user access authorizations approved by the DBA.

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

It is good practice when finding a potential exposure to look for the best controls. Though granting the database administrator (DBA) access to production data might be a common practice, the IS auditor should evaluate the relevant controls. The DBA should have access based on a need-to-know and need-to-do

basis; therefore, revocation may remove the access required. The DBA, typically, may need to have access to some production data. Granting user authorizations is the responsibility of the data owner and not the DBA.

NEW QUESTION: 626

An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated data. True or false?

- A. True
- B. False

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

An integrated test facility is considered a useful audit tool because it compares processing output with independently calculated data.

NEW QUESTION: 627

Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?

- A. Parity check
- B. Echo check
- C. Block sum check
- D. Cyclic redundancy check

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

The cyclic redundancy check (CRC) can check for a block of transmitted data. The workstations generate the CRC and transmit it with the data. The receiving workstation computes a CRC and compares it to the transmitted CRC. If both of them are equal, then the block is assumed error free, in this case (such as in parity error or echo check), multiple errors can be detected. In general, CRC can detect all single-bit and bubble-bit errors. Parity check (known as vertical redundancy check) also involves adding a bit (known as the parity bit) to each character during transmission. In this case, where there is a presence of bursts of errors (i.e., impulsing noise during high transmission rates), it has a reliability of approximately 50 percent. In higher transmission rates, this limitation is significant. Echo checks detect line errors by retransmitting data to the sending device for comparison with the original transmission.

NEW QUESTION: 628

Which of the following is protocol data unit (PDU) of transport layer in TCP/IP model?

- A. Data
- B. Segment
- C. Packet
- D. Frame

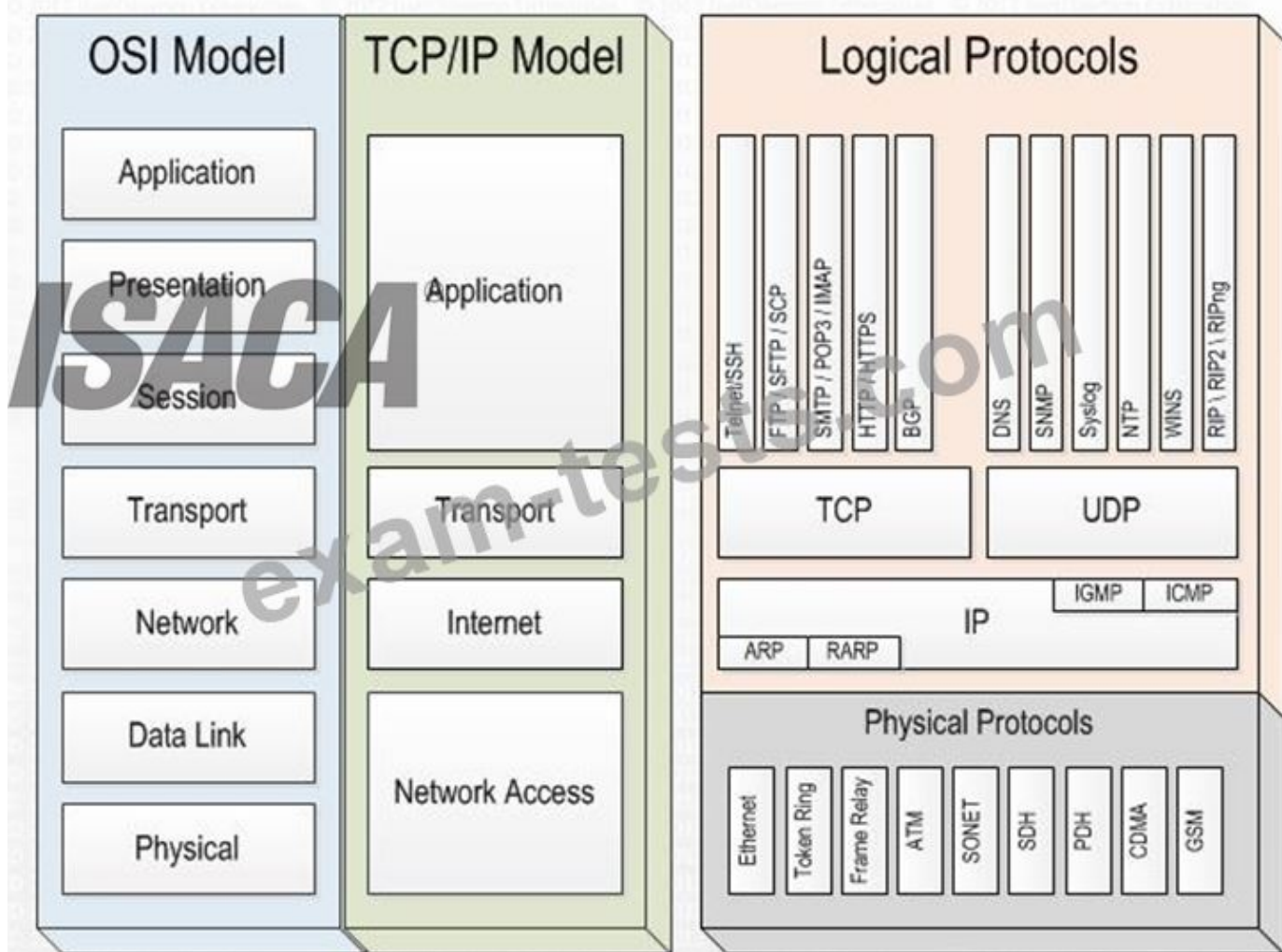
Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

For your exam you should know below information about TCP/IP model:

Network models

NETWORK MODELS



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer

Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

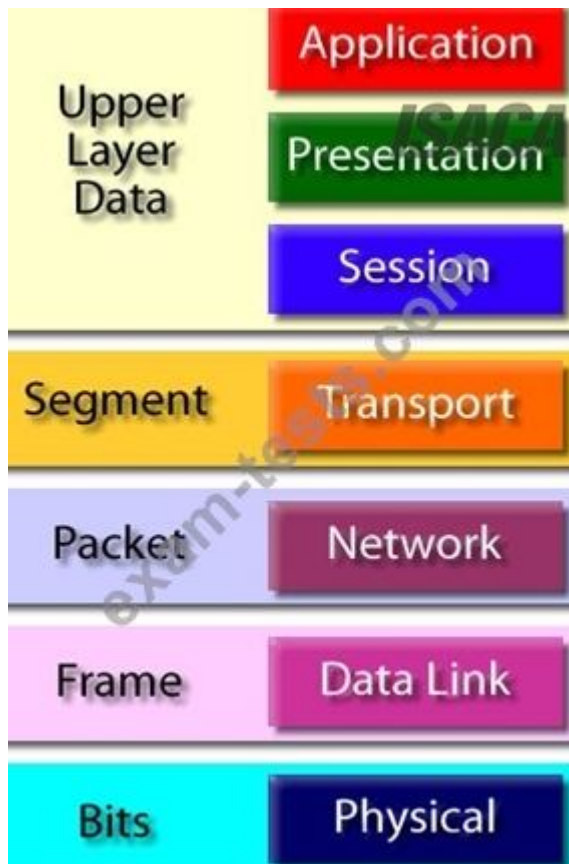
The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to

be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

Data - Application layer PDU

Packet - Network interface layer PDU

Frame/bit - LAN or WAN interface layer PDU

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

NEW QUESTION: 629

How does a switched network reduce the risk of network sniffing?

- A. Packets are not broadcasted throughout the whole subnet.
- B. Switches can detect active packet sniffing devices in their subnet.
- C. Source and destination addresses are encrypted.
- D. Network traffic is generally reduced.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 630

A large insurance company is about to replace a major financial application. Which of the following is the IS auditor's PRIMARY focus when conducting the pre-implementation review?

- A. Migration of data

- B. Procedure updates
- C. System manuals
- D. Unit testing

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 631

Which of the following is the GREATEST security threat when an organization allows remote access to a virtual private network (VPN)?

- A. Client logins are subject to replay attack.
- B. VPN traffic could be sniffed and captured.
- C. Compromised VPN clients could impact the network.
- D. Attackers could compromise the VPN gateway.

Answer: ([SHOW ANSWER](#)**)**

Section: Information System Operations, Maintenance and Support

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 632

Which of the following refers to an important procedure when evaluating database security (choose the BEST answer)?

- A. performing vulnerability assessments against the database.
- B. performing data check against the database.
- C. performing dictionary check against the database.
- D. performing capacity check against the database system.
- E. None of the choices.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Databases provide many layers and types of security, including Access control, Auditing, Authentication, Encryption and Integrity controls. An important procedure when evaluating database security is performing vulnerability assessments against the database. Database administrators or Information security administrators run vulnerability scans on databases to

discover misconfiguration of controls within the layers mentioned above along with known vulnerabilities within the database software.

NEW QUESTION: 633

Which of the following is the BEST recommendation to include in an organization's bring your own device (BYOD) policy to help prevent data leakage?

- A. Require employees to waive privacy rights related to data on BYOD devices.
- B. Require multi-factor authentication on BYOD devices,
- C. Specify employee responsibilities for reporting lost or stolen BYOD devices.
- D. Allow only registered BYOD devices to access the network.

Answer: B ([LEAVE A REPLY](#))

The best recommendation to include in an organization's bring your own device (BYOD) policy to help prevent data leakage is to require multi-factor authentication on BYOD devices. BYOD is a practice that allows employees to use their own personal devices, such as smartphones, tablets, or laptops, to access the organization's network, data, and systems. Data leakage is a risk that involves the unauthorized or accidental disclosure or transfer of sensitive or confidential data from the organization to external parties or devices.

Multi-factor authentication is a security measure that requires users to provide two or more pieces of evidence to verify their identity and access rights, such as passwords, tokens, biometrics, or codes. Multi-factor authentication can help prevent data leakage by reducing the likelihood of unauthorized access to the organization's data and systems through BYOD devices, especially if they are lost, stolen, or compromised. The other options are not as effective as requiring multi-factor authentication on BYOD devices, because they either do not prevent data leakage directly, or they are reactive rather than proactive measures. References: CISA Review Manual (Digital Version)¹, Chapter 5, Section 5.2.3

NEW QUESTION: 634

Which of the following is the BEST reason to certify an organization to an international security standard?

- A. The certification covers enterprise security end-to-end.
- B. The certification reduces information security risk.
- C. The certification ensures that optimal controls are in place.
- D. The certification delivers value to stakeholders.

Answer: ([SHOW ANSWER](#)**)**

Section: Governance and Management of IT

Explanation/Reference:

NEW QUESTION: 635

Which of the following would provide the BEST evidence that a cloud provider's change management process is effective?

- A. Minutes from regular change management meetings with the vendor

- B. Written assurances from the vendor's CEO and CIO
- C. The results of a third-party review provided by the vendor
- D. A copy of change management policies provided by the vendor

Answer: C (LEAVE A REPLY)

The results of a third-party review provided by the vendor would provide the best evidence that a cloud provider's change management process is effective, because it would be an independent and objective assessment of the vendor's compliance with best practices and standards for managing changes in the cloud environment. A third-party review would also include testing of the vendor's change management controls and procedures, and provide recommendations for improvement if needed.

Minutes from regular change management meetings with the vendor would not provide sufficient evidence, because they would only reflect the vendor's self-reported information and may not capture all the changes that occurred or their impact on the cloud services. Written assurances from the vendor's CEO and CIO would also not provide sufficient evidence, because they would be based on the vendor's own opinion and may not be verified by external sources. A copy of change management policies provided by the vendor would not provide sufficient evidence, because it would only show the vendor's intended approach to change management, but not how it is implemented or monitored in practice.

References:

ISACA Cloud Computing Audit Program, Section 4.5: Change Management

Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, Section

4.3: Change Management

NEW QUESTION: 636

What is the PRIMARY benefit of an audit approach which requires reported findings to be issued together with related action plans, owners, and target dates?

- A. it facilitates easier audit follow-up
- B. it enforces action plan consensus between auditors and auditees
- C. it establishes accountability for the action plans
- D. it helps to ensure factual accuracy of findings

Answer: C (LEAVE A REPLY)

The primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates is that it establishes accountability for the action plans. Accountability means that the individuals or groups who are responsible for implementing the action plans are clearly identified and held liable for their completion within the specified time frame. Accountability also implies that the action plans are monitored and evaluated to ensure that they are effective and efficient in addressing the audit findings and mitigating the associated risks¹. Accountability helps to ensure that the audit recommendations are taken seriously and implemented properly, and that the audit value is realized by the organization². The other options are less relevant or incorrect because:

* A. It facilitates easier audit follow-up is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of a secondary or indirect benefit. Audit follow-up is the process of verifying whether the action plans have been implemented and whether they have resolved the audit findings³. While having clear action plans, owners, and target dates may facilitate easier audit follow-up by providing a basis for tracking and reporting the progress and status of the action plans, it does not necessarily guarantee that the action plans will be implemented or effective.

* B. It enforces action plan consensus between auditors and auditees is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of a prerequisite or condition for such an approach. Action plan consensus means that the auditors and auditees agree on the audit findings and recommendations, and on the action plans to address them⁴. While having action plan consensus may enhance the credibility and acceptance of the audit approach, it does not necessarily ensure that the action plans will be implemented or effective.

* D. It helps to ensure factual accuracy of findings is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of an outcome or result of such an approach. Factual accuracy of findings means that the audit findings are based on sufficient, reliable, relevant, and useful evidence⁵. While having factual accuracy of findings may increase the confidence and trust in the audit approach, it does not necessarily ensure that the action plans will be implemented or effective.

References: Accountability - ISACA, Audit Value - ISACA, Audit Follow-up - ISACA, Action Plan Consensus - ISACA, Factual Accuracy of Findings - ISACA

NEW QUESTION: 637

Which of the following is the BEST way to determine whether a test of a disaster recovery plan (DRP) was successful?

- A. Analyze whether predetermined test objectives were met.
- B. Perform testing at the backup data center.
- C. Evaluate participation by key personnel.
- D. Test offsite backup files.

Answer: (SHOW ANSWER)

The best way to determine whether a test of a disaster recovery plan (DRP) was successful is to analyze whether predetermined test objectives were met. Test objectives are specific, measurable, achievable, relevant, and time-bound (SMART) goals that define what the test aims to accomplish and how it will be evaluated.

Test objectives should be aligned with the DRP objectives and scope, and should cover aspects such as recovery time objectives (RTOs), recovery point objectives (RPOs), critical business functions, roles and responsibilities, communication channels, backup systems, and contingency procedures. By comparing the actual test results with the expected test objectives, the IS auditor can measure the effectiveness and efficiency of the DRP and identify any gaps or weaknesses that need to be addressed.

NEW QUESTION: 638

Which of the following threats is prevented by using token-based authentication?

- A. Password sniffing attack on the network
- B. Session eavesdropping attack on the network
- C. Man-in-the-middle attack on the client
- D. Denial of service attack over the network

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

NEW QUESTION: 639

The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

- A. financial results.
- B. customer satisfaction.
- C. internal process efficiency.
- D. innovation capacity.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Financial results have traditionally been the sole overall performance metric. The IT balanced scorecard (BSC) is an IT business governance tool aimed at monitoring IT performance evaluation indicators other than financial results. The IT BSC considers other key success factors, such as customer satisfaction, innovation capacity and processing.

NEW QUESTION: 640

The information security policy that states 'each individual must have their badge read at every controlled door' addresses which of the following attack methods?

- A. Piggybacking
- B. Shoulder surfing
- C. Dumpster diving
- D. Impersonation

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger, if every employee must have their badge read at every controlled door no unauthorized person could enter the sensitive area. Looking over the shoulder of a user to obtain sensitive information could be done by an unauthorized person who has gained access to areas

using piggybacking, but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy.

Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method.

Impersonation refers to a social engineer acting as an employee, trying to retrieve the desired information.

Some forms of social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

NEW QUESTION: 641

An organization has installed blade server technology in its data server. To determine whether higher cooling demands are maintained, which of the following should the IS auditor review?

- A. Duct maintenance
- B. Ventilation systems
- C. Uninterruptable power supply (UPS) systems
- D. Air conditioning capacity

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 642

When an intrusion into an organizations network is detected, which of the foflomng should be performed FIRST?

- A. Identify nodes that have been compromised
- B. Develop a response to the incident
- C. Protect information in the compromised systems
- D. Block all compromised network nodes

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 643

Network Data Management Protocol (NDMP) technology should be used for backup if:

- A. a network attached storage (NAS) appliance is required.
- B. the use of TCP/I P must be avoided.
- C. file permissions that can not be handled by legacy backup systems must be backed up.
- D. backup consistency over several related data volumes must be ensured.

Answer: (SHOW ANSWER)

Section: Protection of Information Assets

Explanation:

NDMP defines three kinds of services: a data service that interfaces with the primary storage to be backed up or restored, a tape service that interfaces with the secondary storage (primarily a tape device), and a translator service performing translations including multiplexing multiple data streams into one data stream and vice versa. NDMP services interact with each other. The result

of this interaction is the establishment of an NDMP control session if the session is being used to achieve control for the backup or restore operation. It would result in an NDMP data session if the session is being used to transfer actual file system or volume data (including metadata). Control sessions are always TCP/IP-based, but data streams can be TCP/IP-or SAN-based. NDMP is more or less NAS-centric and defines a way to back up and restore data from a device, such as a NAS appliance, on which it is difficult to install a backup software agent, in the absence of NDMP, this data must be backed up as a shared drive on the LAN, which is accessed via network file protocols, such as Common Internet File System (CIFS) or Network File System (NFS), degrading backup performance. NDMP works on a block level for transferring payload data (file content) but metadata and traditional file system information needs to be handled by legacy backup systems that initiate NDMP data movement. NDMP does not know about nor takes care of consistency issues regarding related volumes (e.g., a volume to store database files, a volume to store application server data and a volume to store web server data). NDMP can be used to do backups in such an environment (e.g., SAP) but the logic required either must be put into a dedicated piece of software or must be scripted into the legacy backup software.

NEW QUESTION: 644

An IS auditor is examining a front-end subledger and a main ledger. Which of the following would be the GREATEST concern if there are flaws in the mapping of accounts between the two systems?

- A. Double-posting of a single journal entry
- B. Inability to support new business transactions
- C. Unauthorized alteration of account attributes
- D. Inaccuracy of financial reporting

Answer: D ([LEAVE A REPLY](#))

The greatest concern for an IS auditor if there are flaws in the mapping of accounts between a front-end subledger and a main ledger is the inaccuracy of financial reporting. A subledger is a detailed record of transactions for a specific account, such as accounts receivable, accounts payable, inventory, or fixed assets.

A main ledger is a summary record of all transactions for all accounts in an accounting system. The mapping of accounts between a subledger and a main ledger is the process of linking or reconciling the transactions in the subledger with the corresponding entries in the main ledger. If there are flaws in the mapping of accounts, such as missing, duplicated, or incorrect transactions, the main ledger may not reflect the true financial position and performance of the organization. This may lead to inaccurate financial reporting, which may affect decision making, compliance, auditing, taxation, and stakeholder confidence.

Double-posting of a single journal entry, inability to support new business transactions, and unauthorized alteration of account attributes are not the greatest concerns for an IS auditor if there are flaws in the mapping of accounts between a front-end subledger and a main ledger. These are possible consequences or causes of flaws in the mapping of accounts, but they do not have as significant an impact as inaccuracy of financial reporting. Double-posting of a single

journal entry may result in errors or discrepancies in the main ledger balances. Inability to support new business transactions may indicate limitations or inefficiencies in the accounting system design or configuration. Unauthorized alteration of account attributes may suggest weaknesses or breaches in access control or segregation of duties.

NEW QUESTION: 645

Which of the following is MOST important to review when evaluating the performance of a critical web application?

- A. Business-defined application response times
- B. Strategy for application performance monitoring in the cloud
- C. Roles and responsibilities for reporting
- D. Feedback from customer satisfaction surveys

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 646

Audit observations should be FIRST communicated with the auditee:

- A. when drafting the report.
- B. during fieldwork.
- C. at the end of fieldwork.
- D. within the audit report

Answer: B ([LEAVE A REPLY](#))

Explanation

Audit observations are the findings and recommendations that result from an audit engagement. Audit observations should be first communicated with the auditee during fieldwork, which is the stage of the audit process where the auditor collects and analyzes evidence to evaluate the audit objectives¹. Communicating audit observations during fieldwork has several benefits, such as²: It allows the auditor to verify the accuracy and completeness of the observations, and to obtain additional information or clarification from the auditee if needed.

It enables the auditor to discuss the root causes, impacts, and risks of the observations, and to solicit the auditee's input on possible corrective actions and implementation timelines.

It helps to build rapport and trust between the auditor and the auditee, and to avoid surprises or disagreements at the end of the audit.

It facilitates timely resolution of audit observations, and reduces the risk of audit delays or disputes.

Therefore, option B is the correct answer.

Option A is not correct because communicating audit observations when drafting the report is too late, as it may lead to misunderstandings, conflicts, or revisions that could have been avoided if the observations were communicated earlier. Option C is not correct because communicating audit observations at the end of fieldwork is also not ideal, as it may not leave enough time for the auditor and the auditee to discuss and agree on the observations and recommendations. Option

D is not correct because communicating audit observations within the audit report is the final step of the audit process, not the first.

References:

Audit Process Overview¹

Communicating Internal Audit Findings: Best Practices for Success²

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 647

Management has decided to include a compliance manager in the approval process for a new business

that may require changes to the IT infrastructure. Which of the following is the GREATEST benefit of this approach?

- A. Security breach incidents can be identified in early stages.
- B. Regulatory risk exposures can be identified before they materialize.
- C. Fewer reviews are needed when updating the IT compliance process.
- D. Process accountabilities to external stakeholders are improved.

Answer: ([SHOW ANSWER](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 648

Which of the following insurance types provide for a loss arising from fraudulent acts by employees?

- A. Business interruption
- B. Fidelity coverage
- C. Errors and omissions
- D. Extra expense

Answer: B ([LEAVE A REPLY](#))

Fidelity insurance covers the loss arising from dishonest or fraudulent acts by employees.

Business interruption insurance covers the loss of profit due to the disruption in the operations of an organization. Errors and omissions insurance provides legal liability protection in the event that the professional practitioner commits an act that results in financial loss to a client. Extra expense

insurance is designed to cover the extra costs of continuing operations following a disaster/disruption within an organization.

NEW QUESTION: 649

How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?

- A. Modems convert analog transmissions to digital, and digital transmission to analog.
- B. Modems encapsulate analog transmissions within digital, and digital transmissions within analog.
- C. Modems convert digital transmissions to analog, and analog transmissions to digital.
- D. Modems encapsulate digital transmissions within analog, and analog transmissions within digital.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Modems (modulation/demodulation) convert analog transmissions to digital, and digital transmissions to analog, and are required for analog transmissions to enter a digital network.

NEW QUESTION: 650

Which of the following kinds of function are particularly vulnerable to format string attacks?

- A. C functions that perform output formatting
- B. C functions that perform integer computation
- C. C functions that perform real number subtraction
- D. VB functions that perform integer conversion
- E. SQL functions that perform string conversion
- F. SQL functions that perform text conversion

Answer: A ([LEAVE A REPLY](#))

Format string attacks are a new class of vulnerabilities recently discovered. It can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as printf (). A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write arbitrary data to arbitrary locations using the %n format token.

NEW QUESTION: 651

There are many types of audit logs analysis tools available in the market. Which of the following audit logs analysis tools will look for anomalies in user or system behavior?

- A. Attack Signature detection tool
- B. Variance detection tool
- C. Audit Reduction tool
- D. Heuristic detection tool

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Trend/Variance Detection tool are used to look for anomalies in user or system behavior. For example, if a user typically logs in at 9:00 am, but one day suddenly access the system at 4:30 am, this may indicate a security problem that may need to be investigated.

Other types of audit trail analysis tools should also be known for your CISA exam The following were incorrect answers:

Audit Reduction tool - They are preprocessor designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tool can remove many audit records known to have little security significance.

Attack-signature detection tool - They look for an attack signature, which is a specific sequence of events indicative of an unauthorized access attempt. A simple example would be repeated failed logon attempts.

Heuristic detection tool - Heuristic analysis is an expert based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods. MultiCriteria analysis (MCA) is one of the means of weighing. This method differs with statistical analysis, which bases itself on the available data/statistics.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 336

and

http://en.wikipedia.org/wiki/Heuristic_analysis

NEW QUESTION: 652

An organization has a number of branches across a wide geographical area. To ensure that all aspects of the disaster recovery plan are evaluated in a cost effective manner, an IS auditor should recommend the use of a:

- A.** data recovery test.
- B.** full operational test.
- C.** posttest.
- D.** preparedness test.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

A preparedness test should be performed by each local office/area to test the adequacy of the preparedness of local operations in the event of a disaster. This test should be performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence of the plan's adequacy. A data recovery test is a partial test and will not ensure that all aspects are evaluated. A full operational test is not the most cost effective test in light of the geographical dispersion of the branches, and a posttest is a phase of the test execution process.

NEW QUESTION: 653

Which of the following presents the GREATEST risk of data leakage in the cloud environment?

- A. Lack of data retention policy
- B. Multi-tenancy within the same database
- C. Lack of role-based access
- D. Expiration of security certificate

Answer: B ([LEAVE A REPLY](#))

Multi-tenancy within the same database (B) presents the greatest risk of data leakage in the cloud environment, because it means that multiple customers share the same physical database and resources. This can lead to data isolation and security issues, such as unauthorized access, cross-tenant attacks, or data leakage due to misconfiguration or human error. To prevent data leakage in a multi-tenant database, cloud providers need to implement strict access control policies, encryption, isolation mechanisms, and auditing tools.

Lack of data retention policy (A) is not the greatest risk of data leakage in the cloud environment, because it mainly affects the availability and compliance of data, not its confidentiality or integrity. Data retention policy defines how long data should be stored and when it should be deleted or archived. Without a data retention policy, cloud customers may face legal or regulatory issues, storage costs, or performance degradation.

Lack of role-based access is not the greatest risk of data leakage in the cloud environment, because it can be mitigated by implementing proper authentication and authorization mechanisms. Role-based access control (RBAC) is a security model that assigns permissions and privileges to users based on their roles and responsibilities. Without RBAC, cloud customers may face unauthorized access, privilege escalation, or data misuse.

Expiration of security certificate (D) is not the greatest risk of data leakage in the cloud environment, because it can be easily detected and renewed. A security certificate is a digital document that verifies the identity and authenticity of a website or service. It also enables secure communication using encryption. If a security certificate expires, it may cause trust issues, warning messages, or connection errors, but not necessarily data leakage.

References:

* 7 Ways to Prevent Data Leaks in the Cloud | OTAVA

* An analysis of data leakage and prevention techniques in cloud environment

NEW QUESTION: 654

Which of the following is MOST important with regard to an application development acceptance test?

- A. All data files are tested for valid information before conversion.
- B. The quality assurance (QA) team is in charge of the testing process.
- C. The programming team is involved in the testing process.
- D. User management approves the test design before the test is started.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 655

Which of the following should be of GREATEST concern to an IS auditor reviewing an organization's initiative to adopt an enterprise governance framework?

- A. The organization's security department has not been involved with the initiative.
- B. The organization has not provided employees with formal training on the framework.
- C. The organization has not identified the business drivers for adopting the framework.
- D. The organization has tried to adopt the entire framework at once.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 656

The PRIMARY benefit to using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry-pipe system:

- A. is more effective at suppressing flames.
- B. allows more time to abort release of the suppressant.
- C. has a decreased risk of leakage.
- D. disperses dry chemical suppressants exclusively.

Answer: C ([LEAVE A REPLY](#))

The primary benefit of using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry-pipe system has a decreased risk of leakage, as the pipes are filled with pressurized air or nitrogen instead of water until the system is activated. A wet-pipe system has a higher risk of leakage, corrosion, and freezing.

A dry-pipe system is not more effective at suppressing flames, as it uses the same water-based suppressant as a wet-pipe system. A dry-pipe system does not allow more time to abort release of the suppressant, as it has a delay of only a few seconds before the water is released. A dry-pipe system does not disperse dry chemical suppressants exclusively, as it uses water as the primary suppressant. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.2.3

NEW QUESTION: 657

An IS auditor is planning an audit of an organization's accounts payable processes. Which of the following controls is MOST important to assess in the audit?

- A. Segregation of duties between issuing purchase orders and making payments.
- B. Segregation of duties between receiving invoices and setting authorization limits
- C. Management review and approval of authorization tiers
- D. Management review and approval of purchase orders

Answer: A ([LEAVE A REPLY](#))

The most important control to assess in an audit of an organization's accounts payable processes is segregation of duties between issuing purchase orders and making payments. Segregation of duties is a principle that requires different individuals or departments to perform different tasks or functions within a process, in order to prevent fraud, errors, or conflicts of interest. In the accounts payable process, segregation of duties between issuing purchase orders and making payments ensures that no one person can initiate and complete a transaction without proper authorization

and verification. This reduces the risk of duplicate payments, overpayments, unauthorized payments, or payments to fictitious vendors.

References:

- * Accounts payable controls
- * Accounts Payable Internal Controls: A Simple Checklist

NEW QUESTION: 658

Which of the following can BEST reduce the impact of a long-term power failure?

- A. Power conditioning unit
- B. Redundant power source
- C. Battery bank
- D. Emergency power-off switches

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 659

Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

- A. System owners
- B. System users
- C. System designers
- D. System builders

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

System owners are the information systems (project) sponsors or chief advocates. They normally are

responsible for initiating and funding projects to develop, operate and maintain information systems.

System users are the individuals who use or are affected by the information system.

Their requirements are crucial in the testing stage of a project. System designers translate business

requirements and constraints into technical solutions. System builders construct the system based on the

specifications from the systems designers. In most cases, the designers and builders are one and the same.

NEW QUESTION: 660

When reviewing a project to replace multiple manual data entry systems with an artificial intelligence (AI) system, the IS auditor should be MOST concerned with the impact AI will have on

- A. employee retention
- B. enterprise architecture (EA)
- C. future task updates
- D. task capacity output

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 661

Data edits are implemented before processing and are considered which of the following?
Choose the BEST answer.

- A. Deterrent integrity controls
- B. Detective integrity controls
- C. Corrective integrity controls
- D. Preventative integrity controls

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Data edits are implemented before processing and are considered preventive integrity controls.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com
CISA exam **questions have been updated** and **answers have been corrected** get the
newest BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As

Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 662

Which of the following would be the MOST useful metric for management to consider when reviewing a project portfolio?

- A. Cost of projects divided by total IT cost
- B. Expected return divided by total project cost
- C. Net present value (NPV) of the portfolio
- D. Total cost of each project

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 663

What influences decisions regarding criticality of assets?

- A. The business criticality of the data to be protected
- B. Internal corporate politics
- C. The business criticality of the data to be protected, and the scope of the impact upon the organization

as a whole

D. The business impact analysis

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Criticality of assets is often influenced by the business criticality of the data to be protected and by the

scope of the impact upon the organization as a whole. For example, the loss of a network backbone

creates a much greater impact on the organization as a whole than the loss of data on a typical user's

workstation.

NEW QUESTION: 664

Which of the following should be the FIRST step when developing a data loss prevention (DLP) solution for a large organization?

A. Create the DLP policies and templates.

B. Conduct a threat analysis against sensitive data usage.

C. Conduct a data inventory and classification exercise.

D. Identify approved data workflows across the enterprise.

Answer: C ([LEAVE A REPLY](#))

Before implementing a DLP solution, it is crucial to understand the organization's data landscape. Conducting a data inventory and classification exercise helps identify the types of data that need to be protected and their sensitivity levels. This step involves identifying the locations, formats, and repositories where data resides, as well as categorizing the data based on its sensitivity and regulatory requirements. This exercise forms the foundation for developing effective DLP policies and controls.

NEW QUESTION: 665

An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

A. Obtain error codes indicating failed data feeds.

B. Appoint data quality champions across the organization.

C. Purchase data cleansing tools from a reputable vendor.

D. Implement business rules to reject invalid data.

Answer: D ([LEAVE A REPLY](#))

The best way to prevent accepting bad data from a third-party service provider is to implement business rules to reject invalid data. Business rules are logical expressions that define the business requirements and constraints for specific data elements. They can be used to validate, transform, or filter incoming data from external sources, ensuring that only high-quality data is

accepted into the enterprise data warehouse. Business rules can also help to identify and resolve data quality issues, such as missing values, duplicates, outliers, or inconsistencies.

NEW QUESTION: 666

Which of the following testing methods is MOST appropriate for assessing whether system integrity has been maintained after changes have been made?

- A. Regression testing
- B. Unit testing
- C. Integration testing
- D. Acceptance testing

Answer: A ([LEAVE A REPLY](#))

Regression testing is the most appropriate testing method for assessing whether system integrity has been maintained after changes have been made. Regression testing is a type of software testing that ensures that previously developed and tested software still performs as expected after a change¹ Regression testing helps to detect any defects or errors that may have been introduced or uncovered due to the change² Regression testing can be performed at different levels of testing, such as unit, integration, system, and acceptance³ Unit testing is a type of software testing that verifies the functionality of individual components or units of code. Unit testing is usually performed by developers before integrating the code with other components. Unit testing helps to identify and fix errors at an early stage of development, but it does not ensure that the system as a whole works as expected after a change.

Integration testing is a type of software testing that verifies the functionality, performance, and reliability of the interactions between different components or units of code. Integration testing is usually performed after unit testing and before system testing. Integration testing helps to identify and fix errors that may occur when different components are integrated, but it does not ensure that the system as a whole works as expected after a change.

Acceptance testing is a type of software testing that verifies whether the system meets the user requirements and expectations. Acceptance testing is usually performed by end-users or customers after system testing and before deploying the system to production. Acceptance testing helps to ensure that the system delivers the desired value and quality to the users, but it does not ensure that the system as a whole works as expected after a change.

References: 1: What is Regression Testing? Test Cases (Example) - Guru99 2: What is Regression Testing? Definition, Tools, Examples - Katalon 3: Regression testing - Wikipedia : What is Unit Testing?

Definition, Types, Tools & Examples - Guru99 : What is Integration Testing? Definition, Types, Tools & Examples - Guru99 : What is Acceptance Testing? Definition, Types, Tools & Examples - Guru99

NEW QUESTION: 667

Which of the following is the MOST effective control when granting temporary access to vendors?

- A. Vendor access corresponds to the service level agreement (SLA).

- B. User accounts are created with expiration dates and are based on services provided.
- C. Administrator access is provided for a limited period.
- D. User IDs are deleted when the work is completed.

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

The most effective control is to ensure that the granting of temporary access is based on services to be provided and that there is an expiration date (hopefully automated) associated with each ID. The SLA may have a provision for providing access, but this is not a control; it would merely define the need for access.

Vendors require access for a limited period during the time of service. However, it is important to ensure that the access during this period is monitored. Deleting these user, I Dafter the work is completed is necessary, but if not automated, the deletion could be overlooked.

NEW QUESTION: 668

Which of the following should an IS auditor consider FIRST when evaluating firewall rules?

- A. The organization's security policy
- B. The number of remote nodes
- C. The firewalls' default settings
- D. The physical location of the firewalls

Answer: (SHOW ANSWER)

Explanation

This should be the first thing that an IS auditor considers when evaluating firewall rules, because it defines the objectives, standards, and guidelines for securing the organization's network and information assets. The firewall rules should be aligned with the organization's security policy, and reflect the level of risk and protection required for each type of network traffic, system, or data. The IS auditor should compare the firewall rules with the security policy, and identify any discrepancies, gaps, or conflicts that could compromise the security or performance of the network.

The other options are not as important as the organization's security policy when evaluating firewall rules:

The number of remote nodes. This is a factor that may affect the complexity and scalability of the firewall rules, but it is not a primary consideration for the IS auditor. Remote nodes are devices or systems that connect to the network from outside locations, such as teleworkers, mobile users, or branch offices. The IS auditor should ensure that the firewall rules provide adequate security and access control for remote nodes, but this depends on the organization's security policy and business needs.

The firewalls' default settings. These are the predefined configurations that come with the firewall devices or software, and that determine how they handle network traffic by default. The IS auditor should review the firewalls' default settings, and verify that they are appropriate and secure for the organization's network environment. However, the firewalls' default settings may not match

the organization's security policy or specific requirements, and may need to be customized or overridden by firewall rules.

The physical location of the firewalls. This is a factor that may affect the placement and design of the firewall rules, but it is not a critical consideration for the IS auditor. The physical location of the firewalls refers to where they are installed or deployed in relation to the network topology, such as at the network perimeter, between network segments, or on individual hosts. The IS auditor should ensure that the firewall rules are consistent and coordinated across different locations, but this depends on the organization's security policy and network architecture.

NEW QUESTION: 669

Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits vulnerability in a protocol?

- A. Install the vendor's security fix for the vulnerability.
- B. Block the protocol traffic in the perimeter firewall.
- C. Block the protocol traffic between internal network segments.
- D. Stop the service until an appropriate security fix is installed.

Answer: D ([LEAVE A REPLY](#))

Stopping the service and installing the security fix is the safest way to prevent the worm from spreading, if the service is not stopped, installing the fix is not the most effective method because the worm continues spreading until the fix becomes effective. Blocking the protocol on the perimeter does not stop the worm from spreading to the internal network(s). Blocking the protocol helps to slow down the spreading but also prohibits any software that utilizes it from working between segments.

NEW QUESTION: 670

Which of the following statement INCORRECTLY describes device and where they sit within the TCP/IP model?

- A. Layer 4 switch work at Network interface layer in TCP/IP model
- B. Router works at Network interface layer in TCP/IP model
- C. Layer 3 switch work at Network interface layer in TCP/IP model
- D. Hub works at LAN or WAN interface layer of a TCP/IP model

Answer: A ([LEAVE A REPLY](#))

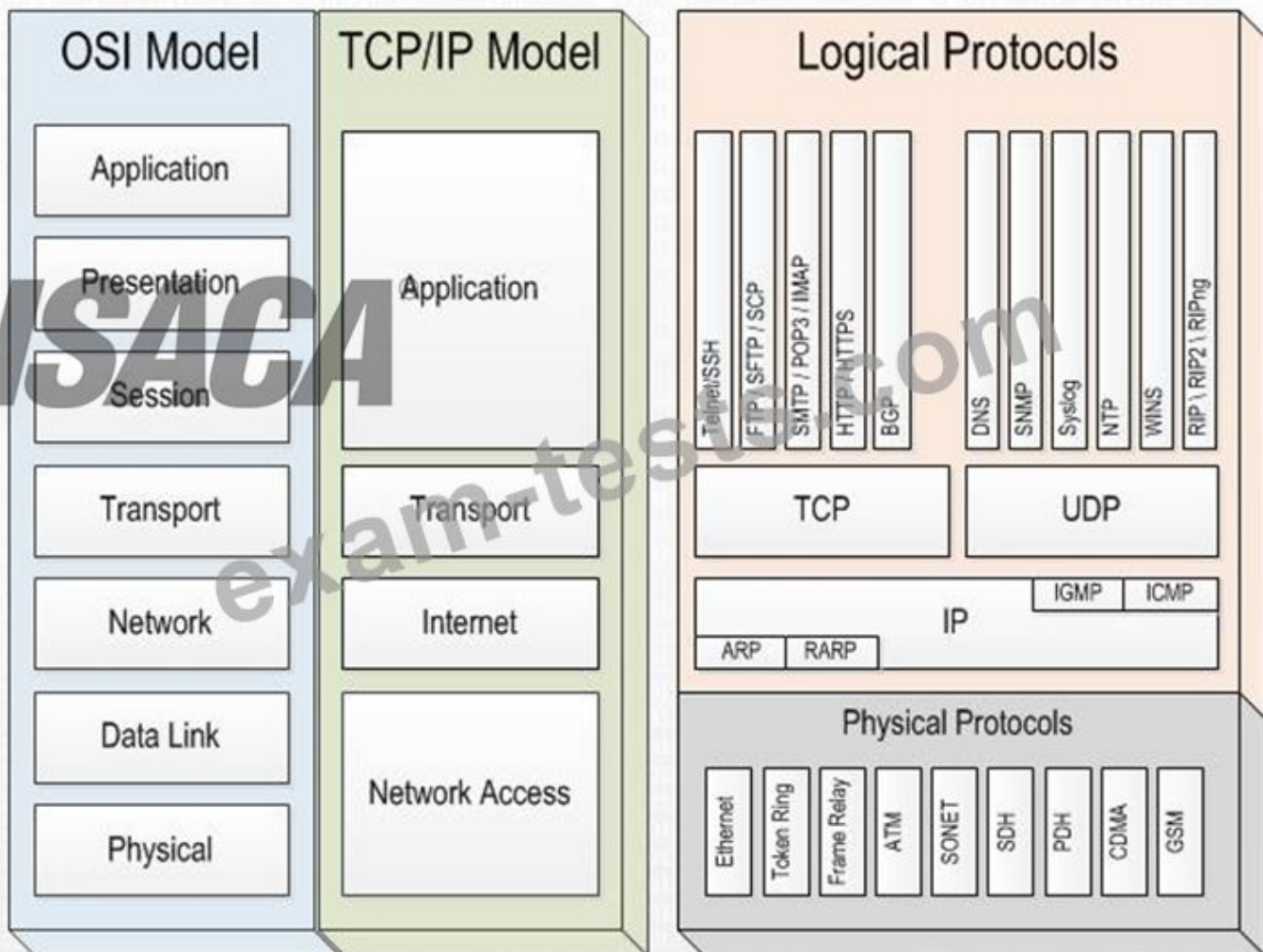
Explanation/Reference:

The keyword within the question is INCORRECTLY. You need to find out incorrect statement.

For your exam you should know below information about TCP/IP model:

Network models

NETWORK MODELS



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :



Protocol Data Unit - PDU

The following answers are incorrect:

The other options correctly describes about network device functioning based on TCP/IP model

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

NEW QUESTION: 671

An IS auditor is mapping controls to risk for an accounts payable system. What is the BEST control to detect errors in the system?

- A. Alignment of the process to business objectives
- B. Quality control review of new payments
- C. Management approval of payments
- D. Input validation

Answer: D ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

NEW QUESTION: 672

The MOST effective control to detect fraud inside an organization's network, is to:

- A. implement an intrusion detection system (IDS)
- B. apply two-factor authentication
- C. review access logs
- D. segregate duties

Answer: C ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 673

What should an IS auditor review FIRST when assessing the results of a recent penetration test to identify potential vulnerabilities?

- A. Skill level of the network support staff
- B. Parameters of the test
- C. Number of critical issues found
- D. Incident response process

Answer: ([SHOW ANSWER](#))

Section: The process of Auditing Information System

NEW QUESTION: 674

When auditing the alignment of IT to the business strategy, it is MOST important (or the IS auditor to:

- A. compare the organization's strategic plan against industry best practice.
- B. interview senior managers (or their opinion of the IT function).
- C. evaluate deliverables of new IT initiatives against planned business services.
- D. ensure an IT steering committee is appointed to monitor new IT projects.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 675

Which of the following is a good time frame for making changes to passwords?

- A. every 180 to 365 days
- B. every 30 to 45 days
- C. every 10 to 20 days
- D. every 90 to 120 days
- E. None of the choices.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password. A good password has mixed-case alphabetic characters, numbers, and symbols. Do use a password that is at least eight or more characters. You may want to run a "password cracker" program periodically, and require users to immediately change any easily cracked passwords. In any case ask them to change their passwords every 90 to 120 days.

NEW QUESTION: 676

Which of the following BEST enables an organization to manage unexpected or on-request jobs?

- A. Service level agreements (SLAs)
- B. Job scheduling by the service desk
- C. Job scheduling software
- D. Console logs

Answer: C ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 677

In a data center audit, an IS auditor finds that the humidity level is very low. The IS auditor would be MOST concerned because of an expected increase in:

- A. backup tape failures.
- B. risk of fire.
- C. employee discomfort.
- D. static electricity problems.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 678

Controls related to authorized modifications to production programs are BEST tested by:

- A. tracing modifications from the original request for change forward to the executable program.
- B. tracing modifications from the executable program back to the original request for change.
- C. testing only the authorizations to implement the new program.
- D. reviewing only the actual lines of source code changed in the program.

Answer: A ([LEAVE A REPLY](#))

Controls related to authorized modifications to production programs are best tested by tracing modifications from the original request for change forward to the executable program, as this ensures that the change management process was followed and that the modifications were approved, documented, tested, and implemented correctly. Tracing modifications from the executable program back to the original request for change may not reveal any unauthorized or undocumented changes that occurred during the process. Testing only the authorizations to implement the new program or reviewing only the actual lines of source code changed in the program are not sufficient to test the controls related to authorized modifications, as they do not cover the entire change management process. References: CISA Review Manual (Digital

Version), Chapter 4: Information Systems Operations, Maintenance and Service Management, Section 4.2: Change Management

NEW QUESTION: 679

How does the digital envelop work? What are the correct steps to follow?

- A.** You encrypt the data using a session key and then encrypt session key using private key of a sender
- B.** You encrypt the data using the session key and then you encrypt the session key using sender's public key
- C.** You encrypt the data using the session key and then you encrypt the session key using the receiver's public key
- D.** You encrypt the data using the session key and then you encrypt the session key using the receiver's private key

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation/Reference:

The process of encrypting bulk data using symmetric key cryptography and then encrypting the session key

using public key algorithm is referred as a digital envelope.

A Digital Envelope is used to send encrypted information using symmetric crypto cipher and then key

session along with it. It is secure method to send electronic document without compromising the data

integrity, authentication and non-repudiation, which were obtained with the use of symmetric keys.

A Digital envelope mechanism works as follows:

The symmetric key used to encrypt the message can be referred to as session key. The bulk of the

message would take advantage of the high speed provided by Symmetric Cipher.

The session key must then be communicated to the receiver in a secure way to allow the receiver to

decrypt the message.

If the session key is sent to receiver in the plain text, it could be captured in clear text over the network and

anyone could access the session key which would lead to confidentiality being compromised.

Therefore it is critical to encrypt the session key with the receiver public key before sending it to the

receiver. The receiver's will use their matching private key to decrypt the session key which then allow them to decrypt the message using the session key. The encrypted message and the encrypted session key are sent to the receiver who, in turn decrypts the session key with the receiver's private key. The session key is then applied to the message cipher text to get the plain text.

The following were incorrect answers:

You encrypt the data using a session key and then encrypt session key using private key of a sender - If

the session key is encrypted using sender's private key, it can be decrypted only using sender's public key.

The sender's public key is known to everyone so anyone can decrypt session key and message. You encrypt the data using the session key and then you encrypt the session key using sender's public key

- If the session key is encrypted by using sender's public key then only sender can decrypt the session key

using his/her own private key and receiver will not be able to decrypt the same.

You encrypt the data using the session key and then you encrypt the session key using the receiver's

private key - Sender should not have access to receiver's private key. This is not a valid option.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 350 and 351

NEW QUESTION: 680

Which of the following should be of MOST concern to an IS auditor reviewing the information systems acquisition, development, and implementation process?

- A.** Data owners are not trained on the use of data conversion tools.
- B.** A post-implementation lessons-learned exercise was not conducted.
- C.** There is no system documentation available for review.
- D.** System deployment is routinely performed by contractors.

Answer: B ([LEAVE A REPLY](#))

It is important for an IS auditor to review the information systems acquisition, development, and implementation process to ensure that it has been performed properly and that any errors or issues have been identified and addressed. A lessons-learned exercise is an important part of this process, as it allows for the identification and rectification of any issues that may have been missed during the initial stages of the process. Without this exercise, any potential issues may go unnoticed and lead to further problems down the line.

NEW QUESTION: 681

Which of the following should be the MOST important consideration in IT portfolio management?

- A. Aligning IT portfolio processes with corporate objectives
- B. Selecting IT investment projects that align with corporate strategy
- C. Increasing the budget and resources allocated for IT investments
- D. Determining the opportunity cost of IT investment projects

Answer: A ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 682

An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

- A. Log all table update transactions.
- B. implement before-and-after image reporting.
- C. Use tracing and tagging.
- D. implement integrity constraints in the database.

Answer: D ([LEAVE A REPLY](#))

Implementing integrity constraints in the database is a preventive control, because data is checked against predefined tables or rules preventing any undefined data from being entered. Logging all table update transactions and implementing before-and-after image reporting are detective controls that would not avoid the situation. Tracing and tagging are used to test application systems and controls and could not prevent out-of-range data.

NEW QUESTION: 683

An IS auditor is conducting a follow-up internal IS audit and determines that several recommendations from the prior year have not been implemented. Which of the following should be the auditor's FIRST course of action?

- A. Continue the audit and disregard prior audit recommendations
- B. Evaluate the recommendations in context of the current IT environment
- C. Request management implement recommendations from the prior year
- D. Add unimplemented recommendations as findings for the new audit

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 684

The PRIMARY benefit to using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry-pipe system:

- A. has a decreased risk of leakage.
- B. is more effective at suppressing flames.
- C. allows more time to abort release of the suppressant.
- D. disperses dry chemical suppressants exclusively.

Answer: ([SHOW ANSWER](#)**)**

Section: Protection of Information Assets

NEW QUESTION: 685

Which of the following should be an IS auditor's GREATEST concern when an international organization intends to roll out a global data privacy policy?

- A. Requirements may become unreasonable.
- B. Local regulations may contradict the policy.
- C. The policy may conflict with existing application requirements.
- D. Local management may not accept the policy.

Answer: B ([LEAVE A REPLY](#))

Comprehensive and Detailed Step-by-Step Explanation:

The biggest concern when implementing a global data privacy policy is that local regulations may contradict the global policy, leading to legal and compliance risks.

- * Local Regulations May Contradict the Policy (Correct Answer - B)
 - * Different countries have varying data privacy laws (e.g., GDPR in Europe, CCPA in California, PDPA in Singapore).
 - * A global policy may conflict with stricter local laws, making compliance challenging.
 - * Example: GDPR requires explicit consent for data processing, but other jurisdictions may allow implied consent.
- * Requirements May Become Unreasonable (Incorrect - A)
 - * Not a primary risk; compliance is more critical.
- * Conflicts with Application Requirements (Incorrect - C)
 - * Applications should adapt to regulations, not the other way around.
- * Local Management Resistance (Incorrect - D)
 - * Management acceptance is important but can be addressed through training.

References:

- * ISACA CISA Review Manual
- * GDPR (General Data Protection Regulation)
- * ISO 27701 (Privacy Information Management System)

NEW QUESTION: 686

Which of the following should be an IS auditor's consideration when scheduling follow-up activities for agreed-upon management responses to remediate audit observations?

- A. Risk rating of original findings
- B. Business interruption due to remediation
- C. Availability of responsible IT personnel
- D. IT budgeting constraints

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 687

When a new system is to be implemented within a short time frame, it is MOST important to:

- A. finish writing user manuals.

- B. perform user acceptance testing.
- C. add last-minute enhancements to functionalities.
- D. ensure that the code has been documented and reviewed.

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

It would be most important to complete the user acceptance testing to ensure that the system to be implemented is working correctly. The completion of the user manuals is similar to the performance of code reviews. If time is tight, the last thing one would want to do is add another enhancement, as it would be necessary to freeze the code and complete the testing, then make any other changes as future enhancements. It would be appropriate to have the code documented and reviewed, but unless the acceptance testing is completed, there is no guarantee that the system will work correctly and meet user requirement.

NEW QUESTION: 688

During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:

- A. ask the auditee to sign a release form accepting full legal responsibility.
- B. elaborate on the significance of the finding and the risks of not correcting it.
- C. report the disagreement to the audit committee for resolution.
- D. accept the auditee's position since they are the process owners.

Answer: ([SHOW ANSWER](#)**)**

If the auditee disagrees with the impact of a finding, it is important for an IS auditor to elaborate and clarify the risks and exposures, as the auditee may not fully appreciate the magnitude of the exposure. The goal should be to enlighten the auditee or uncover new information of which an IS auditor may not have been aware. Anything that appears to threaten the auditee will lessen effective communications and set up an adversarial relationship. By the same token, an IS auditor should not automatically agree just because the auditee expresses an alternate point of view.

NEW QUESTION: 689

The PRIMARY benefit of using secure shell (SSH) to access a server on a network is that it:

- A. provides confidentiality of transmitted data
- B. prevents man-in-the-middle attacks
- C. facilitates communication across platforms.
- D. provides better session reliability

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 690

Which of the following is an IS auditor's BEST recommendation to mitigate the risk of eavesdropping associated with an application programming interface (API) integration implementation?

- A. Encrypt the extensible markup language (XML) file.
- B. Implement Transport Layer Security (TLS).
- C. Implement Simple Object Access Protocol (SOAP).
- D. Mask the API endpoints.

Answer: B ([LEAVE A REPLY](#))

Explanation

The best recommendation to mitigate the risk of eavesdropping associated with an API integration implementation is to implement Transport Layer Security (TLS). TLS is a cryptographic protocol that provides secure communication over a network by encrypting the data in transit and authenticating the parties involved.

TLS can prevent unauthorized parties from intercepting, modifying or tampering with the data exchanged between the API endpoints. Encrypting the XML file, implementing SOAP, and masking the API endpoints are not sufficient to mitigate the risk of eavesdropping, as they do not provide end-to-end encryption or authentication for the API communication. References: IS Audit and Assurance Tools and Techniques, CISA Certification | Certified Information Systems Auditor | ISACA

NEW QUESTION: 691

An organization is shifting to a remote workforce. In preparation, the IT department is performing stress and capacity testing of remote access infrastructure and systems. What type of control is being implemented?

- A. Directive
- B. Preventive
- C. Detective
- D. Compensating

Answer: ([SHOW ANSWER](#)**)**

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As

Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 692

Which of the following protocol uses serial interface for communication between two computers in WAN technology?

- A. Point-to-point protocol
- B. X.25

C. Frame Relay

D. ISDN

Answer: (SHOW ANSWER)

Explanation/Reference:

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer using a MODEM connected by phone line to a server.

For your exam you should know below information about WAN Technologies:

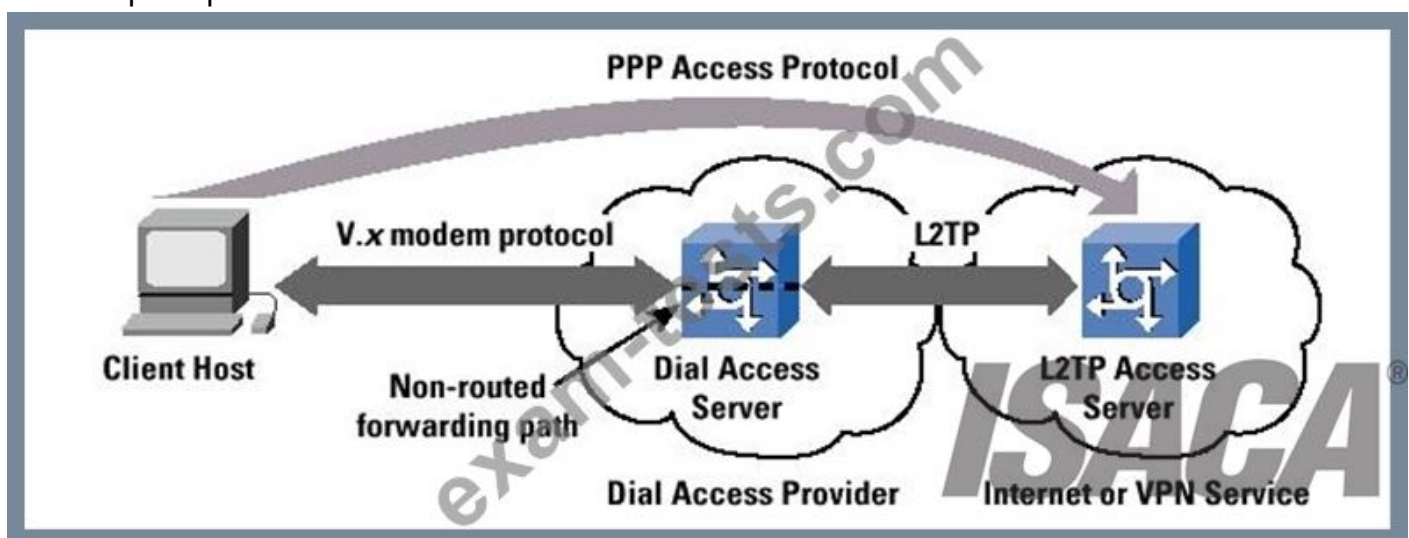
Point-to-point protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

Point-to-point protocol



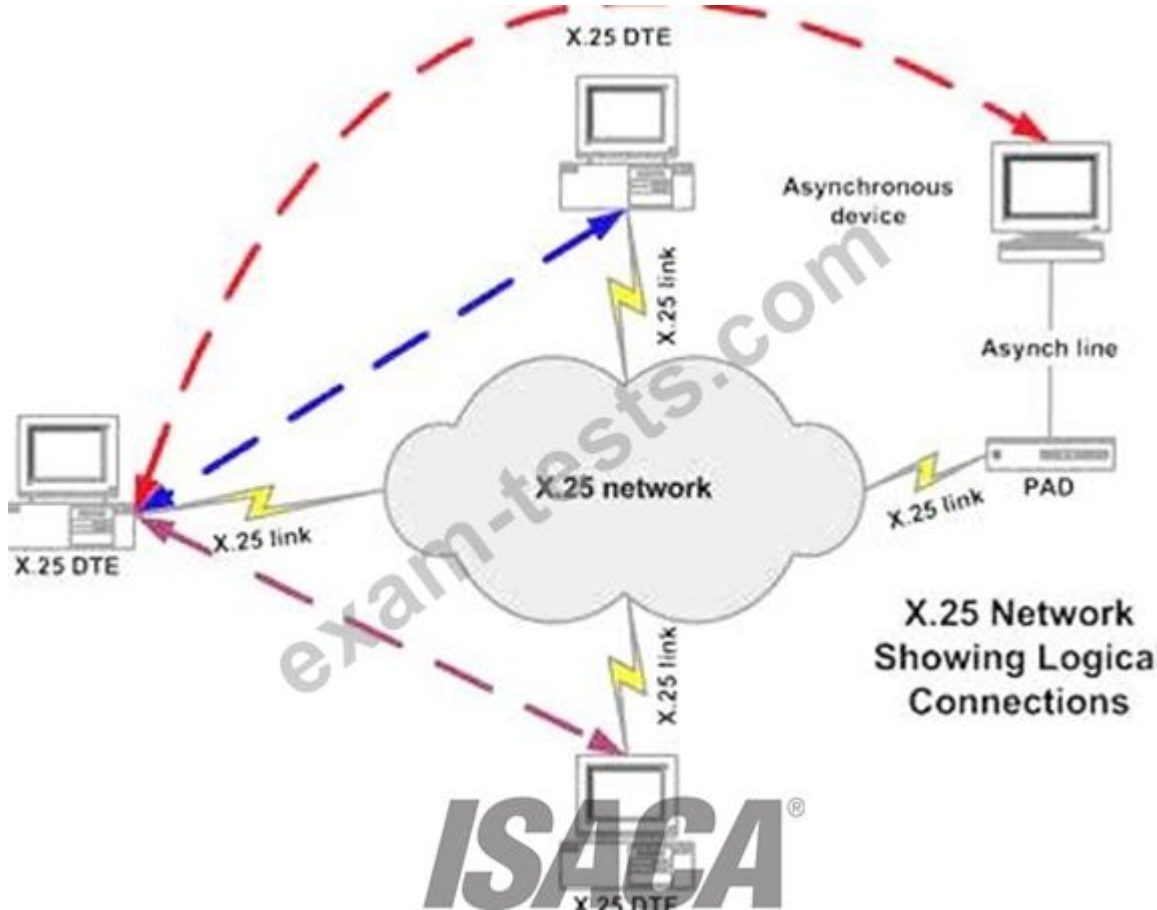
X.25

X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Subscribers are charged based on amount of bandwidth they use. Data are divided into 128 bytes and encapsulated in High Level Data Link Control (HDLC).

X.25 works at network and data link layer of an OSI model.



X.25

Frame Relay

Works on a packet switching

Operates at data link layer of an OSI model

Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR Two main types of equipment's are used in Frame Relay

1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.
2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.



Frame Relay

Integrated Service Digital Network

Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

Same copper telephone wire is used.

Provide digital point-to-point circuit switching medium.

ISDN



Asynchronous Transfer Mode (ATM)

Uses Cell switching method

High speed network technology used for LAN, MAN and WAN

Like a frame relay it is connection oriented technology which creates and uses fixed channel Data are segmented into fixed size cell of 53 bytes Some companies have replaces FDDI back-end with ATM

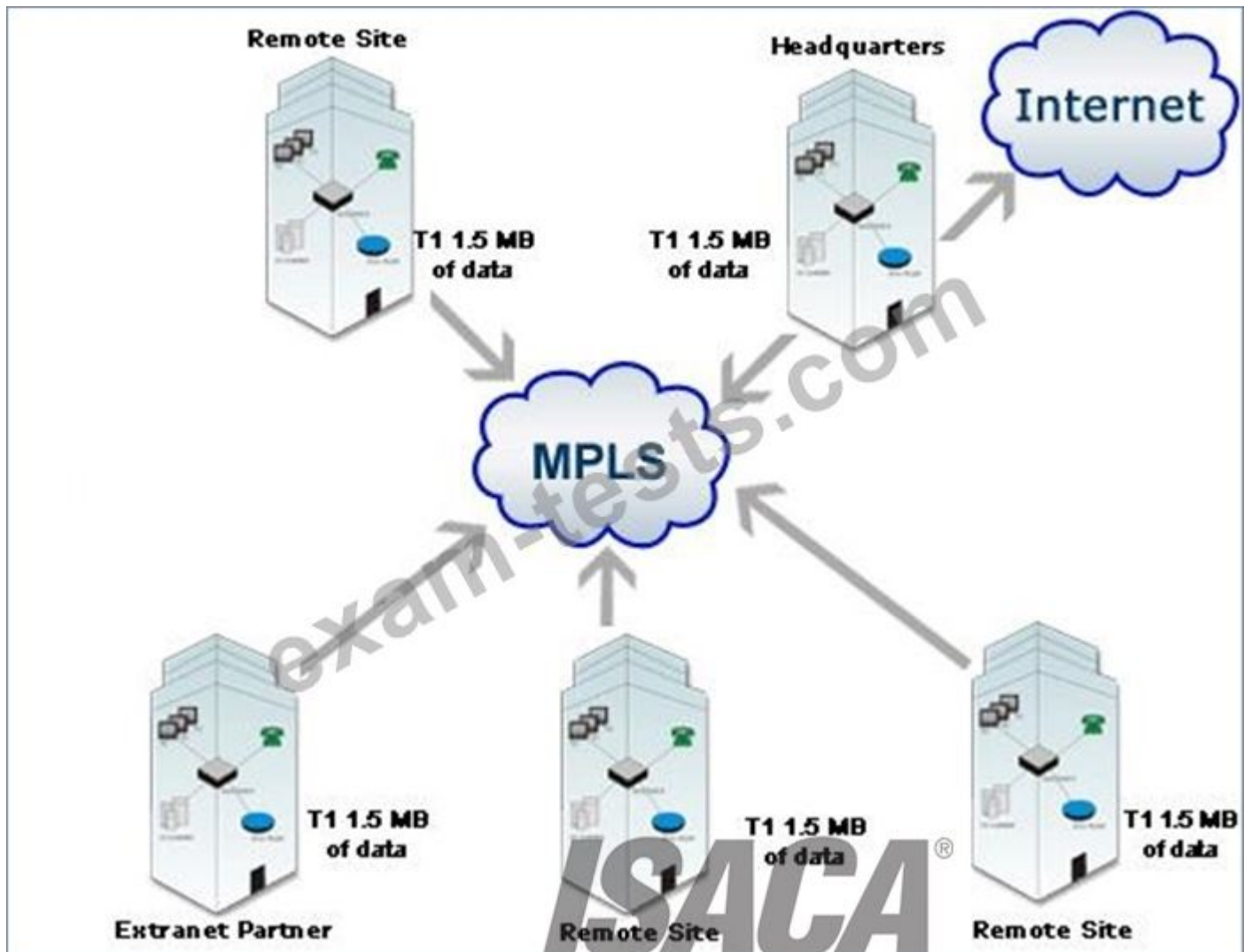
Asynchronous Transfer Mode

Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed

for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS



The following answers are incorrect:

X.25 - X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication. X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Frame Relay - The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.

ISDN - Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission. Same copper telephone wire is used. Provide digital point-to-point circuit switching medium.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 266

NEW QUESTION: 693

Which of the following is MOST helpful to an IS auditor reviewing the alignment of planned IT budget with the organization's goals and strategic objectives?

- A. Enterprise architecture (EA)
- B. Business impact analysis (BIA)
- C. Risk assessment report
- D. Audit recommendations

Answer: A (LEAVE A REPLY)

Enterprise architecture (EA) is the most helpful to an IS auditor reviewing the alignment of planned IT budget with the organization's goals and strategic objectives. EA is a well-defined practice for conducting enterprise analysis, design, planning, and implementation, using a comprehensive approach at all times, for the successful development and execution of strategy¹. EA provides a blueprint for an effective IT strategy and guides the controlled evolution of IT in a way that delivers business benefit in a cost-effective way². By reviewing the EA, the IS auditor can evaluate how well the planned IT budget supports the business vision, strategy, objectives, and capabilities of the organization.

The other options are not as helpful as EA for reviewing the alignment of planned IT budget with the organization's goals and strategic objectives. BIA is a process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption³. BIA quantifies the impacts of disruptions on service delivery, risks to service delivery, and recovery time objectives (RTOs) and recovery point objectives (RPOs)³. BIA is useful for developing strategies, solutions, and plans for business continuity and disaster recovery, but it does not directly address the alignment of planned IT budget with the organization's goals and strategic objectives. Risk assessment report is a document that contains the results of performing a risk assessment or the formal output from the process of assessing risk⁴. Risk assessment is a method to identify, analyze, and control hazards and risks present in a situation or a place⁵. Risk assessment report is useful for identifying and mitigating potential threats and issues that are detrimental to the business or an enterprise, but it does not directly address the alignment of planned IT budget with the organization's goals and strategic objectives. Audit recommendations are guidance that highlights actions to be taken by management⁶. When implemented, process risks should be mitigated, and performance should be enhanced⁶. Audit recommendations are useful for improving the quality and reliability of the information system and its outputs, but they do not directly address the alignment of planned IT budget with the organization's goals and strategic objectives. Therefore, option A is the correct answer.

NEW QUESTION: 694

Which of the following observations should be of GREATEST concern to an IS auditor reviewing a hosted virtualized environment where each guest operating system (OS) is r

- A. There are file shares between the host OS and the guest OS
- B. The test environment of the applications is in a separate guest OS
- C. All virtual machines are launching an application backup job at the same time
- D. Access to virtualization utilities and tools in the host is not restricted

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 695

Which of the following is MOST important for an effective control self-assessment (CSA) program?

- A. Determining the scope of the assessment
- B. Performing detailed test procedures
- C. Evaluating changes to the risk environment
- D. Understanding the business process

Answer: ([SHOW ANSWER](#)**)**

Understanding the business process is the most important factor for an effective control self-assessment (CSA) program. A CSA program is a technique that allows managers and work teams directly involved in business units, functions or processes to participate in assessing the organization's risk management and control processes¹. A CSA program can help identify risks and potential exposures to achieving strategic business objectives, evaluate the adequacy and effectiveness of controls, and implement remediation plans to address any gaps or weaknesses². To conduct a successful CSA, it is essential to have a clear and comprehensive understanding of the business process under review, including its objectives, inputs, outputs, activities, resources, dependencies, stakeholders, performance indicators, etc. This will help to identify the relevant risks and controls associated with the process, as well as to evaluate their impact and likelihood. Determining the scope of the assessment, performing detailed test procedures, and evaluating changes to the risk environment are also important factors for an effective CSA program, but not as important as understanding the business process. These factors are more related to the execution and monitoring phases of the CSA program, while understanding the business process is related to the planning and preparation phase. Without a solid understanding of the business process, the scope, testing, and evaluation of the CSA may not be accurate or complete.

References: ISACA CISA Review Manual 27th Edition, page 310

NEW QUESTION: 696

An IT strategic plan that BEST leverages IT in achieving organizational goals will include:

- A. a comparison of future needs against current capabilities.
- B. a risk-based ranking of projects.
- C. enterprise architecture (EA) impacts.
- D. IT budgets linked to the organization's budget.

Answer: ([SHOW ANSWER](#)**)**

Explanation

An IT strategic plan that best leverages IT in achieving organizational goals will include enterprise architecture (EA) impacts. EA is the practice of analyzing, designing, planning, and implementing enterprise analysis to successfully execute on business strategies¹. EA helps organizations structure IT projects and policies to align with business goals, to stay agile and resilient in the face of rapid change, and to stay on top of industry trends and disruptions¹. EA also describes an organization's processes, information processes and personnel and other organizational subunits aligned with the organization's core goals and strategies². By including EA impacts in the IT strategic plan, an organization can ensure that the IT initiatives are consistent with the business vision, objectives, and tactics, and that they support the desired business outcomes³.

A comparison of future needs against current capabilities, a risk-based ranking of projects, and IT budgets linked to the organization's budget are all important elements of an IT strategic plan, but they do not necessarily leverage IT in achieving organizational goals. A comparison of future needs against current capabilities can help identify gaps and opportunities for improvement, but it does not provide a clear direction or roadmap for how to achieve them. A risk-based ranking of projects can help prioritize the most critical and beneficial projects, but it does not ensure that they are aligned with the business strategy or that they deliver value to the stakeholders. IT budgets linked to the organization's budget can help allocate resources and monitor costs, but they do not reflect the impact or contribution of IT to the business performance or growth.

References:

Implement Agile IT Strategic Planning with Enterprise Architecture - The Open Group Blog
What is enterprise architecture? A framework for transformation | CIO Strategic Planning and Enterprise Architecture

NEW QUESTION: 697

Which of the following technologies has the SMALLEST maximum range for data transmission between devices?

- A. Wi-Fi
- B. Bluetooth
- C. Long-term evolution (LTE)
- D. Near-field communication (NFC)

Answer: D ([LEAVE A REPLY](#))

The technology that has the smallest maximum range for data transmission between devices is near-field communication (NFC). NFC is a short-range wireless technology that enables two devices to communicate when they are in close proximity, usually within a few centimeters. NFC is commonly used for contactless payments, smart cards, and device pairing. According to the Bluetooth® Technology Website¹, the effective range of NFC is less than a meter, while the other technologies have much longer ranges. Wi-Fi can reach up to 100 meters indoors and 300 meters outdoors². Bluetooth can reach up to 800 feet with Bluetooth 5.0 specification³. Long-term evolution (LTE) can reach up to several kilometers depending on the cell tower and the device⁴.

References:

- * 5: What is Wi-Fi? - Definition from WhatIs.com
- * 6: Understanding Bluetooth Range | Bluetooth® Technology Website
- * 7: What is Bluetooth Range? What You Need to Know
- * 8: How far can LTE signals travel? - Quora

NEW QUESTION: 698

Which of the following would an IS auditor recommend as the MOST effective preventive control to reduce the risk of data leakage?

- A. Ensure that paper documents are disposed securely.
- B. Validate that all data files contain digital watermarks.
- C. Verify that application logs capture any changes made.
- D. Implement an intrusion detection system (IDS).

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 699

With regard to resilience, which of the following is the GREATEST risk to an organization that has implemented a new critical system?

- A. A business impact analysis (BIA) has not been performed
- B. Business data is not sanitized in the development environment
- C. There is no plan for monitoring system downtime
- D. The process owner has not signed off on user acceptance testing (UAT)

Answer: A ([LEAVE A REPLY](#))

Explanation

Resilience is the ability of an organization to continue to operate effectively during or after a disruptive event.

A business impact analysis (BIA) is a key process to identify the critical systems and processes that support the organization's objectives and determine the impact of their disruption. Without a BIA, the organization may not be able to prioritize the recovery of the most important systems and processes, which poses the greatest risk to its resilience. The other options are not as significant as a BIA, as they relate to data quality, system monitoring, and user acceptance testing, which are important but not essential for resilience.

References: CISA Review Manual (Digital Version), Domain 4: Information Systems Operations and Business Resilience, Section 4.2 Business Continuity Planning¹

NEW QUESTION: 700

Which of the following is a benefit of a risk-based approach to audit planning? Audit:

- A. scheduling may be performed months in advance.
- B. budgets are more likely to be met by the IS audit staff.
- C. staff will be exposed to a variety of technologies.
- D. resources are allocated to the areas of highest concern

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

The risk-based approach is designed to ensure audit time is spent on the areas of highest risk.

The

development of an audit schedule is not addressed by a risk-based approach. Audit schedules may be

prepared months in advance using various scheduling methods. A risk approach does not have a direct

correlation to the audit staff meeting time budgets on a particular audit, nor does it necessarily mean a

wider variety of audits will be performed in a given year.

NEW QUESTION: 701

Which of the following is MOST important to consider when reviewing an organization's defined data backup and restoration procedures?

A. Mean time between failures (MTBF)

B. Mean time to restore (MTTR)

C. Business continuity plan (BCP)

D. Recovery point objective (RPO)

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 702

What is often the most difficult part of initial efforts in application development?

A. Configuring software

B. Planning security

C. Determining time and resource requirements

D. Configuring hardware

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

Explanation:

Determining time and resource requirements for an application-development project is often the most difficult part of initial efforts in application development.

NEW QUESTION: 703

A review of Internet security disclosed that users have individual user accounts with the Internet service providers (ISPs) and use these accounts for downloading business data. The organization wants to ensure that only corporate network is used. The organization should FIRST:

A. use a proxy server to filter out Internet sites that should not be accessed.

B. keep a manual log of Internal access.

C. monitor remote access activities.

D. include a statement in its security policy about Internet use.

Answer: D (LEAVE A REPLY)

Section: Governance and Management of IT

NEW QUESTION: 704

Which of the following is MOST helpful to an IS auditor reviewing the alignment of planned IT budget with the organization's goals and strategic objectives?

- A. Enterprise architecture (EA)
- B. Risk assessment report
- C. Audit recommendations
- D. Business impact analysis (BIA)

Answer: (SHOW ANSWER)

NEW QUESTION: 705

Documentation of workaround processes to keep a business function operational during recovery of IT

systems is a core part of a:

- A. business impact analysis.
- B. threat and risk assessment.
- C. business continuity plan.
- D. disaster recovery plan.

Answer: C (LEAVE A REPLY)

Section: Protection of Information Assets

NEW QUESTION: 706

In which of the following situations is it MOST appropriate to implement data mirroring as part of a recovery strategy?

- A. When the recovery point objective (RPO) is short
- B. When disaster tolerance is low
- C. When the risk of a ransomware attack is high
- D. When the mean time between failures (MTBF) is long

Answer: A (LEAVE A REPLY)

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 707

Which of the following presents the GREATEST challenge to the alignment of business and IT?

- A. Lack of chief information officer (CIO) involvement in board meetings
- B. Insufficient IT budget to execute new business projects
- C. Lack of information security involvement in business strategy development
- D. An IT steering committee chaired by the chief information officer (CIO)

Answer: A ([LEAVE A REPLY](#))

Explanation

The greatest challenge to the alignment of business and IT is the lack of chief information officer (CIO) involvement in board meetings. The CIO is the senior executive responsible for overseeing the IT strategy, governance, and operations of the organization, and ensuring that they support the business objectives and needs. The CIO should be involved in board meetings to communicate the value and contribution of IT to the organization, to align the IT vision and direction with the business strategy and priorities, and to advocate for the IT resources and investments required to achieve the desired outcomes. The lack of CIO involvement in board meetings can result in a disconnect between business and IT, a loss of trust and confidence in IT, and missed opportunities for innovation and value creation. The other options are not as challenging as the lack of CIO involvement in board meetings, because they either do not affect the strategic alignment of business and IT, or they can be addressed by other means such as collaboration, negotiation, or escalation. References:

CISA Review Manual (Digital Version)¹, Chapter 1, Section 1.2.1

NEW QUESTION: 708

An IS auditor observes that a business-critical application does not currently have any level of fault tolerance.

Which of the following is the GREATEST concern with this situation?

- A. Degradation of services
- B. Limited tolerance for damage
- C. Decreased mean time between failures (MTBF)
- D. Single point of failure

Answer: D ([LEAVE A REPLY](#))

Explanation

The greatest concern with this situation is that a business-critical application does not currently have any level of fault tolerance and thus has a single point of failure. A single point of failure is a component or element of a system that, if it fails, will cause the entire system to stop functioning. Fault tolerance is the ability of a system to continue operating without interruption or degradation in the event of a failure of one or more of its components or elements. Fault tolerance can be achieved by using techniques such as redundancy, replication, backup, or failover. A business-critical application should have a high level of fault tolerance to ensure its availability, reliability, and continuity. References:

CISA Review Manual (Digital Version), Chapter 5, Section 5.51

NEW QUESTION: 709

Which of the following would provide the MOST reliable evidence to indicate whether employee access has been deactivated in a timely manner following termination?

- A. Comparing termination forms with dates in the HR system
- B. Interviewing supervisors to verify employee data is being updated immediately
- C. Comparing termination forms with system transaction log entries
- D. Reviewing hardware return-of-asset forms

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 710

The most common reason for the failure of information systems to meet the needs of users is that:

- A. user needs are constantly changing.
- B. the growth of user requirements was forecast inaccurately.
- C. the hardware system limits the number of concurrent users.
- D. user participation in defining the system's requirements was inadequate.

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Lack of adequate user involvement, especially in the system's requirements phase, will usually result in a

system that does not fully or adequately address the needs of the user. Only users can define what their

needs are, and therefore what the system should accomplish.

NEW QUESTION: 711

Which of the following is the BEST way to mitigate the impact of ransomware attacks?

- A. Backing up data frequently
- B. Requiring password changes for administrative accounts
- C. Invoking the disaster recovery plan (DRP)
- D. Paying the ransom

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 712

If the recovery time objective (RTO) increases:

- A. the disaster tolerance increases.
- B. the cost of recovery increases.
- C. a cold site cannot be used.
- D. the data backup frequency increases.

Answer: ([SHOW ANSWER](#))

The longer the recovery time objective (RTO), the higher disaster tolerance and the lower the recovery cost. It cannot be concluded that a cold site is inappropriate or that the frequency of data backup would increase.

NEW QUESTION: 713

Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

- A. Overlapping controls
- B. Boundary controls
- C. Access controls
- D. Compensating controls

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential

control weakness that may arise when duties cannot be appropriately segregated.

Overlapping controls are two controls addressing the same control objective or exposure. Since primary

controls cannot be achieved when duties cannot or are not appropriately segregated, it is difficult to install

overlapping controls. Boundary controls establish the interface between the would-be user of a computer

system and the computer system itself, and are individual-based, not role-based, controls. Access controls

for resources are based on individuals and not on roles.

NEW QUESTION: 714

Which of the following analytical methods would be MOST useful when trying to identify groups with similar behavior or characteristics in a large population?

- A. Classification
- B. Cluster sampling
- C. Deviation detection
- D. Random sampling

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 715

Which of the following is an advantage of using agile software development methodology over the waterfall methodology?

- A. Quicker deliverables
- B. Quicker end user acceptance
- C. Clearly defined business expectations
- D. Less funding required overall

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 716

Which of the following is the BEST control to ensure data entered into a calculation program is accurate?

- A. Visual verification of data entered
- B. Programmed edit checks to prevent entry of invalid data
- C. Reasonableness checks with a data entry range
- D. Manual recalculation of data

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 717

Which of the following risk scenarios is BEST addressed by implementing policies and procedures related to full disk encryption?

- A. Data leakage as a result of employees leaving to work for competitors
- B. Noncompliance fines related to storage of regulated information
- C. Unauthorized logical access to information through an application interface
- D. Physical theft of media on which information is stored

Answer: ([SHOW ANSWER](#)**)**

Full disk encryption (FDE) is a means of protecting information by encrypting all of the data on a disk, including temporary files, programs, and system files¹. FDE is best suited for addressing the risk scenario of physical theft of media on which information is stored, as it prevents unauthorized access to the data even if the device is lost or stolen². FDE does not prevent data leakage as a result of employees leaving to work for competitors, as they may still have access to the data while using the device or copy the data to another device before leaving. FDE does not prevent noncompliance fines related to storage of regulated information, as it does not ensure that the data is stored in accordance with the applicable laws and regulations. FDE does not prevent unauthorized logical access to information through an application interface, as it does not control the access rights and permissions of users and applications. *References: According to the ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 2402 Planning, "The IS audit and assurance professional should identify and assess risk relevant to the area under review." ³ One of the risk factors to consider is "the sensitivity of information processed, stored or transmitted by the system" ³. FDE is one of the possible controls to mitigate the risk of unauthorized disclosure of sensitive information due to physical theft of media.

NEW QUESTION: 718

The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

- A. understand the business process.
- B. comply with auditing standards.
- C. identify control weakness.
- D. plan substantive testing.

Answer: A ([LEAVE A REPLY](#))

Understanding the business process is the first step an IS auditor needs to perform. Standards do not require an IS auditor to perform a process walkthrough. Identifying control weaknesses is not the primary reason for the walkthrough and typically occurs at a later stage in the audit, while planning for substantive testing is performed at a later stage in the audit.

NEW QUESTION: 719

Which of the following controls should be implemented to BEST minimize system downtime for maintenance?

- A. Warm site
- B. Virtualization
- C. Nightly full backups
- D. Clustering

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 720

An IS auditor is reviewing an organization's business continuity plan (BCP) following a change in organizational structure with significant impact to business processes. Which of the following findings should be the auditor's GREATEST concern?

- A. Key business process end users did not participate in the business impact " analysis (BIA)
- B. Copies of the BCP have not been distributed to new business unit end users since the reorganization
- C. A test plan for the BCP has not been completed during the last two years

Answer: C ([LEAVE A REPLY](#))

A test plan for the BCP is essential to ensure that the plan is effective, updated and aligned with the current business needs and objectives. A change in organizational structure with significant impact to business processes may require a revision of the BCP and a new test plan to validate its adequacy. The lack of a test plan for the BCP for two years indicates a high risk of failure in the event of a disaster or disruption.

Therefore, this should be the auditor's greatest concern among the given options. References: ISACA, IT Control Objectives for Sarbanes-Oxley, 4th Edition, section 5.3.21 ISACA, CISA Review Manual, 27th Edition, chapter 5, section 5.42

NEW QUESTION: 721

Which of the following would provide the important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program?

- A. An inventory of personal devices to be connected to the corporate network
- B. Results of a risk assessment
- C. Policies including BYOD acceptable use statements
- D. Findings from prior audits

Answer: ([SHOW ANSWER](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 722

By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:

- A. reliable products are guaranteed.
- B. programmers' efficiency is improved.
- C. security requirements are designed.
- D. predictable software processes are followed.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

By evaluating the organization's development projects against the CMM, an IS auditor determines whether the development organization follows a stable, predictable software process. Although the likelihood of success should increase as the software processes mature toward the optimizing level, mature processes do not guarantee a reliable product. CMM does not evaluate technical processes such as programming nor does it evaluate security requirements or other application controls.

NEW QUESTION: 723

During an external review, an IS auditor observes an inconsistent approach in classifying system criticality within the organization. Which of the following should be recommended as the PRIMARY factor to determine system criticality?

- A. Key performance indicators (KPIs)
- B. Maximum allowable downtime (MAD)
- C. Recovery point objective (RPO)

D. Mean time to restore (MTTR)

Answer: B ([LEAVE A REPLY](#))

The primary factor to determine system criticality within an organization is the maximum allowable downtime (MAD). MAD is the maximum time frame during which recovery must become effective before an outage compromises the ability of an organization to achieve its business objectives and/or survival. MAD reflects the business impact of a system outage on the organization's operations, reputation, compliance, and finances. MAD can help to prioritize system recovery efforts, allocate resources, and establish recovery objectives.

NEW QUESTION: 724

While auditing a small organization's data classification processes and procedures, an IS auditor noticed that data is often classified at the incorrect level. What is the MOST effective way for the organization to improve this situation?

- A.** Conduct awareness presentations and seminars for information classification policies.
- B.** Use automatic document classification based on content.
- C.** Have IT security staff conduct targeted training for data owners.
- D.** Publish the data classification policy on the corporate web portal.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 725

Which of the following should be included in an organization's IS security policy?

- A.** A list of key IT resources to be secured
- B.** The basis for access authorization
- C.** Identity of sensitive security features
- D.** Relevant software security features

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

The security policy provides the broad framework of security, as laid down and approved by senior management. It includes a definition of those authorized to grant access and the basis for granting the access. Choices A, B and C are more detailed than that which should be included in a policy.

NEW QUESTION: 726

Which of the following would BEST demonstrate that an effective disaster recovery plan (DRP) is in place?

- A.** Periodic risk assessment
- B.** Annual wall-through testing
- C.** Frequent testing of backups
- D.** Full operational test

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 727

Which of the following is the BEST sampling method to use when relatively few errors are expected to be found in a population?

- A. Variable sampling
- B. Judgmental sampling
- C. Stop-or-go sampling
- D. Discovery sampling

Answer: [\(SHOW ANSWER\)](#)

Discovery sampling is a type of statistical sampling that's used when the expected error rate in the population is very low¹. This method is designed to discover at least one instance of an attribute or condition in a population¹. It's often used in auditing to uncover fraud or noncompliance with rules and regulations¹.

References:

* What are sampling methods and how do you choose the best one?

NEW QUESTION: 728

What should an IS auditor evaluate FIRST when reviewing an organization's response to new privacy legislation?

- A. Implementation plan for restricting the collection of personal information
- B. Operational plan for achieving compliance with the legislation
- C. Privacy legislation in other countries that may contain similar requirements
- D. Analysis of systems that contain privacy components

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 729

Which of the following is the BEST method to prevent wire transfer fraud by bank employees?

- A. System-enforced dual control
- B. Independent reconciliation
- C. Re-keying of wire dollar amounts
- D. Two-factor authentication control

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 730

Which of the following is the BEST way for an IS auditor to assess the design of an automated application control?

- A. Obtain management attestation and sign-off.
- B. Review the application implementation documents.
- C. Interview the application developer.
- D. Review system configuration parameters and output.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 731

An organization has implemented periodic reviews of logs showing privileged user activity production servers. Which type of control has been established?

- A. Protective
- B. Detective
- C. Preventive
- D. Corrective

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 732

During a review, an IS auditor discovers that corporate users are able to access cloud-based applications and data any Internet-connected web browser. Which Of the following is the auditors BEST recommendation to prevent unauthorized access?

- A. Implement an intrusion detection system (IDS),
- B. Update security policies and procedures.
- C. Implement multi-factor authentication.
- D. Utilize strong anti-malware controls on all computing devices.

Answer: (SHOW ANSWER)

The best recommendation to prevent unauthorized access in this scenario is to implement multi-factor authentication (MFA). According to the ISACA CISA Study Manual, "MFA is a security technique that requires two or more independent credentials for user authentication. MFA can be used to provide additional security for cloud-based services and applications." Thus, implementing MFA would be an effective way to prevent unauthorized access and maintain a secure environment.

Multi-factor authentication (MFA) is a security measure that requires users to provide two or more pieces of evidence to verify their identity before accessing cloud-based applications and data¹²³. MFA can prevent unauthorized access by making it harder for attackers to compromise user credentials or bypass password protection

NEW QUESTION: 733

An IS auditor identifies key controls that have been overridden by management. The next step the IS auditor should take is to

- A. Report the absence of key controls to regulators
- B. Withdraw from the engagement
- C. Recommend compensating controls
- D. Perform procedures to quantify the irregularities

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 734

Which of the following is a passive attack to a network?

- A. Message modification
- B. Masquerading
- C. Denial of service
- D. Traffic analysis

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

The intruder determines the nature of the flow of traffic (traffic analysis) between defined hosts and is able to guess the type of communication taking place. Message modification involves the capturing of a message and making unauthorized changes or deletions, changing the sequence or delaying transmission of captured messages. Masquerading is an active attack in which the intruder presents an identity other than the original identity. Denial of service occurs when a computer connected to the Internet is flooded with data and/or requests that must be processed.

NEW QUESTION: 735

Which of the following is MOST critical for the effective implementation of IT governance?

- A. Strong risk management practices
- B. Internal auditor commitment
- C. Supportive corporate culture
- D. Documented policies

Answer: C ([LEAVE A REPLY](#))

Explanation

The most critical factor for the effective implementation of IT governance is a supportive corporate culture. A supportive corporate culture is one that fosters collaboration, communication and commitment among all stakeholders involved in IT governance processes. A supportive corporate culture also promotes a shared vision, values and goals for IT governance across the organization. Strong risk management practices, internal auditor commitment or documented policies are important elements for IT governance implementation, but they are not sufficient without a supportive corporate culture. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 41

NEW QUESTION: 736

The PRIMARY purpose of a configuration management system is to:

- A. define baselines for software.
- B. track software updates.
- C. standardize change approval.
- D. support the release procedure.

Answer: A ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 737

Which of the following is an implementation risk within the process of decision support systems?

- A. Management control
- B. Semistructured dimensions
- C. inability to specify purpose and usage patterns
- D. Changes in decision processes

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation:

The inability to specify purpose and usage patterns is a risk that developers need to anticipate while implementing a decision support system (DSS). Choices A, B and D are not risks, but characteristics of a DSS.

NEW QUESTION: 738

Which of the following should be GREATEST concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system?

- A. Data conversion was performed using manual processes.
- B. Backups of the old system and data are not available online.
- C. Unauthorized data modifications occurred during conversion.
- D. The change management process was not formally documented

Answer: C (LEAVE A REPLY)

Explanation

The greatest concern for an IS auditor reviewing data conversion and migration during the implementation of a new application system is unauthorized data modifications occurred during conversion. Unauthorized data modifications are changes or alterations to data that are not authorized, intended, or expected, such as due to errors, fraud, or sabotage. Unauthorized data modifications occurred during conversion can compromise the accuracy, completeness, and integrity of the data being converted and migrated to the new application system, and may result in data loss, corruption, or inconsistency. The other options are not as concerning as unauthorized data modifications occurred during conversion in reviewing data conversion and migration during the implementation of a new application system, as they do not affect the accuracy, completeness, or integrity of the data being converted and migrated. Data conversion was performed using manual processes is a possible factor that may increase the risk or

complexity of data conversion and migration, but it does not necessarily imply that unauthorized data modifications occurred during conversion. Backups of the old system and data are not available online is a possible factor that may affect the availability or accessibility of the old system and data for backup or recovery purposes, but it does not imply that unauthorized data modifications occurred during conversion. The change management process was not formally documented is a possible factor that may affect the quality or consistency of the change management process for implementing the new application system, but it does not imply that unauthorized data modifications occurred during conversion.

References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION: 739

Which of the following findings should be of MOST concern to an IS auditor assessing agile software development practices?

- A. The IT team feels unable to strictly follow standard agile practices.
- B. Testing is performed by both software developers and testers.
- C. There is a low acceptance rate by the business of delivered software.
- D. Release plans have been revised several times before actual release.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 740

When reviewing a database supported by a third-party service provider, an IS auditor found minor control deficiencies. The auditor should FIRST discuss recommendations with the:

- A. organization's service level manager
- B. service provider contract liaison
- C. organization's chief information officer (CIO)
- D. service provider support team manager

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 741

A recent audit concluded that an organization's information security system was weak and that monitoring would likely fail to detect penetration. Which of the following would be the MOST appropriate recommendation?

- A. Identify and periodically remove sensitive data that is no longer needed
- B. Look continually for new criminal behavior and attacks on sensitive data
- C. Establish a clear policy related to security and the handling of sensitive data
- D. Encrypt sensitive data while strengthening the system

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 742

.What is an edit check to determine whether a field contains valid data?

- A. Completeness check

- B. Accuracy check
- C. Redundancy check
- D. Reasonableness check

Answer: A ([LEAVE A REPLY](#))

A completeness check is an edit check to determine whether a field contains valid data .

NEW QUESTION: 743

To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

- A. schedule the audits and monitor the time spent on each audit.
- B. train the IS audit staff on current technology used in the company.
- C. develop the audit plan on the basis of a detailed risk assessment.
- D. monitor progress of audits and initiate cost control measures.

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Monitoring the time (choice A) and audit programs (choice D), as well as adequate training (choice B), will improve the IS audit staff's productivity (efficiency and performance), but that which delivers value to the organization are the resources and efforts being dedicated to, and focused on, the higher-risk areas.

NEW QUESTION: 744

An information security manager is assisting in the development of the request for proposal (RFP) for a

new outsourced service. This will require the third party to have access to critical business information. The

security manager should focus PRIMARILY on defining:

- A. security requirements for the process being outsourced
- B. security metrics
- C. service level agreements (SLAs)
- D. risk-reporting methodologies

Answer: C ([LEAVE A REPLY](#))

Section: Governance and Management of IT

NEW QUESTION: 745

To support an organization's goals, an IS department should have:

- A. a low-cost philosophy.
- B. long- and short-range plans.
- C. leading-edge technology.
- D. plans to acquire new hardware and software.

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

To ensure its contribution to the realization of an organization's overall goals, the IS department should

have long- and short-range plans that are consistent with the organization's broader plans for attaining its

goals. Choices A and C are objectives, and plans would be needed to delineate how each of the objectives

would be achieved. Choice D could be a part of the overall plan but would be required only if hardware or

software is needed to achieve the organizational goals.

NEW QUESTION: 746

Which of the following INCORRECTLY describes the layer function of the Application Layer within the TCP/

IP model?

A. Provides user interface

B. Perform data processing such as encryption, encoding, etc

C. Provides reliable delivery

D. Keeps separate the data of different applications

Answer: (SHOW ANSWER)

Section: Information System Operations, Maintenance and Support

Explanation/Reference:

The word INCORRECTLY keyword is used in the question.

You need to find out the service or functionality which is not performed by application layer of a TCP/IP

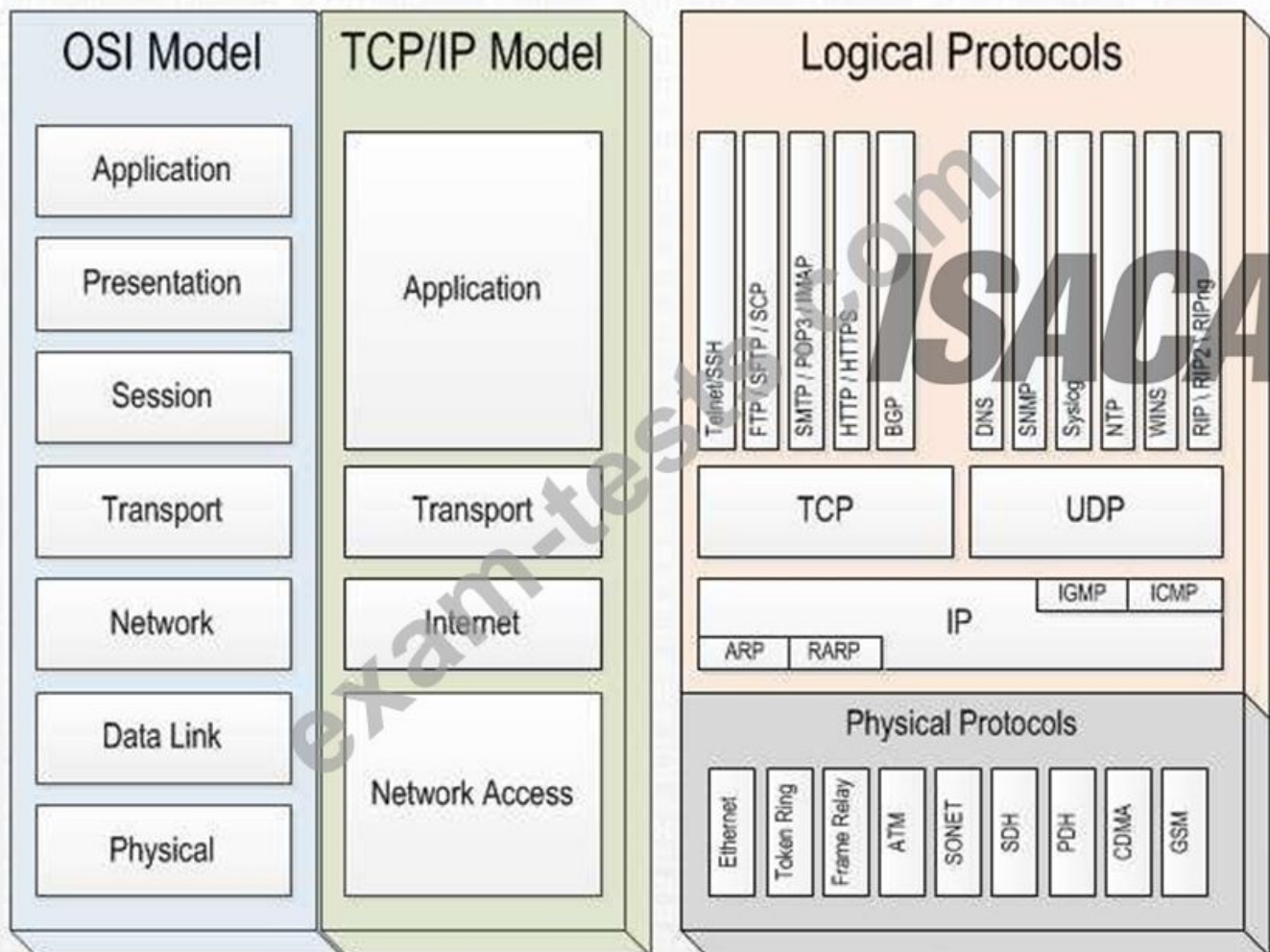
model.

The reliable or unreliable delivery of a message is the functionality of transport layer of a TCP/IP model.

For your exam you should know below information about TCP/IP model:

Network Models

NETWORK MODELS



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of

the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface

with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer

Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DHCP

(Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is

between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the

source and destination hosts to carry on a conversation. Transport layer defines the level of service and

status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between

Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP

datagram's, which contain source and destination address (logical address or IP address) information that

is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as

Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than

they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network

applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message

Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP

(Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines

details of how data is physically sent through the network, including how bits are electrically or optically

signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical

fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access

Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when

Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire

when the wire is free from network traffic. When a host wants to place data on the wire, it will check the

wire to find whether another host is already using the medium. If there is traffic already in the medium, the

host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on

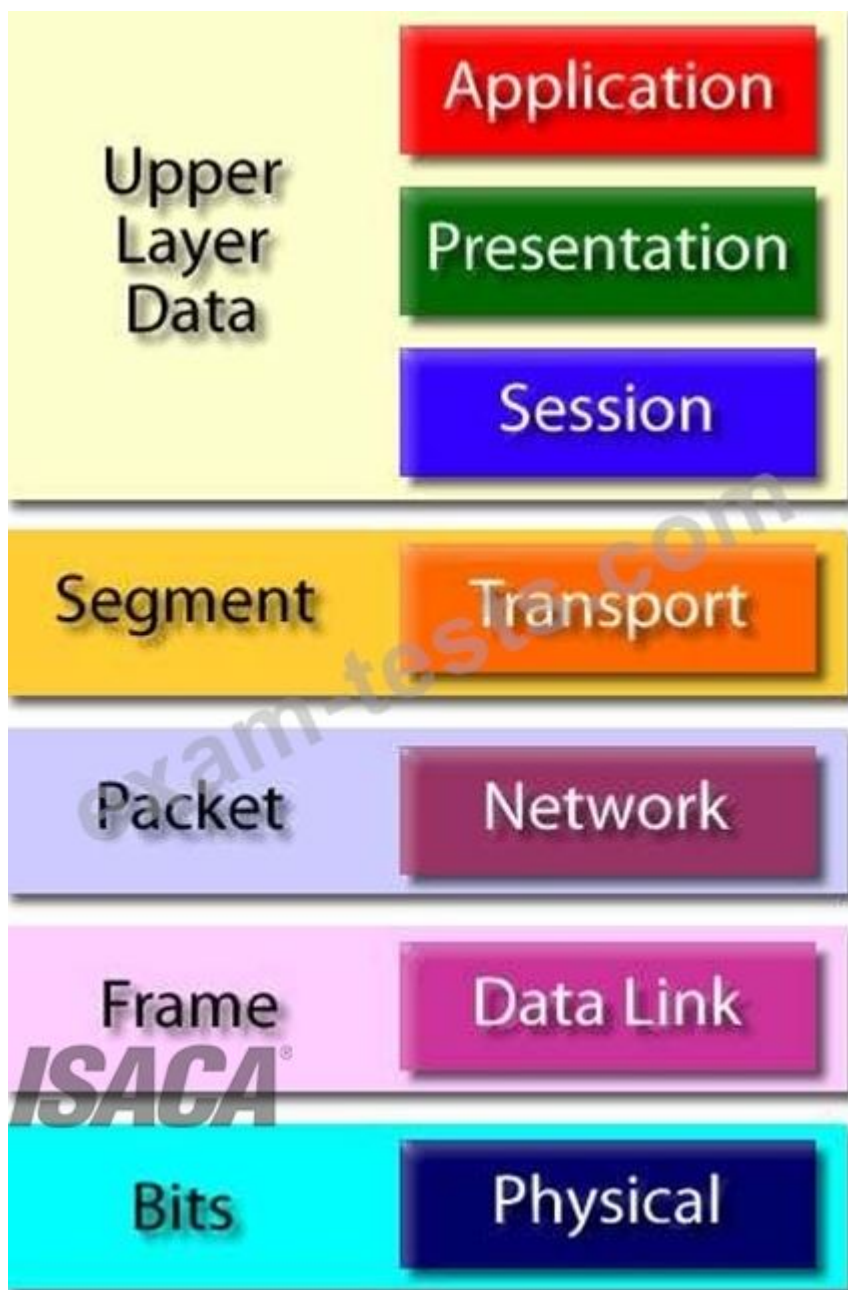
the medium at the same instance, they will collide with each other, destroying the data. If the data is

destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for

a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

The other options correctly describe functionalities of application layer in TCP/IP model.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

NEW QUESTION: 747

Which of the following measures BEST mitigates the risk of exfiltration during a cyberattack?

- A. Perimeter firewall
- B. Hashing of sensitive data
- C. Data loss prevention (DLP) system
- D. Network access controls (NAC)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 748

What method might an IS auditor utilize to test wireless security at branch office locations?

- A. War dialing
- B. Social engineering
- C. War driving
- D. Password cracking

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

War driving is a technique for locating and gaining access to wireless networks by driving or walking with a wireless equipped computer around a building. War dialing is a technique for gaining access to a computer or a network through the dialing of defined blocks of telephone numbers, with the hope of getting an answer from a modem. Social engineering is a technique used to gather information that can assist an attacker in gaining logical or physical access to data or resources. Social engineering exploits human weaknesses. Password crackers are tools used to guess users' passwords by trying combinations and dictionary words.

NEW QUESTION: 749

Which of the following poses the GREATEST risk to the enforceability of networking policies in a virtualized environment?

- A. Lack of encryption for data at rest
- B. Use of a public key infrastructure
- C. Transmission of data on public networks
- D. Lack of visibility into the networks

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 750

Which of the following is the MOST critical element impacting the success of an information security program?

- A. Implementation of industry-standard information security tools
- B. Adequate budget to support the information security strategy
- C. Mandatory information security awareness training
- D. Senior management commitment to information security initiatives

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 751

Which of the following observations would an IS auditor consider the GREATEST risk when conducting an audit of a virtual server farm for potential software vulnerabilities?

- A. Guest operating systems are updated monthly
- B. The hypervisor is updated quarterly.
- C. Antivirus software has been implemented on the guest operating system only.
- D. A variety of guest operating systems operate on one virtual server

Answer: C ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 752

Which of the following is the BEST method to defend against social engineering attacks?

- A. Periodically perform antivirus scans to identify malware.
- B. Communicate guidelines to limit information posted to public sites.
- C. Monitor for unauthorized access attempts and failed logins.
- D. Employ the use of a web-content filtering solution.

Answer: D ([LEAVE A REPLY](#))

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 753

Which of the following an IS audit, which of the following types of risk would be MOST critical to communicate to key stakeholders?

- A. Control
- B. Audit
- C. Residual
- D. inherent

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 754

To ensure confidentiality through the use of asymmetric encryption, a message is encrypted with which of the following?

- A. Recipient's public key
- B. Sender's private key
- C. Sender's public key
- D. Recipient's private key

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 755

A global bank plans to use a cloud provider for backup of customer financial data. Which of the following should be the PRIMARY focus of this project?

- A. Data confidentiality
- B. Data retention policy
- C. Transfer frequency
- D. Backup testing schedule

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 756

An IS auditor learns an organization does not perform full disaster recovery (DR) testing because past tests have confirmed that all critical systems can individually be recovered within four hours, in line with business requirements. Which of the following should be the auditor's GREATEST concern"

- A. The tests did not take into account the DR dependencies between different systems
- B. Critical systems should be recoverable in less than four hours
- C. Performing many individual tests required more effort in total than a full DR test
- D. The individual tests did not consider non-critical systems

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 757

A trojan horse simply cannot operate autonomously.

- A. true
- B. false

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

As a common type of Trojan horses, a legitimate software might have been corrupted with malicious code which runs when the program is used. The key is that the user has to invoke the program in order to trigger the malicious code. In other words, a trojan horse simply cannot operate autonomously. You would also want to know that most but not all trojan horse payloads are harmful - a few of them are harmless.

NEW QUESTION: 758

Management decided to accept the residual risk of an audit finding and not take the recommended actions.

The internal audit team believes the acceptance is inappropriate and has discussed the situation with

executive management. After this discussion, there is still disagreement regarding the decision.

Which of

the following is the BEST course of action by internal audit?

- A. Report this matter to the audit committee without notifying executive management.
- B. Document in the audit report that management has accepted the residual risk and take no further

actions.

C. Report the issue to the audit committee in a joint meeting with executive management for resolution.

D. Schedule another meeting with executive management to convince them of taking action as recommended.

Answer: C ([LEAVE A REPLY](#))

Section: Governance and Management of IT

NEW QUESTION: 759

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

A. End-user involvement

B. Senior management involvement

C. Security administration involvement

D. IS auditing involvement

Answer: A ([LEAVE A REPLY](#))

End-user involvement is critical during the business impact assessment phase of business continuity planning.

NEW QUESTION: 760

What is often assured through table link verification and reference checks?

A. Database integrity

B. Database synchronization

C. Database normalcy

D. Database accuracy

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

Explanation:

Database integrity is most often ensured through table link verification and reference checks.

NEW QUESTION: 761

Which of the following provides the MOST effective protection against ransomware attacks?

A. Obtaining cybersecurity and ransomware insurance

B. Ensuring appropriate backups are secured and isolated from the primary facility

C. Ensuring the primary facility is compatible with the hot site

D. Familiarizing employees with the business continuity plan (BCP) and routinely testing

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 762

When an information security manager presents an information security program status report to senior management, the MAIN focus should be:

- A. key performance indicators (KPIs)
- B. critical risks indicators
- C. net present value (NPV)
- D. key controls evaluation

Answer: [\(SHOW ANSWER\)](#)

Section: Governance and Management of IT

NEW QUESTION: 763

As an outcome of information security governance, strategic alignment provides:

- A. security requirements driven by enterprise requirements.
- B. baseline security following best practices.
- C. institutionalized and commoditized solutions.
- D. an understanding of risk exposure.

Answer: A [\(LEAVE A REPLY\)](#)

Section: Protection of Information Assets

Explanation:

Information security governance, when properly implemented, should provide four basic outcomes:

strategic alignment, value delivery, risk management and performance measurement. Strategic alignment

provides input for security requirements driven by enterprise requirements. Value delivery provides a

standard set of security practices, i.e., baseline security following best practices or institutionalized and

commoditized solutions. Risk management provides an understanding of risk exposure.

NEW QUESTION: 764

Which of the following is the MOST significant risk when an application uses individual end-user accounts to access the underlying database?

- A. Multiple connects to the database are used and slow the process_
- B. User accounts may remain active after a termination.
- C. Users may be able to circumvent application controls.
- D. Application may not capture a complete audit trail.

Answer: C [\(LEAVE A REPLY\)](#)

The most significant risk when an application uses individual end-user accounts to access the underlying database is that users may be able to circumvent application controls. Application controls are the policies, procedures, and mechanisms that ensure the accuracy, completeness, validity, and authorization of transactions and data within an application. Application controls can include input validation, output verification, processing logic, reconciliation, exception handling, and audit trails. Application controls can help prevent or detect errors, fraud, or unauthorized access or modification of data.

However, if an application uses individual end-user accounts to access the underlying database, it means that the users have direct access to the database without going through the application layer. This can expose the database to potential risks such as:

- * Users may be able to bypass the application controls and manipulate the data in the database directly using SQL commands or other tools. For example, users may be able to change their own or others' salaries, grades, or balances without proper authorization or validation.
- * Users may be able to access or disclose sensitive or confidential data that they are not supposed to see or share. For example, users may be able to view other users' personal information, passwords, or credit card numbers.
- * Users may be able to introduce errors or inconsistencies in the data by entering invalid or incorrect data or by deleting or modifying existing data. For example, users may be able to create duplicate records, break referential integrity, or cause data loss or corruption.
- * Users may be able to compromise the security and performance of the database by creating unauthorized objects, granting excessive privileges, executing malicious code, or consuming excessive resources. For example, users may be able to create backdoors, viruses, or denial-of-service attacks.

Therefore, using individual end-user accounts to access the underlying database can pose a serious threat to the integrity, confidentiality, availability, and reliability of the data and the application.

The other options are not as significant as option C. Multiple connects to the database are used and slow the process is a performance issue that can affect the efficiency and responsiveness of the application and the database, but it does not necessarily compromise the data quality or security. User accounts may remain active after a termination is a security issue that can increase the risk of unauthorized access or misuse of data by former employees or others who have access to their credentials, but it can be mitigated by implementing proper account management and monitoring processes. Application may not capture a complete audit trail is a compliance issue that can affect the accountability and traceability of transactions and data within the application and the database, but it does not directly affect the data accuracy or protection.

References:

- * Should application users be database users? - Stack Overflow¹
- * An Approach Toward Sarbanes-Oxley ITGC Risk Assessment - ISACA²
- * ISACA CISA Certified Information Systems Auditor Exam ... - PUPUWEB³
- * Why inactive accounts are a security risk | Stratosphere⁴

NEW QUESTION: 765

If a database is restored from information backed up before the last system image, which of the following is recommended?

- A.** The system should be restarted after the last transaction.
- B.** The system should be restarted before the last transaction.
- C.** The system should be restarted at the first transaction.
- D.** The system should be restarted on the last transaction.

Answer: B (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

If a database is restored from information backed up before the last system image, the system should be restarted before the last transaction because the final transaction must be reprocessed.

NEW QUESTION: 766

Which of the following is MOST critical when creating data for testing the logic in a new or modified application system?

- A. A sufficient quantity of data for each test case
- B. Data representing conditions that are expected in actual processing
- C. Completing the test on schedule
- D. A random sample of actual data

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Selecting the right kind of data is key in testing a computer system. The data should not only include valid and invalid data but should be representative of actual processing; quality is more important than quantity.

It is more important to have adequate test data than to complete the testing on schedule. It is unlikely that a random sample of actual data would cover all test conditions and provide a reasonable representation of actual data.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 767

When using public key encryption to secure data being transmitted across a network:

- A. both the key used to encrypt and decrypt the data are public.
- B. the key used to encrypt is private, but the key used to decrypt the data is public.
- C. the key used to encrypt is public, but the key used to decrypt the data is private.
- D. both the key used to encrypt and decrypt the data are private.

Answer: C (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

Public key encryption, also known as asymmetric key cryptography, uses a public key to encrypt the message and a private key to decrypt it.

NEW QUESTION: 768

Which of the following provide(s) near-immediate recoverability for time-sensitive systems and transaction processing?

- A. Automated electronic journaling and parallel processing
- B. Data mirroring and parallel processing
- C. Data mirroring
- D. Parallel processing

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Data mirroring and parallel processing are both used to provide near- immediate recoverability for time-sensitive systems and transaction processing.

NEW QUESTION: 769

Parity bits are a control used to validate:

- A. Data authentication
- B. Data completeness
- C. Data source
- D. Data accuracy

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Parity bits are a control used to validate data completeness.

NEW QUESTION: 770

An organization's business continuity plan (BCP) should be:

- A. tested whenever new applications are implemented
- B. updated based on changes to personnel and environments
- C. updated before an independent audit review
- D. tested after an intrusion attempt into the organization's hot site

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 771

Which of the following is a concern associated with virtualization?

- A. The physical footprint of servers could decrease within the data center.
- B. Performance issues with the host could impact the guest operating systems.
- C. Processing capacity may be shared across multiple operating systems.

D. One host may have multiple versions of the same operating system.

Answer: B ([LEAVE A REPLY](#))

Explanation

A concern associated with virtualization is that performance issues with the host could impact the guest operating systems, which are the operating systems that run on virtual machines within the host. For example, if the host has insufficient memory, CPU, disk space, or network bandwidth, it could affect the performance and availability of the guest operating systems and the applications running on them. The physical footprint of servers could decrease within the data center, processing capacity may be shared across multiple operating systems, and one host may have multiple versions of the same operating system are not concerns associated with virtualization, but rather benefits or features of virtualization that can help reduce costs, improve efficiency, and enhance flexibility. References: CISA Review Manual (Digital Version), Chapter 4: Information Systems Operations and Business Resilience, Section 4.2: IT Service Delivery and Support

NEW QUESTION: 772

Which of the following processes are performed during the design phase of the systems development life cycle (SDLC) model?

- A.** Develop test plans.
- B.** Baseline procedures to prevent scope creep.
- C.** Define the need that requires resolution, and map to the major requirements of the solution.
- D.** Program and test the new system. The tests verify and validate what has been developed.

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Procedures to prevent scope creep are baselined in the design phase of the systems-development life cycle (SDLC) model.

NEW QUESTION: 773

Who is responsible for implementing cost-effective controls in an automated system?

- A.** Security policy administrators
- B.** Business unit management
- C.** Senior management
- D.** Board of directors

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

Business unit management is responsible for implementing cost-effective controls in an automated system.

NEW QUESTION: 774

An online retailer is receiving customer about receiving different items from what they ordered on the

organization's website. The root cause has been traced to poor data quality. Despite efforts to clean

erroneous data from the system, multiple data quality issues continue to occur. Which of the following

recommendations would be the BEST way to reduce the likelihood of future occurrences?

- A. Implement business rules to validate employee data entry.
- B. Invest in additional employee training for data entry.
- C. Assign responsibility for improving data quality.
- D. Outsource data cleansing activities to reliable third parties.

Answer: A ([LEAVE A REPLY](#))

Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 775

Which of the following refers to a method of bypassing normal system authentication procedures?

- A. virus
- B. worm
- C. trojan horse
- D. spyware
- E. rootkits
- F. backdoor
- G. None of the choices.

Answer: F ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

A backdoor is a method of bypassing normal authentication procedures.

Many computer manufacturers used to preinstall backdoors on their systems to provide technical support for customers. Hackers typically use backdoors to secure remote access to a computer, while attempting to remain hidden from casual inspection. To install backdoors, hackers prefer to use either Trojan horse or computer worm.

NEW QUESTION: 776

Which of the following organizational functions is MOST appropriate to monitor the budget associated with an IT project?

- A. IT strategy committee
- B. Risk committee
- C. IT steering committee
- D. Executive committee

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 777

Which of the following should be used to assess the level of security required to protect information on a corporate network?

- A. Access rights
- B. Data classification
- C. Access control matrix
- D. Business intelligence

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 778

An IS auditor should be MOST concerned with what aspect of an authorized honeypot?

- A. The data collected on attack methods
- B. The information offered to outsiders on the honeypot
- C. The risk that the honeypot could be used to launch further attacks on the organization's infrastructure
- D. The risk that the honeypot would be subject to a distributed denial-of-service attack

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Choice C represents the organizational risk that the honeypot could be used as a point of access to launch further attacks on the enterprise's systems. Choices A and B are purposes for deploying a honeypot, not a concern. Choice D, the risk that the honeypot would be subject to a distributed denial-of-service (DDoS) attack, is not relevant, as the honeypot is not a critical device for providing service.

NEW QUESTION: 779

In a review of the organization standards and guidelines for IT management, which of the following should be included in an IS development methodology?

- A. Access control rules
- B. Risk management techniques
- C. Value-added activity analysis
- D. Incident management techniques

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 780

What is the MAIN objective when implementing security controls within an application?

- A. To optimize user functionality of the application
- B. To minimize reputational risk to the organization
- C. To optimize the level of Data protection achieved against cost
- D. To minimize the exposure to the fullest extent possible

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 781

A transaction processing system interfaces with the general ledger. Data analytics has identified that some transactions are being recorded twice in the general ledger. While management states a system fix has been implemented, what should the IS auditor recommend to validate the interface is working in the future?

- A. Ensure system owner sign-off for the system fix.
- B. Improve user acceptance testing (UAT).
- C. Perform periodic reconciliations.
- D. Conduct functional testing.

Answer: ([SHOW ANSWER](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 782

Which of the following is a method to prevent disclosure of classified documents printed on a shared printer?

- A. Using passwords to allow authorized users to send documents to the printer
- B. Requiring a key code to be entered on the printer to produce hard copy
- C. Encrypting the data stream between the user's computer and the printer
- D. Producing a header page with classification level for printed documents

Answer: ([SHOW ANSWER](#))

Requiring a key code to be entered on the printer to produce hard copy is a method to prevent disclosure of classified documents printed on a shared printer. This is because requiring a key code adds an extra layer of security and authentication to the printing process, ensuring that only authorized users can access and retrieve the printed documents. Requiring a key code also prevents unauthorized users from viewing or tampering with the documents while they are in the printer's queue or output tray¹.

Using passwords to allow authorized users to send documents to the printer is not a sufficient method to prevent disclosure of classified documents printed on a shared printer. This is because passwords only protect the transmission of the documents from the user's computer to the printer, but they do not protect the documents once they are printed. Passwords can also be compromised or forgotten by users, making them vulnerable to unauthorized access or denial of service².

Encrypting the data stream between the user's computer and the printer is not a sufficient method to prevent disclosure of classified documents printed on a shared printer. This is because encryption only protects the confidentiality and integrity of the documents while they are in transit, but they do not protect the documents once they are printed. Encryption can also introduce performance issues or compatibility problems with different printers or devices².

Producing a header page with classification level for printed documents is not a method to prevent disclosure of classified documents printed on a shared printer. This is because producing a header page only informs the users about the sensitivity and handling of the documents, but it does not prevent unauthorized users from accessing or viewing them. Producing a header page can also waste paper and ink, as well as increase the risk of misplacing or mixing up the documents

NEW QUESTION: 783

While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The MOST important concern for an IS auditor is the:

- A.** effectiveness of the QA function because it should interact between project management and user management
- B.** efficiency of the QA function because it should interact with the project implementation team.
- C.** effectiveness of the project manager because the project manager should interact with the QA function.
- D.** efficiency of the project manager because the QA function will need to communicate with the project implementation team.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

To be effective the quality assurance (QA) function should be independent of project management. The QA function should never interact with the project implementation team since this can impact effectiveness.

The project manager does not interact with the QA function, which should not impact the effectiveness of the project manager. The QA function does not interact with the project implementation team, which should not impact the efficiency of the project manager.

NEW QUESTION: 784

An IS auditor is reviewing the business requirements for the deployment of a new website Which of the following cryptographic systems would provide the BEST evidence of secure communications on the internet?

- A.** IP Security (IPSEC)
- B.** Transport Layer Security (TLS)
- C.** Wi-Fi Protected Access 2 (WPA2)
- D.** Secure Shell (SSH)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 785

An example of a direct benefit to be derived from a proposed IT-related business investment is:

- A. enhanced reputation.
- B. enhanced staff morale.
- C. the use of new technology.
- D. increased market penetration.

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

A comprehensive business case for any proposed IT-related business investment should have clearly defined business benefits to enable the expected return to be calculated. These benefits usually fall into two categories: direct and indirect, or soft. Direct benefits usually comprise the quantifiable financial benefits that the new system is expected to generate. The potential benefits of enhanced reputation and enhanced staff morale are difficult to quantify, but should be quantified to the extent possible. IT investments should not be made just for the sake of new technology but should be based on a quantifiable business need.

NEW QUESTION: 786

An IS auditor should be aware of various analysis models used by data architecture. Which of the following analysis model outline the major process of an organization and the external parties with which business interacts?

- A. Context Diagrams
- B. Activity Diagrams
- C. Swim-lane diagrams
- D. Entity relationship diagrams

Answer: A ([LEAVE A REPLY](#))

Section: Information System Acquisition, Development and Implementation Explanation:

Context diagram - Outline the major processes of an organization and the external parties with which business interacts.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.

To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components The enterprise data flow architecture

(EDFA) A logical data architecture Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer - This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced score cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data - Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data - Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data - Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse - This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A properly constituted DW should support three basic form of an inquiry.

Drilling up and drilling down - Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across - Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis - The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer - This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer - This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer - This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to pre-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies

patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer - The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer - This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer - This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram - De-construct business processes.

Entity relationship diagram - Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Context diagram - Outline the major processes of an organization and the external parties with which business interacts.

Activity or swim-lane diagram - De-construct business processes.

Reference:

CISA review manual 2014 Page number 188

NEW QUESTION: 787

Which of the following would be of GREATEST concern to an IS auditor reviewing backup and recovery controls?

- A. Backup procedures are not documented
- B. Backups are stored in an external hard drive
- C. Weekly and monthly backups are stored onsite
- D. Restores from backups are not periodically tested

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 788

Which of the following statement INCORRECTLY describes the Control self-assessment (CSA) approach?

- A. CSA is policy or rule driven
- B. CSA Empowered/accountable employees
- C. CSA focuses on continuous improvement/learning curve
- D. In CSA, Staffs at all level, in all functions, are the primary control analyst.

Answer: (SHOW ANSWER)

Section: The process of Auditing Information System

Explanation:

The word INCORRECTLY is the keyword used in the question. You need to find out an option which

incorrectly describes Control Self-assessment.

For your exam you should know the information below about control self-assessment:

Control self-assessment is an assessment of controls made by the staff and management of the unit or

units involved. It is a management technique that assures stakeholders, customers and other parties that

the internal controls of the organization are reliable.

Benefits of CSA

Early detection of risk

More efficient and improved internal controls

Creation of cohesive teams through employee involvement

Developing a sense of ownership of the controls in the employees and process owners, and reducing their

resistance to control improvement initiatives

Increased employee awareness of organizational objectives, and knowledge of risk and internal controls

Highly motivated employees

Improved audit training process

Reduction in control cost

Assurance provided to stakeholders and customers

Traditional and CSA attributes

Traditional Historical CSA

Assign duties/supervises staff Empowered/accountable employees

Policy/rule driven Continuous improvement/learning curve

Limited employee participation Extensive employee participation and training

Narrow stakeholders focus Broad stakeholders focus

Auditors and other specialist Staff at all level, in all functions, are the primary control analysts

The following answers are incorrect:

The other options specified are correctly describes about CSA.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 61, 62 and 63

NEW QUESTION: 789

An organization performs nightly backups but does not have a formal policy. An IS auditor should FIRST:

- A. evaluate current backup procedures
- B. escalate to senior management
- C. document a policy for the organization
- D. recommend automated backup

Answer: A ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

Explanation

NEW QUESTION: 790

Which of the following is the dominating objective of BCP and DRP?

- A. To protect human life
- B. To mitigate the risk and impact of a business interruption
- C. To eliminate the risk and impact of a business interruption
- D. To transfer the risk and impact of a business interruption

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Although the primary business objective of BCP and DRP is to mitigate the risk and impact of a business interruption, the dominating objective remains the protection of human life.

NEW QUESTION: 791

Which of the following approaches would present the GREATEST concern for the implementation of a quality assurance (QA) function?

- A. Developers introducing the changes will review the work, as they are most familiar with them.
- B. Peer developers from the same development team who are unfamiliar with the changes will review them.
- C. Developers from a separate development team in the organization will review the submitted changes.
- D. Reviewers outside the development group who do not have development roles will review the changes.

Answer: A ([LEAVE A REPLY](#))

Comprehensive and Detailed Step-by-Step Explanation:

A strong QA function requires an independent review of changes to avoid bias and ensure objectivity.

* Option A (Correct): If developers review their own changes, there is a high risk of bias and overlooking issues, making this the greatest concern. This violates separation of duties and best practices for quality assurance.

* Option B (Incorrect): Peer reviews within the same team reduce risks since fresh eyes review the changes, though it is not as strong as an external review.

* Option C (Incorrect): Having developers from a separate team review the code provides better objectivity and reduces risks associated with self-review.

* Option D (Incorrect): While non-developers may lack technical expertise, their review ensures independence, making it a stronger control than self-review.

Reference: ISACA CISA Review Manual - Domain 3: Information Systems Acquisition, Development, and Implementation - Covers quality assurance, code reviews, and segregation of duties.

NEW QUESTION: 792

Is it appropriate for an IS auditor from a company that is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?

- A.** Yes, because an IS auditor will evaluate the adequacy of the service bureau's plan and assist their company in implementing a complementary plan.
- B.** Yes, because based on the plan, an IS auditor will evaluate the financial stability of the service bureau and its ability to fulfill the contract.
- C.** No, because the backup to be provided should be specified adequately in the contract.
- D.** No, because the service bureau's business continuity plan is proprietary information.

Answer: [\(SHOW ANSWER\)](#)

The primary responsibility of an IS auditor is to assure that the company assets are being safeguarded. This is true even if the assets do not reside on the immediate premises. Reputable service bureaus will have a well-designed and tested business continuity plan.

NEW QUESTION: 793

An IS auditor is evaluating controls for monitoring the regulatory compliance of a third party that provides IT services to the organization. Which of the following should be the auditor's GREATEST concern?

- A.** The organization has not communicated regulatory requirements to the third party.
- B.** The organization has not reviewed the third party's policies and procedures.
- C.** The third-party disclosed a policy-related issue of noncompliance.
- D.** A gap analysis against regulatory requirements has not been conducted.

Answer: **A** [\(LEAVE A REPLY\)](#)

NEW QUESTION: 794

An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. What would be the next task?

- A.** Report the risks to the CIO and CEO immediately
- B.** Examine e-business application in development
- C.** Identify threats and likelihood of occurrence
- D.** Check the budget available for risk management

Answer: **C** [\(LEAVE A REPLY\)](#)

Section: Protection of Information Assets

Explanation:

An IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence. Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.

NEW QUESTION: 795

An internal audit team is deciding whether to use an audit management application hosted by a third party in a different country.

What should be the MOST important consideration related to the uploading of payroll audit documentation in the hosted application?

- A.** Financial regulations affecting the organization
- B.** Data center physical access controls where the application is hosted
- C.** Privacy regulations affecting the organization
- D.** Per-unit cost charged by the hosting services provider for storage

Answer: C ([LEAVE A REPLY](#))

Explanation

This is because privacy regulations are laws or rules that protect the personal information of individuals from unauthorized access, use, disclosure, or transfer by third parties. Payroll audit documentation may contain sensitive and confidential data, such as employee names, salaries, benefits, taxes, deductions, and bank accounts. If the audit management application is hosted by a third party in a different country, the organization may need to comply with the privacy regulations of both its own country and the host country, as well as any international or regional agreements or frameworks that apply. Privacy regulations may impose various requirements and obligations on the organization, such as obtaining consent from the data subjects, implementing appropriate security measures, notifying data breaches, and ensuring data quality and accuracy. Privacy regulations may also grant various rights to the data subjects, such as accessing, correcting, deleting, or transferring their data. Failing to comply with privacy regulations may expose the organization to significant risks and consequences, such as legal actions, fines, sanctions, reputational damage, or loss of trust.

Some examples of privacy regulations affecting the organization are:

The General Data Protection Regulation (GDPR), which is a comprehensive and strict privacy regulation that applies to any organization that processes personal data of individuals in the European Union (EU) or offers goods or services to them, regardless of where the organization or the data is located¹.

The California Consumer Privacy Act (CCPA), which is a broad and influential privacy regulation that applies to any organization that collects personal information of California residents and meets certain thresholds of revenue, data volume, or data sharing².

The Health Insurance Portability and Accountability Act (HIPAA), which is a sector-specific privacy regulation that applies to any organization that handles protected health information (PHI)

of individuals in the United States, such as health care providers, health plans, or health care clearinghouses³.

Therefore, before using an audit management application hosted by a third party in a different country, the internal audit team should conduct a thorough assessment of the privacy regulations affecting the organization and ensure that they have adequate policies, procedures, and controls in place to comply with them.

NEW QUESTION: 796

Establishing data ownership is an important first step for which of the following processes?

- A. Assigning user access privileges
- B. Developing organizational security policies
- C. Creating roles and responsibilities
- D. Classifying data

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

To properly implement data classification, establishing data ownership is an important first step.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 797

Which of the following access rights in the production environment should be granted to a developer to maintain segregation of duties?

- A. System administration
- B. Database administration
- C. IT operations
- D. Emergency support

Answer: D (LEAVE A REPLY)

NEW QUESTION: 798

As an auditor it is very important to ensure confidentiality, integrity, authenticity and availability are implemented appropriately in an information system. Which of the following definitions incorrectly describes

these parameters?

1. Authenticity - A third party must be able to verify that the content of a message has been sent by a specific entity and nobody else.
 2. Non-repudiation - The origin or the receipt of a specific message must be verifiable by a third party. A person cannot deny having sent a message if the message is signed by the originator.
 3. Accountability - The action of an entity must be uniquely traceable to different entities
 4. Availability - The IT resource must be available on a timely basis to meet mission requirements or to avoid substantial losses.
- A.** All of the options presented
B. None of the options presented
C. Options number 1 and 2
D. Option number 3

Answer: D (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation/Reference:

It is important to read carefully the question. The word "incorrectly" was the key word. You had to find which

one of the definitions presented is incorrect. The definition of Accountability was NOT properly described.

Below you have the proper definition.

The correct definitions are as follows

Authenticity - A third party must be able to verify that the content of a message is from a specific entity and nobody else.

Non-repudiation - The origin or the receipt of a specific message must be verifiable by a third party. A

person cannot deny having sent a message if the message is signed by the originator.

Accountability - The action of an entity must be uniquely traceable to that entity

Network availability - The IT resource must be available on a timely basis to meet mission requirements or to avoid substantial losses.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 34

NEW QUESTION: 799

An IS auditor is evaluating the risk associated with moving from one database management system (DBMS) to another. Which of the following would be MOST helpful to ensure the integrity of the system throughout the change?

- A. Preserving the same data classifications
- B. Preserving the same data inputs
- C. Preserving the same data structure
- D. Preserving the same data interfaces

Answer: ([SHOW ANSWER](#))

Explanation

The most helpful thing to ensure the integrity of the system throughout the change when moving from one database management system (DBMS) to another is preserving the same data structure. A DBMS is a software system that manages and manipulates data stored in a database, such as creating, updating, querying, deleting, etc. A database is a collection of structured or organized data that can be accessed or manipulated by a DBMS.

A data structure is a way of organizing or arranging data in a database, such as tables, columns, rows, keys, indexes, etc. Preserving the same data structure when moving from one DBMS to another can help ensure the integrity of the system throughout the change, by maintaining the consistency and accuracy of data in the database, and avoiding any errors or issues that may arise from incompatible or inconsistent data structures between different DBMSs. Preserving the same data classifications is a possible thing to ensure the integrity of the system throughout the change when moving from one DBMS to another, but it is not the most helpful one.

Data classifications are categories or labels that define the level of sensitivity or importance of data in a database, such as public, confidential, secret, etc. Data classifications can help protect the security and privacy of data in the database by applying appropriate controls or restrictions on data access or use based on their classifications. Preserving the same data classifications when moving from one DBMS to another can help ensure the integrity of the system throughout the change by preventing unauthorized or inappropriate access or use of data in the database.

However, this may not be directly related to the DBMS change, as it may apply to any data migration or transfer process. Preserving the same data inputs is a possible thing to ensure the integrity of the system throughout the change when moving from one DBMS to another, but it is not the most helpful one. Data inputs are sources or methods that provide data to a database, such as user inputs, sensors, files, etc. Data inputs can affect the quality and validity of data in the database by introducing errors or inconsistencies in data entry or collection. Preserving the same data inputs when moving from one DBMS to another can help ensure the integrity of the system throughout the change by reducing errors or inconsistencies in data input or collection.

NEW QUESTION: 800

An organization outsources its payroll function to a third-party service provider. Which of the following is MOST important for an IS auditor to verify when reviewing the outsourcing agreement?

- A. The provider aligns with payroll industry best practices.
- B. The provider has an extensive security training program.
- C. The provider has agreed to a right-to-audit clause.
- D. The provider has a good service reputation.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 801

To reduce operational costs, IT management plans to reduce the number of servers currently used to run business applications. Which of the following is MOST helpful to review when identifying which servers are no longer required?

- A.** Performance feedback from the user community
- B.** Contract with the server vendor
- C.** Server CPU usage trends
- D.** Mean time between failure (MTBF) of each server

Answer: C ([LEAVE A REPLY](#))

Explanation

When identifying which servers are no longer required, reviewing server CPU usage trends is the most helpful approach. Monitoring the CPU usage over time provides insights into how actively a server is being utilized.

Servers with consistently low CPU usage may be candidates for consolidation or decommissioning. By analyzing CPU utilization patterns, IT management can make informed decisions about which servers can be retired without impacting performance or availability¹.

References:

ISACA. "Technical Guide on IT Migration Audit." 1

(<http://kb.icai.org/pdfs/PDFFile5b278a12a66758.27269499.pdf>)

Zapier. "IT audit: The ultimate guide [with checklist]." 2(<https://zapier.com/blog/it-audit/>) ISACA.

"CISA Certification | Certified Information Systems Auditor."

3(<https://www.isaca.org/credentialing/cisa>)

NEW QUESTION: 802

Which of the following is MOST important to determine when conducting an audit Of an organization's data privacy practices?

- A.** Whether a disciplinary process is established for data privacy violations
- B.** Whether strong encryption algorithms are deployed for personal data protection
- C.** Whether privacy technologies are implemented for personal data protection
- D.** Whether the systems inventory containing personal data is maintained

Answer: D ([LEAVE A REPLY](#))

The systems inventory containing personal data is a crucial element for auditing an organization's data privacy practices. The systems inventory is a list of all the systems, applications, databases, and devices that collect, store, process, or transmit personal data within the organization¹². The systems inventory helps the auditor to identify the scope, location, ownership, and classification of personal data, as well as the risks and controls associated with them¹². The systems inventory also helps the auditor to verify compliance with data privacy laws, regulations, and internal policies that apply to different types of personal data

NEW QUESTION: 803

Electrical surge protectors BEST

- A. sags and spikes
- B. reduced voltage.
- C. power outages.
- D. electromagnetic interference.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 804

Which of the following provides a new IS auditor with the MOST useful information to evaluate overall IT performance?

- A. Vulnerability assessment report
- B. IT balanced scorecard
- C. IT value analysis
- D. Prior audit reports

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 805

Which of the following threats is MOST effectively controlled by a firewall?

- A. Network congestion
- B. Denial of service (DoS) attack
- C. Network sniffing
- D. Password cracking

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

NEW QUESTION: 806

An IS auditor notes that due to the small size of the organization, human resources staff can create new employees in the payroll system as well as process payroll. Which of the following is the BEST recommendation to address this situation?

- A. Implement a periodic user access review over the payroll system.
- B. Hire additional staff so that access for the two functions can be segregated.
- C. Outsource the processing of payroll to a third party.
- D. Implement periodic reviews of employees in the payroll system.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 807

During an audit of an organization's risk management practices, an IS auditor finds several documented IT risk acceptances have not been renewed in a timely manner after the assigned expiration date. When assessing the severity of this finding, which mitigating factor would MOST significantly minimize the associated impact?

- A. The business environment has not significantly changed since the risk acceptances were approved.
- B. The risk acceptances were previously reviewed and approved by appropriate senior management.
- C. The risk acceptances with issues reflect a small percentage of the total population.
- D. There are documented compensating controls over the business processes.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 808

Which of the following is the PRIMARY reason for an IS auditor to issue an interim audit report?

- A. To enable the auditor to complete the engagement in a timely manner
- B. To avoid issuing a final audit report
- C. To provide feedback to the auditee for timely remediation
- D. To provide follow-up opportunity during the audit

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 809

Which of the following is the BEST way to reduce the risk of vulnerabilities introduced by rapid deployment of applications?

- A. Conduct a post-deployment security audit to identify vulnerabilities.
- B. Perform security audits during the development life cycle.
- C. Review a sample of historical production changes to identify abnormalities.
- D. Review change management policies and procedures.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 810

Which of the following access control situations represents the MOST serious control weakness?

- A. End users have access to program development tools.
- B. System developers have access to production data
- C. Programmers have access to development hardware
- D. Computer operators have access to system level flowcharts

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 811

When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

- A. incorporates state of the art technology.
- B. addresses the required operational controls.
- C. articulates the IT mission and vision.
- D. specifies project management practices.

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not address the technology, operational controls or project management practices.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 812

Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures. True or false?

- A. True
- B. False

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

Fourth-generation languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures.

NEW QUESTION: 813

When planning an audit of a network setup, an IS auditor should give highest priority to obtaining which of the following network documentation?

- A. Wiring and schematic diagram
- B. Users' lists and responsibilities
- C. Application lists and their details
- D. Backup and recovery procedures

Answer: A ([LEAVE A REPLY](#))

The wiring and schematic diagram of the network is necessary to carry out a network audit. A network audit may not be feasible if a network wiring and schematic diagram is not available. All other documents are important but not necessary.

NEW QUESTION: 814

Which of the following is the BEST way for an IS auditor to determine whether an organization's disaster recovery plan (DRP) is current?

- A. Verify the DRP identifies appropriate staff with up-to-date contact details.
- B. Review critical system documentation and related recovery time objectives (RTOs).
- C. Verify the DRP is periodically tested.
- D. Ensure all staff is trained on business continuity.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 815

In wireless communication, which of the following controls allows the device receiving the communications to verify that the received communications have not been altered in transit?

- A. Device authentication and data origin authentication
- B. Wireless intrusion detection (IDS) and prevention systems (IPS)
- C. The use of cryptographic hashes
- D. Packet headers and trailers

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation

Explanation:

Calculating cryptographic hashes for wireless communications allows the device receiving the communications to verify that the received communications have not been altered in transit. This prevents masquerading and message modification attacks. Device authentication and data origin authentication is not the correct answer since authenticating wireless endpoints to each other prevents man-in-the-middle attacks and masquerading. Wireless IDS/IPSs is not the correct answer since wireless IDS/IPS have the ability to detect misconfigured devices and rogue devices, and detect and possibly stop certain types of attacks. Packet headers and trailers alone do not ensure that the content has not been altered.

NEW QUESTION: 816

As part of business continuity planning, which of the following is MOST important to assess when conducting a business impact analysis (BIA)?

- A. Recovery scenarios
- B. Risk appetite
- C. Completeness of critical asset inventory
- D. Critical applications in the cloud

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 817

Which of the following is a core functionality of a configuration and release management system?

- A. Managing privileged access to databases, servers, and infrastructure
- B. Identifying other configuration items that will be impacted by a given change
- C. Identifying vulnerabilities in configuration settings
- D. Deploying a configuration change to the sandbox environment

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 818

A bank is selecting a server for its retail accounts application. To ensure that the server can handle a high volume of transactions with the required response times, which test should the IS auditor recommend?

- A. Regression
- B. Acceptance
- C. Benchmark
- D. Integration

Answer: C ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

Explanation/Reference:

NEW QUESTION: 819

An IS auditor performing an application development review attends development team meetings. The IS auditor's independence will be compromised if the IS auditor:

- A. assists in developing an integrated test facility on the system.
- B. re-performs test procedures used by the development team.
- C. designs and executes the user's acceptance test plan.
- D. reviews the result of systems tests that were performed by the development team.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 820

Which of the following are designed to detect network attacks in progress and assist in post-attack forensics?

- A. Intrusion Detection Systems
- B. Audit trails
- C. System logs
- D. Tripwire
- E. None of the choices.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

Intrusion Detection Systems are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.

NEW QUESTION: 821

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 ([LEAVE A REPLY](#))

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)

NEW QUESTION: 822

When an IS audit reveals that a firewall was unable to recognize a number of attack attempts the auditor's BEST recommendation is to place an Intrusion detection system ID between the firewall and:

- A. the Internet.
- B. the organization's web server.
- C. the organization's network
- D. the demilitarized zone(DMZ).

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 823

A small organization is experiencing rapid growth and plans to create a new information security policy.

Which of the following is MOST relevant to creating the policy?

- A. Previous audit recommendations
- B. Industry standards
- C. The business objectives
- D. The business impact analysis (BIA)

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 824

Which of the following should be reviewed FIRST when planning an IS audit?

- A. Recent financial information
- B. Annual business unit budget
- C. IS audit standards
- D. The business environment

Answer: (SHOW ANSWER)

Section: The process of Auditing Information System

NEW QUESTION: 825

During the review of a data conversion process for a retail application, an IS auditor noticed changes were made to a price listing. Whose approval is MOST appropriate for these changes?

- A. System analyst
- B. Marketing manager
- C. Warehouse manager

D. Business owner

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 826

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

- A. Hashing algorithms ensure data confidentiality.
- B. Hashing algorithms are irreversible.
- C. Encryption algorithms ensure data integrity.
- D. Encryption algorithms are not irreversible.

Answer: B ([LEAVE A REPLY](#))

A key distinction between encryption and hashing algorithms is that hashing algorithms are irreversible.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 827

.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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 828

Which of the following risks is BEST mitigated by implementing an automated three-way match?

- A. Inaccurate customer records
- B. Inaccurate customer discounts
- C. Invalid payment processing
- D. Purchase order delays

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 829

Which of the following attack involves sending forged ICMP Echo Request packets to the broadcast address on multiple gateways in order to illicit responses from the computers behind the gateway where they all respond back with ICMP Echo Reply packets to the source IP address of the ICMP Echo Request packets?

- A. Reflected attack
- B. Brute force attack
- C. Buffer overflow
- D. Pulsing Zombie

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Reflected attack involves sending forged requests to a large number of computers that will reply to the requests. The source IP address is spoofed to that of the targeted victim, causing replies to flood.

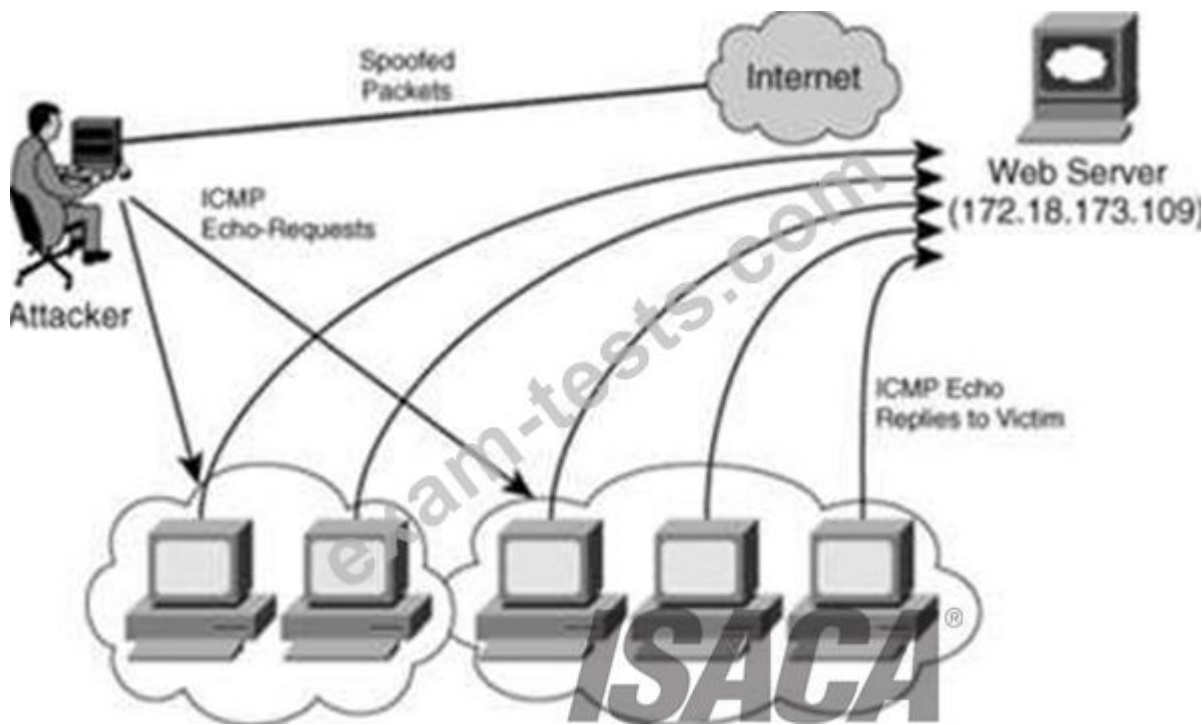
A distributed denial of service attack may involve sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet Protocol address spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target.

(This reflected attack form is sometimes called a "DRDOS".

ICMP Echo Request attacks (Smurf Attack) can be considered one form of reflected attack, as the flooding host(s) send Echo Requests to the broadcast addresses of mix-configured networks, thereby enticing hosts to send Echo Reply packets to the victim. Some early DDoS programs implemented a distributed form of this attack.

In the surf attack, the attacker sends an ICMP ECHO REQUEST packet with a spoofed source address to a victim's network broadcast address. This means that each system on the victim's subnet receives an ICMP ECHO REQUEST packet. Each system then replies to that request with an ICMP ECHO REPLY packet to the spoof address provided in the packets-which is the victim's address. All of these response packets go to the victim system and overwhelm it because it is being bombarded with packets it does not necessarily know how to process. The victim system may freeze, crash, or reboot. The Smurf attack is illustrated in Figure below:

surf-attack



The following answers are incorrect:

Brute force attack - Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

Buffer overflow - A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Pulsing Zombie - A Dos attack in which a network is subjected to hostile pinging by different attacker computer over an extended time period.

Reference:

CISA review manual 2014 Page number 322

NEW QUESTION: 830

As an IS auditor it is very important to understand software release management process. Which of the following software release normally contains small enhancements and fixes?

- A. Major software Release
- B. Minor software Release
- C. Emergency software release
- D. General software Release

Answer: B (LEAVE A REPLY)

Section: Information System Operations, Maintenance and Support

Explanation:

Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place.

For example, version

6.10 would change to version 6.20.

For CISA exam you should know below information about software release management:

Software Release Management is the process of ensuring releases can be reliably planned, scheduled and successfully transitioned (deployed) to Test and Live Environments. Software Release Management is not just about "automating the path to production" although that is certainly an important part. It also about adopting a holistic view of application changes, using the "Release" as the container to ensure that changes are packaged, released and tested in a repeatable and controlled manner. Release Management is often likened to the conductor of an orchestra, with the individual changes to be implemented the various instruments within it. Software Release Management is intrinsically linked with the more well understood and adopted Software Change and Configuration Management disciplines.

Software Release management is a process through which software is made available to user.

Each update or upgrade of a Configuration Item is referred to as a release.

There are three levels of releases. These levels related to releasing hardware or software into your IT infrastructure. Some may be a single change, others may implement many changes at a time.

Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.

Minor - Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

The following were incorrect answers:

Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

General software Release - Not a valid type of software release.

Reference:

CISA review manual 2014 Page number 244

NEW QUESTION: 831

When verifying the accuracy and completeness of migrated data for a new application system replacing a legacy system. It is MOST effective for an IS auditor 10 review;

- A. audit trails
- B. acceptance lasting results
- C. rollback plans
- D. data analytics findings.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 832

Which of the following should an IS auditor consider FIRST when evaluating firewall rules?

- A. The physical location of the firewalls
- B. The number of remote nodes
- C. The firewalls' default settings
- D. The organization's security policy

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 833

An IS auditor issues an audit report pointing out the lack of firewall protection features at the perimeter network gateway and recommends a vendor product to address this vulnerability. The IS auditor has failed to exercise:

- A. professional independence
- B. organizational independence.
- C. technical competence.
- D. professional competence.

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

When an IS auditor recommends a specific vendor, they compromise professional independence. Organizational independence has no relevance to the content of an audit report and should be considered at the time of accepting the engagement. Technical and professional competence is not relevant to the requirement of independence.

NEW QUESTION: 834

The independence of an IS auditor auditing an application is maintained if the auditor's role is limited to:

- A. creating system specifications.
- B. defining user requirements.
- C. recommending system enhancements.
- D. designing access control rules.

Answer: B ([LEAVE A REPLY](#))

Section: The process of Auditing Information System

NEW QUESTION: 835

Which of the following is the MOST effective control to ensure electronic records beyond their retention periods are deleted from IT systems?

- A. Perform a sample check of current data against the retention schedule.
- B. Review the record retention register regularly to initiate data deletion.
- C. Build in system logic to trigger data deletion at predefined times.
- D. Execute all data deletions at a predefined month during the year.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 836

An organization has implemented a disaster recovery plan. Which of the following steps should be carried out next?

- A. Obtain senior management sponsorship.
- B. Identify business needs.
- C. Conduct a paper test.
- D. Perform a system restore test.

Answer: C ([LEAVE A REPLY](#))

A best practice would be to conduct a paper test. Senior management sponsorship and business needs identification should have been obtained prior to implementing the plan. A paper test should be conducted first, followed by system or full testing.

NEW QUESTION: 837

A CFO has requested an audit of IT capacity management due to a series of finance system slowdowns during month-end reporting. What would be MOST important to consider before including this audit in the program?

- A. Whether system delays result in more frequent use of manual processing
- B. Whether the system's performance poses a significant risk to the organization
- C. Whether stakeholders are committed to assisting with the audit
- D. Whether internal auditors have the required skills to perform the audit

Answer: B ([LEAVE A REPLY](#))

The most important thing to consider before including an audit of IT capacity management in the program is whether the system's performance poses a significant risk to the organization. IT capacity management is a process that ensures that IT resources are sufficient to meet current and future business needs, and that they are optimized for cost and performance. A poor IT capacity management can result in system slowdowns, outages, failures, or breaches, which can affect the availability, reliability, security, and efficiency of IT services and business processes. Therefore, before conducting an audit of IT capacity management, the auditor should assess the potential impact and likelihood of these risks on the organization's objectives, reputation, compliance, and customer satisfaction.

Whether system delays result in more frequent use of manual processing (option A) is not the most important thing to consider before including an audit of IT capacity management in the program, as it is only one possible consequence of poor IT capacity management. Manual processing can introduce errors, delays, inefficiencies, and inconsistencies in the data and reports, which can affect the quality and accuracy of financial information. However, manual processing is not the only or the worst outcome of poor IT capacity management; there may be other more severe or frequent risks that need to be considered.

Whether stakeholders are committed to assisting with the audit (option C) is also not the most important thing to consider before including an audit of IT capacity management in the program, as it is a factor that affects the feasibility and effectiveness of the audit, not the necessity or priority of it. Stakeholder commitment is important for ensuring that the auditor has access to relevant information, documents, data, and personnel, as well as for facilitating communication, collaboration, and feedback during the audit process. However, stakeholder commitment is not a sufficient reason to conduct an audit of IT capacity management; there must be a clear risk-based rationale for selecting this area for audit.

Whether internal auditors have the required skills to perform the audit (option D) is also not the most important thing to consider before including an audit of IT capacity management in the program, as it is a factor that affects the quality and credibility of the audit, not the urgency or importance of it. Internal auditors should have the appropriate knowledge, skills, and experience to perform an audit of IT capacity management, which may include technical, business, analytical, and communication skills. However, internal auditors can also acquire or supplement these skills through training, coaching, consulting, or outsourcing. Therefore, internal auditors' skills are not a decisive factor for choosing this area for audit.

Therefore, option B is the correct answer.

References:

- * Guide to IT Capacity Management | Smartsheet
- * ISO 27001 capacity management: How to implement control A.12.1.3 - Advisera
- * ISO 27002:2022 - Control 8.6 - Capacity Management

NEW QUESTION: 838

Which of the following is the BEST way to address potential data privacy concerns associated with inadvertent disclosure of machine identifier information contained within security logs?

- A.** Only collect logs from servers classified as business critical
- B.** Restrict the transfer of log files from host machine to online storage
- C.** Limit log collection to only periods of increased security activity
- D.** Limit the use of logs to only those purposes for which they were collected

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 839

Which of the following statement correctly describes the difference between total flooding and local application extinguishing agent?

- A.** The local application design contain physical barrier enclosing the fire space where as physical barrier is not present in total flooding extinguisher
- B.** The total flooding design contain physical barrier enclosing the fire space where as physical barrier is not present in local application design extinguisher
- C.** The physical barrier enclosing fire space is not present in total flooding and local application extinguisher agent
- D.** The physical barrier enclosing fire space is present in total flooding and local application extinguisher agent

Answer: (SHOW ANSWER)

Explanation/Reference:

For CISA exam you should know below information about Fire Suppression Systems Fire Suppression System

These system are designed to automatically activate immediately after detection of heat, typically generated by fire. Like smoke detectors, the system will produce an audible alarm when activated and be linked to a central guard station that is regularly monitored. The system should also be inspected and tested annually. Testing interval should comply with industry and insurance standard and guideline.

Broadly speaking there are two methods for applying an extinguisher agent: total flooding and local application.

Total Flooding - System working under total flooding application apply an extinguishing agent to a three dimensional enclosed space in order to achieve a concentration of the agent (volume percentage of agent in air) adequate to extinguish the fire. These type of system may be operated automatically by detection and related controls or manually by the operation of a system actuator.

Local Application - System working under a local application principle apply an extinguishing agent directly onto a fire (usually a two dimensional area) or into a three dimensional region immediately surrounding the substance or object on a fire. The main difference between local application and total flooding design is the absence of physical barrier enclosing the fire space in the local application design.

The medium of fire suppression varies but usually one of the following:

Water based systems are typically referred to as sprinkler system. These systems are effective but are also unpopular because they damage equipment and property. The system can be dry-pipe or charged (water is always in system piping). A charged system is more reliable but has the disadvantage of exposing the facility to expensive water damage if the pipe leak or break.

Dry-pipe sprinkling system do not have water in the pipe until an electronic fire alarm activates the water to send water into system. This is opposed to fully charged water pipe system. Dry-pipe system has the advantage that any failure in the pipe will not result in water leaking into sensitive equipment from above.

Since water and electricity do not mix these systems must be combined with an automatic switch to shut down the electric supply to the area protected.

Holon system releases pressurize halos gases that removes oxygen from air, thus starving the fire. Holon was popular because it is an inert gas and does not damage and does not damage

equipment like water does. Because halos adversely affect the ozone layer, it was banned in Montreal (Canada) protocol 1987, which stopped Holon production as of 1 January 1994. As a banned gas, all Holon installation are now required by international agreement to be removed. The Holon substitute is FM-200, which is the most effective alternative.

FM-220TM: Also called heptafluoropropane, HFC-227 or HFC-227ea(ISO Name)is a colorless odorless gaseous fire suppression agent. It is commonly used as a gaseous fire suppression agent.

Aragonite is the brand name for a mixture of 50% argon and 50% nitrogen. It is an inert gas used in gaseous fire suppression systems for extinguishing fires where damage to equipment is to be avoided.

Although argon is a nontoxic, it does not satisfy the body's need for oxygen and is simple asphyxiate.

CO2 system releases pressurized carbon dioxide gas into the area protected to replace the oxygen required for combustion. Unlike halos and its later replacement, however, CO2 is unable to sustain human life. Therefore, in most of countries it is illegal to for such a system to be set to automatic release if any human may be in the area. Because of this, these systems are usually discharged manually, introducing an additional delay in combating fire.

The following were incorrect answers:

The other presented options do not describe valid difference between total flooding and local application extinguishing agent.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number373 and 374

NEW QUESTION: 840

The sophistication and formality of IS audit programs may vary significantly depending on which of the following factors?

- A. the target's management hands-on involvement.
- B. the target's location.
- C. the target's size and complexity.
- D. the target's budget.
- E. the target's head count.
- F. None of the choices.

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Properly planned risk-based audit programs shall increase audit efficiency and effectiveness. The sophistication and formality of this kind of audit do vary a lot depending on the target's size and complexity.

NEW QUESTION: 841

Which of the following controls BEST provides confidentiality and nonrepudiation for an online business looking for digital payment data security?

- A. Data Encryption Standard (DES)
- B. Advanced Encryption Standard (AES)
- C. Public Key Infrastructure (PKI)
- D. Virtual Private Network (VPN)

Answer: (SHOW ANSWER)

Comprehensive and Detailed Step-by-Step Explanation:

For online payment security, both confidentiality (protection of data) and nonrepudiation (ensuring the sender cannot deny a transaction) are essential.

* Option A (Incorrect): DES is outdated and insecure for modern encryption needs. It has been replaced by stronger algorithms.

* Option B (Incorrect): AES provides strong encryption (confidentiality) but does not handle nonrepudiation on its own.

* Option C (Correct): PKI (Public Key Infrastructure) is the best solution because it provides encryption for confidentiality and digital signatures for nonrepudiation, ensuring both secure transactions and authentication of parties involved.

* Option D (Incorrect): VPN secures network traffic, but it does not address nonrepudiation, which is critical in online payments.

Reference: ISACA CISA Review Manual - Domain 5: Protection of Information Assets - Covers encryption, PKI, and secure payment processing.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As

Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 842

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 (LEAVE A REPLY)

Explanation/Reference:

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.

NEW QUESTION: 843

The most common problem in the operation of an intrusion detection system (IDS) is:

- A. the detection of false positives.
- B. receiving trap messages.
- C. reject-error rates.
- D. denial-of-service attacks.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Because of the configuration and the way IDS technology operates, the main problem in operating IDSs is the recognition (detection) of events that are not really security incidents- false positives, the equivalent of a false alarm. An IS auditor needs to be aware of this and should check for implementation of related controls, such as IDS tuning, and incident handling procedures, such as the screening process to know if an event is a security incident or a false positive. Trap messages are generated by the Simple Network Management Protocol (SNMP) agents when an important event happens, but are not particularly related to security or IDSs. Reject-error rate is related to biometric technology and is not related to IDSs. Denial-of-service is a type of attack and is not a problem in the operation of IDSs.

NEW QUESTION: 844

An IS auditor is reviewing the process followed in identifying and prioritizing the critical business processes.

This process is part of the:

- A. operations component of the business continuity plan (BCP).
- B. business impact analysis (BIA).
- C. balanced scorecard.
- D. enterprise risk management plan.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 845

What must an IS auditor understand before performing an application audit?

- A. The potential business impact of application risks.
- B. Application risks must first be identified.
- C. Relative business processes.
- D. Relevant application risks.

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

An IS auditor must first understand relative business processes before performing an application audit.

NEW QUESTION: 846

A top-down approach to the development of operational policies will help ensure:

- A. that they are consistent across the organization.
- B. that they are implemented as a part of risk assessment.
- C. compliance with all policies.
- D. that they are reviewed periodically.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Deriving lower level policies from corporate policies {a top-down approach} aids in ensuring consistency

across the organization and consistency with other policies. The bottom-up approach to the development of

operational policies is derived as a result of risk assessment. A top-down approach of itself does not

ensure compliance and development does not ensure that policies are reviewed.

NEW QUESTION: 847

A data center's physical access log system captures each visitor's identification document numbers along with the visitor's photo. Which of the following sampling methods would be MOST useful to an IS auditor conducting compliance testing for the effectiveness of the system?

- A. Quota sampling
- B. Haphazard sampling
- C. Attribute sampling
- D. Variable sampling

Answer: C ([LEAVE A REPLY](#))

Attribute sampling is a method of audit sampling that is used to test the effectiveness of controls by measuring the rate of deviation from a prescribed procedure or attribute. Attribute sampling is suitable for testing compliance with the data center's physical access log system, as the auditor can compare the identification document numbers and photos of the visitors with the records in the system and determine whether there are any discrepancies or errors. Attribute sampling can also provide an estimate of the deviation rate in the population and allow the auditor to draw a conclusion about the operating effectiveness of the control.

Variable sampling, on the other hand, is a method of audit sampling that is used to estimate the amount or value of a population by measuring a characteristic of interest, such as monetary value, quantity, or size.

Variable sampling is not appropriate for testing compliance with the data center's physical access log system, as the auditor is not interested in estimating the value of the population, but rather in testing whether the system is operating as intended.

Quota sampling and haphazard sampling are both examples of non-statistical sampling methods that do not use probability theory to select a sample. Quota sampling involves selecting a sample based on certain criteria or quotas, such as age, gender, or location. Haphazard sampling involves selecting a sample without any specific plan or method. Both methods are not suitable for testing compliance with the data center's physical access log system, as they do not ensure that the sample is representative of the population and do not allow the auditor to measure the sampling risk or project the results to the population.

Therefore, attribute sampling is the most useful sampling method for an IS auditor conducting compliance testing for the effectiveness of the data center's physical access log system.

References:

* Audit Sampling - What Is It, Methods, Example, Advantage, Reason

* ISA 530: Audit sampling | ICAEW

NEW QUESTION: 848

A bank wants to outsource a system to a cloud provider residing in another country. Which of the following would be the MOST appropriate IS audit recommendation?

- A.** Find an alternative provider in the bank's home country.
- B.** Ensure the provider's internal control system meets bank requirements.
- C.** Proceed as intended, as the provider has to observe all laws of the clients countries.
- D.** Ensure the provider has disaster recovery capability.

Answer: B (LEAVE A REPLY)

The most appropriate IS audit recommendation for a bank that wants to outsource a system to a cloud provider residing in another country is to ensure the provider's internal control system meets bank requirements. This is because the cloud provider will be handling the bank's data, so it is important to ensure that the provider has appropriate controls in place to protect the data and to ensure its integrity. Additionally, the provider should have policies and procedures in place to ensure the security and privacy of the data, as well as to ensure compliance with applicable laws and regulations. For more information, please refer to the ISACA CISA Study Guide section 4.13.2.2.

NEW QUESTION: 849

Which of the following is the MOST effective control for protecting the confidentiality and integrity of data stored unencrypted on virtual machines?

- A.** Monitor access to stored images and snapshots of virtual machines.
- B.** Restrict access to images and snapshots of virtual machines.

- C. Limit creation of virtual machine images and snapshots.
- D. Review logical access controls on virtual machines regularly.

Answer: A ([LEAVE A REPLY](#))

Explanation

The most effective control for protecting the confidentiality and integrity of data stored unencrypted on virtual machines is to monitor access to stored images and snapshots of virtual machines. Images and snapshots are copies of virtual machines that can be used for backup, restoration, or cloning purposes. If data stored on virtual machines are unencrypted, they may be exposed or compromised if unauthorized or malicious users access or copy the images or snapshots. Therefore, monitoring access to stored images and snapshots can help detect and prevent any unauthorized or suspicious activities, and provide audit trails for accountability and investigation.

Restricting access to images and snapshots of virtual machines, limiting creation of virtual machine images and snapshots, and reviewing logical access controls on virtual machines regularly are not the most effective controls for protecting the confidentiality and integrity of data stored unencrypted on virtual machines. These controls may help reduce the risk or impact of data exposure or compromise, but they do not provide sufficient visibility or assurance of data protection. Restricting access to images and snapshots may not prevent authorized users from abusing their privileges or credentials. Limiting creation of virtual machine images and snapshots may not address the existing copies that may contain sensitive data. Reviewing logical access controls on virtual machines regularly may not reflect the actual access activities on images and snapshots.

NEW QUESTION: 850

in a post-implementation review of a recently purchased system it is MOST important for the IS auditor to determine whether the:

- A. stakeholder expectations were identified
- B. vendor product offered a viable solution.
- C. user requirements were met.
- D. test scenarios reflected operating activities.

Answer: C ([LEAVE A REPLY](#))

The most important thing for the IS auditor to determine in a post-implementation review of a recently purchased system is whether the user requirements were met. User requirements are the specifications and expectations of the users of the system, such as the features, functions, performance, quality, and security of the system. User requirements are usually defined and documented in the early stages of the system acquisition process, such as in the request for proposal (RFP) or the contract. User requirements are also used as the basis for testing and evaluating the system before and after implementation.

Determining whether the user requirements were met can help the IS auditor assess whether the system is fit for purpose and delivers value and benefits to the users and the organization.

Determining whether the user requirements were met can also help the IS auditor identify any

gaps, issues, or problems with the system that may affect its functionality, usability, or reliability. Determining whether the user requirements were met can also help the IS auditor provide feedback and recommendations for improvement or enhancement of the system.

Stakeholder expectations were identified is not the most important thing for the IS auditor to determine in a post-implementation review of a recently purchased system, but rather a prerequisite or input for it.

Stakeholder expectations are the needs and wants of the various parties who have an interest or influence in the system, such as users, managers, customers, suppliers, regulators, or auditors.

Stakeholder expectations are usually identified and analyzed in the initial stages of the system acquisition process, such as in the feasibility study or the business case. Stakeholder expectations are also used as inputs for defining and prioritizing the user requirements.

Vendor product offered a viable solution is not the most important thing for the IS auditor to determine in a post-implementation review of a recently purchased system, but rather an outcome or result of it. Vendor product is the system that is provided by an external supplier or service provider to meet the user requirements. Vendor product offered a viable solution means that the vendor product satisfied or exceeded the user requirements and delivered value and benefits to the users and organization. Vendor product offered a viable solution can be determined by comparing and evaluating the user requirements and the vendor product performance and quality.

Test scenarios reflected operating activities is not the most important thing for the IS auditor to determine in a post-implementation review of a recently purchased system, but rather a factor or criterion for it. Test scenarios are sets of conditions or situations that are used to test and verify whether the system meets the user requirements. Test scenarios reflected operating activities means that test scenarios simulated or replicated real-world scenarios that occur during normal operations of business processes or functions that use or depend on the system. Test scenarios reflected operating activities can help ensure that test results are valid, reliable, and relevant.

References:

Post Implementation Review: How to conduct and its Benefits 1

Post-implementation reviews - Department of Prime Minister and Cabinet 2 How To Conduct A Post Implementation Audit of Your Recently Installed System 3

NEW QUESTION: 851

An IS auditor is evaluating the risk associated with moving from one database management system (DBMS) to another. Which of the following would be MOST helpful to ensure the integrity of the system throughout the change?

- A. Preserving the same data interfaces
- B. Preserving the same data classifications
- C. Preserving the same data structure
- D. Preserving the same data inputs

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 852

During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

- A. Dumping the memory content to a file
- B. Generating disk images of the compromised system
- C. Rebooting the system
- D. Removing the system from the network

Answer: C ([LEAVE A REPLY](#))

Rebooting the system may result in a change in the system state and the loss of files and important evidence stored in memory. The other choices are appropriate actions for preserving evidence.

NEW QUESTION: 853

Which of the following is the BEST compensating control when segregation of duties is lacking in a small IS department?

- A. Background checks
- B. User awareness training
- C. Transaction log review
- D. Mandatory holidays

Answer: C ([LEAVE A REPLY](#))

The best compensating control when segregation of duties is lacking in a small IS department is transaction log review. Transaction log review can help detect any unauthorized or fraudulent activities performed by IS staff who have access to multiple functions or systems. Transaction log review can also provide an audit trail for accountability and investigation purposes. The other options are not as effective as transaction log review in compensating for the lack of segregation of duties. Background checks are preventive controls that can help screen potential employees for any criminal records or dishonest behavior, but they do not prevent existing employees from abusing their access privileges. User awareness training is a detective control that can help educate users on how to report any suspicious or abnormal activities in the IS environment, but it does not monitor or verify the actions of IS staff. Mandatory holidays are deterrent controls that can discourage IS staff from engaging in fraudulent activities by requiring them to take periodic leave, but they do not prevent or detect such activities when they occur. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 854

An IS auditor reviewing an organization's IT strategic plan should FIRST review:

- A. the existing IT environment.
- B. the business plan.
- C. the present IT budget.
- D. current technology trends.

Answer: ([SHOW ANSWER](#)**)**

The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, an IS auditor would first need to familiarize themselves with the business plan.

NEW QUESTION: 855

Prior to the migration of acquired software into production, it is MOST important that the IS auditor review the:

- A. user acceptance test (UAT) report.
- B. source code escrow agreement.
- C. system documentation.
- D. vendor testing report.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 856

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 ([LEAVE A REPLY](#))

Section: Protection of Information Assets

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.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As

Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 857

Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?

- A. Overwriting the tapes
- B. initializing the tape labels

C. Degaussing the tapes

D. Erasing the tapes

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

The best way to handle obsolete magnetic tapes is to degauss them. This action leaves a very low residue of magnetic induction, essentially erasing the data from the tapes. Overwriting or erasing the tapes may cause magnetic errors but would not remove the data completely. Initializing the tape labels would not remove the data that follows the label.

NEW QUESTION: 858

Which of the following is the BEST reason for an organization to use clustering?

A. To improve the recovery time objective (RTO)

B. To decrease system response time

C. To improve system resiliency

D. To facilitate faster backups

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 859

An IS auditor finds that a document related to a client has been leaked. Which of the following should be the auditor's NEXT step?

A. Notify appropriate law enforcement.

B. Determine the classification of data leaked

C. Report data leakage finding to regulatory authorities

D. Report data leakage finding to senior management

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 860

The PRIMARY focus of a post-implementation review is to verify that:

A. enterprise architecture (EA) has been complied with.

B. user requirements have been met.

C. acceptance testing has been properly executed.

D. user access controls have been adequately designed.

Answer: (SHOW ANSWER)

Explanation

The primary focus of a post-implementation review is to verify that user requirements have been met. User requirements are specifications that define what users need or expect from a system or service, such as functionality, usability, reliability, etc. User requirements are usually gathered and documented at the beginning of a project, and used as a basis for designing, developing, testing, and implementing a system or service. A post-implementation review is an evaluation that assesses whether a system or service meets its objectives and delivers its expected benefits after

it has been implemented. The primary focus of a post-implementation review is to verify that user requirements have been met, as this can indicate whether the system or service satisfies the user needs and expectations, provides value and quality to the users, and supports the user goals and tasks. Enterprise architecture (EA) has been complied with is a possible focus of a post-implementation review, but it is not the primary one. EA is a framework that defines how an organization's business processes, information systems, and technology infrastructure are aligned and integrated to support its vision and strategy. EA has been complied with, as this can indicate whether the system or service fits with the organization's current and future state, and follows the organization's standards and principles. Acceptance testing has been properly executed is a possible focus of a post-implementation review, but it is not the primary one. Acceptance testing is a process that verifies whether a system or service meets the user requirements and expectations before it is accepted by the users or stakeholders. Acceptance testing has been properly executed, as this can indicate whether the system or service has been tested and validated by the users or stakeholders, and whether any issues or defects have been identified and resolved.

User access controls have been adequately designed is a possible focus of a post-implementation review, but it is not the primary one. User access controls are mechanisms that ensure that only authorized users can access or use a system or service, and prevent unauthorized access or use. User access controls have been adequately designed, as this can indicate whether the system or service has appropriate security and privacy measures in place, and whether any risks or threats have been mitigated.

NEW QUESTION: 861

Which of the following should be the MOST important consideration when implementing an information security framework?

- A. Compliance requirements
- B. Audit findings
- C. Technical capabilities
- D. Risk appetite

Answer: A ([LEAVE A REPLY](#))

Section: Governance and Management of IT

NEW QUESTION: 862

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 cost-effective test of the DRP?

- A. Full operational test
- B. Preparedness test
- C. Paper test
- D. Regression test

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

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. A paper test is a structured walk-through of the disaster recovery plan and should be conducted before a preparedness test. A full operational test is conducted after the paper and preparedness test. A regression test is not a disaster recovery planning (DRP) test and is used in software maintenance.

NEW QUESTION: 863

Which of the following should be the GREATEST concern to an IS auditor reviewing the information security framework of an organization?

- A. The information security policy has not been updated in the last two years.
- B. Senior management was not involved in the development of the information security policy.
- C. A list of critical information assets was not included in the information security policy.
- D. The information security policy is not aligned with regulatory requirements.

Answer: D ([LEAVE A REPLY](#))

The effectiveness of an organization's security awareness program can be measured by capturing data on changes in the way people react to threats, such as the ability to recognize and avoid social engineering attacks¹. An increase in the number of phishing emails reported by employees indicates that they are more aware of the signs and risks of phishing, and are more likely to take appropriate actions to prevent or mitigate the impact of such attacks²³.

References

1: The Importance Of Measuring Security Awareness 2: Measuring the effectiveness of your security awareness program 3: How effective is security awareness training?

NEW QUESTION: 864

In a high-volume, real-time system, the MOST effective technique by which to continuously monitor and analyze transaction processing is:

- A. integrated test facility (ITF).
- B. parallel simulation.
- C. transaction tagging.
- D. embedded audit modules.

Answer: ([SHOW ANSWER](#))

Transaction tagging is a technique by which transactions are marked with unique identifiers or headers and traced through the system using agents or sensors at each processing point¹. Transaction tagging allows for continuous monitoring and analysis of transaction processing in a high-volume, real-time system by providing visibility into the performance, availability, and reliability of each transaction and its components¹. Transaction tagging can also help to identify and isolate errors, bottlenecks, anomalies, and security issues in the system¹.

NEW QUESTION: 865

An organization has selected a web-based solution to reduce transaction costs and improve productivity. Before implementation, an IS auditor should ensure that the organization has:

- A. validated the solution against the current IT infrastructure.
- B. performed a vulnerability assessment.
- C. addressed the level of risk exposure
- D. Implemented electronic data interchange.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 866

An external audit team is deciding whether to rely on internal audits work for an annual compliance audit Which of the following Is the GREATEST consideration when making this decision?

- A. The level of documentation maintained by internal audit and the collect evidence
- B. Independence of the internal audit department from management's influence
- C. Years of experience each of the internal auditors have in performing compliance audits
- D. Professional certifications held by the internal audit learn members

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 867

An IS auditor notes that several users have not logged into an application for more than one year. Which of the following would be the BEST audit recommendation?

- A. Delete the affected users' IDs.
- B. Periodically review the information security policy.
- C. Periodically review user access.
- D. Update the termination procedures

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 868

Which of the following is the INCORRECT "layer - protocol data unit (PDU)" mapping within the TCP/IP model?

- A. Application layer - Data
- B. Transport layer - Segment
- C. Network layer - Frame
- D. Physical layer - bits

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

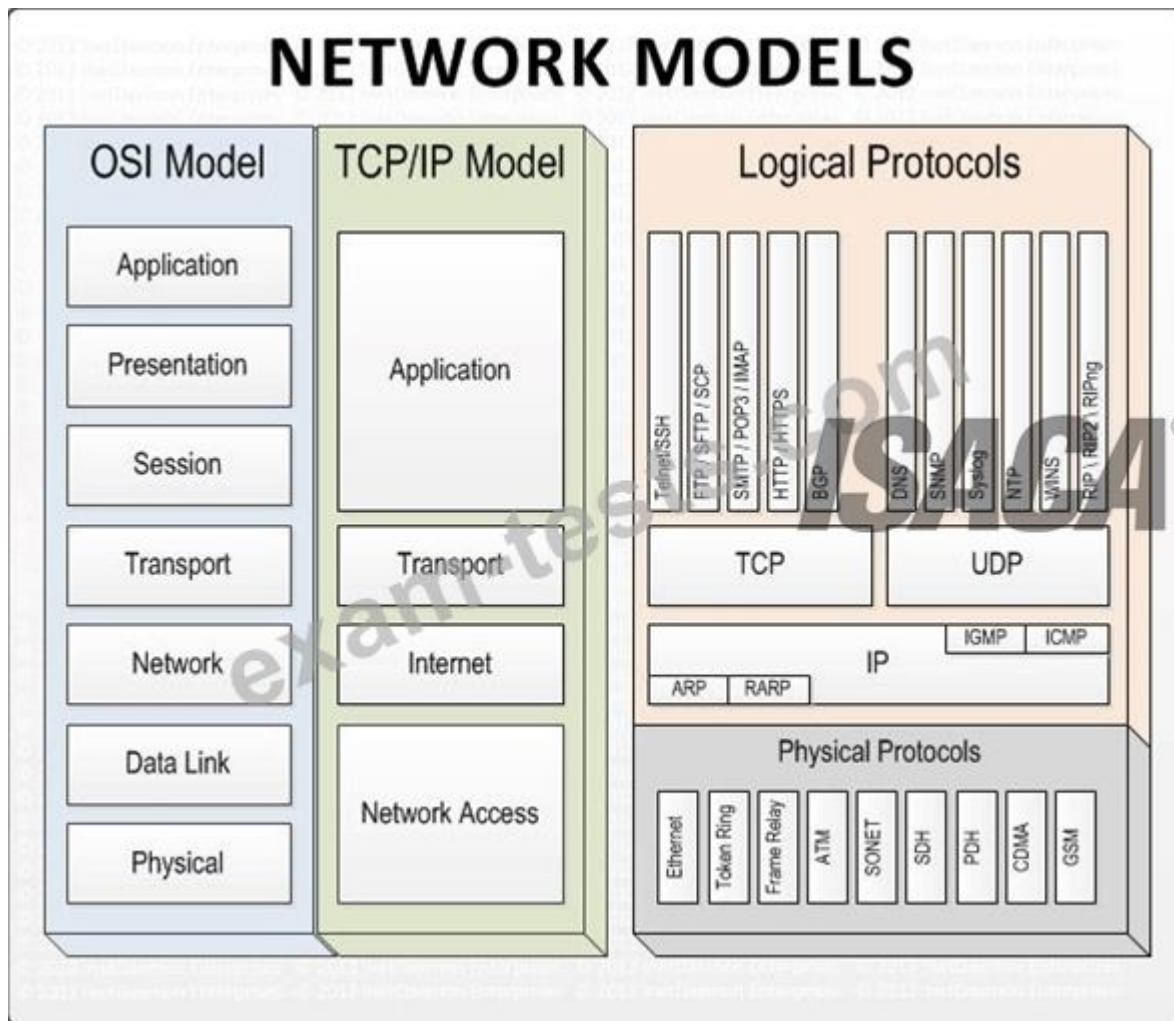
The word INCORRECT is the keyword used in the question. You need to find out incorrect layer-protocol mapping from give options.

The correct mapping is Network layer - Packet.

The LAN or WAN interface layer creates frame.

For your exam you should know below information about TCP/IP model:

Network Models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

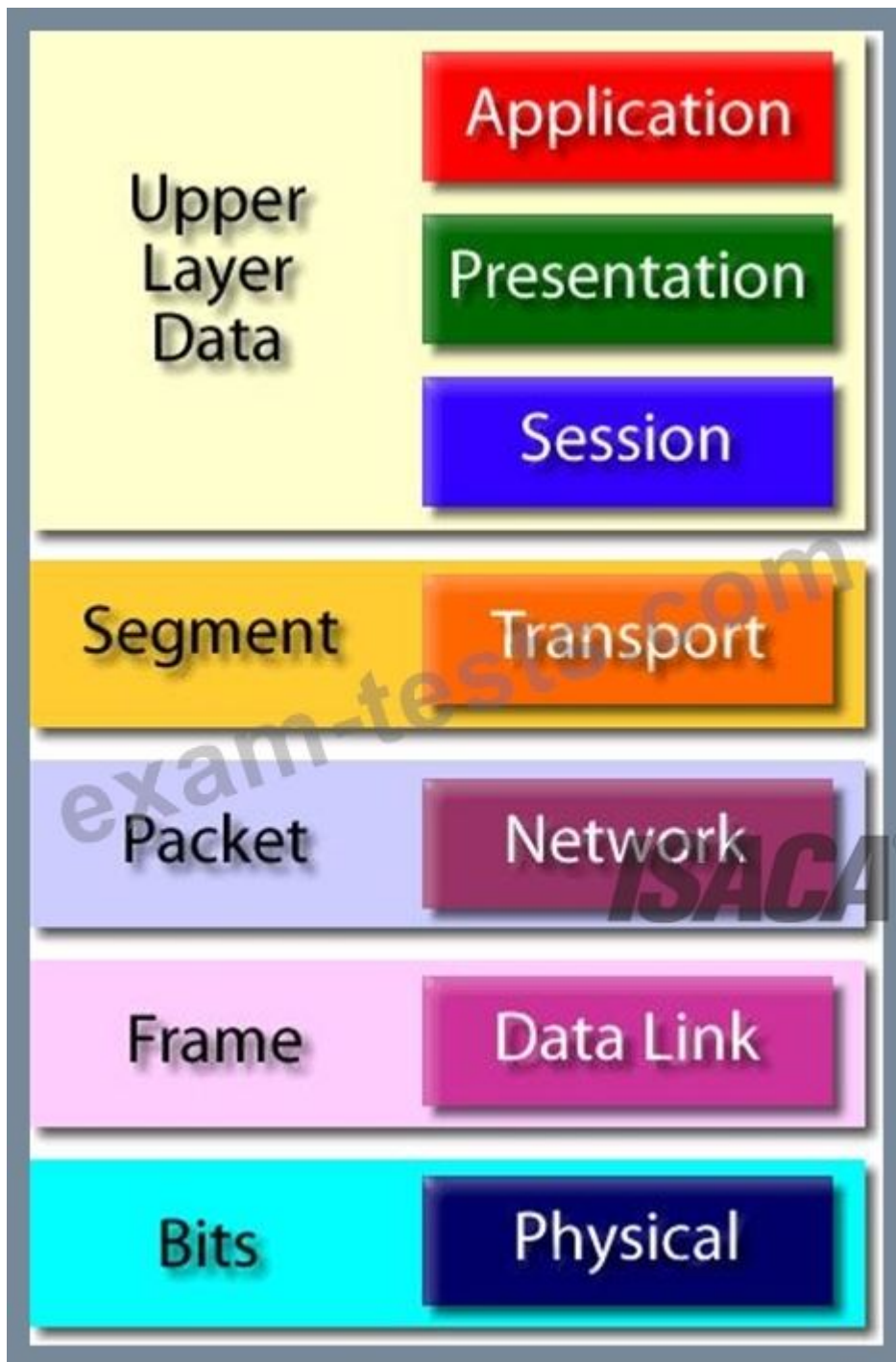
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

The other options correctly describe layer-PDU mapping in TCP/IP protocol.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

NEW QUESTION: 869

An organization has a recovery time objective (RTO) equal to zero and a recovery point objective (RPO) close to 1 minute for a critical system. This implies that the system can tolerate:

- A. a data loss of up to 1 minute, but the processing must be continuous.
- B. a 1-minute processing interruption but cannot tolerate any data loss.
- C. a processing interruption of 1 minute or more.

D. both a data loss and a processing interruption longer than 1 minute.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

The recovery time objective (RTO) measures an organization's tolerance for downtime and the recovery point objective (RPO) measures how much data loss can be accepted. Choices B, C and D are incorrect since they exceed the RTO limits set by the scenario.

NEW QUESTION: 870

When continuous monitoring systems are being implemented, an IS auditor should FIRST identify:

- A.** the location and format of output files
- B.** applications that provide the highest financial risk
- C.** high-risk areas within the organization
- D.** the controls on which to focus

Answer: ([SHOW ANSWER](#)**)**

Section: The process of Auditing Information System

NEW QUESTION: 871

The purpose of a mainframe audit is to provide assurance that processes are being implemented as

required, the mainframe is operating as it should, security is strong, and that procedures in place are

working and are updated as needed. The auditor may accordingly make recommendations for improvement. Which of the following types of audit always takes high priority over the others?

(Choose

five.)

- A.** System audit
- B.** Application audit
- C.** Software audit
- D.** License audit
- E.** Security server audit
- F.** None of the choices.

Answer: A,B,C,D,E ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com
CISA exam **questions have been updated** and **answers have been corrected** get the

newest BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As

Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 872

Which of the following is MOST helpful for measuring benefits realization for a new system?

- A. Balanced scorecard review
- B. Function point analysis
- C. Post-implementation review
- D. Business impact analysis (BIA)

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 873

An organization allows its employees to use personal mobile devices for work. Which of the following would BEST maintain information security without compromising employee privacy?

- A. Installing security software on the devices
- B. Partitioning the work environment from personal space on devices
- C. Preventing users from adding applications
- D. Restricting the use of devices for personal purposes during working hours

Answer: B ([LEAVE A REPLY](#))

Partitioning the work environment from personal space on devices. This would best maintain information security without compromising employee privacy by creating a separate and secure area on the personal mobile devices for work-related data and applications. This way, the organization can protect its information from unauthorized access, loss, or leakage, while respecting the employees' personal data and preferences on their own devices.

The other options are not as effective as option B in balancing information security and employee privacy.

Option A, installing security software on the devices, is a good practice but may not be sufficient to prevent data breaches or comply with regulatory requirements. Option C, preventing users from adding applications, is too restrictive and may interfere with the employees' personal use of their devices. Option D, restricting the use of devices for personal purposes during working hours, is impractical and difficult to enforce.

References:

ISACA, CISA Review Manual, 27th Edition, 2019

ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

Personal Cellphone Privacy at Work¹ Protecting your personal information and privacy on a company phone² Mobile Devices and Protected Health Information (PHI)³ Using your personal phone for work? Here's how to separate your apps and data⁴

9 Ways to Improve Mobile Security and Privacy in the Age of Remote Work⁵

NEW QUESTION: 874

.If a database is restored from information backed up before the last system image, which of the following is recommended?

- A. The system should be restarted after the last transaction.
- B. The system should be restarted before the last transaction.
- C. The system should be restarted at the first transaction.
- D. The system should be restarted on the last transaction.

Answer: ([SHOW ANSWER](#))

If a database is restored from information backed up before the last system image, the system should be restarted before the last transaction because the final transaction must be reprocessed.

NEW QUESTION: 875

Which of the following message services provides the strongest evidence that a specific action has occurred?

- A. Proof of delivery
- B. Nonrepudiation
- C. Proof of submission
- D. Message origin authentication

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

Nonrepudiation services provide evidence that a specific action occurred. Nonrepudiation services are similar to their weaker proof counterparts, i.e., proof of submission, proof of delivery and message origin authentication. However, nonrepudiation provides stronger evidence because the proof can be demonstrated to a third party. Digital signatures are used to provide nonrepudiation. Message origination authentication will only confirm the source of the message and does not confirm the specification that has been completed.

NEW QUESTION: 876

Before implementing controls, management should FIRST ensure that the controls:

- A. satisfy a requirement in addressing a risk issue.
- B. do not reduce productivity.
- C. are based on a cost-benefit analysis.
- D. are detective or corrective.

Answer: A ([LEAVE A REPLY](#))

When designing controls, it is necessary to consider all the above aspects. In an ideal situation, controls that address all these aspects would be the best controls. Realistically, it may not be possible to design them all and cost may be prohibitive; therefore, it is necessary to first consider the preventive controls that attack the cause of a threat.

NEW QUESTION: 877

An IS auditor should know information about different network transmission media. Which of the following transmission media is used for short distance transmission?

- A. Copper cable
- B. Fiber Optics
- C. Satellite Radio Link
- D. Satellite Radio Link

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

For your exam you should know below information about transmission media:

Copper Cable

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the

1820s. The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts.

Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable



Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880. Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable is expensive and does not support many LAN's. It supports data and video.



Coaxial Cable

Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building. Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics



Radio System

Radio systems are used for short distance, cheap and easy to intercept.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to tap.

Microwave Radio System

Satellite Radio Link

Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to intercept.

The following answers are incorrect:

Fiber optics - Fiber optics cables are used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Radio System - Radio systems are used for short distance, cheap and easy to tap.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 265

NEW QUESTION: 878

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

- A. Controls testing starts earlier.
- B. Auditing resources are allocated to the areas of highest concern.
- C. Auditing risk is reduced.
- D. Controls testing is more thorough.

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Allocation of auditing resources to the areas of highest concern is a benefit of a risk-based approach to audit planning.

NEW QUESTION: 879

An external attacker spoofing an internal Internet Protocol (IP) address can BEST be detected by which of the following?

- A. Comparing the source address to the domain name server (DNS) entry
- B. Comparing the source address to the interface used as the entry point
- C. Using static IP addresses for identification
- D. Using a state table to compare the message states of each packet as it enters the system

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 880

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

- A. Identify and evaluate the existing controls
- B. Conduct a business impact analysis (BIA)
- C. Report on existing controls
- D. Propose new controls

Answer: A ([LEAVE A REPLY](#))

After an IS auditor has identified threats and potential impacts, the auditor should then identify and evaluate the existing controls.

NEW QUESTION: 881

Which of the following is the MOST critical step in planning an audit?

- A. Implementing a prescribed auditing framework such as COBIT
- B. Identifying current controls
- C. Identifying high-risk audit targets
- D. Testing controls

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

Explanation:

In planning an audit, the most critical step is identifying the areas of high risk.

NEW QUESTION: 882

In a typical SDLC, which group is PRIMARILY responsible for confirming compliance with requirements?

- A. Steering committee
- B. Risk management
- C. Quality assurance
- D. Internal audit

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 883

Which of the following is MOST effective in detecting an intrusion attempt?

- A. Using packet fitter software
- B. Analyzing system logs
- C. Using smart cards with one-time passwords
- D. Installing biometrics-based authentication

Answer: B [\(LEAVE A REPLY\)](#)

NEW QUESTION: 884

A data leakage prevention (DLP) solution has identified that several employees are sending confidential company data to their personal email addresses in violation of company policy. The information security manager should FIRST:

- A. initiate an investigation to determine the full extent of noncompliance
- B. notify senior management that employees are breaching policy
- C. limit access to the Internet for employees involved
- D. contact the employees involved to retake security awareness training

Answer: A [\(LEAVE A REPLY\)](#)

Section: Protection of Information Assets

NEW QUESTION: 885

An IS auditor finds that client requests were processed multiple times when received from different independent departmental databases, which are synchronized weekly. What would be the BEST recommendation?

- A. increase the frequency for data replication between the different department systems to ensure timely updates.
- B. Centralize all request processing in one department to avoid parallel processing of the same request.
- C. Change the application architecture so that common data are held in just one shared database for all departments.
- D. implement reconciliation controls to detect duplicates before orders are processed in the systems.

Answer: C [\(LEAVE A REPLY\)](#)

Keeping the data in one place is the best way to ensure that data are stored without redundancy and that all users have the same data on their systems. Although increasing the frequency may help to minimize the problem, the risk of duplication cannot be eliminated completely because parallel data entry is still possible. Business requirements will most likely dictate where data processing activities are performed. Changing the business structure to solve an IT problem is not practical or politically feasible. Detective controls do not solve the problem of duplicate processing, and would require that an additional process be implemented to handle the discovered duplicates.

NEW QUESTION: 886

An external IS auditor is reviewing the continuous monitoring system for a large bank and notes several potential issues. Which of the following would present the GREATEST concern regarding the reliability of the monitoring system?

- A. The monitoring system was configured by IT.
- B. The measurement method is periodically varied.
- C. The system results are not regularly reviewed by management.
- D. The alert threshold is updated periodically.

Answer: C ([LEAVE A REPLY](#))

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 887

Which of the following should be an IS auditor's GREATEST concern when an international organization intends to roll out a global data privacy policy?

- A. Requirements may become unreasonable.
- B. The policy may conflict with existing application requirements.
- C. Local regulations may contradict the policy.
- D. Local management may not accept the policy.

Answer: C ([LEAVE A REPLY](#))

The greatest concern for an IS auditor when an international organization intends to roll out a global data privacy policy is that local regulations may contradict the policy. Data privacy regulations vary across different countries and regions, and they may impose different or conflicting requirements on how personal data can be collected, processed, stored, transferred, and disclosed. The organization should ensure that its global data privacy policy complies with

the applicable local regulations in each jurisdiction where it operates, or risk facing legal sanctions or reputational damage. Requirements may become unreasonable, but this is not a major concern for an IS auditor, as it is a business decision that should be based on a cost-benefit analysis. The policy may conflict with existing application requirements, but this is not a serious concern for an IS auditor, as it can be resolved by modifying or updating the applications to align with the policy. Local management may not accept the policy, but this is not a critical concern for an IS auditor, as it can be mitigated by providing adequate training and awareness on the policy and its benefits. References:

* CISA Review Manual, 27th Edition, pages 406-4071

* CISA Review Questions, Answers & Explanations Database, Question ID: 2592

NEW QUESTION: 888

The PRIMARY benefit to using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry-pipe system:

- A. is more effective at suppressing flames.
- B. allows more time to abort release of the suppressant.
- C. has a decreased risk of leakage.
- D. disperses dry chemical suppressants exclusively.

Answer: C ([LEAVE A REPLY](#))

Explanation

The primary benefit of using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry-pipe system has a decreased risk of leakage, as the pipes are filled with pressurized air or nitrogen instead of water until the system is activated. A wet-pipe system has a higher risk of leakage, corrosion, and freezing.

A dry-pipe system is not more effective at suppressing flames, as it uses the same water-based suppressant as a wet-pipe system. A dry-pipe system does not allow more time to abort release of the suppressant, as it has a delay of only a few seconds before the water is released. A dry-pipe system does not disperse dry chemical suppressants exclusively, as it uses water as the primary suppressant. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.2.3

NEW QUESTION: 889

An organization is running servers with critical business applications that are in an area subject to frequent but brief power outages. Knowledge of which of the following would allow the organization's management to monitor the ongoing adequacy of the uninterruptible power supply (UPS)?

- A. Duration and interval of the power outages
- B. Number of servers supported by the UPS
- C. Mean time to recover servers after failure
- D. Business impact of server downtime

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 890

An IS auditor is reviewing processes for importing market price data from external data providers. Which of the following findings should the auditor consider MOST critical?

- A. The quality of the data is not monitored.
- B. The transfer protocol is not encrypted.
- C. Imported data is not disposed of frequently.
- D. The transfer protocol does not require authentication.

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 891

Which of the following would BEST deter the theft of corporate information from a laptop?

- A. Protect files with passwords.
- B. Install biometric access controls.
- C. Encrypt the file allocation table (FAT).
- D. Encrypt all data on the hard drive.

Answer: D [\(LEAVE A REPLY\)](#)

NEW QUESTION: 892

Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?

- A. Session keys are dynamic
- B. Private symmetric keys are used
- C. Keys are static and shared
- D. Source addresses are not encrypted or authenticated

Answer: A [\(LEAVE A REPLY\)](#)

Section: Protection of Information Assets

Explanation:

WPA uses dynamic session keys, achieving stronger encryption than wireless encryption privacy (WEP),

which operates with static keys (same key is used for everyone in the wireless network). All other choices

are weaknesses of WEP.

NEW QUESTION: 893

A configuration management audit identified that predefined automated procedures are used when deploying and configuring application infrastructure in a cloud-based environment. Which of the following is MOST important for the IS auditor to review?

- A. Storage location of configuration management documentation
- B. Processes for making changes to cloud environment specifications
- C. Contracts of vendors responsible for maintaining provisioning tools
- D. Number of administrators with access to cloud management consoles

Answer: (SHOW ANSWER)

The IS auditor should review the processes for making changes to cloud environment specifications, as these are the inputs for the predefined automated procedures that deploy and configure the application infrastructure.

The IS auditor should verify that the changes are authorized, documented, tested, and approved before they are applied to the cloud environment. The IS auditor should also check that the changes are aligned with the business requirements and do not introduce any security or performance issues.

References

ISACA CISA Review Manual, 27th Edition, page 254

Configuration Management in Cloud Computing - ScienceDirect

Cloud Configuration Management - BMC Software

NEW QUESTION: 894

If an IS auditor observes that an IS department fails to use formal documented methodologies, policies,

and standards, what should the auditor do?

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

B. The auditor should at least document the informal standards and policies. Furthermore, the IS auditor

should create formal documented policies to be implemented.

C. The auditor should at least document the informal standards and policies, and test for a compliance.

Furthermore, the IS auditor should recommend management that formal documented policies be developed and implemented.

D. The auditor should at least document the informal standards and policies, and test for compliance.

Furthermore, the IS auditor should create formal documented policies to be implemented.

Answer: C (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

If an IS auditor observes that an IS department fails to use formal documented methodologies, policies,

and standards, the auditor should at least document the informal standards and policies, and test for

compliance. Furthermore, the IS auditor should recommend to management that formal documented

policies be developed and implemented.

NEW QUESTION: 895

Which of the following BEST Indicates that an incident management process is effective?

- A. Decreased time for incident resolution
- B. Increased number of incidents reviewed by IT management
- C. Decreased number of calls to the help desk
- D. Increased number of reported critical incidents

Answer: A ([LEAVE A REPLY](#))

Decreased time for incident resolution is the best indicator that an incident management process is effective.

Incident management is a process that aims to restore normal service operation as quickly as possible after an incident, which is an unplanned interruption or reduction in quality of an IT service. Decreased time for incident resolution means that the incident management process is able to identify, analyze, respond to, and resolve incidents efficiently and effectively. The other indicators do not necessarily reflect the effectiveness of the incident management process, as they may depend on other factors such as the nature, frequency, and severity of incidents.

References: CISA Review Manual, 27th Edition, page 372

NEW QUESTION: 896

Which of the following is the BEST indication of control maturity in an organization's systems development and implementation processes?

- A. Code changes are tested and deployed manually.
- B. Code changes are deployed to a test server and then to production.
- C. Code changes are documented and approved.
- D. Code changes are tested and deployed through automation.

Answer: D ([LEAVE A REPLY](#))

Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 897

.Test and development environments should be separated. True or false?

- A. True
- B. False

Answer: ([SHOW ANSWER](#))

Test and development environments should be separated, to control the stability of the test environment.

NEW QUESTION: 898

Which of the following should be the FIRST step when developing a data loss prevention (DLP) solution for a large organization?

- A. Conduct a data inventory and classification exercise
- B. Identify approved data workflows across the enterprise.
- C. Create the DLP policies and templates
- D. Conduct a threat analysis against sensitive data usage.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 899

When reviewing a data classification scheme, it is MOST important for an IS auditor to determine if.

- A. each information asset is assigned to a different classification.
- B. the security criteria are clearly documented for each classification
- C. Senior IT managers are identified as information owner.
- D. the information owner is required to approve access to the asset

Answer: ([SHOW ANSWER](#))

When reviewing a data classification scheme, it is most important for an IS auditor to determine if the security criteria are clearly documented for each classification. This will help the IS auditor to evaluate if the data classification scheme is consistent, comprehensive, and aligned with the organizational objectives and regulatory requirements. The security criteria should define the level of confidentiality, integrity, and availability for each data classification, as well as the corresponding controls such as access control, rights management, and cryptographic protection¹. The other options are less important or incorrect because:

- * A. Each information asset is not necessarily assigned to a different classification. Data classification schemes usually have a limited number of categories, such as "Sensitive," "Confidential," and "Public," and multiple information assets can belong to the same category².
- * C. Senior IT managers are not necessarily identified as information owners. Information owners are typically the business units or functions that create, use, or maintain the information assets, and they may or may not be senior IT managers³.
- * D. The information owner is not required to approve access to the asset. The information owner is responsible for defining the access requirements and rules for the asset, but the actual approval of access requests may be delegated to other roles, such as data custodians or administrators³. References: Simplify and Contextualize Your Data Classification Efforts - ISACA, 3.7: Establish and Maintain a Data Classification Scheme, Data Classification and Practices - NIST, CISA Exam Content Outline | CISA Certification | ISACA

NEW QUESTION: 900

A credit card company has decided to outsource the printing of customer statements. It is MOST important for the company to verify whether:

- A. the provider has alternate service locations.
- B. the contract includes compensation for deficient service levels.
- C. the provider's information security controls are aligned with the company's.
- D. the provider adheres to the company's data retention policies.

Answer: C ([LEAVE A REPLY](#))

The most important thing for the company to verify when outsourcing the printing of customer statements is whether the provider's information security controls are aligned with the company's. This is because customer statements contain sensitive personal and financial information that need to be protected from unauthorized access, disclosure, modification or destruction. The

provider's information security controls should be consistent with the company's policies, standards and regulations, and should be audited periodically to ensure compliance. The other options are also relevant, but not as critical as information security. References: CISA Review Manual (Digital Version)¹, Chapter 3, Section 3.2.2

NEW QUESTION: 901

Which of the following represents the GREATEST potential risk in an EDI environment?

- A. Transaction authorization
- B. Loss or duplication of EDI transmissions
- C. Transmission delay
- D. Deletion or manipulation of transactions prior to or after establishment of application controls

Answer: (SHOW ANSWER)

Section: Protection of Information Assets

Explanation:

Since the interaction between parties is electronic, there is no inherent authentication occurring; therefore, transaction authorization is the greatest risk. Choices B and D are examples of risks, but the impact is not as great as that of unauthorized transactions. Transmission delays may terminate the process or hold the line until the normal time for processing has elapsed; however, there will be no loss of data.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here: <https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 902

An IS auditor is performing a follow-up audit for findings identified in an organization's user provisioning process Which of the following is the MOST appropriate population to sample from when testing for remediation?

- A. All users provisioned after the finding was originally identified
- B. All users provisioned after management resolved the audit issue
- C. All users provisioned after the final audit report was issued
- D. All users who have followed user provisioning processes provided by management

Answer: C (LEAVE A REPLY)

Explanation

The most appropriate population to sample from when testing for remediation of findings identified in an organization's user provisioning process is all users provisioned after the final audit report was issued. This is because the final audit report is the official document that communicates the audit findings, recommendations, and action plans to the management and other stakeholders. It also establishes a baseline for measuring the progress and effectiveness of the remediation efforts. Therefore, sampling from the users provisioned after the final audit report was issued would provide the most relevant and reliable evidence of whether the audit issues have been resolved or not.

The other options are not as appropriate as option C, as they may not reflect the actual status of the remediation efforts. All users provisioned after the finding was originally identified may include users who were provisioned before the final audit report was issued, which may not capture the full impact of the remediation actions. All users provisioned after management resolved the audit issue may not be accurate, as management's resolution may not be verified or validated by an independent party. All users who have followed user provisioning processes provided by management may not be representative, as there may be exceptions or deviations from the processes that could affect the remediation results.

References:

6: What Is User Provisioning? Definition, Process and Best Practices - Spiceworks

7: What Is User Provisioning? All You Need to Know in One Place - G2

8: What is User Account Provisioning? - Tools4ever

9: What Is Provisioning and Deprovisioning? | Okta

NEW QUESTION: 903

A checksum is classified as which type of control?

- A. Detective control
- B. Preventive control
- C. Corrective control
- D. Administrative control

Answer: A ([LEAVE A REPLY](#))

A checksum is classified as a detective control. A checksum is a mathematical value that is calculated from a data set and used to verify the integrity of the data. A checksum can detect if the data has been altered or corrupted during transmission or storage. A checksum does not prevent or correct the data corruption, but it alerts the user or system of the problem. Therefore, it is a detective control. A preventive control is a control that prevents an error or incident from occurring. A corrective control is a control that restores normal operations after an error or incident has occurred. An administrative control is a control that involves policies, procedures, standards, guidelines, or organizational structures. References: CISA Review Manual (Digital Version)¹, page 439.

NEW QUESTION: 904

When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

- A. incorporates state of the art technology.
- B. addresses the required operational controls.
- C. articulates the IT mission and vision.
- D. specifies project management practices.

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not address the technology, operational controls or project management practices.

NEW QUESTION: 905

Why is it not preferable for a firewall to treat each network frame or packet in isolation?

- A. Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.
- B. Such a firewall is costly to setup.
- C. Such a firewall is too complicated to maintain.
- D. Such a firewall is CPU hungry.
- E. Such a firewall offers poor compatibility.
- F. None of the choices.

Answer: A ([LEAVE A REPLY](#))

A stateless firewall treats each network frame or packet in isolation.

Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.

NEW QUESTION: 906

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

- A. Evidence collected through personal observation
- B. Evidence collected through systems logs provided by the organization's security administration
- C. Evidence collected through surveys collected from internal staff
- D. Evidence collected through transaction reports provided by the organization's IT administration

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

An IS auditor usually places more reliance on evidence directly collected, such as through personal observation.

NEW QUESTION: 907

Which of the following is the MOST important operational aspect for an IS auditor to consider when assessing an assembly line with quality control sensors accessible via wireless techno

- A. Known vulnerabilities

- B. Device security
- C. Resource utilization
- D. Device updates

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 908

An IS auditor notes that patches for the operating system used by an organization are deployed by the IT department as advised by the vendor. The MOST significant concern an IS auditor should have with this practice is the nonconsideration by IT of:

- A. the training needs for users after applying the patch.
- B. any beneficial impact of the patch on the operational systems.
- C. delaying deployment until testing the impact of the patch.
- D. the necessity of advising end users of new patches.

Answer: C ([LEAVE A REPLY](#))

Deploying patches without testing exposes an organization to the risk of system disruption or failure. Normally, there is no need for training or advising users when a new operating system patch has been installed. Any beneficial impact is less important than the risk of unavailability that could be avoided with proper testing.

NEW QUESTION: 909

A global company has been using a publicly available AI tool to obtain information about global laws and regulations that could impact the business. Which of the following should be of MOST concern to an IS auditor?

- A. Accuracy and quality of the data provided by the AI tool
- B. Whether the organization is using a paid version of the AI tool
- C. Version and provider of the AI tool being utilized
- D. Whether the tool is utilized by competitors in the same industry

Answer: A ([LEAVE A REPLY](#))

The biggest risk is reliance on inaccurate or low-quality legal/regulatory information, which could result in compliance failures. Other concerns (paid tier, provider, competitors) are secondary. References (ISACA): ISACA Digital Trust Framework - Reliability of Data.

NEW QUESTION: 910

For an organization that has plans to implement web-based trading, it would be MOST important for an IS auditor to verify the organization's information security plan includes:

- A. attributes for system passwords.
- B. the firewall configuration for the web server.
- C. security requirements for the new application.
- D. security training prior to implementation.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 911

Time constraints and expanded needs have been found by an IS auditor to be the root causes for recent violations of corporate data definition standards in a new business intelligence project.

Which of the following is the MOST appropriate suggestion for an auditor to make?

- A. Achieve standards alignment through an increase of resources devoted to the project
- B. Align the data definition standards after completion of the project
- C. Delay the project until compliance with standards can be achieved
- D. Enforce standard compliance by adopting punitive measures against violators

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Provided that data architecture, technical, and operational requirements are sufficiently documented, the alignment to standards could be treated as a specific work package assigned to new project resources.

The usage of nonstandard data definitions would lower the efficiency of the new development, and increase the risk of errors in critical business decisions. To change data definition standards after project conclusion (choice B) is risky and is not a viable solution. On the other hand, punishing the violators (choice D) or delaying the project (choice C) would be an inappropriate suggestion because of the likely damage to the entire project profitability.

NEW QUESTION: 912

Which of the following BEST indicates to an IS auditor that an IT-related project will deliver value to the organization?

- A. The project will use existing infrastructure to deliver services.
- B. The cost of the project is within the organization's risk appetite.
- C. Requirements are based on stakeholder expectations.
- D. Competitors are considering similar IT-based solutions.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 913

Which of the following provides the MOST assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system?

- A. Comparing code between old and new systems
- B. Running historical transactions through the new system
- C. Reviewing quality assurance (QA) procedures
- D. Loading balance and transaction data to the new system

Answer: (SHOW ANSWER)

The most assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system can be obtained by running historical transactions through the new system.

Historical transactions are transactions that have been processed and recorded by the old system in the past.

Running historical transactions through the new system can provide the most assurance over the completeness and accuracy of loan application processing, by comparing the results and outputs of the new system with those of the old system, and verifying whether they match or differ. This can help identify and resolve any errors or issues that may arise from the new system, such as data conversion, functionality, compatibility, etc.

Comparing code between old and new systems is a possible way to obtain some assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system, but it is not the most effective one. Code is a set of instructions or commands that define how a system operates or functions. Comparing code between old and new systems can provide some assurance over the completeness and accuracy of loan application processing, by checking whether the logic, algorithms, or functions of the new system are consistent or equivalent with those of the old system. However, this may not be sufficient or reliable, as code may not reflect the actual performance or outcomes of the system, and may not detect any errors or issues that may occur at the data or user level. Reviewing quality assurance (QA) procedures is a possible way to obtain some assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system, but it is not the most effective one. QA procedures are steps or activities that ensure that a system meets its quality standards and requirements, such as testing, verification, validation, etc. Reviewing QA procedures can provide some assurance over the completeness and accuracy of loan application processing, by evaluating whether the new system has been properly tested and verified before implementation. However, this may not be adequate or accurate, as QA procedures may not cover all aspects or scenarios of loan application processing, and may not reveal any errors or issues that may arise after implementation. Loading balance and transaction data to the new system is a possible way to obtain some assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system, but it is not the most effective one. Balance and transaction data are data that reflect the status and history of loan applications in a system, such as amounts, dates, payments, etc. Loading balance and transaction data to the new system can provide some assurance over the completeness and accuracy of loan application processing, by transferring data from the old system to the new system and ensuring that they are consistent and correct. However, this may not be enough or valid, as balance and transaction data may not represent all aspects or features of loan application processing, and may not indicate any errors or issues that may arise

NEW QUESTION: 914

In a public key infrastructure, a registration authority:

- A.** verifies information supplied by the subject requesting a certificate.
- B.** issues the certificate after the required attributes are verified and the keys are generated.
- C.** digitally signs a message to achieve nonrepudiation of the signed message.
- D.** registers signed messages to protect them from future repudiation.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

A registration authority is responsible for verifying information supplied by the subject requesting a certificate, and verifies the requestor's right to request certificate attributes and that the requestor actually possesses the private key corresponding to the public key being sent. Certification authorities, not registration authorities, actually issue certificates once verification of the information has been completed; because of this, choice B is incorrect. On the other hand, the sender who has control of their private key signs the message, not the registration authority. Registering signed messages is not a task performed by registration authorities.

NEW QUESTION: 915

Upon receipt of the initial signed digital certificate the user will decrypt the certificate with the public key of the:

- A. registration authority (RA).
- B. certificate authority (CA).
- C. certificate repository.
- D. receiver.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

A certificate authority (CA) is a network authority that issues and manages security credentials and public keys for message encryption. As a part of the public key infrastructure, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can issue a certificate. The CA signs the certificate with its private key for distribution to the user. Upon receipt, the user will decrypt the certificate with the CA's public key.

NEW QUESTION: 916

Minimum password length and password complexity verification are examples of:

- A. detection controls.
- B. control objectives.
- C. audit objectives.
- D. control procedures.

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Control procedures are practices established by management to achieve specific control objectives.

Password controls are preventive controls, not detective controls. Control objectives are declarations of expected results from implementing controls and audit objectives are the specific goals of an audit.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 917

Which of the following is a social engineering attack method?

- A.** An unauthorized person attempts to gain access to secure premises by following an authorized person through a secure door.
- B.** An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone.
- C.** A hacker walks around an office building using scanning tools to search for a wireless network to gain access.
- D.** An intruder eavesdrops and collects sensitive information flowing through the network and sells it to third parties.

Answer: ([SHOW ANSWER](#))

Explanation

An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone. This is a social engineering attack method that exploits the trust or curiosity of the employee to obtain sensitive information that can be used to access or compromise the network. According to the web search results, social engineering is a technique that uses psychological manipulation to trick users into making security mistakes or giving away sensitive information¹. Phishing, whaling, baiting, and pretexting are some of the common forms of social engineering attacks². Social engineering attacks are often more effective and profitable than purely technical attacks, as they rely on human error rather than system vulnerabilities

NEW QUESTION: 918

The GREATEST benefit of using a polo typing approach in software development is that it helps to:

- A.** minimize scope changes to the system.

- B. decrease the time allocated for user testing and review.
- C. conceptualize and clarify requirements.
- D. Improve efficiency of quality assurance (QA) testing

Answer: C ([LEAVE A REPLY](#))

The greatest benefit of using a prototyping approach in software development is that it helps to conceptualize and clarify requirements. A prototyping approach is a method of creating a simplified or partial version of a software product to demonstrate its features and functionality. A prototyping approach can help to elicit, validate, and refine the requirements of the software product, as well as to obtain feedback from the users and stakeholders. The other options are not the greatest benefits of using a prototyping approach, but rather possible outcomes or advantages of doing so. References:

* CISA Review Manual (Digital Version), Chapter 4, Section 4.3.11

* CISA Review Questions, Answers & Explanations Database, Question ID 227

NEW QUESTION: 919

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

- A. Referential integrity controls
- B. Normalization controls
- C. Concurrency controls
- D. Run-to-run totals

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

Explanation:

Concurrency controls are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information.

NEW QUESTION: 920

Which of the following is normally a responsibility of the chief security officer (CSO)?

- A. Periodically reviewing and evaluating the security policy
- B. Executing user application and software testing and evaluation
- C. Granting and revoking user access to IT resources
- D. Approving access to data and applications

Answer: ([SHOW ANSWER](#)**)**

Section: Protection of Information Assets

Explanation:

The role of a chief security officer (CSO) is to ensure that the corporate security policy and controls are adequate to prevent unauthorized access to the company assets, including data, programs and equipment.

User application and other software testing and evaluation normally are the responsibility of the staff assigned to development and maintenance. Granting and revoking access to IT resources is

usually a function of network or database administrators. Approval of access to data and applications is the duty of the data owner.

NEW QUESTION: 921

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 ([LEAVE A REPLY](#))

Explanation/Reference:

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.

NEW QUESTION: 922

When planning an audit, it is acceptable for an IS auditor to rely on a third-party provider's external audit report on service level management when the

- A. scope and methodology meet audit requirements
- B. service provider is independently certified and accredited
- C. report confirms that service levels were not violated
- D. report was released within the last 12 months

Answer: A ([LEAVE A REPLY](#))

Explanation

It is acceptable for an IS auditor to rely on a third-party provider's external audit report on service level management when the scope and methodology meet audit requirements. This means that the external audit report covers the same objectives, criteria, standards and procedures that the IS auditor would use to assess the service level management. This way, the IS auditor can avoid duplication of work and reduce audit costs and efforts. The service provider's certification and accreditation, the report's confirmation of service levels and the report's release date are not sufficient to justify reliance on the external audit report. References: CISA Review Manual (Digital Version) , Chapter 2, Section 2.3.3.

NEW QUESTION: 923

mission-critical applications with a low recovery time objective (RTO). which of the following is the BEST backup strategy?

- A. Use of virtual tape libraries
- B. Frequent back-ups to tape
- C. Archiving to conventional disk
- D. Mirroring

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 924

Backup procedures for an organization's critical data are considered to be which type of control?

- A. Corrective
- B. Compensating
- C. Detective
- D. Directive

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 925

IS management is considering a Voice-over Internet Protocol (VoIP) network to reduce telecommunication costs and management asked the IS auditor to comment on appropriate security controls. Which of the following security measures is MOST appropriate?

- A. Review and, where necessary, upgrade firewall capabilities
- B. Install modems to allow remote maintenance support access
- C. Create a physically distinct network to handle VoIP traffic
- D. Redirect all VoIP traffic to allow clear text logging of authentication credentials

Answer: A ([LEAVE A REPLY](#))

Firewalls used as entry points to a Voice-over Internet Protocol (VoIP) network should be VoIPcapable. VoIP network services such as H.323 introduce complexities that are likely to strain the capabilities of older firewalls. Allowing for remote support access is an important consideration. However, a virtual private network (VPN) would offer a more secure means of enabling this access than reliance on modems. Logically separating the VoIP and data network is a good idea. Options such as virtual LANs (VLANs), traffic shaping, firewalls and network address translation (NAT) combined with private IP addressing can be used; however, physically separating the networks will increase both cost and administrative complexity. Transmitting or storing clear text information, particularly sensitive information such as authentication credentials, will increase network vulnerability. When designing a VoIP network, it is important to avoid introducing any processing that will unnecessarily increase latency since this will adversely impact VoIP quality.

NEW QUESTION: 926

Due to a recent business divestiture, an organization has limited IT resources to deliver critical projects.

Reviewing the IT staffing plan against which of the following would BEST guide IT management when

estimating resource requirements for future projects?

- A. Peer organizational staffing benchmarks
- B. Budgeted forecast for the next financial year
- C. Human resources sourcing strategy
- D. Records of actual time spent on projects

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

NEW QUESTION: 927

In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

- A. Diskless workstations
- B. Data encryption techniques
- C. Network monitoring devices
- D. Authentication systems

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Network monitoring devices may be used to inspect activities from known or unknown users and can identify client addresses, which may assist in finding evidence of unauthorized access. This serves as a detective control. Diskless workstations prevent access control software from being bypassed. Data encryption techniques can help protect sensitive or propriety data from unauthorized access, thereby serving as a preventive control. Authentication systems may provide environment wide, logical facilities that can differentiate among users, before providing access to systems.

NEW QUESTION: 928

Functionality is a characteristic associated with evaluating the quality of software products throughout their life cycle, and is BEST described as the set of attributes that bear on the:

- A. existence of a set of functions and their specified properties.
- B. ability of the software to be transferred from one environment to another.
- C. capability of software to maintain its level of performance under stated conditions.
- D. relationship between the performance of the software and the amount of resources used.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Functionality is the set of attributes that bears on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs. Choice B refers to portability; choice C refers to reliability and choice D refers to efficiency.

NEW QUESTION: 929

Which of the following should an IS auditor expect to see in a network vulnerability assessment?

- A. Misconfiguration and missing updates
- B. Malicious software and spyware
- C. Zero-day vulnerabilities
- D. Security design flaws

Answer: (SHOW ANSWER)

A network vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network that could be exploited by attackers to compromise the confidentiality, integrity, or availability of the network or its resources. A network vulnerability assessment typically involves scanning the network devices, such as routers, switches, firewalls, servers, and workstations, using automated tools that compare the device configurations, software versions, and patch levels against a database of known vulnerabilities. A network vulnerability assessment can also include manual testing and verification of the network architecture, design, policies, and procedures. One of the main objectives of a network vulnerability assessment is to detect and report any misconfiguration and missing updates in the network devices that could pose a security risk¹.

Misconfiguration refers to any deviation from the recommended or best practice settings for the network devices, such as weak passwords, open ports, unnecessary services, default accounts, or incorrect permissions. Missing updates refer to any outdated or unsupported software or firmware that has not been patched with the latest security fixes or enhancements from the vendors². Misconfiguration and missing updates are common sources of network vulnerabilities that can be exploited by attackers to gain unauthorized access, execute malicious code, cause denial of service, or escalate privileges on the network devices³.

Therefore, an IS auditor should expect to see misconfiguration and missing updates in a network vulnerability assessment. The other options are less relevant or incorrect because:

* B. Malicious software and spyware are not usually detected by a network vulnerability assessment, as they are more related to the content and behavior of the network traffic rather than the configuration and patch level of the network devices. Malicious software and spyware are programs that infect or monitor the network devices or their users for malicious purposes, such as stealing data, displaying ads, or performing remote commands. Malicious software and spyware can be detected by other security tools, such as antivirus software, firewalls, or intrusion detection systems⁴.

* C. Zero-day vulnerabilities are not usually detected by a network vulnerability assessment, as they are unknown or undisclosed vulnerabilities that have not been reported or patched by the vendors or the security community. Zero-day vulnerabilities are rare and difficult to discover, as they require advanced techniques and skills to exploit them. Zero-day vulnerabilities can be detected by other security tools, such as intrusion prevention systems, anomaly detection systems, or artificial intelligence systems⁵.

* D. Security design flaws are not usually detected by a network vulnerability assessment, as they are more related to the logic and functionality of the network rather than the configuration and patch level of the network devices. Security design flaws are errors or weaknesses in the network architecture, design, policies, or procedures that could compromise the security objectives of the network. Security design flaws can be detected by other security methods, such as security reviews, audits, or assessments⁶. References: Network Vulnerability Assessment - ISACA, Network Vulnerability Scanning - NIST, Network Vulnerabilities - SANS, Malware - ISACA, Zero-Day Attacks

NEW QUESTION: 930

In which of the following payment mode, the payer creates payment transfer instructions, signs it digitally

and sends it to issuer?

- A. Electronic Money Model
- B. Electronics Checks model
- C. Electronic transfer model
- D. Electronic withdraw model

Answer: (SHOW ANSWER)

Section: Information System Acquisition, Development and Implementation

Explanation/Reference:

Electronic systems are simplest of three payment models. The payer simply creates a payment transfer

instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and

performs the transfer. This type of systems requires payer to be on-line and not payee.

For CISA exam you should know below information about payment systems

There are two types of parties involved in all payment systems - the issuer and the user. An issuer is an

entity that operates the payment service. An issuer holds the items that the payment represents.

The user

of the payment service performs two main functions- making payments and receiving payments - and

therefore can be described as a payer or payee receptively.

Electronic Money Model -The objective of electronic money systems is emulating physical cash.

An issuer

attempts to do this by creating digital certificates, which are then purchased by users who redeem them

with the issuer at a later date. In the interim, certificates can be transferred among users to trade for goods

or services. For the certificate to take on some of the attributes of physical cash, certain techniques are

used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the

certificate. This provides an electronic certificate with unconditional uncertainty.

Electronic Check Model -Electronic check system model real-world checks quite well and thus relatively

simple to understand and implement. A users write an electronic check, which is digitally signed instruction

to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

Electronic Transfer Model -Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

The following were incorrect answers:

Electronic Money Model -The objective of electronic money systems is emulating physical cash. An issuer attempts to do this by creating digital certificates, which are then purchased by users who redeem them with the issuer at a later date. In the interim, certificates can be transferred among users to trade for goods or services. For the certificate to take on some of the attributes of physical cash, certain techniques are used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the certificate. This provides an electronic certificate with unconditional uncertainty.

Electronic Check Model -Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

Electronic Withdraw Model - Not a valid type of payment system.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 183

NEW QUESTION: 931

An IS auditor is reviewing the release management process for an in-house software development solution. In which environment Is the software version MOST likely to be the same as production?

- A. Staging
- B. Testing
- C. Integration
- D. Development

Answer: ([SHOW ANSWER](#))

Explanation

A staging environment is a replica of the production environment that is used to test and verify software before deploying it to production. A staging environment is most likely to have the same software version as production, as it mimics the real-world conditions and configurations that will be encountered in production. A testing environment is a separate environment that is used to perform various types of testing on software, such as functional testing, performance testing, security testing, etc. A testing environment may not have the same software version as production, as it may undergo frequent changes or updates based on testing results or feedback. An integration environment is a separate environment that is used to combine and test software components or modules from different developers or sources, to ensure that they work together as expected.

An integration environment may not have the same software version as production, as it may involve different versions or branches of software from different sources. A development environment is a separate environment that is used by developers to create and modify software code. A development environment may not have the same software version as production, as it may contain unfinished or untested code that has not been released yet.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPass.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 932

Which of the following functionality is NOT performed by the application layer of a TCP/IP model?

- A. Print service, application services
- B. Data encryption and compression
- C. Dialog management
- D. End-to-end connection

Answer: ([SHOW ANSWER](#))

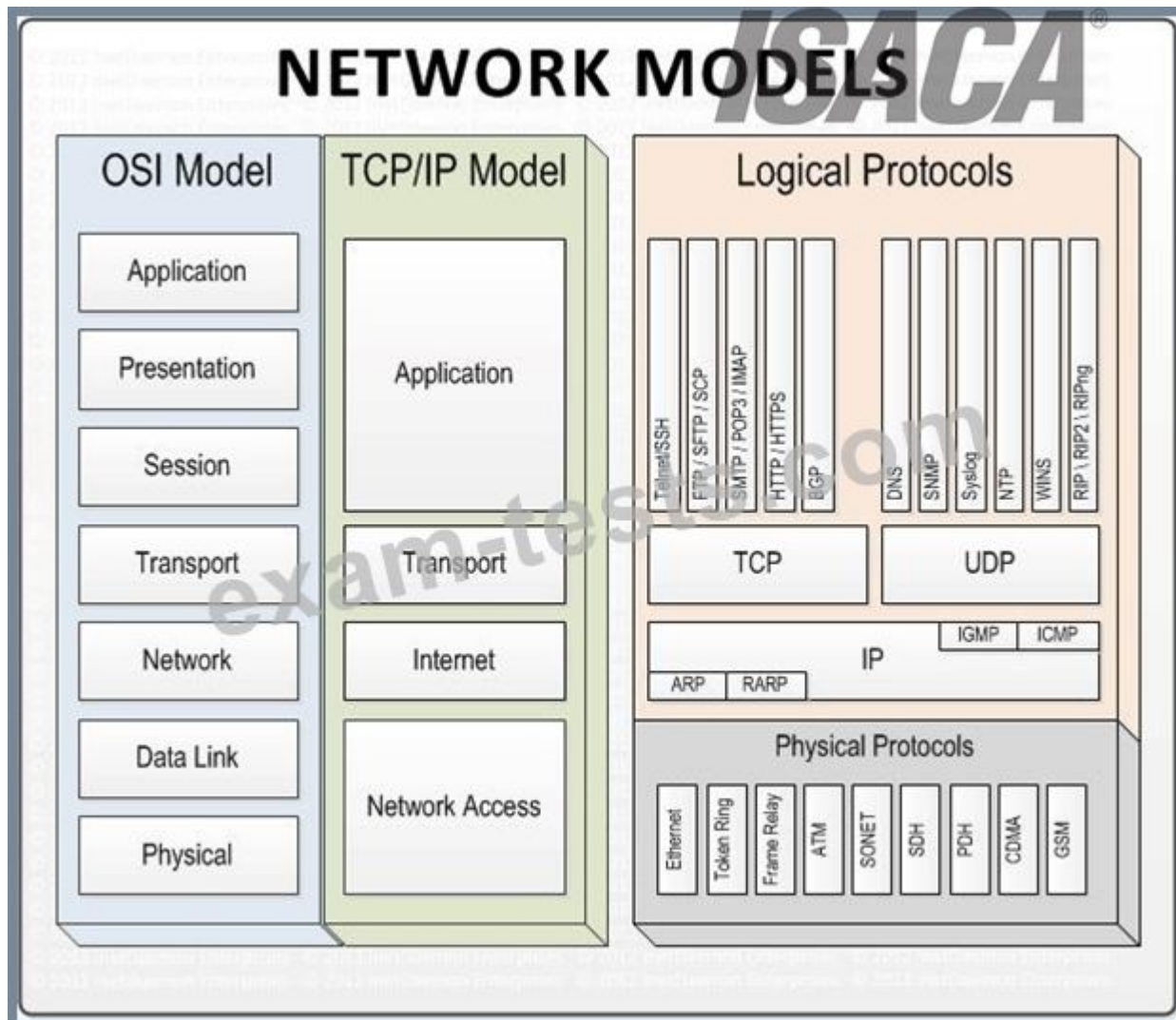
Explanation/Reference:

The word NOT is the keyword used in the question, You need to find out a functionality which is not performed by application layer of a TCP/IP model.

End-to-end connection is the Transport layer functionality in TCP/IP model.

For your exam you should know below information about TCP/IP model:

Network Models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

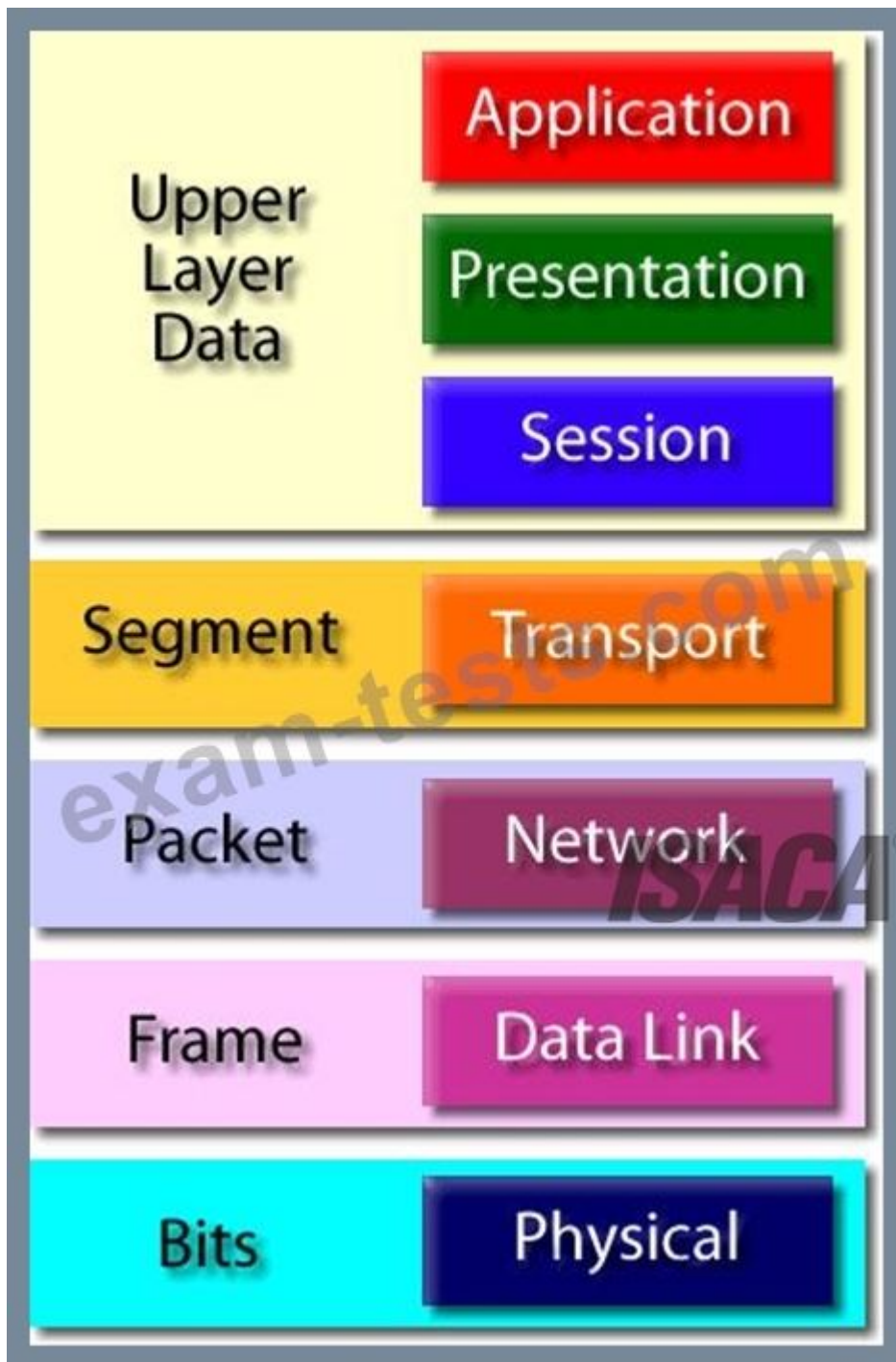
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

The other functionalities described in the options are performed by application layer in TCP/IP model.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

NEW QUESTION: 933

Which of the following would impair the independence of a quality assurance team?

- A.** Ensuring compliance with development methods
- B.** Checking the testing assumptions
- C.** Correcting coding errors during the testing process

D. Checking the code to ensure proper documentation

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Correction of code should not be a responsibility of the quality assurance team as it would not ensure segregation of duties and would impair the team's independence. The other choices are valid quality assurance functions.

NEW QUESTION: 934

In what way is a common gateway interface (CGI) MOST often used on a webserver?

- A.** Consistent way for transferring data to the application program and back to the user
- B.** Computer graphics imaging method for movies and TV
- C.** Graphic user interface for web design
- D.** interface to access the private gateway domain

Answer: ([SHOW ANSWER](#)**)**

Section: Protection of Information Assets

Explanation:

The common gateway interface (CGI) is a standard way for a web server to pass a user's request to an application program and to move data back and forth to the user. When the user requests a web page (for example, by clicking on a highlighted word orienteering a web site address), the server sends back the requested page. However, when a user fills out a form on a web page and submits it, it usually needs to be processed by an application program. The web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method, or convention, for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the web's HTTP protocol.

NEW QUESTION: 935

A small organization does not have enough employees to implement adequate segregation of duties in accounts payable. Which of the following is the BEST compensating control to mitigate the risk associated with this situation?

- A.** Regular reconciliation of key transactions approved by a supervisor
- B.** Supervisory review of logs to detect changes in vendors
- C.** Review of transactions exceeding a specific threshold
- D.** Rotation of duties among existing personnel

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 936

A benefit of quality of service (QoS) is that the:

- A. entire network's availability and performance will be significantly improved.
- B. telecom carrier will provide the company with accurate service-level compliance reports.
- C. participating applications will have guaranteed service levels.
- D. communications link will be supported by security controls to perform secure online transactions.

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

The main function of QoS is to optimize network performance by assigning priority to business applications and end users, through the allocation of dedicated parts of the bandwidth to specific traffic. Choice A is not true because the communication itself will not be improved. While the speed of data exchange for specific applications could be faster, availability will not be improved. The QoS tools that many carriers are using do not provide reports of service levels; however, there are other tools that will generate service-level reports. Even when QoS is integrated with firewalls, VPNs, encryption tools and others, the tool itself is not intended to provide security controls.

NEW QUESTION: 937

During a disaster recovery audit, an IS auditor finds that a business impact analysis (BIA) has not been performed. The auditor should FIRST:

- A. perform a business impact analysis (BIA).
- B. issue an intermediate report to management.
- C. evaluate the impact on current disaster recovery capability.
- D. conduct additional compliance testing.

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation/Reference:

NEW QUESTION: 938

An IS auditor reviewing a production support team's incident management procedures is evaluating whether appropriate prioritization criteria have been defined. Which of the following is MOST important to include as part of the prioritization criteria?

- A. Business impact
- B. Restore point
- C. Cost to restore
- D. Time to repair

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 939

The application systems quality assurance (QA) function should:

- A. assist programmers in designing and developing applications.
- B. ensure adherence of programs to standards.
- C. design and develop quality applications by employing system development methodology.
- D. compare programs to approved system changes.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 940

The following findings are the result of an IS auditor's post-implementation review of a newly implemented system. Which of the following findings is of GREATEST significance?

- A. A lessons-learned session was never conducted.
- B. The projects 10% budget overrun was not reported to senior management.
- C. Measurable benefits were not defined.
- D. Monthly dashboards did not always contain deliverables.

Answer: (SHOW ANSWER)

Explanation

A post-implementation review (PIR) is a process to evaluate whether the objectives of the project were met, determine how effectively this was achieved, learn lessons for the future, and ensure that the organisation gets the most benefit from the implementation of projects¹. A PIR is an important tool for assessing the success and value of a project, as well as identifying the areas for improvement and best practices for future projects.

One of the key elements of a PIR is to measure the benefits of the project against the expected outcomes and benefits that were defined at the beginning of the project. Measurable benefits are the quantifiable and verifiable results or outcomes that the project delivers to the organisation or its stakeholders, such as increased revenue, reduced costs, improved quality, enhanced customer satisfaction, or compliance with regulations².

Measurable benefits should be aligned with the organisation's strategy, vision, and goals, and should be SMART (specific, measurable, achievable, relevant, and time-bound).

The finding that measurable benefits were not defined is of greatest significance among the four findings, because it implies that:

The project did not have a clear and agreed-upon purpose, scope, objectives, and deliverables
The project did not have a valid and realistic business case or justification for its initiation and implementation
The project did not have a robust and effective monitoring and evaluation mechanism to track its progress, performance, and impact
The project did not have a reliable and transparent way to demonstrate its value proposition and return on investment to the organisation or its stakeholders
The project did not have a meaningful and actionable way to learn from its achievements and challenges, and to improve its processes and practices
Therefore, an IS auditor should recommend that measurable benefits are defined for any project before its

implementation, and that they are reviewed and reported regularly during and after the project's completion.

The other possible findings are:

A lessons-learned session was never conducted: This is a significant finding, but not as significant as the lack of measurable benefits. A lessons-learned session is a process of capturing and documenting the knowledge, experience, and feedback gained from a project, both positive and negative. A lessons-learned session helps to identify the strengths and weaknesses of the project management process, as well as the best practices and lessons for future projects. A lessons-learned session should be conducted at the end of each project phase or milestone, as well as at the end of the project. However, even without a formal lessons-learned session, some learning may still occur informally or implicitly among the project team members or stakeholders.

The projects 10% budget overrun was not reported to senior management: This is a significant finding, but not as significant as the lack of measurable benefits. A budget overrun is a situation where the actual cost of a project exceeds its planned or estimated cost. A budget overrun may indicate poor planning, estimation, or control of the project resources, or unexpected changes or risks that occurred during the project implementation. A budget overrun should be reported to senior management as soon as possible, along with the reasons for it and the corrective actions taken or proposed. However, a budget overrun may not necessarily affect the quality or value of the project deliverables or outcomes if they are still within acceptable standards or expectations.

Monthly dashboards did not always contain deliverables: This is a significant finding, but not as significant as the lack of measurable benefits. A dashboard is a visual tool that displays key performance indicators (KPIs) or metrics related to a project's progress, status, or results. A dashboard helps to monitor and communicate the performance of a project to various stakeholders in a concise and clear manner. A dashboard should include deliverables as one of its components, along with other elements such as schedule, budget, quality, risks, issues, or benefits. However, even without deliverables in monthly dashboards, some information about them may still be available from other sources such as reports or documents.

References: 1: What is Post-Implementation Review in Project Management? 2: The role & importance of the Post Implementation Review

NEW QUESTION: 941

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

- A.** Identify and evaluate the existing controls
- B.** Conduct a business impact analysis (BIA)
- C.** Report on existing controls
- D.** Propose new controls

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

After an IS auditor has identified threats and potential impacts, the auditor should then identify and evaluate the existing controls.

NEW QUESTION: 942

During an audit of a payroll system, an IS auditor identifies that two employees share the same bank account.

The auditor is concerned they may be ghost employees. Which of the following should the auditor do NEXT?

- A. Advise payroll management to suspend both employees accounts until further investigated.
- B. Notify the human resources executive immediately.
- C. Draft a report with a finding that there may be ghost employees.
- D. Conduct inquiries to determine whether the two employees have a relationship.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 943

When deploying an application that was created using the programming language and tools supported by the cloud provider, the MOST appropriate cloud computing model for an organization to adopt is:

- A. Platform as a Service (PaaS).
- B. Software as a Service (SaaS).
- C. Identity as a Service (IDaaS).
- D. Infrastructure as a Service (IaaS).

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 944

When deciding whether a third party can be used in resolving a suspected security breach, which of the following should be the MOST important consideration for IT management?

- A. Incident priority rating
- B. Audit approval
- C. Third-party cost
- D. Data sensitivity

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 945

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: ([SHOW ANSWER](#)**)**

Explanation/Reference:

Time stamps are an effective control for detecting duplicate transactions such as payments made or received.

NEW QUESTION: 946

Which of the following is the BEST reason for an organization to develop a business continuity plan?

- A. To develop a detailed description of information systems and processes
- B. To identify the users of information systems and processes
- C. To avoid the costs resulting from the failure of key systems and processes
- D. To establish business unit prioritization of systems, projects, and strategies

Answer: (SHOW ANSWER)

Section: Protection of Information Assets

Explanation/Reference: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Business-Continuity-Management-Audit-Assurance-Program.aspx>

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here: <https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 947

A message is being sent with a hash. The risk of an attacker changing the message and generating an authentic hash value can be mitigated by:

- A. requiring the recipient to use a different hash algorithm.
- B. generating hash output that is the same size as the original message.
- C. using a secret key in conjunction with the hash algorithm.
- D. using the sender's public key to encrypt the message.

Answer: (SHOW ANSWER)

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 948

Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceeding?

- A. Documentation evidence handling by personnel throughout the forensic investigation
- B. Engaging an independent third party to perform the forensic investigation

C. Performing investigate procedures on the original hard drives rather than images of the hard drives

D. Restricting evidence access to professionally certified forensic investigation

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 949

During an audit of a mortgage processing application, an IS auditor identifies that the application allows all users to export large quantities of sensitive customer data. Which of the following is the BEST control for the auditor to recommend to mitigate this risk?

A. Mask sensitive data within the application.

B. Periodically recertify user access.

C. Require strong passwords for application login.

D. Restrict download capability to authorized users.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 950

Which of the following environment controls is MOST appropriate in an area where power outages lasting up to 8 hours are frequent?

A. Data mirroring

B. A power generator

C. A surge protector

D. An alternate power supply line

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 951

The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

A. comply with regulatory requirements.

B. provide a basis for drawing reasonable conclusions.

C. ensure complete audit coverage.

D. perform the audit according to the defined scope.

Answer: B ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

The scope of an IS audit is defined by its objectives. This involves identifying control weaknesses relevant to the scope of the audit. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them. Complying with regulatory requirements, ensuring coverage and the execution of audit are all relevant to an audit but are not the reason why sufficient and relevant evidence is required.

NEW QUESTION: 952

The use of access control lists (ACLs) is the MOST effective method to mitigate security risk for routers because they: (Identify Correct answer and related explanation/references from CISA Certification - Information Systems Auditor official Manual or book)

- A. are recommended by security standards.
- B. can limit Telnet and traffic from the open Internet.
- C. act as fitters between the world and the network.
- D. can detect cyberattacks.

Answer: ([SHOW ANSWER](#))

The use of access control lists (ACLs) is the most effective method to mitigate security risk for routers because they can limit Telnet and traffic from the open Internet. Telnet is a protocol that allows remote access to a device, which can pose a security threat if not properly controlled. Traffic from the open Internet can also contain malicious packets that can harm the network or the router itself. ACLs act as filters that can block or allow specific types of traffic based on predefined criteria, such as source and destination addresses, protocols, ports, and flags. By using ACLs, routers can prevent unauthorized access and reduce the exposure to potential attacks.

References:

- * Protecting Your Core: Infrastructure Protection Access Control Lists
- * Definition, purposes, benefits, and functions of ACL
- * CISA Review Manual 27th Edition, page 336

NEW QUESTION: 953

Which of the following is MOST important to ensure when developing an effective security awareness program?

- A. Training personnel are information security professionals.
- B. Outcome metrics for the program are established.
- C. Security threat scenarios are included in the program content.
- D. Phishing exercises are conducted post-training

Answer: B ([LEAVE A REPLY](#))

The most important factor to ensure when developing an effective security awareness program is B. Outcome metrics for the program are established. This is because outcome metrics are measures that evaluate the impact and results of the security awareness program on the behavior and performance of the users, and the security posture and objectives of the organization¹. Outcome metrics can help ensure the effectiveness of the security awareness program by: Providing feedback and evidence on whether the security awareness program is achieving its goals and expectations, such as reducing the number of incidents, improving the compliance rate, or increasing the reporting rate¹. Identifying and quantifying the strengths and weaknesses of the security awareness program, and enabling continuous improvement and optimization of the program content, delivery, and frequency¹.

Demonstrating and communicating the value and return on investment of the security awareness program to the stakeholders and management, and securing their support and commitment for the program¹.

NEW QUESTION: 954

Sending a message and a message hash encrypted by the sender's private key will ensure:

- A. authenticity and integrity.
- B. authenticity and privacy.
- C. integrity and privacy.
- D. privacy and nonrepudiation.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

If the sender sends both a message and a message hash encrypted by its private key, then the receiver can apply the sender's public key to the hash and get the message hash. The receiver can apply the hashing algorithm to the message received and generate a hash. By matching the generated hash with the one received, the receiver is ensured that the message has been sent by the specific sender, i.e., authenticity, and that the message has not been changed enroute. Authenticity and privacy will be ensured by first using the sender's private key and then the receiver's public key to encrypt the message. Privacy and integrity can be ensured by using the receiver's public key to encrypt the message and sending a message hash/digest. Only nonrepudiation can be ensured by using the sender's private key to encrypt the message. The sender's public key, available to anyone, can decrypt a message; thus, it does not ensure privacy.

NEW QUESTION: 955

An IS auditor should expect the responsibility for authorizing access rights to production data and systems to be entrusted to the:

- A. process owners.
- B. system administrators.
- C. security administrator.
- D. data owners.

Answer: D ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Data owners are primarily responsible for safeguarding the data and authorizing access to production data on a need-to-know basis.

NEW QUESTION: 956

Which of the following BEST determines if a batch update job was successfully executed?

- A. Reviewing a copy of the script for the job
- B. Testing a sample of transactions to confirm updates were applied

- C. Verifying the timestamp from the job log
- D. Obtaining process owner confirmation that the job was completed

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 957

Responsibility for the governance of IT should rest with the:

- A. IT strategy committee.
- B. chief information officer (CIO).
- C. audit committee.
- D. board of directors.

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly. The audit committee, the chief information officer (CIO) and the IT strategy committee all play a significant role in the successful implementation of IT governance within an organization, but the ultimate accountability resides with the board of directors.

NEW QUESTION: 958

Which of the following is MOST important for an IS auditor to consider when evaluating an organization's effectiveness in mitigating Internal fraud risk?

- A. Segregation of duty controls
- B. Network monitoring controls
- C. Data leakage prevention controls
- D. Data encryption controls

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 959

During the design of a business continuity plan, the business impact analysis (BIA) identifies critical processes and supporting applications. This will PRIMARILY influence the:

- A. responsibility for maintaining the business continuity plan.
- B. criteria for selecting a recovery site provider.
- C. recovery strategy.
- D. responsibilities of key personnel.

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

The most appropriate strategy is selected based on the relative risk level and criticality identified in the business impact analysis (BIA.) The other choices are made after the selection or design of the appropriate recovery strategy.

NEW QUESTION: 960

Which of the following indicates that an internal audit organization is structured to support the independence and clarity of the reporting process?

- A.** Auditors are responsible for performing operational duties or activities.
- B.** The internal audit manager reports functionally to a senior management official.
- C.** The internal audit manager has a reporting line to the audit committee.
- D.** Auditors are responsible for assessing and operating a system of internal controls.

Answer: ([**SHOW ANSWER**](#)**)**

Explanation

The internal audit manager should have a reporting line to the audit committee, which is an independent body that oversees the internal audit function and ensures its objectivity and accountability. Reporting functionally to a senior management official may compromise the independence and clarity of the internal audit reporting process, as senior management may have a vested interest in the audit results or influence the audit scope and priorities. *References: According to the ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 1002 Independence, "The chief audit executive (CAE) should report functionally to the board or its equivalent (e.g., audit committee) and administratively to executive management." 1

NEW QUESTION: 961

What are trojan horse programs?

- A.** A common form of internal attack
- B.** Malicious programs that require the aid of a carrier program such as email
- C.** Malicious programs that can run independently and can propagate without the aid of a carrier program such as email
- D.** A common form of Internet attack

Answer: D ([**LEAVE A REPLY**](#)**)**

Explanation/Reference:

Explanation: Trojan horse programs are a common form of Internet attack.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

NEW QUESTION: 962

IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

- A. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.
- B. The service provider does not have incident handling procedures.
- C. Recently a corrupted database could not be recovered because of library management problems.
- D. incident logs are not being reviewed.

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

The lack of a disaster recovery provision presents a major business risk. Incorporating such a provision into the contract will provide the outsourcing organization leverage over the service provider. Choices B, C and D are problems that should be addressed by the service provider, but are not as important as contract requirements for disaster recovery.

NEW QUESTION: 963

AN IS auditor has been asked to perform an assurance review of an organization's mobile computing security.

To ensure the organization is able to centrally manage mobile devices to protect against data disclosure. It is MOST important for the auditor to determine whether:

- A. procedures for lost devices include remote wiping of data
- B. lost devices can be located remotely
- C. a security exist for mobile devices.
- D. a mobile security awareness training program exists.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 964

To support an organization's goals, an IS department should have:

- A. a low-cost philosophy.
- B. long- and short-range plans.
- C. leading-edge technology.
- D. plans to acquire new hardware and software.

Answer: ([SHOW ANSWER](#)**)**

To ensure its contribution to the realization of an organization's overall goals, the IS department should have long- and short-range plans that are consistent with the organization's broader plans for attaining its goals. Choices A and C are objectives, and plans would be needed to delineate

how each of the objectives would be achieved. Choice D could be a part of the overall plan but would be required only if hardware or software is needed to achieve the organizational goals.

NEW QUESTION: 965

An IS auditor is following up on prior period items and finds management did not address an audit finding.

Which of the following should be the IS auditor's NEXT course of action?

- A.** Note the exception in a new report as the item was not addressed by management.
- B.** Recommend alternative solutions to address the repeat finding.
- C.** Conduct a risk assessment of the repeat finding.
- D.** Interview management to determine why the finding was not addressed.

Answer: D ([LEAVE A REPLY](#))

If an IS auditor finds that management did not address a prior period audit finding, the next course of action should be to interview management to determine why the finding was not addressed, as this would help to understand the root cause, the impact, and the risk level of the issue. Noting the exception in a new report, recommending alternative solutions, or conducting a risk assessment are possible subsequent steps, but they should not precede interviewing management. References: CISA Review Manual (Digital Version), Chapter 1, Section 1.6

NEW QUESTION: 966

Which of the following BEST describes the concept of fault tolerance in system resiliency?

- A.** It enables switching to redundant systems in case of faults.
- B.** It minimizes downtime and ensures continuous operations.
- C.** It allows systems to continue operating in the presence of faults.
- D.** It distributes workloads across multiple servers to prevent overload.

Answer: ([SHOW ANSWER](#)**)**

Comprehensive and Detailed Explanation:

Fault tolerance refers to the ability of a system to continue functioning despite the occurrence of faults or hardware failures.

- * Option A: Describes failover, not fault tolerance.
- * Option B: Is a benefit but not the exact definition.
- * Option D: Refers to load balancing, not fault tolerance.

ISACA Reference: CISA Review Manual 27th Edition, Domain 2, section on system availability, resilience, and fault tolerance.

NEW QUESTION: 967

Which of the following is the GREATEST advantage of maintaining an internal IS audit function within an organization?

- A.** Increased IS audit staff visibility and availability throughout the year
- B.** Ability to negotiate recommendations with management
- C.** Increased independence and impartiality of recommendations

D. Better understanding of the business and processes

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 968

Which of the following is a technique that could be used to capture network user passwords?

A. Encryption

B. Sniffing

C. Spoofing

D. Data destruction

Answer: B ([LEAVE A REPLY](#))

Sniffing is an attack that can be used to capture sensitive pieces of information (e.g., a password) passing through the network. Encryption is a method of scrambling information to prevent unauthorized individuals from understanding the transmission. Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication. Data destruction is erasing information or removing it from its original location.

NEW QUESTION: 969

An IS auditor invited to a development project meeting notes that no project risks have been documented.

When the IS auditor raises this issue, the project manager responds that it is too early to identify risks and that, if risks do start impacting the project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

A. stress the importance of spending time at this point in the project to consider and document risks, and to develop contingency plans.

B. accept the project manager's position as the project manager is accountable for the outcome of the project.

C. offer to work with the risk manager when one is appointed.

D. inform the project manager that the IS auditor will conduct a review of the risks at the completion of the requirements definition phase of the project.

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

The majority of project risks can typically be identified before a project begins, allowing mitigation/avoidance plans to be put in place to deal with these risks. A project should have a clear link back to corporate strategy and tactical plans to support this strategy. The process of setting corporate strategy, setting objectives and developing tactical plans should include the consideration of risks. Appointing a risk manager is a good practice but waiting until the project has been impacted by risks is misguided. Risk management needs to be forward looking; allowing risks to evolve into issues that adversely impact the project represents a failure of risk management. With or without a risk manager, persons within and outside of the project team need to be consulted and encouraged to comment when they believe new risks have emerged or risk priorities have

changed. The IS auditor has an obligation to the project sponsor and the organization to advise on appropriate project management practices. Waiting for the possible appointment of a risk manager represents an unnecessary and dangerous delay to implementing risk management.

NEW QUESTION: 970

An organization shares some of its customers' personally Identifiable Information (PII) with third-party suppliers for business purposes. What is MOST important for the IS auditor to evaluate to ensure that risk associated with leakage of privacy-related data during transmission is effectively managed?

- A. The third party's privacy and data security policies
- B. Nondisclosure and indemnity agreements
- C. Service and operational level agreements
- D. Encrypting and masking of customer data

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 971

During a disaster recovery audit, an IS auditor finds that a business impact analysis (BIA) has not been performed. The auditor should FIRST.

- A. evaluate the impact on current disaster recovery capability.
- B. issue an intermediate report to management
- C. perform business impact analysis
- D. conduct additional compliance testing

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 972

The information security policy that states 'each individual must have their badge read at every controlled door' addresses which of the following attack methods?

- A. Piggybacking
- B. Shoulder surfing
- C. Dumpster diving
- D. Impersonation

Answer: A ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into

restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger, if

every employee must have their badge read at every controlled door no unauthorized person could enter

the sensitive area. Looking over the shoulder of a user to obtain sensitive information could be done by an unauthorized person who has gained access to areas using piggybacking, but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method. Impersonation refers to a social engineer acting as an employee, trying to retrieve the desired information. Some forms of social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

NEW QUESTION: 973

Of the following alternatives, the FIRST approach to developing a disaster recovery strategy would be to assess whether:

- A. all threats can be completely removed.
- B. a cost-effective, built-in resilience can be implemented.
- C. the recovery time objective can be optimized.
- D. the cost of recovery can be minimized.

Answer: (SHOW ANSWER)

It is critical to initially identify information assets that can be made more resilient to disasters, e.g., diverse routing, alternate paths or multiple communication carriers. It is impossible to remove all existing and future threats. The optimization of the recovery time objective and efforts to minimize the cost of recovery come later in the development of the disaster recovery strategy.

NEW QUESTION: 974

Which of the following observations should be of GREATEST concern to an IS auditor performing an audit of change and release management controls for a new complex system developed by a small in-house IT team?

- A. Access to change testing strategy and results is not restricted to staff outside the IT team.
- B. Some user acceptance testing (UAT) was completed by members of the IT team.
- C. IT administrators have access to the production and development environment
- D. Post-implementation testing is not conducted for all system releases.

Answer: (SHOW ANSWER)

Post-implementation testing is the process of verifying and validating the functionality, performance, and security of a system after it has been deployed to the production environment¹. Post-implementation testing is important for ensuring that the system meets the user requirements and expectations, as well as the operational and business objectives. Post-

implementation testing also helps to identify and resolve any defects, errors, or issues that may have occurred during the deployment process or that may have been missed during the previous testing stages².

Therefore, the observation that post-implementation testing is not conducted for all system releases should be of greatest concern to an IS auditor performing an audit of change and release management controls for a new complex system developed by a small in-house IT team. This observation indicates that the system may have quality, reliability, or security problems that could affect the user satisfaction, system performance, or data integrity. This observation also suggests that the change and release management controls are not adequate or effective, as they do not ensure that all system releases are properly tested and validated before and after deployment.

Option A is not correct because access to change testing strategy and results is not restricted to staff outside the IT team is not a major concern for an IS auditor. While it is good practice to limit access to sensitive or confidential information, such as test data or test cases, to authorized personnel only, access to change testing strategy and results may not pose a significant risk to the system or the organization. Moreover, access to change testing strategy and results may be beneficial for some stakeholders outside the IT team, such as business users, project managers, or auditors, who may need to review or evaluate the testing process or outcomes.

Option B is not correct because some user acceptance testing (UAT) was completed by members of the IT team is not a major concern for an IS auditor. User acceptance testing is the process of verifying and validating that the system meets the user requirements and expectations by involving actual or representative users in the testing process³. While it is preferable to have independent and unbiased users perform UAT, it may not be feasible or practical for some organizations, especially those with small or limited resources. Therefore, some UAT may be completed by members of the IT team, as long as they have sufficient knowledge and experience of the user needs and expectations, and as long as they follow the UAT plan and criteria.

Option C is not correct because IT administrators have access to the production and development environment is not a major concern for an IS auditor. IT administrators are responsible for managing and maintaining the IT infrastructure, including the production and development environments⁴. Therefore, it is reasonable and necessary for them to have access to both environments, as long as they follow the appropriate policies and procedures for accessing, using, and securing them. Moreover, IT administrators may need to perform tasks such as backup, restore, patching, or troubleshooting in both environments.

References:

- * What Is Post Implementation Testing?¹
- * Post Implementation Review (PIR) - Definition & Process²
- * User Acceptance Testing (UAT): Definition & Examples³
- * What Is an IT Administrator? Definition & Examples⁴

NEW QUESTION: 975

Which of the following encrypt/decrypt steps provides the GREATEST assurance of achieving

confidentiality, message integrity and nonrepudiation by either sender or recipient?

- A. The recipient uses their private key to decrypt the secret key.
- B. The encrypted prehash code and the message are encrypted using a secret key.
- C. The encrypted prehash code is derived mathematically from the message to be sent.
- D. The recipient uses the sender's public key, verified with a certificate authority, to decrypt the prehash code.

Answer: ([SHOW ANSWER](#))

Section: Protection of Information Assets

Explanation:

Most encrypted transactions use a combination of private keys, public keys, secret keys, hash functions

and digital certificates to achieve confidentiality, message integrity and nonrepudiation by either sender or

recipient. The recipient uses the sender's public key to decrypt the prehash code into a posthash code,

which when equaling the prehash code, verifies the identity of the sender and that the message has not

been changed in route; this would provide the greatest assurance. Each sender and recipient has a private

key known only to themselves and a public key, which can be known by anyone. Each encryption/decryption process requires at least one public key and one private key, and both must be from the same

party. A single, secret key is used to encrypt the message, because secret key encryption requires less

processing power than using public and private keys. A digital certificate, signed by a certificate authority,

validates senders' and recipients' public keys.

NEW QUESTION: 976

Which of the following human resources management practices BEST leads to the detection of fraudulent activity?

- A. Background checks
- B. Time reporting
- C. Employee code of ethics
- D. Mandatory time off

Answer: D ([LEAVE A REPLY](#))

Section: Governance and Management of IT

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 977

Which of the following findings would be of MOST concern to an IS auditor performing a review of an end-user developed application that generates financial statements?

- A. There is not adequate training in the use of the application.
- B. There is no adequate user license for the application.
- C. The application is not sufficiently supported by the IT department
- D. There is no control to ensure accuracy of the processed data.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 978

The use of control totals reduces the risk of:

- A. posting to the wrong record.
- B. incomplete processing.
- C. improper backup.
- D. improper authorization.

Answer: ([SHOW ANSWER](#)**)**

Explanation

Control totals are a method of verifying the accuracy and completeness of data processing by comparing the totals of key fields in input and output records¹. Control totals can be used to reduce the risk of incomplete processing, which is the failure to process all the data or transactions that are expected or required².

Incomplete processing can result in data loss, inconsistency, or incompleteness, which can affect the quality and reliability of the information system and its outputs. Incomplete processing can be caused by various factors, such as:

Hardware or software failures that interrupt the processing or transmission of data² Human errors or omissions that skip or miss some data or transactions² Malicious attacks or unauthorized access that delete or modify some data or transactions² Environmental hazards or disasters that damage or destroy some data or transactions² Control totals can help detect and prevent incomplete processing by:

Providing a benchmark or reference point to compare the input and output data or transactions¹ Identifying any discrepancies or deviations from the expected or required totals¹ Alerting the users or operators to investigate and resolve the causes of incomplete processing¹ Ensuring that all the data or transactions are properly transmitted, converted, and processed¹ The other options

are not as relevant as control totals for reducing the risk of incomplete processing. Posting to the wrong record is the error of assigning or transferring data or transactions to an incorrect account, file, or record³. Improper backup is the failure to create, store, or restore copies of data or transactions in case of loss, corruption, or damage⁴. Improper authorization is the lack of proper permission or approval to access, modify, or process data or transactions. Control totals may not be able to prevent or detect these errors or failures, as they are not related to the completeness of data processing. Therefore, option B is the correct answer.

References:

control totals - Barrons Dictionary - AllBusiness.com

What is control total amount? - Sage Advice US

Posting Error Definition

Backup Definition

[Authorization Definition]

NEW QUESTION: 979

Which of the following findings from a database security audit presents the GREATEST risk of critical security exposures?

- A. Legacy data has not been purged.
- B. Admin account passwords are not set to expire.
- C. Default settings have not been changed.
- D. Database activity logging is not complete.

Answer: ([SHOW ANSWER](#))

Admin accounts typically have the highest level of privileges and access to sensitive data. If the passwords for these accounts are not set to expire, it increases the risk of unauthorized access and potential security breaches. This is especially true if an admin's credentials are compromised, as the attacker could have ongoing access to critical systems and data¹.

References:

Database Auditing - Satori

NEW QUESTION: 980

The FIRST step in establishing a firewall security policy is to determine the:

- A. expected data Throughput.
- B. business requirements,
- C. necessary logical access rights
- D. existing firewall configuration,

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 981

Which of the following statements appearing in an organization's acceptable use policy BEST demonstrates alignment with data classification standards related to the protection of information assets?

- A. Any information assets transmitted over a public network must be approved by executive management.
- B. All information assets must be encrypted when stored on the organization's systems.
- C. Information assets should only be accessed by persons with a justified need.
- D. All information assets will be assigned a clearly defined level to facilitate proper employee handling.

Answer: ([SHOW ANSWER](#))

Explanation

The statement that BEST demonstrates alignment with data classification standards related to the protection of information assets is D. All information assets will be assigned a clearly defined level to facilitate proper employee handling. Data classification involves categorizing information assets based on their sensitivity, importance, and usage. Assigning clearly defined levels (such as public, internal, confidential, etc.) to information assets ensures that appropriate security controls are applied based on their classification. By doing so, organizations can manage access, encryption, and other protective measures effectively¹².

References:

IFRC. "Information Security: Acceptable Use

Policy." 1(<https://www.ifrc.org/sites/default/files/2021-11/IFRC-Information-Security-Acceptable-Use-Po> UNSW Sydney. "Data Classification Standard."

2(<https://www.unsw.edu.au/content/dam/pdfs/governance/policy/2022-01-policies/datastandard> Digital Guardian. "What is a Data Classification Policy?"

3(<https://www.digitalguardian.com/blog/what-data-classification-policy>) Microsoft Service Trust Portal. "Data classification & sensitivity label taxonomy." 4(<https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-classification-and-label> Clark University ITS Policies.

"Data Classification - Data Security Policies."

5(https://www2.clarku.edu/offices/its/policies/data_classification.cfm)

NEW QUESTION: 982

An IS auditor is reviewing vulnerability scanning results of an organization's critical systems. Which of the following is the BEST way to validate that the vulnerabilities have been remediated?

- A. Interview owners of vulnerability scanning systems for evidence.
- B. Review change management documentation for remediation.
- C. Re-scan the vulnerable systems.
- D. Review patch management documentation.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 983

Which of the following is the MOST appropriate testing approach when auditing a daily data flow between two systems via an automated interface to confirm that it is complete and accurate?

- A. Confirm that the encryption standard applied to the interface is in line with best practice.
- B. Inspect interface configurations and an example output of the systems.

- C. Perform data reconciliation between the two systems for a sample of 25 days.
- D. Conduct code review for both systems and inspect design documentation.

Answer: C ([LEAVE A REPLY](#))

Explanation

The most appropriate testing approach when auditing a daily data flow between two systems via an automated interface is to perform data reconciliation between the two systems for a sample of 25 days. Data reconciliation is a process of verifying that the data transferred from one system to another is complete and accurate, and that there are no discrepancies or errors in the data flow¹. Data reconciliation can be performed by using generalized audit software, which is a type of computer-assisted audit technique (CAAT) that allows the IS auditor to perform various audit tasks on the data stored in different file formats and databases². By performing data reconciliation for a sample of 25 days, the IS auditor can test the reliability and consistency of the data flow over a reasonable period of time, and identify any potential issues or anomalies that could affect the quality of the data or the functionality of the systems.

References

1: Data Flow Testing - GeeksforGeeks 2: Generalized Audit Software (GAS) - ISACA

NEW QUESTION: 984

Which of the following findings would be of GREATEST concern when reviewing a business impact analysis (BIA)?

- A. There is not adequate documentation to perform a recovery
- B. Several key business processes were not included.
- C. The recovery point objective (RPO) is not accreted.
- D. The business continuity plan (BCP) does not align with corporate strategy.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 985

Which of the following is a reason for implementing a decentralized IT governance model?

- A. Greater responsiveness to business needs
- B. Standardized controls and economies of scale
- C. IT synergy among business units
- D. Greater consistency among business units

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 986

An organization implemented a cybersecurity policy last year Which of the following is the GREATE ST indicator that the policy may need to be revised"⁷ :

- A. A significant increase in cybersecurity audit findings
- B. A significant increase in external attack attempts
- C. A significant increase in authorized connections to third parties
- D. A significant increase in approved exceptions

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 987

During a review of a production schedule, an IS auditor observes that a staff member is not complying with mandatory operational procedures. The auditor's NEXT step should be to:

- A. Include the noncompliance in the audit report
- B. Determine why the procedures were not followed
- C. Note the noncompliance in the audit working papers
- D. Issue an audit memorandum identifying the incompliance

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 988

What is the definition of a work breakdown structure?

- A. A detailed staffing plan
- B. Sequence of steps with milestones in support of the project scope
- C. The levels of authority delegated by the project manager
- D. Decomposition of tasks

Answer: ([SHOW ANSWER](#))

A work breakdown structure is the decomposition of tasks necessary to perform the required work for the project.

NEW QUESTION: 989

Which of the following activities would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA)?

- A. Implementing the remediation plan
- B. Partially completing the CSA
- C. Developing the remediation plan
- D. Developing the CSA questionnaire

Answer: D ([LEAVE A REPLY](#))

Explanation

Developing the CSA questionnaire is an activity that would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA). An IS auditor can design and provide a CSA questionnaire to help the business units or process owners to evaluate their own controls and identify any issues or improvement opportunities. This will enable an IS auditor to support and guide the CSA process without compromising their objectivity or independence. The other options are activities that would impair an IS auditor's independence while facilitating a CSA, as they involve implementing, completing, or developing remediation actions for control issues. References:

CISA Review Manual (Digital Version), Chapter 2, Section 2.41

CISA Review Questions, Answers & Explanations Database, Question ID 215

NEW QUESTION: 990

An IS auditor has completed a service level management audit related to order management services provided by a third party. Which of the following is the MOST significant finding?

- A. The third party has offshore support arrangements.
- B. The service level agreement does not define how availability is measured.
- C. Penalties for missing service levels are limited.
- D. Service desk support is not available outside the company's business hours.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 991

An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the GREATEST risk?

- A. Pilot
- B. Parallel
- C. Direct cutover
- D. Phased

Answer: C ([LEAVE A REPLY](#))

Section: Protection of Information Assets

Explanation:

Direct cutover implies switching to the new system immediately, usually without the ability to revert to the old system in the event of problems. All other alternatives are done gradually and thus provide greater recoverability and are therefore less risky.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam! BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:

<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As

Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 992

A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:

- A. payroll reports should be compared to input forms.
- B. gross payroll should be recalculated manually.
- C. checks (cheques) should be compared to input forms.
- D. checks (cheques) should be reconciled with output reports.

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

Explanation:

The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports. Hence, comparing payroll reports with input forms is the best mechanism of verifying data accuracy. Recalculating gross payroll manually would only verify whether the processing is correct and not the data accuracy of inputs.

Comparing checks (cheques) to input forms is not feasible as checks (cheques) have the processed information and input forms have the input data. Reconciling checks (cheques) with output reports only confirms that checks (cheques) have been issued as per output reports.

NEW QUESTION: 993

Adding security requirements late in the software development life cycle would MOST likely result in:

- A. cost savings
- B. clearer understanding of requirements
- C. operational efficiency
- D. compensating controls

Answer: [\(SHOW ANSWER\)](#)

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 994

A business unit cannot achieve desired segregation of duties between operations and programming due to size constraints. Which of the following is MOST important for the IS auditor to identify*?

- A. Controls over operational effectiveness
- B. Additional control weaknesses
- C. Unauthorized user controls
- D. Compensating controls

Answer: D [\(LEAVE A REPLY\)](#)

NEW QUESTION: 995

Off-site data storage should be kept synchronized when preparing for recovery of time-sensitive data such as that resulting from which of the following? Choose the BEST answer.

- A. Financial reporting
- B. Sales reporting
- C. Inventory reporting
- D. Transaction processing

Answer: D [\(LEAVE A REPLY\)](#)

Off-site data storage should be kept synchronized when preparing for the recovery of timesensitive data such as that resulting from transaction processing.

NEW QUESTION: 996

Which of the following features would BEST address risk associated with data at rest when evaluating a data loss prevention (DLP) solution?

- A. File movement detection
- B. Printing of scan files
- C. Enforcement of access policies
- D. Storage-scanning technology

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 997

Which of the following is the MAIN responsibility of the IT steering committee?

- A. Reviewing and assisting with IT strategy integration efforts
- B. Developing and assessing the IT security strategy
- C. Implementing processes to integrate security with business objectives
- D. Developing and implementing the secure system development framework

Answer: A ([LEAVE A REPLY](#))

Explanation

This means that the IT steering committee is responsible for ensuring that the IT strategy aligns with and supports the business strategy, vision, and goals of the organization. The IT steering committee is also responsible for overseeing and approving major IT initiatives, projects, and investments, and allocating resources and priorities accordingly¹².

Developing and assessing the IT security strategy (B) is not the main responsibility of the IT steering committee, but rather a specific aspect of the IT strategy that may be delegated to a subcommittee or a dedicated security function. The IT steering committee may provide guidance and oversight for the IT security strategy, but it is not directly involved in developing and assessing it¹².

Implementing processes to integrate security with business objectives is not the main responsibility of the IT steering committee, but rather an operational task that may be performed by the IT management and staff. The IT steering committee may monitor and evaluate the effectiveness of the security processes, but it is not directly involved in implementing them¹².

Developing and implementing the secure system development framework (D) is not the main responsibility of the IT steering committee, but rather a technical task that may be performed by the IT developers and engineers. The IT steering committee may approve and endorse the secure system development framework, but it is not directly involved in developing and implementing it¹².

NEW QUESTION: 998

The PRIMARY purpose for an IS auditor to review previous audit reports during the planning phase of a current audit is to:

- A. become informed about the auditee's business processes.

- B. identify applicable regulatory requirements for the current audit.
- C. adjust audit scope to reduce testing in areas related to previous findings.
- D. ensure that previously identified risks are addressed in the audit program.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 999

An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

- A. variable sampling.
- B. substantive testing.
- C. compliance testing.
- D. stop-or-go sampling.

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized. Variable sampling is used to estimate numerical values, such as dollar values. Substantive testing substantiates the integrity of actual processing, such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be minimized. Stop-or-go sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.

Valid CISA Dumps shared by BraindumpsPass.com for Helping Passing CISA Exam!
BraindumpsPass.com now offer the **newest CISA exam dumps**, the BraindumpsPass.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com CISA dumps with Test Engine here:
<https://www.braindumpsPASS.com/ISACA/CISA-practice-exam-dumps.html> (1435 Q&As
Dumps, **40%OFF** Special Discount: **Exam-Tests**)