ISACA.CISA.v2025-09-01.q454

Exam Code:	CISA
Exam Name:	Certified Information Systems Auditor
Certification Provider:	ISACA
Free Question Number:	454
Version:	v2025-09-01
# of views:	132
# of Questions views:	4540
https://www.dumpsdb.com/dumps/ISACA/CISA/ISACA.CISA.v2025-09-01.q454	

NEW QUESTION: 1
Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:
A. include the statement of management in the audit report.
B. identify whether such software is, indeed, being used by the organization.
C. reconfirm with management the usage of the software.
D. discuss the issue with senior management since reporting this could have a negative impact on the organization.
Answer: (SHOW ANSWER)
When there is an indication that an organization might be using unlicensed software, the IS auditor should obtain sufficient evidence before including it in the report. With respect to this matter, representations obtained from management cannot be independently verified. If the organization is using software that is not licensed, the auditor, to maintain objectivity and independence, must include this in the report.

NEW QUESTION: 2
What is the BEST backup strategy for a large database with data supporting online sales?
A. Weekly full backup with daily incremental backup
B. Daily full backup
C. Clustered servers
D. Mirrored hard disks
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:

Weekly full backup and daily incremental backup is the best backup strategy; it ensures the ability to recover the database and yet reduces the daily backup time requirements. A full backup normally requires a couple of hours, and therefore it can be impractical to conduct a full backup every day. Clustered servers provide a redundant processing capability, but are not a backup. Mirrored hard disks will not help in case of disaster.

NEW QUESTION: 3
Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?
A. Field checks
B. Control totals
C. Reasonableness checks
D. A before-and-after maintenance report
Answer: D (LEAVE A REPLY)
A before-and-after maintenance report is the best answer because a visual review would provide the most positive verification that updating was proper.

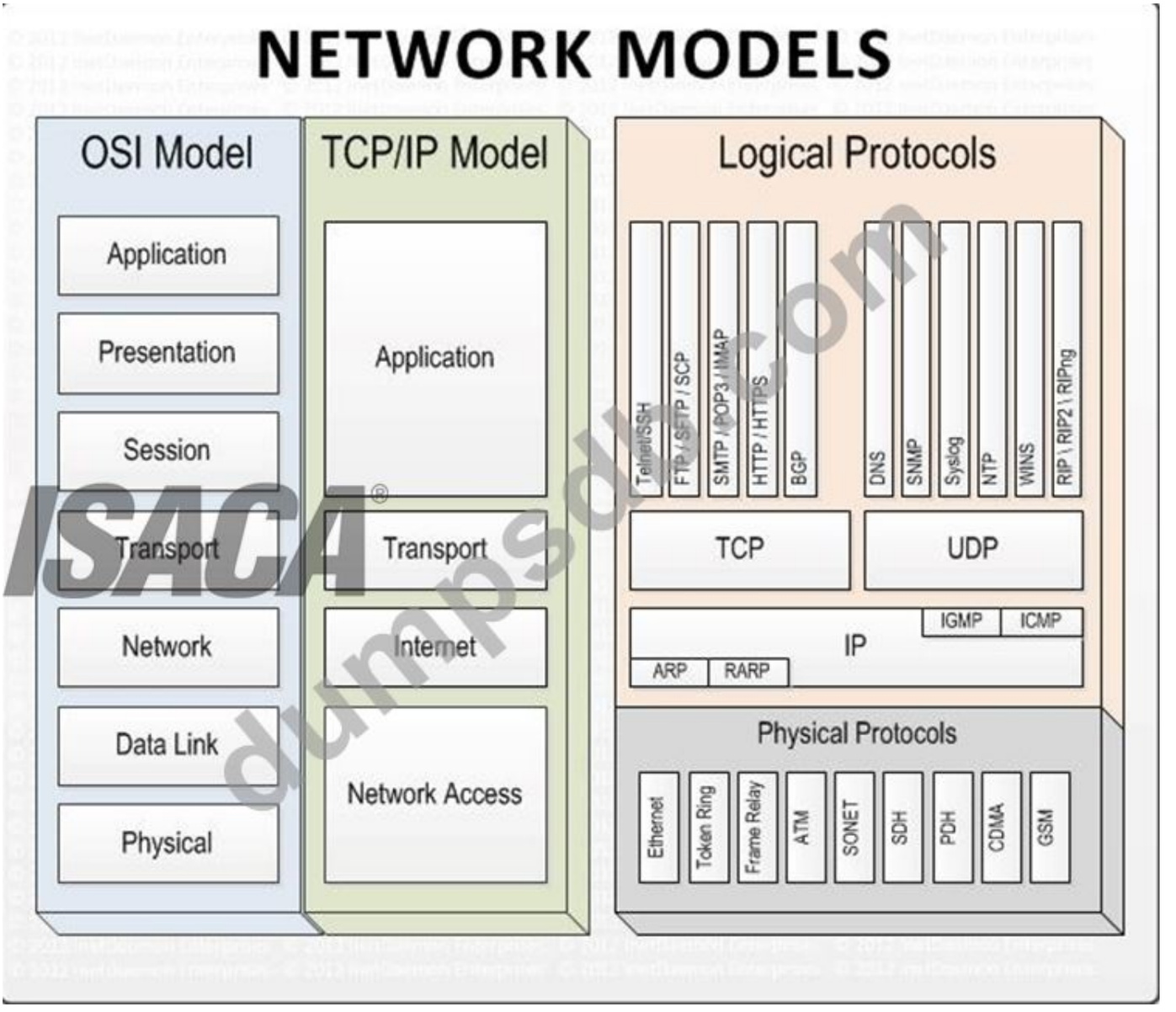
NEW QUESTION: 4
When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:
A. allow changes, which will be completed using after-the-fact follow-up.
B. allow undocumented changes directly to the production library.
C. do not allow any emergency changes.
D. allow programmers permanent access to production programs.
Answer: (SHOW ANSWER)
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 becompleted using after-thefact 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: 5
Which of the following types of firewalls provide the GREATEST degree and granularity of control?
A. Screaming router
B. Packet filter
C. Application gateway
D. Circuit gateway

Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The application gateway is similar to a circuit gateway, but it has specific proxies for each service. To handle web services, it has an HTTP proxy that acts as an intermediary between externals and internals, but is specifically for HTTP. This means that it not only checks the packet IP addresses (layer 3) and the ports it is directed to (in this case port 80, or layer 4), it also checks every HTTP command (layers 5 and
7). Therefore, it works in a more detailed (granularity) way than the others. Screening router and packet filter (choices A and BJ work at the protocol, service and/or port level. This means that they analyze packets from layers 3 and 4, and not from higher levels. A circuit gateway (choice D) is based on a proxy or program that acts as an intermediary between external and internal accesses. This means that during an external access, instead of opening a single connection to the internal server, two connections are established-one from the external server to the proxy (which conforms the circuit-gateway) and one from the proxy to the internal server. Layers 3 and 4 (IP and TCP) and some general features from higher protocols are used to perform these tasks.

NEW QUESTION: 6
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: (SHOW ANSWER)
Section: Governance and Management of IT

NEW QUESTION: 7
Which of the following is protocol data unit (PDU) of data at LAN or WAN interface layer in TCP/IP model?
A. Data
B. Segment
C. Packet
D. Frame and bits
Answer: D (LEAVE A REPLY)
Explanation/Reference:
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.

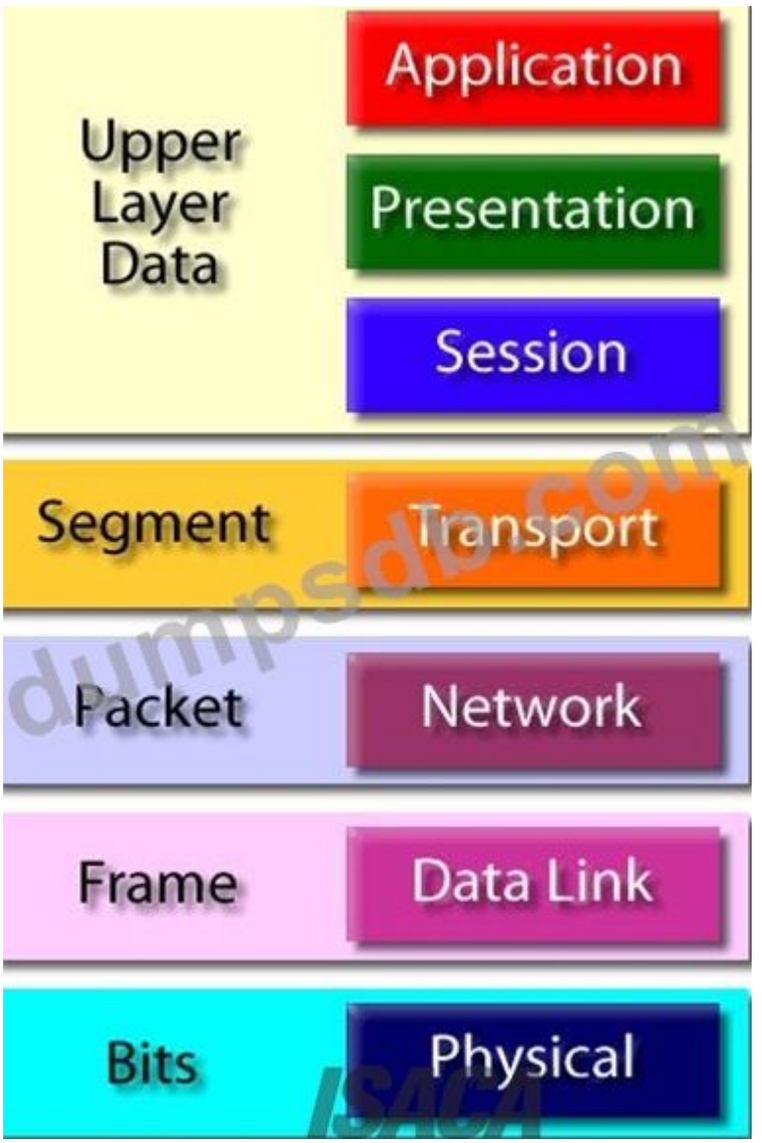
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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:
Data - Application layer data PDU
Segment - Transport layer data PDU
Packet - Network interface layer data PDU
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 272

NEW QUESTION: 8
Which of the following should be of MOST concern to an IS auditor during the review of a quality management system?
A. Indicators are not fully represented in the quality management system.
B. The quality management system includes training records for IT personnel.
C. There are no records to document actions for minor business processes.
D. Important quality checklists are maintained outside the quality management system.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9

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: 10

An organization is planning to develop a system using rapid application development (RAD) in order to meet quick turnaround times. Which of the following is the GREATEST potential risk associated with this type of application development?

A. Costs could spiral out of control.

B. The project deadline could be delayed.
C. User requirements may not be met.
D. Users may be unavailable to contribute.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
When performing an audit of access rights, an IS auditor should be suspicious of which of the following if
allocated to a computer operator?
A. Read access to data
B. Delete access to transaction data files
C. Logged read/execute access to programs
D. Update access to job control language/script files
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation:
Deletion of transaction data files should be a function of the application support team, not operations staff.
Read access to production data is a normal requirement of a computer operator, as is logged access to
programs and access to JCL to control job execution.

NEW QUESTION: 12
Which of the following would lead an IS auditor to conclude that the evidence collected during a digital forensic investigation would not be admissible in court?
A. The person who collected the evidence is not qualified to represent the case.
B. The logs failed to identify the person handling the evidence.
C. The evidence was collected by the internal forensics team.
D. The evidence was not fully backed up using a cloud-based solution prior to the trial.
Answer: (SHOW ANSWER)
The evidence collected during a digital forensic investigation would not be admissible in court if the logs failed to identify the person handling the evidence. This would violate the chain of custody principle, which requires that the evidence be properly documented, secured, and tracked throughout the investigation process.
The chain of custody ensures that the evidence is authentic, reliable, and trustworthy, and that it has not been tampered with or altered. The person who collected the evidence, whether qualified or not, is not relevant to the admissibility of the evidence, as long as they followed the proper procedures and protocols. The evidence collected by the internal forensics team can be admissible in court, as long as they are independent, objective, and competent. The evidence does not need to be fully backed up using a cloud-based solution prior to the trial, as long as it is

preserved and protected from damage or loss. References: ISACA Journal Article: Digital Forensics: Chain of Custody

NEW QUESTION: 13
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. Incident response roles and responsibilities
B. Incident response staff experience and qualifications
C. Results from management testing of incident response procedures
D. Past incident response actions
Answer: (SHOW ANSWER)

NEW QUESTION: 14
A bank has a combination of corporate customer accounts (higher monetary value) and small business accounts (lower monetary value) as part of online banking. Which of the following is the BEST sampling approach for an IS auditor to use for these accounts?
A. Difference estimation sampling
B. Stratified mean per unit sampling
C. Customer unit sampling
D. Unstratified mean per unit sampling
Answer: B (LEAVE A REPLY)
Stratified mean per unit sampling is a method of audit sampling that divides the population into subgroups (strata) based on some characteristic, such as monetary value, and then selects a sample from each stratum using mean per unit sampling. Mean per unit sampling is a method of audit sampling that estimates the total value of a population by multiplying the average value of the sample items by the number of items in the population. Stratified mean per unit sampling is suitable for populations that have a high variability or a skewed distribution, such as the bank accounts in this question. By stratifying the population, the auditor can reduce the sampling error and increase the precision of the estimate.
Difference estimation sampling (option A) is not the best sampling approach for these accounts. Difference estimation sampling is a method of audit sampling that estimates the total error or misstatement in a population by multiplying the average difference between the book value and the audited value of the sample items by the number of items in the population. Difference estimation sampling is suitable for populations that have a low variability and a symmetrical distribution, which is not the case for the bank accounts in this question.
Customer unit sampling (option C) is not a sampling approach, but a type of monetary unit sampling.
Monetary unit sampling is a method of audit sampling that selects sample items based on their monetary value, rather than their physical units. Customer unit sampling is a variation of monetary unit sampling that treats each customer account as a single unit, regardless of how many transactions or balances it contains.

Customer unit sampling may be appropriate for testing existence or occurrence assertions, but not for estimating total values.
Unstratified mean per unit sampling (option D) is not the best sampling approach for these accounts.
Unstratified mean per unit sampling is a method of audit sampling that applies mean per unit sampling to the entire population without dividing it into subgroups. Unstratified mean per unit sampling may result in a larger sample size and a lower precision than stratified mean per unit sampling, especially for populations that have a high variability or a skewed distribution, such as the bank accounts in this question.
Therefore, option B is the correct answer.
References:
* Audit Sampling - AICPA
* Audit Sampling: Examples and Guidance To The Sampling Methods
* Audit Sampling | Audit | Financial Audit - Scribd

NEW QUESTION: 15
Phishing attack works primarily through:
A. email and hyperlinks
B. SMS
C. chat
D. email attachment
E. news
F. file download
G. None of the choices.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Phishing applies to email appearing to come from a legitimate business, requesting ""verification"" of information and warning of some dire consequence if it is not done. The letter usually contains a link to a fradulent web page that looks legitimate and has a form requesting everything from a home address to an ATM card's PIN.

NEW QUESTION: 16
Tunneling provides additional security for connecting one host to another through the Internet by:
A. preventing password cracking and replay attacks
B. providing end-to-end encryption.
C. enabling the use of stronger encryption keys
D. facilitating the exchange of public key infrastructure (PKI) certificates
Answer: A (LEAVE A REPLY)

NEW QUESTION: 17
Codes from exploit programs are frequently reused in:
A. trojan horses only.
B. computer viruses only.
C. OS patchers.
D. eavedroppers.
E. trojan horses and computer viruses.
F. None of the choices.
Answer: E (LEAVE A REPLY)
"The term ""exploit"" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in trojan horses and computer viruses. In some cases, a vulnerability can lie in a certain programs processing of a specific file type, such as a non-executable media file."

NEW QUESTION: 18
Hamid needs to shift users from using the application from the existing (Old) system to the replacing (new)
system. His manager Lily has suggested he uses an approach in which the newer system is changed over
from the older system on a cutoff date and time and the older system is discontinued once the changeover
to the new system takes place. Which of the following changeover approach is suggested by Lily?
A. Parallel changeover
B. Phased changeover
C. Abrupt changeover
D. Pilot changeover
Answer: C (LEAVE A REPLY)
Section: Information System Acquisition, Development and Implementation
Explanation/Reference:
In the abrupt changeover approach the newer system is changed over from the older system on a cutoff
date and time, and the older system is discontinued once changeover to the new system takes place.

Changeover refers to an approach to shift users from using the application from the existing (old) system to
the replacing (new) system.
Changeover to newer system involves four major steps or activities
Conversion of files and programs; test running on test bed
Installation of new hardware, operating system, application system and the migrated data.
Training employees or user in groups
Scheduling operations and test running for go-live or changeover
Some of the risk areas related to changeover includes:
Asset safeguarding
Data integrity
System effectiveness
Change management challenges
Duplicate or missing records
The following were incorrect answers:
Parallel changeover - This technique includes running the old system, then running both the old and new
systems in parallel and finally full changing over to the new system after gaining confidence in the working
of new system.
Phased Changeover -In this approach the older system is broken into deliverables modules. Initially, the
first module of older system is phased out using the first module of a new system. Then, the second
module of the newer system is phased out, using the second module of the newer system and so forth until
reaching the last module.
Pilot changeover - Not a valid changeover type.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 172

NEW QUESTION: 19
Due to the increasing size of a database, user access times and daily backups continue to increase. Which of the following would be the BEST way to address this situation?
A. Data mining
B. Data modeling
C. Data visualization
D. Data purging
Answer: (SHOW ANSWER)

NEW QUESTION: 20

An organization has introduced a capability maturity model to the system development life cycle (SDLC) to measure improvements. Which of the following is the BEST indication of successful process improvement?

A. Evaluation results align with defined business goals

B. Evaluation results exceed process maturity benchmarks against competitors.

C. Processes demonstrate the mitigation of inherent business risk

D. Process maturity reaches the highest state of process optimization

Answer: A (LEAVE A REPLY)

NEW QUESTION: 21

Which of the following is the PRIMARY reason for an IS auditor to select a statistical sampling method?

A. Statistical sampling methods are the most effective way to avoid sampling risk.

B. Statistical sampling methods must be used to mitigate audit risk.

C. Statistical sampling methods help the auditor to determine the tolerable error rate.

D. Statistical sampling methods enable the auditor to objectively quantify the probability of error.

Answer: (SHOW ANSWER)

NEW QUESTION: 22

Which of the following is the BEST way to determine il IT is delivering value to the business?

A. Interview key IT managers and service providers.

B. Analyze downtime frequency and duration.

C. Review IT service level agreement (SLA) results.

D. Perform control self-assessments (CSAs).

Answer: C (LEAVE A REPLY)

NEW QUESTION: 23

During an audit of a disaster recovery plan (DRP) for a critical business area, an IS auditor finds that not all critical systems are covered. What should the auditor do NEXT?

A. Verify whether the systems are part of the business impact analysis (BIA).

B. Evaluate the impact of not covering the systems.

C. Evaluate the prior year's audit results regarding critical system coverage.

D. Escalate the finding to senior management.

Answer: (SHOW ANSWER)

NEW QUESTION: 24

Which of the following provides the MOST protection against emerging threats?

A. Demilitarized zone (DMZ)

B. Signature-based intrusion detection system (IDS)

C. Real-time updating of antivirus software

D. Heuristic intrusion detection system (IDS)

Answer: (SHOW ANSWER)

NEW QUESTION: 25
What is the PRIMARY objective of implementing data classification?
A. Employ data leakage prevention tools.
B. Establish appropriate data protection methods.
C. Create awareness among users.
D. Establish appropriate encryption methods.
Answer: (SHOW ANSWER)
Section: Protection of Information Assets

NEW QUESTION: 26
Which of the following is a feature of an intrusion detection system (IDS)?
A. Gathering evidence on attack attempts
B. Identifying weaknesses in the policy definition
C. Blocking access to particular sites on the Internet
D. Preventing certain users from accessing specific servers
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation:
An IDS can gather evidence on intrusive activity such as an attack or penetration attempt. Identifying weaknesses in the policy definition is a limitation of an IDS. Choices C and D are features of firewalls, while choice B requires a manual review, and therefore is outside the functionality of an IDS.

NEW QUESTION: 27
Which of the following observations would an IS auditor consider the GREATEST risk when conducting an audit of a virtual server farm tor potential software vulnerabilities?
A. Guest operating systems are updated monthly
B. The hypervisor is updated quarterly.
C. A variety of guest operating systems operate on one virtual server
D. Antivirus software has been implemented on the guest operating system only.
Answer: D (LEAVE A REPLY)
Antivirus software has been implemented on the guest operating system only is the observation that an IS auditor would consider the greatest risk when conducting an audit of a virtual server farm for potential software vulnerabilities. A virtual server farm is a collection of servers that run multiple virtual machines (VMs) on a single physical host using a software layer called a hypervisor. A guest operating system is the operating system installed on each VM. Antivirus software is a software program that detects and removes malicious software from a computer system. If antivirus software has been implemented on the guest operating system only, it means

that the hypervisor and the host operating system are not protected from malware attacks, which could compromise the security and availability of all VMs running on the same host.
Therefore, antivirus software should be implemented on both the guest and host operating systems as well as on the hypervisor. References: CISA Review Manual, 27th Edition, page 378

NEW QUESTION: 28
An IS auditor discovers that validation controls in a web application have been moved from the server side into the browser to boost performance. This would MOST likely increase the risk of a successful attack by:
A. structured query language (SQL) injection
B. buffer overflow.
C. denial of service (DoS).
D. phishing.
Answer: A (LEAVE A REPLY)
Validation controls are used to check the input data from the user before processing it on the server. If the validation controls are moved from the server side to the browser, it means that the user can modify or bypass them using tools such as browser developer tools, JavaScript console, or proxy tools. This would increase the risk of a successful attack by structured query language (SQL) injection, which is a technique that exploits a security vulnerability in an application's software layer that allows an attacker to execute arbitrary SQL commands on the underlying database. SQL injection can result in data theft, data corruption, or unauthorized access to the system.
Buffer overflow, denial of service (DoS), and phishing are not directly related to the validation controls in a web application. Buffer overflow is a type of attack that exploits a memory management flaw in an application or system that allows an attacker to write data beyond the allocated buffer size and overwrite adjacent memory locations. DoS is a type of attack that prevents legitimate users from accessing a service or resource by overwhelming it with requests or traffic. Phishing is a type of attack that uses fraudulent emails or websites to trick users into revealing sensitive information or installing malware.
References:
* Client-side form validation - Learn web development | MDN
* JavaScript: client-side vs. server-side validation - Stack Overflow
* SQL Injection - OWASP

NEW QUESTION: 29
The GREATEST benefit of using a prototyping approach in software development is that it helps to:
A. improve efficiency of quality assurance (QA) testing
B. decrease the time allocated for user testing and review.
C. conceptualize and classify requirements.
D. minimize scope changes to the system.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 30
The GREATEST concern for an IS auditor reviewing vulnerability assessments by the auditee would be if the assessments are:
A. Conducted once per year just before system audits are scheduled.
B. Conducted by the internal technical team instead of external experts.
C. Performed for critical systems, not for the entire infrastructure.
D. Performed using open-source testing tools.
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Conducting vulnerability assessmentsonly once per year, right before an audit,creates a false sense of securityandleaves systems exposedbetween assessments.
* Annual Testing Before Audit (Correct Answer - A)
* Risksundetected vulnerabilitiesfor extended periods.
* Example:A company only tests security before acompliance audit, allowingzero-day threatsto persist for months.
* Internal Team Conducting Assessments (Incorrect - B)
* Not ideal, butregular assessmentsare more critical.
* Focusing on Critical Systems (Incorrect - C)
* Not perfect, butbetter than no testing at all.
* Using Open-Source Tools (Incorrect - D)
* Open-source toolscan be effective ifproperly configured.
References:
* ISACA CISA Review Manual
* NIST 800-115 (Technical Guide to Security Testing)

NEW QUESTION: 31
Which of the following is an IS auditor's BEST approach when prepanng to evaluate whether the IT strategy supports the organization's vision and mission?
A. Review strategic projects tor 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: C (LEAVE A REPLY)
Explanation
The best approach for an IS auditor to evaluate whether the IT strategy supports the organization's vision and mission is to meet with senior management to understand the business goals and how IT can enable them. This will help the IS auditor to assess the alignment and integration of IT with the business strategy and to identify any gaps or opportunities for improvement. Reviewing ROIs, KPIs, or feedback from other departments may provide some

insights, but they are not sufficient to evaluate the IT strategy. References: IS Audit and Assurance Standards, section "Standard 1201: Engagement Planning"

NEW QUESTION: 32
What control detects transmission errors by appending calculated bits onto the end of each segment of data?
A. Reasonableness check
B. Parity check
C. Redundancy check
D. Check digits
Answer: (SHOW ANSWER)
A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of datA . A reasonableness check compares data to predefined reasonability limits or occurrence rates established for the datA . A parity check isa hardware control that detects data errors when data are read from one computer to another, from memory or during transmission. Check digits detect transposition and transcription errors.

NEW QUESTION: 33
Which of the following establishes the role of the internal audit function?
A. Audit objectives
B. Audit governance
C. Audit charter
D. Audit project plan
Answer: C (LEAVE A REPLY)

NEW QUESTION: 34
Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?
A. implement segregation of duties.
B. Apply single sign-on tot access control.
C. Enforce the use of digital signatures
D. Enforce an internal data access policy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 35
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 seventy of this finding, which mitigating factor would MOST significantly minimize the associated impact?
A. There are documented compensating controls over the business processes.
B. The risk acceptances were previously reviewed and approved by appropriate senior management
C. The business environment has not significantly changed since the risk acceptances were approved.
D. The risk acceptances with issues reflect a small percentage of the total population
Answer: A (LEAVE A REPLY)
Explanation
The mitigating factor that would most significantly minimize the impact of not renewing IT risk acceptances in a timely manner is having documented compensating controls over the business processes. Compensating controls are alternative controls that reduce or eliminate the risk when the primary control is not feasible or cost-effective. The other factors, such as previous approval by senior management, unchanged business environment, and small percentage of issues, do not mitigate the risk as effectively as compensating controls.
References: ISACA CISA Review Manual 27th Edition Chapter 1

NEW QUESTION: 36
Which of the following is MOST critical to the success of an information security program?
A. User accountability for information security
B. Management's commitment to information security
C. Integration of business and information security
D. Alignment of information security with IT objectives
Answer: (SHOW ANSWER)
Management's commitment to information security is the most critical factor for the success of an information security program, as it sets the tone and direction for the organization's security culture and practices. Management's commitment is demonstrated by establishing a clear security policy, providing adequate resources, assigning roles and responsibilities, enforcing compliance, and supporting continuous improvement. The other options are important elements of an information security program, but they depend on management's commitment to be effective. References: CISA Review Manual (Digital Version) 1, page
439.

NEW QUESTION: 37
An IS auditor who was instrumental m designing an application is called upon to review the application. The auditor should:

A. use the knowledge of the application to carry out the audit
B. into in audit management of the earlier involvement
C. modify the scope of the audit
D. refuse the assignment to avoid conflict of interest
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38
To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:
A. during data preparation.
B. in transit to the computer.
C. between related computer runs.
D. during the return of the data to the user department.
Answer: A (LEAVE A REPLY)
During data preparation is the best answer, because it establishes control at the earliest point.

NEW QUESTION: 39
Which of the following is MOST important for the IS auditor to verify when reviewing the development process of a security policy?
A. Output from the enterprise's risk management system
B. Identification of the control framework
C. Evidence of management approval
D. Evidence of active involvement of key stakeholders
Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
Which of the following would provide the BEST evidence that a cloud provider's change management process is effective?
A. A copy of change management policies provided by the vendor
B. Minutes from regular change management meetings with the vendor
C. The results of a third-party review provided by the vendor
D. Written assurances from the vendor's CEO and CIO
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41
Talking about biometric authentication, which of the following is often considered as a mix of both physical and behavioral characteristics?
A. Voice
B. Finger measurement
C. Body measurement
D. Signature

E. None of the choices.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Biometric authentication refers to technologies that measure and analyze human physical and behavioral characteristics for authentication purposes.
Physical characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while behavioral characteristics include signature, gait and typing patterns. Voice is often considered as a mix of both physical and behavioral characteristics.

NEW QUESTION: 42
Users are complaining that a newly released enterprise resource planning (ERP) system is functioning too slowly. Which of the following tests during the quality assurance (QA) phase would have identified this concern?
A. Stress
B. Regression
C. Interface
D. Integration
Answer: A (LEAVE A REPLY)
Stress testing is a type of performance testing that evaluates how a system behaves under extreme load conditions, such as high user traffic, large data volumes, or limited resources. It is useful for identifying potential bottlenecks, errors, or failures that may affect the system's functionality or availability. Stress testing during the quality assurance (QA) phase would have identified the concern of users complaining that a newly released ERP system is functioning too slowly. The other options are not as relevant for this concern, as they relate to different aspects of testing, such as regression testing (verifying that existing functionality is not affected by new changes), interface testing (verifying that the system interacts correctly with other systems or components), or integration testing (verifying that the system works as a whole after combining different modules or units). References: CISA Review Manual (Digital Version), Domain 5: Protection of Information Assets, Section 5.4 Testing Techniques1

NEW QUESTION: 43
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: (SHOW ANSWER)

Section: The process of Auditing Information System

NEW QUESTION: 44
Which of the following audit procedures would provide the BEST assurance that an application program is functioning as designed?
A. Using a continuous auditing module
B. Interviewing business management
C. Confirming accounts
D. Reviewing program documentation
Answer: (SHOW ANSWER)
Using a continuous auditing module is an audit procedure that would provide the best assurance that an application program is functioning as designed. A continuous auditing module is a software tool that performs automated and continuous testing and monitoring of an application program's inputs, outputs, processes, and controls. A continuous auditing module can help to verify the accuracy, completeness, validity, reliability, and timeliness of the application program's data and transactions. A continuous auditing module can also help to identify and report any errors, anomalies, deviations, or exceptions in the application program's performance or compliance.
The other options are not as effective or relevant as using a continuous auditing module for providing assurance that an application program is functioning as designed. Interviewing business management is a technique for obtaining information and opinions from the users or owners of the application program, but it does not directly test or verify the functionality or quality of the application program. Confirming accounts is a technique for verifying the existence and accuracy of account balances or transactions, but it does not necessarily reflect the design or operation of the application program. Reviewing program documentation is a technique for examining the specifications, requirements, and procedures of the application program, but it does not provide evidence of the actual implementation or execution of the application program.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2361
* Continuous audit and monitoring - PwC2

NEW QUESTION: 45
Which of the following projects would be MOST important to review in an audit of an organizations financial statements?
A. Automation of operational risk management processes
B. Security enhancements to the customer relationship database
C. Outsourcing of the payroll system to an external service provider
D. Resource optimization of the enterprise resource planning (ERP) system
Answer: C (LEAVE A REPLY)

NEW QUESTION: 46

Which of the following metrics would BEST measure the agility of an organization's IT function?
A. Average number of learning and training hours per IT staff member
B. Frequency of security assessments against the most recent standards and guidelines
C. Average time to turn strategic IT objectives into an agreed upon and approved initiative
D. Percentage of staff with sufficient IT-related skills for the competency required of their roles
Answer: C (LEAVE A REPLY)
The metric that would best measure the agility of an organization's IT function is average time to turn strategic IT objectives into an agreed upon and approved initiative. IT agility is the ability of an IT function to respond quickly and effectively to changing business needs and opportunities. By measuring how fast an IT function can translate strategic IT objectives into actionable initiatives, such as projects or programs, an organization can assess how well its IT function can align with and support its business strategy. Average number of learning and training hours per IT staff member, frequency of security assessments against the most recent standards and guidelines, and percentage of staff with sufficient IT-related skills for the competency required of their roles are metrics that may indicate other aspects of IT performance, such as capability development, security maturity, and skills gap analysis, but they do not directly measure IT agility.
References: ISACA Journal Article: Measuring IT Agility

NEW QUESTION: 47
An IS auditor found that a company executive is encouraging employee use of social networking sites for business purposes. Which of the following recommendations would BEST help to reduce the risk of data leakage?
A. Monitoring employees social networking usage
B. Requiring policy acknowledgment and nondisclosure agreements signed by employees
C. Providing education and guidelines to employees on use of social networking sites
D. Establishing strong access controls on confidential data
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
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)
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: 49
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. system integration testing was performed.
C. all errors found in the testing process have been corrected.
D. the business process owner has signed off on the results.
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Which of the following would MOST effectively control the usage of universal storage bus (USB) storage devices?
A. Policies that require instant dismissal if such devices are found
B. Software for tracking and managing USB storage devices
C. Administratively disabling the USB port
D. Searching personnel for USB storage devices at the facility's entrance
Answer: B (LEAVE A REPLY)
Software for centralized tracking and monitoring would allow a USB usage policy to be applied to each user based on changing business requirements, and would provide for monitoring and reporting exceptions to management. A policy requiring dismissalmay result in increased employee attrition and business requirements would not be properly addressed. Disabling ports would be complex to manage and might not allow for new business needs. Searching of personnel for USB storage devices at the entrance to a facility is not a practical solution since these devices are small and could be easily hidden.

NEW QUESTION: 51
A national tax administration agency with a distributed network experiences service disruptions due to a large influx of traffic to a regional office near the end of each year. Which of the following would BEST enable the agency to improve the performance of its servers during the busy period?
A. Virtual firewall

B. Proxy server
C. Load balancer
D. Virtual private network (VPN)
Answer: C (LEAVE A REPLY)
Explanation
A load balancer is a tool or application that distributes incoming network traffic among multiple servers in a server farm, so that no server is overwhelmed and the performance of the system is optimized1. A load balancer can help the agency to handle the large influx of traffic to a regional office by balancing the workload among the available servers and preventing service disruptions. A load balancer can also provide high availability and fault tolerance by rerouting traffic to online servers if a server becomes unavailable2.
A virtual firewall is a software-based firewall that protects a virtual network or environment from unauthorized access and malicious attacks. A virtual firewall can enhance the security of the agency's network, but it does not improve the performance of its servers.
A proxy server is an intermediary server that acts as a gateway between the client and the destination server, hiding the client's IP address and providing caching and filtering functions. A proxy server can improve the security and privacy of the agency's network, but it does not improve the performance of its servers.
A virtual private network (VPN) is a secure connection between two or more devices over a public network, such as the internet. A VPN can encrypt and protect the data transmitted over the network, but it does not improve the performance of the agency's servers.

NEW QUESTION: 52
During the course of fieldwork, an internal IS auditor observes a critical vulnerability within a newly deployed application. What is the auditor's BEST course of action?
A. Notify IT management.
B. Document the finding in the report.
C. Identify other potential vulnerabilities.
D. Report the finding to the external auditors.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 53
To address an organization's disaster recovery requirements, backup intervals should not exceed the:
A. service level objective (SLO).
B. recovery time objective (RTO).
C. recovery point objective (RPO).
D. maximum acceptable outage (MAO).
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:

The recovery point objective (RPO) defines the point in time to which data must be restored after a disaster so as to resume processing transactions. Backups should be performed in a way that the latest backup is no older than this maximum time frame. If service levels are not met, the usual consequences are penalty payments, not cessation of business. Organizations will try to set service level objectives (SLOs) so as to meet established targets. The resulting time for the service level agreement (SLA) will usually be longer than the RPO. The recovery time objective (RTO) defines the time period after the disaster in which normal business functionality needs to be restored. The maximum acceptable outage (MAO) is the maximum amount of system downtime that is tolerable. It can be used as a synonym for RTO. However, the RTO denotes an objective/target, while the MAO constitutes a vital necessity for an organization's survival.

NEW QUESTION: 54
An organization is developing a web portal using some external components. Which of the following should be of MOST concern to an IS auditor?
A. Staff require additional training in order to perform cede review.
B. The organization has not reviewed the components for known exploits.
C. Open-source components were integrated during development.
D. Some of the developers are located in another country.
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Which of the following is the BEST way to prevent social engineering incidents?
A. Maintain an onboarding and annual security awareness program.
B. Ensure user workstations are running the most recent version of antivirus software.
C. Include security responsibilities in job descriptions and require signed acknowledgment.
D. Enforce strict email security gateway controls
Answer: (SHOW ANSWER)
Explanation
Maintaining an onboarding and annual security awareness program is the best way to prevent social engineering incidents because it can educate the users about the common techniques and tactics used by social engineers and how to avoid falling victim to them. Ensuring user workstations are running the most recent version of antivirus software, including security responsibilities in job descriptions and requiring signed acknowledgment, and enforcing strict email security gateway controls are all good security practices, but they do not directly address the human factor that is exploited by social engineering. References:
ISACA, CISA Review Manual, 27th Edition, 2020, p. 3671
ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2

NEW QUESTION: 56
Which of the following should occur EARLIEST in a business continuity management lifecycle?
A. Identifying critical business processes

B. Developing a training and awareness program
C. Carrying out a threat and risk assessment
D. Defining business continuity procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 57
While evaluating logical access control the IS auditor should follow all of the steps mentioned below EXCEPT one?
1. Obtain general understanding of security risk facing information processing, through a review of relevant documentation, inquiry and observation,etc
2. Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness
3. Test Control over access paths to determine whether they are functioning and effective by applying appropriate audit technique
4. Evaluate the access control environment to determine if the control objective are achieved by analyzing test result and other audit evidence
5. Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures, and comparing them with appropriate security standard or practice and procedures used by other organization.
6. Evaluate and deploy technical controls to mitigate all identified risks during audit.
A. 2
B. 3
C. 1
D. 6
Answer: D (LEAVE A REPLY)
Explanation/Reference:
The word EXCEPT is the keyword used in the question. You need find out the item an IS auditor should not perform while evaluating logical access control. It is not an IT auditor's responsibility to evaluate and deploy technical controls to mitigate all identified risks during audit.
For CISA exam you should know below information about auditing logical access:
Obtain general understanding of security risk facing information processing, through a review of relevant documentation, inquiry and observation,etc
Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness
Test Control over access paths to determine whether they are functioning and effective by applying appropriate audit technique
Evaluate the access control environment to determine if the control objective are achieved by analyzing test result and other audit evidence
Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures, and comparing them with appropriate security standard or practice and procedures used by other organization.

The following were incorrect answers:
The other options presented are valid choices which IS auditor needs to follow while evaluating logical access control.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number362

NEW QUESTION: 58
Which of the following is the MOST important Issue for an IS auditor to consider with regard to Voice-over IP (VoIP) communications?
A. Continuity of service
B. Identity management
C. Homogeneity of the network
D. Nonrepudiation
Answer: (SHOW ANSWER)
The most important issue for an IS auditor to consider with regard to Voice-over IP (VoIP) communications is the homogeneity of the network, because it affects the quality, security, and reliability of the VoIP service. A homogeneous network is one that uses a single protocol or standard for VoIP communication, such as Session Initiation Protocol (SIP) or H.32312. A homogeneous network can reduce the complexity, latency, and interoperability issues that may arise from using different or incompatible protocols or devices for VoIP communication12. Continuity of service, identity management, and nonrepudiation are also important issues for VoIP communications, but not as important as the homogeneity of the network. References: 1: CISA Review Manual (Digital Version), Chapter 4, Section 4.4.3 2: CISA Online Review Course, Module 4, Lesson 4

NEW QUESTION: 59
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: 60
During a follow-up audit, an IS auditor finds that the auditee has updated virus scanner definitions without adopting the original audit recommendation to increase the frequency of using the scanner. The MOST appropriate action for the auditor is to:
A. modify the audit opinion based on the new information available.
B. conclude that the residual risk is beyond tolerable levels of risk.

C. prepare a follow-up audit report reiterating the recommendation.
D. escalate the issue to senior management.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 61
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: (SHOW ANSWER)
Section: Protection of Information Assets
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: 62
What often results in project scope creep when functional requirements are not defined as well as they could be?
A. Inadequate software baselining
B. Insufficient strategic planning
C. Inaccurate resource allocation
D. Project delays
Answer: (SHOW ANSWER)
Explanation/Reference:
Inadequate software baselining often results in project scope creep because functional requirements are not defined as well as they could be.

NEW QUESTION: 63

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: (SHOW ANSWER)
Explanation/Reference:
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: 64
An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long.
Which of the following could be caused by the length of the cable?
A. Electromagnetic interference (EMI)
B. Cross-talk
C. Dispersion
D. Attenuation
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Attenuation is the weakening of signals during transmission. When the signal becomes weak, it begins to read a 1 for a 0, and the user may experience communication problems. UTP faces attenuation around
100 meters. Electromagnetic interference (EMI)is caused by outside electromagnetic waves affecting the desired signals, which is not the case here. Cross-talk has nothing to do with the length of the UTP cable.

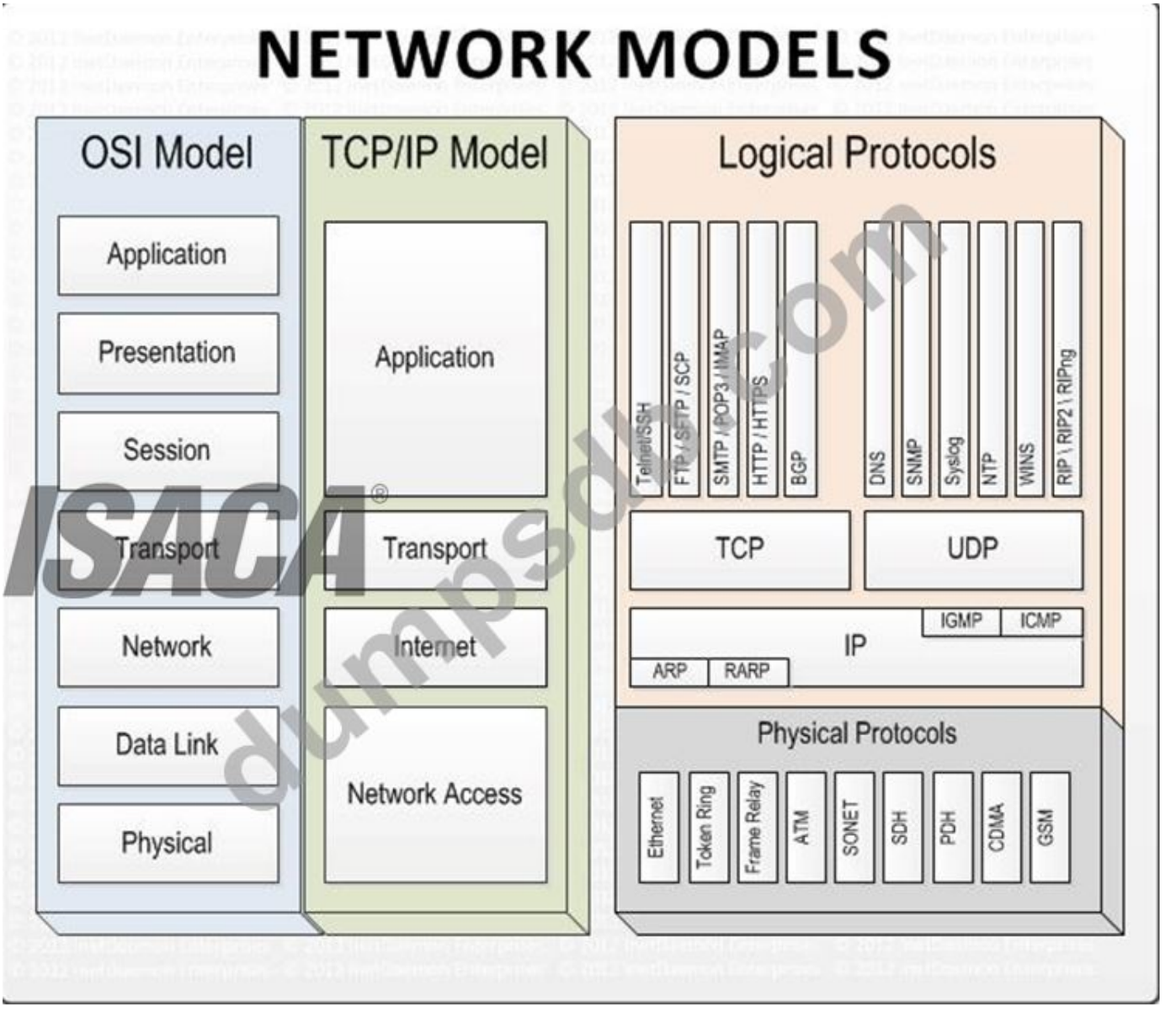
NEW QUESTION: 65
Which of the following tools is MOST helpful in estimating budgets for tasks within a large IT business application project?

A. Balanced scorecard
B. Gantt chart
C. Function point analysis (FPA)
D. Critical path methodology (CPM)
Answer: (SHOW ANSWER)
Section: Information System Operations, Maintenance and Support

NEW QUESTION: 66
An existing system is being replaced with a new application package. User acceptance testing (UAT) should ensure that:
A. data from the old system has been converted correctly
B. the new system functions as expected
C. the new system is better than the old system
D. there is a business need for the new system
Answer: B (LEAVE A REPLY)
Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 67
Which of the following could be used to evaluate the effectiveness of IT operations?
A. Balanced scorecard
B. Net present value
C. Total cost of ownership
D. Internal rate of return
Answer: A (LEAVE A REPLY)

NEW QUESTION: 68
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: C (LEAVE A REPLY)
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



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.

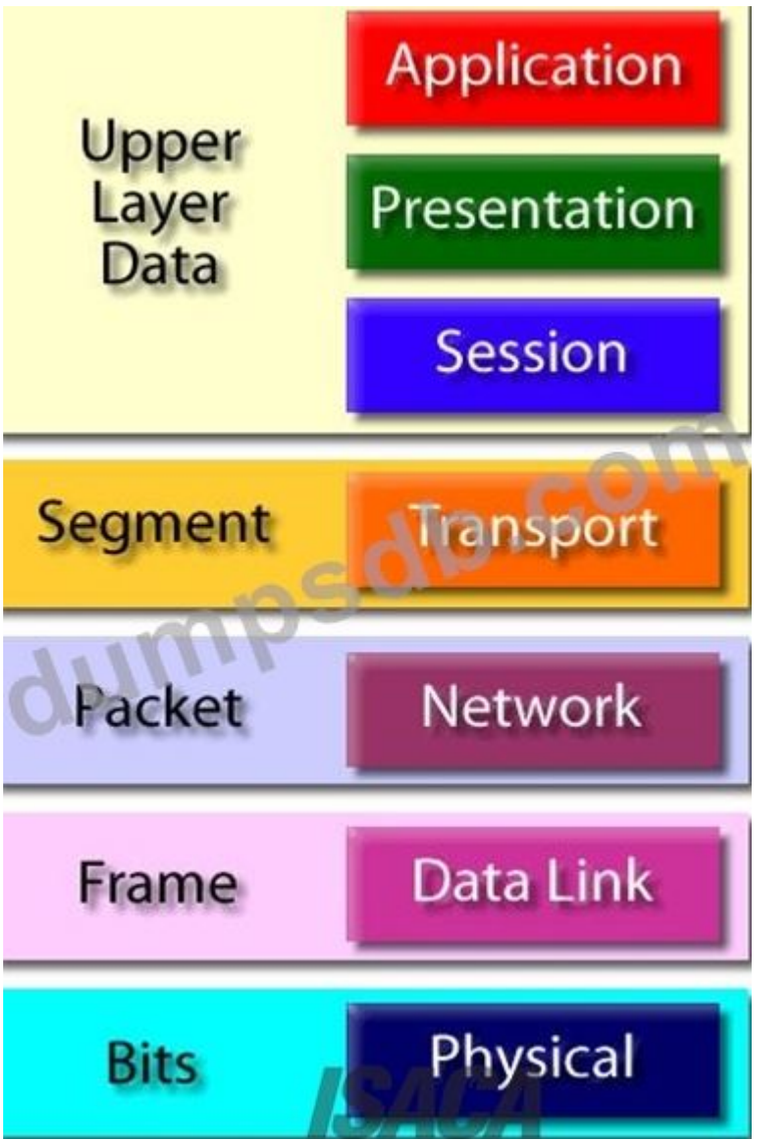
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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: 69

Which of the following would BEST enable effective decision-making?

A. Annualized loss estimates determined from past security events.

B. A universally applied list of generic threats impacts, and vulnerabilities

C. Formalized acceptance of risk analysis by business management

D. A consistent process to analyze new and historical information risk

Answer: D (LEAVE A REPLY)

Section: Governance and Management of IT

Explanation/Reference:

NEW QUESTION: 70

What is the GREATEST concern for an IS auditor reviewing contracts for licensed software that executes a critical business process?
A. Software escrow was not negotiated.
B. An operational level agreement (OLA) was not negotiated.
C. Several vendor deliverables missed the commitment date.
D. The contract does not contain a right-to-audit clause.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 71
Authentication techniques for sending and receiving data between EDI systems is crucial to prevent which of the following? Choose the BEST answer.
A. Unsynchronized transactions
B. Unauthorized transactions
C. Inaccurate transactions
D. Incomplete transactions
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Authentication techniques for sending and receiving data between EDI systems are crucial to prevent unauthorized transactions.

NEW QUESTION: 72
Which of the following should be the FIRST step in an organization's forensics process to preserve evidence?
A. Duplicate digital evidence and validate it using a hash function
B. Perform analytics on digital evidence obtained using forensic methods
C. Create the forensics analysis reporting template
D. Determine which forensic tools to use
Answer: (SHOW ANSWER)

NEW QUESTION: 73
An IS auditor notes that the previous year's disaster recovery test was not completed within the scheduled time frame due to insufficient hardware allocated by a third-party vendor. Which of the following provides the BEST evidence that adequate resources are now allocated to successfully recover the systems?
A. Service level agreement (SLA)
B. Hardware change management policy
C. Vendor memo indicating problem correction
D. An up-to-date RACI chart
Answer: A (LEAVE A REPLY)
Explanation

The best evidence that adequate resources are now allocated to successfully recover the systems is a service level agreement (SLA). An SLA is a contract between a service provider and a customer that defines the scope, quality, and terms of the service delivery. An SLA should include measurable and verifiable indicators of the service performance, such as availability, reliability, capacity, security, and recovery. An SLA should also specify the roles, responsibilities, and expectations of both parties, as well as the remedies and penalties for non-compliance. An SLA can help to ensure that the third-party vendor has allocated sufficient hardware and other resources to meet the recovery objectives and requirements of the organization. References:
CISA Review Manual (Digital Version)
CISA Questions, Answers & Explanations Database

NEW QUESTION: 74
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)
Explanation/Reference:
Explanation:
Firewalls used as entry points to a Voice-over Internet Protocol (VoIP) network should be VoIP-capable.
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 (VLA.NS), 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 in crease latency since this will adversely impact VoIP quality.

NEW QUESTION: 75
The technique of rummaging through commercial trash to collect useful business information is known as:
A. Information diving
B. Intelligence diving

C. Identity diving
D. System diving
E. Program diving
F. None of the choices.
Answer: (SHOW ANSWER)
Dumpster diving in the form of information diving describes the practice of rummaging through commercial trash to find useful information such as files, letters, memos, passwords ...etc.

NEW QUESTION: 76
In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:
A. there is an integration of IS and business staffs within projects.
B. there is a clear definition of the IS mission and vision.
C. a strategic information technology planning methodology is in place.
D. the plan correlates business objectives to IS goals and objectives.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan.
Choices B, C and D are areas covered by a strategic plan.

NEW QUESTION: 77
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 me auditor's GREATEST concern?
A. Key business process end users did not participate in the business impact analysis (BIA)
B. The most recent business impact analysts (BIA) was performed two years before the reorganization
C. A test plan for the BCP has not been completed during the last two years.
D. Copies of the BCP have not been distributed to new business unit end users since the reorganization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78
The practice of periodic secure code reviews is which type of control?
A. Corrective
B. Compensating
C. Detective
D. Preventive
Answer: D (LEAVE A REPLY)

NEW QUESTION: 79
When reviewing a business case for a proposed implementation of a third-party system, which of the following should be an IS auditor's GREATEST concern?
A. Lack of ongoing maintenance costs
B. Lack of training materials
C. Lack of plan for pilot implementation
D. Lack of detailed work breakdown structure
Answer: A (LEAVE A REPLY)
Explanation
The IS auditor's greatest concern when reviewing a business case for a proposed implementation of a third-party system should be A. Lack of ongoing maintenance costs. This is because ongoing maintenance costs are an essential part of the total cost of ownership (TCO) of a third-party system, and they can have a significant impact on the return on investment (ROI) and the feasibility of the project. If the business case does not include ongoing maintenance costs, it may underestimate the true cost of the project and overestimate the benefits. This could lead to poor decision making and unrealistic expectations.
Lack of training materials (B), lack of plan for pilot implementation , and lack of detailed work breakdown structure (D) are also potential issues that could affect the quality and success of the project, but they are not as critical as lack of ongoing maintenance costs. Training materials can be developed or acquired later, pilot implementation can be planned during the project initiation or planning phase, and work breakdown structure can be refined as the project progresses.
However, ongoing maintenance costs are difficult to change or estimate once the project is approved and implemented, and they can have long-term implications for the organization. Therefore, they should be included and analyzed in the business case.

NEW QUESTION: 80
The difference between a vulnerability assessment and a penetration test is that a vulnerability assessment:
A. searches and checks the infrastructure to detect vulnerabilities, whereas penetration testing intends to exploit the vulnerabilities to probe the damage that could result from the vulnerabilities.
B. and penetration tests are different names for the same activity.
C. is executed by automated tools, whereas penetration testing is a totally manual process.

D. is executed by commercial tools, whereas penetration testing is executed by public processes.
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
The objective of a vulnerability assessment is to find the security holds in the computers and elements analyzed; its intent is not to damage the infrastructure. The intent of penetration testing is to imitate a hacker's activities and determine how far they could go into the network. They are not the same; they have different approaches. Vulnerability assessments and penetration testing can be executed by automated or manual tools or processes and can be executed by commercial or free tools.

NEW QUESTION: 81
Which of the following statement correctly describes one way SSL authentication between a client (e.g.
browser) and a server (e.g. web server)?
A. Only the server is authenticated while client remains unauthenticated
B. Only the client is authenticated while server remains authenticated
C. Client and server are authenticated
D. Client and server are unauthenticated
Answer: A (LEAVE A REPLY)
Explanation/Reference:
In one way authentication only server needs to be authenticated where as in mutual authentication both the client and the server needs to be authenticated.
For CISA exam you should know the information below about Secure Socket Layer (SSL) and Transport Layer Security (TLS)
These are cryptographic protocols which provide secure communication on Internet. There are only slight difference between SSL 3.0 and TLS 1.0. For general concept both are called SSL.
SSL is session-connection layer protocol widely used on Internet for communication between browser and web servers, where any amount of data is securely transmitted while a session is established. SSL provides end point authentication and communication privacy over the Internet using cryptography. In typical use, only the server is authenticated while client remains unauthenticated. Mutual authentication requires PKI development to clients. The protocol allows application to communicate in a way designed to prevent eavesdropping, tampering and message forging.
SSL involves a number of basic phases
Peer negotiation for algorithm support
Public-key, encryption based key exchange and certificate based authentication Symmetric cipher based traffic encryption.
SSL runs on a layer beneath application protocol such as HTTP, SMTP and Network News Transport Protocol (NNTP) and above the TCP transport protocol, which forms part of TCP/IP suite.

SSL uses a hybrid hashed, private and public key cryptographic processes to secure transmission over the INTERNET through a PKI.
The SSL handshake protocol is based on the application layer but provides for the security of the communication session too. It negotiates the security parameter for each communication section. Multiple session can belong to one SSL session and the participating in one session can take part in multiple simultaneous sessions.
The following were incorrect answers:
The other choices presented in the options are not valid as in one way authentication only server needs to be authenticated where as client will remain unauthenticated.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 352

NEW QUESTION: 82
Which of the following responsibilities of an organization's quality assurance (QA) function should raise concern for an IS auditor?
A. Ensuring standards are adhered to within the development process
B. Ensuring the test work supports observations
C. Updating development methodology
D. Implementing solutions to correct defects
Answer: D (LEAVE A REPLY)
Implementing solutions to correct defects is a responsibility of the development function, not the quality assurance (QA) function. The QA function should ensure that the development process follows the established standards and methodologies, and that the defects are identified and reported. The QA function should not be involved in fixing the defects, as this would compromise its independence and objectivity. The other options are valid responsibilities of the QA function, and they should not raise concern for an IS auditor. References:
CISA Review Manual (Digital Version) 1, page 300.

NEW QUESTION: 83
Which of the following transmission media is MOST difficult to tap?
A. Copper cable
B. Fiber Optics
C. Satellite Radio Link
D. Radio System
Answer: B (LEAVE A REPLY)
Section: Information System Operations, Maintenance and Support
Explanation:
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.
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

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 intercept.

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.

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.

The following answers are incorrect:

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.

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.

Reference:

CISA review manual 2014 page number 265

NEW QUESTION: 84

A benefit of open system architecture is that it:

A. facilitates interoperability.

B. facilitates the integration of proprietary components.

C. will be a basis for volume discounts from equipment vendors.
D. allows for the achievement of more economies of scale for equipment.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Open systems are those for which suppliers provide components whose interfaces are defined by public standards, thus facilitating interoperability between systems made by different vendors. In contrast, closed system components are built to proprietary standards so that other suppliers' systems cannot or will not interface with existing systems.

NEW QUESTION: 85
Which of the following is MOST important to consider when developing a service level agreement (SLAP)?
A. Description of the services from the viewpoint of the provider
B. Detailed identification of work to be completed
C. Provisions for regulatory requirements that impact the end users' businesses
D. Description of the services from the viewpoint of the client organization
Answer: D (LEAVE A REPLY)
The most important factor to consider when developing a service level agreement (SLA) is the description of the services from the viewpoint of the client organization, because the SLA should reflect the needs and expectations of the client and specify the measurable outcomes and performance indicators that the provider must deliver34. The description of the services from the viewpoint of the provider, the detailed identification of work to be completed, and the provisions for regulatory requirements that impact the end users' businesses are also important elements of an SLA, but not as crucial as the client's perspective. References: 3: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.1 4: CISA Online Review Course, Module 5, Lesson 3

NEW QUESTION: 86
Off-site data backup and storage should be geographically separated so as to _____ (fill in the blank) the risk of a widespread physical disaster such as a hurricane or earthquake.
A. Accept
B. Eliminate
C. Transfer
D. Mitigate
Answer: D (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Off-site data backup and storage should be geographically separated, to mitigate the risk of a widespread physical disaster such as a hurricane or an earthquake.

NEW QUESTION: 87
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. Restrict download capability to authorized users.
B. Require strong passwords for application login.
C. Periodically recertify user access.
D. Mask sensitive data within the application.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 88
An organization can ensure that the recipients of e-mails from its employees can authenticate the identity of the sender by:
A. digitally signing all e-mail messages.
B. encrypting all e-mail messages.
C. compressing all e-mail messages.
D. password protecting all e-mail messages.
Answer: A (LEAVE A REPLY)
By digitally signing all e-mail messages, the receiver will be able to validate the authenticity of the sender. Encrypting all e-mail messages would ensure that only the intended recipient will be able to open the message; however, it would not ensure the authenticity of the sender. Compressing all e-mail messages would reduce the size of the message, but would not ensure the authenticity. Password protecting all e-mail messages would ensure that only those who have the password would be able toopen the message; however, it would not ensure the authenticity of the sender.

NEW QUESTION: 89
Which of the following findings is the GREATES concern when reviewing a disaster recovery plan (DRP) with high availability requirements?
A. Current vendor contact information is not included.
B. Disaster recovery testing is not required.
C. Recovery time objectives (RTO) are not defined.
D. Responsibilities are not defined for the recovery team.
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Which of the following should be the PRIMARY audience for a third-party technical security assessment report?
A. Operational IT management
B. External regulators
C. Board of directors
D. Legal counsel

Answer: (SHOW ANSWER)

NEW QUESTION: 91
An IS auditor has identified the lack of an authorization process for users of an application. The IS auditor's main concern should be that:
A. more than one individual can claim to be a specific user.
B. there is no way to limit the functions assigned to users.
C. user accounts can be shared.
D. users have a need-to-know privilege.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Without an appropriate authorization process, it will be impossible to establish functional limits and accountability. The risk that more than one individual can claim to be a specific user is associated with the authentication processes, rather than with authorization. The risk that user accounts can be shared is associated with identification processes, rather than with authorization. The need-to-know basis is the best approach to assigning privileges during the authorization process.

NEW QUESTION: 92
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)
Section: Protection of Information Assets
Explanation:
Procedures to prevent scope creep are baselined in the design phase of the systems-development life
cycle (SDLC) model.

NEW QUESTION: 93
Which of the following is MOST important to include in a business continuity plan (BCP)?
A. Vendor contact information
B. Documentation of critical systems
C. Backup site location information
D. Documentation of data center floor plans
Answer: C (LEAVE A REPLY)

NEW QUESTION: 94
An organization allows employees to use personally owned mobile devices to access customers' personal information Which of the following is MOST important for an IS auditor to verify?
A. Devices have adequate storage and backup capabilities
B. Mobile device security policies have been implemented
C. Mobile devices are compatible with company infrastructure
D. Employees have signed off on an acceptable use policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 95
The PRIMARY purpose of requiring source code escrow in a contractual agreement is to:
A. comply with vendor management policy
B. convert source code to new executable code.
C. satisfy regulatory requirements.
D. ensure the source code is available.
Answer: D (LEAVE A REPLY)
The primary purpose of requiring source code escrow in a contractual agreement is to ensure the source code is available. Source code escrow is a service that involves depositing the source code of a software or system with a third-party agent or escrow provider, who can release it to a designated beneficiary under specific conditions, such as bankruptcy, termination, or breach of contract by the software vendor or developer.
Source code escrow can help to protect the interests and rights of the software user or licensee, who may need access to the source code for maintenance, modification, enhancement, or troubleshooting purposes. The IS auditor should verify that the contractual agreement specifies the terms and conditions for source code escrow, such as the escrow agent, the escrow fees, the deposit frequency and format, the release events and procedures, and the verification and audit requirements. References: CISA Review Manual (Digital Version)
1, Chapter 3, Section 3.2.2

NEW QUESTION: 96
Which of the following functions is performed by a virtual private network (VPN)?
A. Hiding information from sniffers on the net

B. Enforcing security policies
C. Detecting misuse or mistakes
D. Regulating access
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A VPN hides information from sniffers on the net using encryption. It works based on tunneling. A VPN does not analyze information packets and, therefore, cannot enforce security policies, it also does not check the content of packets, so it cannot detect misuse or mistakes. A VPN also does not perform an authentication function and, therefore, cannot regulate access.

NEW QUESTION: 97
.Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?
A. Redundancy check
B. Completeness check
C. Accuracy check
D. Parity check
Answer: A (LEAVE A REPLY)
A redundancy check can help detect transmission errors by appending especially calculated bits onto the end of each segment of datA .

NEW QUESTION: 98
Which of the following is MOST important for an IS auditor to do during an exit meeting with an auditee?
A. Ensure that the facts presented in the report are correct.
B. Specify implementation dates for the recommendations.
C. Request input in determining corrective action.
D. Communicate the recommendations to senior management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
Which of the following is MOST critical to the success of an information security program?
A. Management's commitment to information security
B. User accountability for information security
C. Alignment of information security with IT objectives
D. Integration of business and information security
Answer: A (LEAVE A REPLY)
Explanation
The most critical factor for the success of an information security program is management's commitment to information security. Management's commitment to information security means

that the senior management supports, sponsors, funds, monitors and enforces the information security program within the organization.
Management's commitment to information security also demonstrates leadership, sets the tone and culture, and establishes the strategic direction and objectives for information security. User accountability for information security, alignment of information security with IT objectives, and integration of business and information security are also important factors for the success of an information security program, but they are not as critical as management's commitment to information security, as they depend on or derive from it.
References: Info Technology & Systems Resources | COBIT, Risk, Governance ... - ISACA, IT Governance and Process Maturity

NEW QUESTION: 100
Which of the following provides the BEST quality control for data being loaded into an organization's data warehouse?
A. Warehouse
B. Landing
C. Source
D. Staging
Answer: D (LEAVE A REPLY)

NEW QUESTION: 101
A maturity model is useful in the assessment of IT service management because it:
A. provides a benchmark for process improvement
B. defines the level of control required to meet business needs
C. indicates the service levels required for the business area
D. specifies the mechanism needed to achieve defined service levels
Answer: (SHOW ANSWER)
Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 102
Which significant risk is introduced by running the file transfer protocol (FTP) service on a server in a demilitarized zone (DMZ)?
A. A user from within could send a file to an unauthorized person.
B. FTP services could allow a user to download files from unauthorized sources.
C. A hacker may be able to use the FTP service to bypass the firewall.
D. FTP could significantly reduce the performance of a DMZ server.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:

Since file transfer protocol (FTP) is considered an insecure protocol, it should not be installed on a server in a demilitarized zone (DMZ). FTP could allow an unauthorized user to gain access to the network.
Sending files to an unauthorized person and the risk of downloading unauthorized files are not as significant as having a firewall breach. The presence of the utility does not reduce the performance of a DMZ server; therefore, performance degradation is not a threat.

NEW QUESTION: 103
An information systems security officer's PRIMARY responsibility for business process applications is to:
A. Authorize secured emergency access.
B. Ensure access rules agree with policies
C. Create role-based rules for each business process.
D. Approve the organization's security policy.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 104
During an audit, the client learns that the IS auditor has recently completed a similar security review at a competitor. The client inquires about the competitor's audit results. What is the BEST way for the auditor to address this inquiry?
A. Obtain permission from the competitor to use the audit results as examples for future clients.
B. Explain that it would be inappropriate to discuss the results of another audit client
C. Escalate the question to the audit manager for further action.
D. Discuss the results of the audit omitting specifics related to names and products.
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Which of the following is the PRIMARY reason for using a digital signature?
A. Provide availability to the transmission
B. Authenticate the sender of a message
C. Provide confidentiality to the transmission
D. Verify the integrity of the data and the identity of the recipient
Answer: (SHOW ANSWER)
A digital signature is a mathematical algorithm that validates the authenticity and integrity of a message or document by generating a unique hash of the message or document and encrypting it using the sender's private key1. The primary reason for using a digital signature is to authenticate the sender of a message, as only the sender has access to their private key and can produce a valid signature2. A digital signature also verifies the integrity of the data, as any modification to the message or document will result in a different hash value and invalidate the signature1. However, a digital signature does not provide availability or confidentiality to the

transmission, as it does not prevent denial-of-service attacks or encrypt the entire message or document3.
References
1: Understanding Digital Signatures | CISA
2: Signature Verification | CISA
3: SECFND: Digital Signatures from Skillsoft | NICCS

NEW QUESTION: 106
When using a universal storage bus (USB) flash drive to transport confidential corporate data to an offsite location, an effective control would be to:
A. carry the flash drive in a portable safe.
B. assure management that you will not lose the flash drive.
C. request that management deliver the flash drive by courier.
D. encrypt the folder containing the data with a strong key.
Answer: (SHOW ANSWER)
Encryption, with a strong key, is the most secure method for protecting the information on the flash drive. Carrying the flash drive in a portable safe does not guarantee the safety of the information in the event that the safe is stolen or lost. Nomatter what measures you take, the chance of losing the flash drive still exists. It is possible that a courier might lose the flash drive or that it might be stolen.

NEW QUESTION: 107
Disabling which of the following would make wireless local area networks more secure against unauthorized access?
A. MAC (Media Access Control) address filtering
B. WPA (Wi-Fi Protected Access Protocol)
C. LEAP (Lightweight Extensible Authentication Protocol)
D. SSID (service set identifier) broadcasting
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Disabling SSID broadcasting adds security by making it more difficult for unauthorized users to find the name of the access point. Disabling MAC address filtering would reduce security. Using

MAC filtering makes it more difficult to access a WLAN, because it would be necessary to catch traffic and forge the MAC address. Disabling WPA reduces security. Using WPA adds security by encrypting the traffic.
Disabling LEAP reduces security. Using LEAP adds security by encrypting the wireless traffic.

NEW QUESTION: 108
What is the MOST effective way for an IS auditor to determine whether employees understand the organization's information security policy?
A. Survey employees.
B. Review the organization's employee training log.
C. Ensure the policy is communicated throughout the organization.
D. Ensure the policy is current.
Answer: (SHOW ANSWER)

NEW QUESTION: 109
During a network security review, the system log indicates an unusually high number of unsuccessful login attempts. Which of the following sampling techniques is MOST appropriate for selecting a sample of user IDs for further investigation?
A. Stratified
B. Attribute
C. Monetary unit
D. Variable
Answer: A (LEAVE A REPLY)
Section: Governance and Management of IT

NEW QUESTION: 110
Which of the following database model allow many-to-many relationships in a tree-like structure that allows multiple parents?
A. Hierarchical database model
B. Network database model
C. Relational database model
D. Object-relational database model
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Network database model-The network model expands upon the hierarchical structure, allowing many-to- many relationships in a tree-like structure that allows multiple parents.
For your exam you should know below information about database models:
A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized, and manipulated. The most popular example of a database model is the relational model, which uses a table-based format.

Common logical data models for databases include:
Hierarchical database model
Network model
Relational model
Object-relational database models
Hierarchical database model
In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order. Hierarchical structures were widely used in the early mainframe database management systems, such as the Information Management System (IMS) by IBM, and now describe the structure of XML documents. This structure allows one one-to-many relationship between two types of data. This structure is very efficient to describe many relationships in the real world; recipes, table of contents, ordering of paragraphs/verses, any nested and sorted information.
This hierarchy is used as the physical order of records in storage. Record access is done by navigating through the data structure using pointers combined with sequential accessing. Because of this, the hierarchical structure is inefficient for certain database operations when a full path (as opposed to upward link and sort field) is not also included for each record. Such limitations have been compensated for in later IMS versions by additional logical hierarchies imposed on the base physical hierarchy.
Hierarchical database model

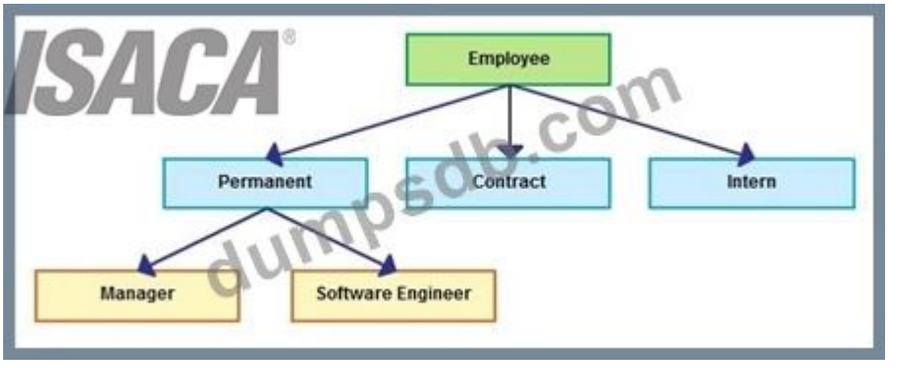
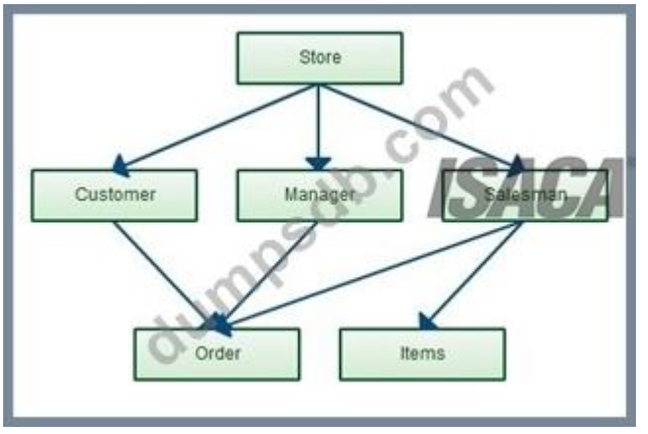


Image source: http://creately.com/blog/wp-content/uploads/2012/06/hierarchical-database-model.png Network database model
The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents. It was the most popular before being replaced by the relational model, and is defined by the CODASYL specification.
The network model organizes data using two fundamental concepts, called records and sets. Records contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between records: one owner, many members. A record may be an owner in any number of sets, and a member in any number of sets.
A set consists of circular linked lists where one record type, the set owner or parent, appears once in each circle, and a second record type, the subordinate or child, may appear multiple

times in each circle. In this way a hierarchy may be established between any two record types, e.g., type A is the owner of B.
At the same time another set may be defined where B is the owner of A Thus all the sets comprise a general directed graph (ownership defines a direction), or network construct. Access to records is either sequential (usually in each record type) or by navigation in the circular linked lists.
The network model is able to represent redundancy in data more efficiently than in the hierarchical model, and there can be more than one path from an ancestor node to a descendant.
The operations of the network model are navigational in style: a program maintains a current position, and navigates from one record to another by following the relationships in which the record participates. Records can also be located by supplying key values.
Network Database model



Source of Image:http://creately.com/blog/wp-content/uploads/2012/06/database-design-network-model.png
Relational database model
In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database.
In the relational model, related records are linked together with a "key".
The purpose of the relational model is to provide a declarative method for specifying data and queries:
users directly state what information the database contains and what information they want from it, and let the database management system software take care of describing data structures for storing the data and retrieval procedures for answering queries.
Most relational databases use the SQL data definition and query language; these systems implement what can be regarded as an engineering approximation to the relational model. A table in an SQL database schema corresponds to a predicate variable; the contents of a table to a relation; key constraints, other constraints, and SQL queries correspond to predicates. However, SQL databases, including DB2, deviate from the relational model in many details, and Cod fiercely argued against deviations that compromise the original principles.
Relational database model

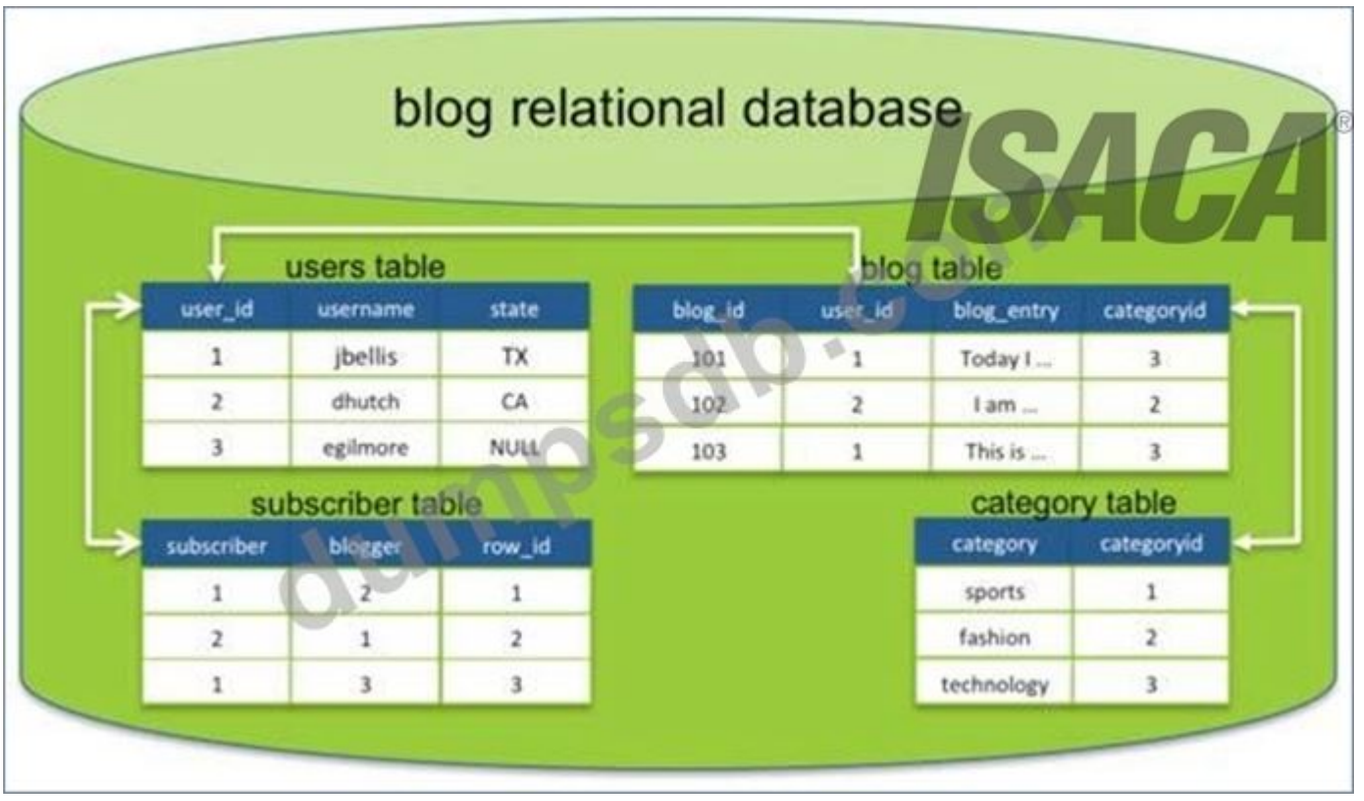


Image Source: http://www.datastax.com/docs/_images/relational_model.png Object-relational database Model

An object-relational database (ORD), or object-relational database management system (ORDBMS), is a database management system (DBMS) similar to a relational database, but with an object-oriented database model: objects, classes and inheritance are directly supported in database schemas and in the query language. In addition, just as with pure relational systems, it supports extension of the data model with custom data-types and methods.

Example of an object-oriented database model

An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following were incorrect answers:

Hierarchical database model - In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order.

Relational model- In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database. In the relational model, related records are linked together with a "key".

Object-relational database models- An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in

the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 254

NEW QUESTION: 111
.What is an acceptable recovery mechanism for extremely time-sensitive transaction processing?
A. Off-site remote journaling
B. Electronic vaulting
C. Shadow file processing
D. Storage area network
Answer: C (LEAVE A REPLY)
Shadow file processing can be implemented as a recovery mechanism for extremely time-sensitive transaction processing.

NEW QUESTION: 112
Who is ultimately accountable for the development of an IS security policy?
A. The board of directors
B. Middle management
C. Security administrators
D. Network administrators
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The board of directors is ultimately accountable for the development of an IS security policy.

NEW QUESTION: 113
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: A (LEAVE A REPLY)
Explanation
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: 114
An IS auditor has found that despite an increase in phishing attacks over the past two years, there has been a significant decrease in the success rate. Which of the following is the MOST likely reason for this decline?
A. Development of an incident response plan
B. Implementation of an intrusion detection system (IDS)
C. Enhanced training for incident responders
D. Implementation of a security awareness program
Answer: C (LEAVE A REPLY)

NEW QUESTION: 115
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: 116
An organization's information security department has recently created a centralized governance model to ensure that network-related findings are remediated within the service level agreement (SLA). What should the IS auditor use to assess the maturity and capability of this governance model?
A. Key performance indicators (KPIs)
B. Key risk indicators (KRIs)
C. Key data elements
D. Key process controls
Answer: A (LEAVE A REPLY)

NEW QUESTION: 117
Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?
A. increase the time allocated for system testing
B. implement formal software inspections
C. increase the development staff
D. Require the sign-off of all project deliverables
Answer: B (LEAVE A REPLY)
Inspections of code and design are a proven software quality technique. An advantage of this approach is that defects are identified before they propagate through the development life cycle. This reduces the cost of correction as less rework is involved. Allowing more time for testing may discover more defects; however, little is revealed as to why the quality problems are occurring and the cost of the extra testing, and the cost of rectifying the defects found will be greater than if they had been discovered earlier in the development process. The ability of the development staff can have a bearing on the quality of what is produced; however, replacing staff can be expensive and disruptive, and the presence of a competent staff cannot guarantee quality in the absence of effective quality management processes. Sign-off of deliverables may help detect defects if

signatories are diligent about reviewing deliverable content; however, this is difficult to enforce. Deliverable reviews normally do not go down to the same level of detail as software inspections.

NEW QUESTION: 118
Which of the following is the PRIMARY objective of implementing privacy-related controls within an organization?
A. To prevent confidential data loss
B. To comply with legal and regulatory requirements
C. To identify data at rest and data in transit for encryption
D. To provide options to individuals regarding use of their data
Answer: (SHOW ANSWER)
The primary objective of implementing privacy-related controls within an organization is B. To comply with legal and regulatory requirements. According to the ISACA Certified Information Systems Auditor (CISA) Study Guide [1], organizations must comply with laws and regulations that affect the handling of personal information. This includes laws related to the use, collection, storage, retention and disposal of personal data, as well as laws related to the privacy of personal data. Additionally, organizations must implement controls to ensure that they are in compliance with these laws and regulations.

NEW QUESTION: 119
In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:
A. identify and assess the risk assessment process used by management.
B. identify information assets and the underlying systems.
C. disclose the threats and impacts to management.
D. identify and evaluate the existing controls.
Answer: D (LEAVE A REPLY)
It is important for an IS auditor to identify and evaluate the existing controls and security once the potential threats and possible impacts are identified. Upon completion of an audit an IS auditor should describe and discuss with management the threats and potential impacts on the assets.

NEW QUESTION: 120
When introducing a maturity model to the IT management process, it is BEST to align the maturity level to a point that reflects which of the following?
A. Minimum cost expenditure level
B. Industry standard practice level
C. Ideal business production level
D. Maximum risk tolerance level
Answer: (SHOW ANSWER)

NEW QUESTION: 121

Which of the following would be the GREATEST cause for concern when data are sent over the Internet using HTTPS protocol?
A. Presence of spyware in one of the ends
B. The use of a traffic sniffing tool
C. The implementation of an RSA-compliant solution
D. A symmetric cryptography is used for transmitting data
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation:
Encryption using secure sockets layer/transport layer security (SSL/TLS) tunnels makes it difficult to intercept data in transit, but when spyware is running on an end user's computer, data are collected before encryption takes place. The other choices are related to encrypting the traffic, but the presence of spyware in one of the ends captures the data before encryption takes place.

NEW QUESTION: 122
Which of the following system conversion strategies provides the GREATEST redundancy?
A. Parallel run
B. Phased approach
C. Pilot study
D. Direct cutover
Answer: A (LEAVE A REPLY)

NEW QUESTION: 123
A check digit is an effective edit check to:
A. Detect data-transcription errors
B. Detect data-transposition and transcription errors
C. Detect data-transposition, transcription, and substitution errors
D. Detect data-transposition errors
Answer: (SHOW ANSWER)
Explanation/Reference:
A check digit is an effective edit check to detect data-transposition and transcription errors.

NEW QUESTION: 124

Which of the following metrics would be MOST helpful to an IS auditor in evaluating an organizations security incident response management capability?
A. Number of alerts generated by intrusion detection systems (IDS) per minute
B. Number of IT security incidents reported per month
C. Number of malware infections in business applications detected per day
D. Number of business interruptions due to IT security incidents per year
Answer: D (LEAVE A REPLY)

NEW QUESTION: 125
Which of the following is the BEST control to help prevent sensitive data leaving an organization via email?
A. Providing encryption solutions for employees
B. Conducting periodic phishing tests
C. Blocking outbound emails sent without encryption
D. Scanning outgoing emails
Answer: C (LEAVE A REPLY)

NEW QUESTION: 126
An organization is planning to outsource its customer relationship management (CRM) system to a software as a service (SaaS) provider. Which of the following is most important to include in the contract?
A. CRM system intellectual property rights
B. Maximum number of licenses allowed
C. Service levels for change management
D. Nondisclosure agreement
Answer: D (LEAVE A REPLY)

NEW QUESTION: 127
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 with customer personal information
B. Data supporting financial statements
C. Data impacting business objectives
D. Data reported to the regulatory body
Answer: D (LEAVE A REPLY)

NEW QUESTION: 128

A hearth 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: 129

What process allows IS management to determine whether the activities of the organization differ from the planned or expected levels? Choose the BEST answer.

A. Business impact assessment

B. Risk assessment

C. IS assessment methods

D. Key performance indicators (KPIs)

Answer: (SHOW ANSWER)

Explanation/Reference:

IS assessment methods allow IS management to determine whether the activities of the organization differ from the planned or expected levels.

NEW QUESTION: 130

An organization has replaced all of the storage devices at its primary data center with new higher-capacity units The replaced devices have been installed at the disaster recovery site to replace older units An IS auditor s PRIMARY concern would be whether

A. the recovery site devices can handle the storage requirements

B. hardware maintenance contract is in place for both old and new storage devices

C. the procurement was in accordance with corporate policies and procedures

D. the relocation plan has been communicated to all concerned parties

Answer: (SHOW ANSWER)

An IS auditor's primary concern would be whether the recovery site devices can handle the storage requirements. The storage requirements are determined by the amount and type of data that needs to be backed up and restored in case of a disaster at the primary data center. The recovery site devices should have enough capacity, performance, reliability, and compatibility to meet these requirements.
If the recovery site devices cannot handle the storage requirements, then there is a risk that some data may not be backed up properly or may not be available for recovery when needed. This could result in data loss, corruption, or inconsistency, which could affect the business continuity and integrity of the organization.
Therefore, an IS auditor should verify that:
* The recovery site devices have sufficient storage space to accommodate all the data that needs to be backed up from the primary data center.
* The recovery site devices have adequate bandwidth and speed to transfer and access data efficiently and effectively.
* The recovery site devices have appropriate security features and controls to protect data from unauthorized access or modification.
* The recovery site devices are compatible with the primary data center devices in terms of hardware, software, format, and protocol.
References:
* 10: What Is a Disaster Recovery Site? Hot, Cold & Warm Site
* 11: Disaster recovery site - What is the ideal distance to mitigate risks? - Advisera
* 12: Offsite Data Backup Storage vs Disaster Recovery (DR) - LINBIT

NEW QUESTION: 131
Which of the following would MOST effectively control the usage of universal storage bus (USB) storage devices?
A. Policies that require instant dismissal if such devices are found
B. Software for tracking and managing USB storage devices
C. Administratively disabling the USB port
D. Searching personnel for USB storage devices at the facility's entrance
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Software for centralized tracking and monitoring would allow a USB usage policy to be applied to each user based on changing business requirements, and would provide for monitoring and reporting exceptions to management. A policy requiring dismissal may result in increased employee attrition and business requirements would not be properly addressed. Disabling ports would be complex to manage and might not allow for new business needs. Searching of personnel for USB storage devices at the entrance to a facility is not a practical solution since these devices are small and could be easily hidden.

NEW QUESTION: 132
Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital?
A. Multiplexer
B. Modem
C. Protocol converter
D. Concentrator
Answer: (SHOW ANSWER)
A modem is a device that translates data from digital to analog and back to digital.

NEW QUESTION: 133
Which of the following would BEST determine whether a post-implementation review (PIR) performed by the project management office (PMO) was effective?
A. Lessons learned were implemented
B. Management approved the PIR report.
C. Project outcomes have been realized
D. The review was performed by an external provider
Answer: (SHOW ANSWER)

NEW QUESTION: 134
Which of the following should be performed FIRST before key performance indicators (KPIs) can be implemented?
A. Analysis of industry benchmarks
B. Implementation of a balanced scorecard
C. Analysis of quantitative benefits
D. Identification of organizational goals
Answer: D (LEAVE A REPLY)

NEW QUESTION: 135
Which of the following fourth generation language depends on self-contained database management systems?
A. Query and report generator
B. Embedded database 4GLs
C. Relational database 4GL
D. Application generators
Answer: B (LEAVE A REPLY)
Section: Information System Acquisition, Development and Implementation Explanation: Embedded database 4GLsare depend on self-contained database management systems. These characteristics often makes them more user-friendly but also may lead to applications that are not integrated well with other product applications. Example includes FOCUS, RAMIS II and NOMAD 2.

For CISA exam you should know below mentioned types of 4GLs
Query and report generator - These specialize language can extract and produce reports.
Recently more powerful language has been produced that can access database records, produce complex on-line output and be developed in an almost natural language.
Embedded database 4GLs - These depend on self-contained database management systems. These characteristics often makes them more user-friendly but also may lead to applications that are not integrated well with other product applications. Example includes FOCUS, RAMIS II and NOMAD 2.
Relational database 4GLs - These high level language products are usually an optional feature on vendor's DBMS product line. These allow the application developer to make better use of DBMS product, but they often are not end-user-oriented. Example include SQL+ MANTIS and NATURAL.
Application generators - These development tools generate lower level programming languages(3GL) such as COBOL and C. The application can be further tailored and customized. Data processing development personnel, not end user, use application generators.
The following were incorrect answers:
Query and report generator - These specialize language can extract and produce reports.
Relational database 4GLs - These high level language products are usually an optional feature on vendor's DBMS product line.
Application generators - These development tools generate lower level programming languages(3GL) such as COBOL and C.
Reference:
CISA review manual 2014 Page number 209

NEW QUESTION: 136
An IS auditor has found that a vendor has gone out of business and the escrow has an older version of the source code. What is the auditor's BEST recommendation for the organization?
A. Analyze a new application that moots the current re
B. Perform an analysis to determine the business risk
C. Bring the escrow version up to date.
D. Develop a maintenance plan to support the application using the existing code
Answer: (SHOW ANSWER)
Explanation
This means that the organization should obtain the source code from the escrow agent and compare it with the current version of the application that they are using. The organization should then identify and apply any changes or updates that are missing or different in the escrow version, so that it matches the current version.
This way, the organization can ensure that they have a complete and accurate copy of the source code that reflects their current needs and requirements.
Bringing the escrow version up to date can help the organization to avoid or reduce the risks and costs associated with using an outdated or incompatible version of the source code. For example,

an older version of the source code may have bugs, errors, or vulnerabilities that could affect the functionality, security, or performance of the application. An older version of the source code may also lack some features, enhancements, or integrations that could improve the usability, efficiency, or value of the application. An older version of the source code may also not comply with some standards, regulations, or contracts that could affect the quality, reliability, or legality of the application1.
The other options are not as good as bringing the escrow version up to date for the organization. Option A, analyzing a new application that meets the current requirements, is a possible option but it may be more time-consuming, expensive, and risky than updating the existing application. The organization may have to go through a complex and lengthy process of selecting, acquiring, implementing, testing, and migrating to a new application, which could disrupt their operations and performance. The organization may also have to deal with compatibility, interoperability, or data quality issues when switching to a new application2. Option B, performing an analysis to determine the business risk, is a necessary step but not a recommendation for the organization. The organization should already be aware of the business risk of using an application whose vendor has gone out of business and whose escrow has an older version of the source code. The organization should focus on finding and implementing a solution to mitigate or eliminate this risk3. Option D, developing a maintenance plan to support the application using the existing code, is not a feasible option because it assumes that the organization has access to the existing code. However, this is not the case because the vendor has gone out of business and the escrow has an older version of the source code. The organization cannot support or maintain an application without having a complete and accurate copy of its source code.
References:
How Important Is Source Code Escrow - ISACA1
The What and Why of Source Code Escrow2
Unlocking Source Code In Escrow 2023: A Guide To Secure Software3

NEW QUESTION: 137
Which of the following level in CMMI model focuses on process definition and process deployment?
A. Level 4
B. Level 5
C. Level 3

D. Level 2

Answer: C (LEAVE A REPLY)

Section: Information System Acquisition, Development and Implementation Explanation:

Level 3 is the defined step and focus on process definition and process deployment.

For CISA Exam you should know below information about Capability Maturity Model Integration (CMMI) mode:

Maturity model

A maturity model can be viewed as a set of structured levels that describe how well the behaviors, practices and processes of an organization can reliably and sustainable produce required outcomes.

CMMI Levels

A maturity model can be used as a benchmark for comparison and as an aid to understanding - for example, for comparative assessment of different organizations where there is something in common that can be used as a basis for comparison. In the case of the CMM, for example, the basis for comparison would be the organizations' software development processes.

Structure

The model involves five aspects:

Maturity Levels: a 5-level process maturity continuum - where the uppermost (5th) level is a notional ideal state where processes would be systematically managed by a combination of process optimization and continuous process improvement.

Key Process Areas: a Key Process Area identifies a cluster of related activities that, when performed together, achieve a set of goals considered important.

Goals: the goals of a key process area summarize the states that must exist for that key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator of how much capability the organization has established at that maturity level.
The goals signify the scope, boundaries, and intent of each key process area.
Common Features: common features include practices that implement and institutionalize a key process area. There are five types of common features: commitment to perform, ability to perform, activities performed, measurement and analysis, and verifying implementation.
Key Practices: The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the area.
Levels
There are five levels defined along the continuum of the model and, according to the SEI: "Predictability, effectiveness, and control of an organization's software processes are believed to improve as the organization moves up these five levels. While not rigorous, the empirical evidence to date supports this belief".[citation needed] Initial (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.
Repeatable - the process is at least documented sufficiently such that repeating the same steps may be attempted.
Defined - the process is defined/confirmed as a standard business process, and decomposed to levels 0, 1 and 2 (the last being Work Instructions).
Managed - the process is quantitatively managed in accordance with agreed-upon metrics.
Optimizing - process management includes deliberate process optimization/improvement.
Within each of these maturity levels are Key Process Areas which characteristic that level, and for each such area there are five factors: goals, commitment, ability, measurement, and verification. These are not necessarily unique to CMM, representing - as they do - the stages that organizations must go through on the way to becoming mature.
The model provides a theoretical continuum along which process maturity can be developed incrementally from one level to the next. Skipping levels is not allowed/feasible.
Level 1 - Initial (Chaotic)
It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events.
This provides a chaotic or unstable environment for the processes.
Level 2 - Repeatable
It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.
Level 3 - Defined
It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These

standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.
Level 4 - Managed
It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.
Level 5 - Optimizing
It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.
At maturity level 5, processes are concerned with addressing statistical common causes of process variation and changing the process (for example, to shift the mean of the process performance) to improve process performance. This would be done at the same time as maintaining the likelihood of achieving the established quantitative process-improvement objectives.
The following were incorrect answers:
Level 4 - Focus on process management and process control
Level 5 - Process innovation and continuous optimization.
Level 2 - Performance management and work product management.
Reference:
CISA review manual 2014 Page number 188

NEW QUESTION: 138
In the risk assessment process, which of the following should be identified FIRST?
A. Threats
B. Vulnerabilities
C. Impact
D. Assets
Answer: D (LEAVE A REPLY)

NEW QUESTION: 139
Which of the following is the MAIN objective of enterprise architecture (EA) governance?
A. To ensure new processes and technologies harmonize with existing processes
B. To ensure the EA can adapt to emerging technology trends
C. To ensure the EA is compliant with local laws and regulations
D. To ensure new initiatives produce an acceptable return on investment (ROI)
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:Enterprise architecture (EA) governance ensures that IT and business alignment is maintained and that new processes and technologies integrate well with existing structures.

* Option A (Correct):The primary purpose of EA governance is to ensure that new technologies, processes, and systems align and harmonize with existing architecture to maintain operational efficiency and consistency.
* Option B (Incorrect):While adaptability to emerging technology trends is important, EA governance focuses more on structure, consistency, and compliance rather than just adaptability.
* Option C (Incorrect):Compliance with regulations is crucial, but it is just one component of governance.
EA governance has a broader scope, including strategic alignment and process integration.
* Option D (Incorrect):Ensuring ROI is an important financial consideration, but it is not themainobjective of EA governance.
Reference:ISACA CISA Review Manual -Domain 1: Information Systems Auditing Process-Covers governance, risk management, and ensuring alignment of EA with business objectives.

NEW QUESTION: 140
You should keep all computer rooms at reasonable temperatures, which is in between (choose all that apply):
A. 60 - 75 degrees Fahrenheit
B. 10 - 25 degrees Celsius
C. 30 - 45 degrees Fahrenheit
D. 1 - 15 degrees Celsius
E. 20 - 35 degrees Fahrenheit
F. 0 - 5 degrees Celsius
Answer: A,B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
You should keep all computer rooms at reasonable temperatures, which is in between 60 - 75 degrees Fahrenheit or 10 - 25 degrees Celsius. You should also keep humidity levels at 20 - 70 percent.

NEW QUESTION: 141
An IS auditor finds a high-risk vulnerability in a public-facing web server used to process online customer payments. The IS auditor should FIRST
A. document the exception in an audit report.
B. review security incident reports.
C. identify compensating controls.
D. notify the audit committee.
Answer: C (LEAVE A REPLY)
The first action that an IS auditor should take when finding a high-risk vulnerability in a public-facing web server used to process online customer payments is to identify compensating controls. Compensating controls are alternative or additional controls that provide reasonable assurance of mitigating the risk of exploiting the vulnerability. The IS auditor should assess the effectiveness of

the compensating controls and determine whether they reduce the risk to an acceptable level. If not, the IS auditor should recommend remediation actions to address the vulnerability. Documenting the exception in an audit report is an important action, but it should not be the first action, as it does not address the urgency of the situation. Reviewing security incident reports is a useful action, but it should not be the first action, as it does not provide assurance of preventing future incidents. Notifying the audit committee is a necessary action, but it should not be the first action, as it does not involve taking any corrective measures. References:
* CISA Review Manual, 27th Edition, pages 295-2961
* CISA Review Questions, Answers & Explanations Database, Question ID: 260

NEW QUESTION: 142
When auditing an organization's software acquisition process the BEST way for an IS auditor to understand the software benefits to the organization would be to review the
A. alignment with IT strategy
B. request for proposal (RFP)
C. business case
D. feasibility study
Answer: C (LEAVE A REPLY)

NEW QUESTION: 143
An organization requires the use of a key card to enter its data center. Recently, a control was implemented that requires biometric authentication for each employee.
Which type of control has been added?
A. Corrective
B. Detective
C. Preventive
D. Compensating
Answer: (SHOW ANSWER)

NEW QUESTION: 144
Which of the following would be the BEST access control procedure?
A. The data owner formally authorizes access and an administrator implements the user authorization tables.
B. Authorized staff implements the user authorization tables and the data owner sanctions them.
C. The data owner and an IS manager jointly create and update the user authorization tables.
D. The data owner creates and updates the user authorization tables.
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:

The data owner holds the privilege and responsibility for formally establishing the access rights. An IS administrator should then implement or update user authorization tables. Choice B alters the desirable order. Choice C is not a formal procedure for authorizing access.

NEW QUESTION: 145
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)
Explanation/Reference:
Explanation:
Iipchains 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: 146
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. business continuity plan.
C. threat and risk assessment
D. disaster recovery plan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 147
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. Detective
B. Preventive
C. Corrective
D. Directive
Answer: D (LEAVE A REPLY)

NEW QUESTION: 148
When assessing the overall effectiveness of an organization's disaster recovery planning process, which of the following is MOST important for the IS auditor to verify?

A. Management contracts with a third party for warm site services.
B. Management schedules an annual tabletop exercise.
C. Management documents and distributes a copy of the plan to all personnel.
D. Management reviews and updates the plan annually or as changes occur.
Answer: D (LEAVE A REPLY)
Explanation
The overall effectiveness of an organization's disaster recovery planning process depends on how well the plan reflects the current and future needs and risks of the organization, and how well the plan is tested, communicated, and maintained. Among the four options given, the most important one for the IS auditor to verify is that management reviews and updates the plan annually or as changes occur.
A disaster recovery plan is not a static document that can be created once and forgotten. It is a dynamic and evolving process that requires regular review and update to ensure that it remains relevant, accurate, and effective. A disaster recovery plan should be reviewed and updated at least annually, or whenever there are significant changes in the organization's structure, operations, environment, or regulations. These changes could affect the business impact analysis, risk assessment, recovery objectives, recovery strategies, roles and responsibilities, or resources of the disaster recovery plan. If the plan is not updated to reflect these changes, it could become obsolete, incomplete, or inconsistent, and fail to meet the organization's recovery needs or expectations.
The other three options are not as important as reviewing and updating the plan, although they may also contribute to the effectiveness of the disaster recovery planning process. Contracting with a third party for warm site services is a possible recovery strategy that involves using a partially equipped facility that can be quickly activated in case of a disaster. However, this strategy may not be suitable or sufficient for every organization or scenario, and it does not guarantee the success of the disaster recovery plan. Scheduling an annual tabletop exercise is a good practice that involves simulating a disaster scenario and testing the plan in a hypothetical setting. However, this exercise may not be enough to evaluate the feasibility or readiness of the plan, and it should be complemented by other types of tests, such as walkthroughs, drills, or full-scale exercises. Documenting and distributing a copy of the plan to all personnel is an essential step that ensures that everyone involved in or affected by the plan is aware of their roles and responsibilities, and has access to the relevant information and instructions. However, this step alone does not ensure that the plan is understood or followed by all personnel, and it should be accompanied by proper training, education, and awareness programs.
Therefore, reviewing and updating the plan annually or as changes occur is the best answer.

NEW QUESTION: 149
Demonstrated support from which of the following roles in an organization has the MOST influence over information security governance?
A. Chief information security officer (CISO)
B. Information security steering committee

C. Board of directors
D. Chief information officer (CIO)
Answer: C (LEAVE A REPLY)
Information security governance is the subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risk appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security program. Information security governance is essential for ensuring that an organization's information assets are protected from internal and external threats, and that the organization complies with relevant laws and standards.
Demonstrated support from which of the following roles in an organization has the most influence over information security governance? The answer is C, the board of directors. The board of directors is the highest governing body of an organization, responsible for overseeing its strategic direction, performance, and accountability. The board of directors sets the tone at the top for information security governance by:
* Establishing a clear vision, mission, and values for information security
* Approving and reviewing information security policies and standards
* Allocating sufficient resources and budget for information security
* Appointing and empowering a chief information security officer (CISO) or equivalent role
* Holding management accountable for information security performance and compliance
* Communicating and promoting information security awareness and culture The board of directors has the most influence over information security governance because it has the ultimate authority and responsibility for ensuring that information security is aligned with the organization's business objectives, risks, and stakeholder expectations.
References:
* 10: What is Information Security Governance? - RiskOptics - Reciprocity
* 11: Information Security Governance and Risk Management | Moss Adams
* 12: ISO/IEC 27014:2020 - Information security, cybersecurity and privacy ...

NEW QUESTION: 150
Which of the following would be MOST useful when analyzing computer performance?
A. Report of off-peak utilization and response time
B. Tuning of system software to optimize resource usage
C. Operations report of user dissatisfaction with response time
D. Statistical metrics measuring capacity utilization
Answer: (SHOW ANSWER)
Section: Protection of Information Assets

NEW QUESTION: 151
Which of the following type of network service maps Domain Names to network IP addresses or network IP
addresses to Domain Names?

A. DHCP
B. DNS
C. Directory Service
D. Network Management
Answer: B (LEAVE A REPLY)
Section: Information System Operations, Maintenance and Support
Explanation/Reference:
Domain Name System(DNS) - Translates the names of network nodes into network IP address.
For your exam you should know below information about network services:
In computer networking, a network service is an application running at the network application layer and
above, that provides data storage, manipulation, presentation, communication or other capability which is
often implemented using a client-server or peer-to-peer architecture based on application layer network
protocols.
Each service is usually provided by a server component running on one or more computers (often a
dedicated server computer offering multiple services) and accessed via a network by client components
running on other devices. However, the client and server components can both be run on the same
machine.
Clients and servers will often have a user interface, and sometimes other hardware associated with them.
Different types of network services are as follows:
Network File System - Network File System (NFS) is a distributed file system protocol originally developed
by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much like
local storage is accessed.
Remote Access Service - Remote Access Services (RAS) refers to any combination of hardware and
software to enable the remote access tools or information that typically reside on a network of IT devices.
Directory Services - A directory service is the software system that stores, organizes and provides access
to information in a directory. In software engineering, a directory is a map between names and values. It
allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have

multiple definitions, in a directory, a name may be associated with multiple, different pieces of information.
Likewise, as a word may have different parts of speech and different definitions, a name in a directory may
have many different types of data.
Network Management - In computer networks, network management refers to the activities, methods,
procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of
networked systems. Network management is essential to command and control practices and is generally
carried out of a network operations center.
Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a
standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing
network configuration parameters, such as IP addresses for interfaces and services. With DHCP,
computers request IP addresses and networking parameters automatically from a DHCP server, reducing
the need for a network administrator or a user to configure these settings manually.
Email service - Provides the ability, through a terminal or PC connected to a communication network, to
send an entrusted message to another individual or group of people.
Print Services - Provide the ability, typically through a print server on a network, to manage and execute
print request services from other devices on the network
Domain Name System(DNS) - Translates the names of network nodes into network IP address.
The following were incorrect answers:
Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a
standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing
network configuration parameters, such as IP addresses for interfaces and services. With DHCP,
computers request IP addresses and networking parameters automatically from a DHCP server, reducing
the need for a network administrator or a user to configure these settings manually.
Directory Services - A directory service is the software system that stores, organizes and provides access
to information in a directory. In software engineering, a directory is a map between names and values. It

allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have
multiple definitions, in a directory, a name may be associated with multiple, different pieces of information.
Likewise, as a word may have different parts of speech and different definitions, a name in a directory may
have many different types of data.
Network Management - In computer networks, network management refers to the activities, methods,
procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of
networked systems. Network management is essential to command and control practices and is generally
carried out of a network operations center.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 258

NEW QUESTION: 152
A successful risk-based IT audit program should be based on:
A. an effective scoring system.
B. an effective PERT diagram.
C. an effective departmental brainstorm session.
D. an effective organization-wide brainstorm session.
E. an effective yearly budget.
F. None of the choices.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A successful risk-based IT audit program could be based on an effective scoring system. In establishing a scoring system, management should consider all relevant risk factors and avoid subjectivity. Auditors should develop written guidelines on the use of risk assessment tools and risk factors and review these guidelines with the audit committee.

NEW QUESTION: 153
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. Note the noncompliance in the audit working papers
B. Include the noncompliance in the audit report
C. Issue an audit memorandum identifying the incompliance
D. Determine why the procedures were not followed
Answer: (SHOW ANSWER)

NEW QUESTION: 154
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: 155
.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. Ahalon sprinkler system
Answer: A (LEAVE A REPLY)
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: 156
There are many firewall implementations provided by firewall manufacturers. Which of the following implementation utilize two packet filtering routers and a bastion host? This approach creates the most secure firewall system since it supports network and application level security while defining a separate DMZ.
A. Dual Homed firewall
B. Screened subnet firewall
C. Screened host firewall
D. Anomaly based firewall
Answer: B (LEAVE A REPLY)

Explanation/Reference:
In network security, a screened subnet firewall is a variation of the dual-homed gateway and screened host firewall. It can be used to separate components of the firewall onto separate systems, thereby achieving greater throughput and flexibility, although at some cost to simplicity. As each component system of the screened subnet firewall needs to implement only a specific task, each system is less complex to configure.
A screened subnet firewall is often used to establish a demilitarized zone (DMZ).
Below are few examples of Firewall implementations:
Screened host Firewall
Utilizing a packet filtering router and a bastion host, this approach implements a basic network layer security and application server security.
An intruder in this configuration has to penetrate two separate systems before the security of the private network can be compromised This firewall system is configured with the bastion host connected to the private network with a packet filtering router between internet and the bastion host Dual-homed Firewall
A firewall system that has two or more network interface, each of which is connected to a different network In a firewall configuration, a dual homed firewall system usually acts to block or filter some or all of the traffic trying to pass between the network A dual-homed firewall system is more restrictive form of screened-host firewall system Demilitarize Zone (DMZ) or screened-subnet firewall Utilizing two packet filtering routers and a bastion host
This approach creates the most secure firewall system since it supports network and application level security while defining a separate DMZ network Typically, DMZs are configured to limit access from the internet and organization's private network.
The following were incorrect answers:
The other types of firewall mentioned in the option do not utilize two packet filtering routers and a bastion host.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 346

NEW QUESTION: 157
Which of the following BEST protects private health information from data loss for clients that utilize remote health-monitoring devices?
A. Remote device wipe functionality
B. Encrypted device storage
C. Information security training
D. Digital certificates
Answer: B (LEAVE A REPLY)

NEW QUESTION: 158
Which of the following BEST enables an IS auditor to objectively determine the performance of an IT business process?

A. Recalculated key performance indicators (KPIs)
B. Management sign-off on performance reports
C. Capability maturity models
D. Control self-assessment (CSA) questionnaire
Answer: (SHOW ANSWER)

NEW QUESTION: 159
A review of IT interface controls finds an organization does not have a process to identify and correct records that do not get transferred to the receiving system.
Which of the following is the IS auditor's BEST recommendation?
A. Implement software to perform automatic reconciliations of data between systems.
B. Automate the transfer of data between systems as much as feasible.
C. Enable automatic encryption, decryption, and electronic signing of data files.
D. Have coders perform manual reconciliation of data between systems.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 160
Stress testing should ideally be carried out under a:
A. test environment with production workloads.
B. test environment with test data.
C. production environment with production workloads.
D. production environment with test data.
Answer: A (LEAVE A REPLY)
Stress testing is designed to evaluate a system's performance under extreme conditions1. It is typically carried out in a test environment that closely mirrors the production environment, using production workloads1. This approach ensures that the test results accurately reflect how the system would perform under similar conditions in the production environment1. Using a test environment also prevents any disruptions or damage to the production environment during testing1.
References:
* Stress Testing Best Practices: A Seven Steps Model

NEW QUESTION: 161
When developing a risk management program, what is the FIRST activity to be performed?
A. Threat assessment
B. Classification of data
C. Inventory of assets
D. Criticality analysis
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:

Identification of the assets to be protected is the first step in the development of a risk management program. A listing of the threats that can affect the performance of these assets and criticality analysis are later steps in the process. Data classification is required for defining access controls and in criticality analysis.

NEW QUESTION: 162
Proper segregation of duties does not prohibit a quality control administrator from also being responsible
for change control and problem management. True or false?
A. True
B. False
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Proper segregation of duties does not prohibit a quality-control administrator from also being responsible
for change control and problem management.

NEW QUESTION: 163
Which of the following would a digital signature MOST likely prevent?
A. Corruption
B. Unauthorized change
C. Repudiation
D. Disclosure
Answer: C (LEAVE A REPLY)
Explanation
Digital signature enforces non-repudiation. Thereby it prevents repudiation.

NEW QUESTION: 164
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: D (LEAVE A REPLY)
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: 165
An organization outsourced its IS functions to meet its responsibility for disaster recovery, the organization should:
A. discontinue maintenance of the disaster recovery plan (DRP>
B. coordinate disaster recovery administration with the outsourcing vendor
C. delegate evaluation of disaster recovery to a third party
D. delegate evaluation of disaster recovery to internal audit
Answer: (SHOW ANSWER)
Explanation
An organization outsourced its IS functions. To meet its responsibility for disaster recovery, the organization should coordinate disaster recovery administration with the outsourcing vendor. This is because the organization remains accountable for ensuring the continuity and availability of its IS functions, even if they are outsourced to a third party. The organization should establish clear roles and responsibilities, communication channels, testing procedures, and escalation processes with the outsourcing vendor for disaster recovery purposes. The organization should not discontinue maintenance of the disaster recovery plan (DRP), as it still needs to have a documented and updated plan for restoring its IS functions in case of a disaster. The organization should not delegate evaluation of disaster recovery to a third party or internal audit, as it still needs to monitor and review the performance and compliance of the outsourcing vendor with respect to disaster recovery objectives and standards. References: CISA Review Manual (Digital Version), [ISACA Auditing Standards]

NEW QUESTION: 166
Loading of illegal software packages onto a network by an employee is MOST effectively detected by:
A. diskless workstations.
B. regular scanning of hard drives
C. maintaining current antivirus software.
D. logging of activity on network drives.
Answer: B (LEAVE A REPLY)
Section: Protection of Information Assets

NEW QUESTION: 167
Which of the following is the STRONGEST indication of a mature risk management program?
A. Risk assessment results are used for informed decision-making.
B. All attributes of risk are evaluated by the risk owner.
C. A metrics dashboard has been approved by senior management.
D. The risk register is regularly updated by risk practitioners.
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
A mature risk management program ensures that risk assessmentsdirectly influence decision-makingto align IT risks with business objectives.
* Risk Assessment Results Used for Decision-Making (Correct Answer - A)
* Demonstrates that risk management is embedded in business processes.
* Enables proactive risk mitigation strategies.
* Example:A company identifies a cybersecurity risk and delays the launch of a new cloud service until additional controls are in place.
* Risk Owner Evaluating All Risk Attributes (Incorrect - B)
* Important, but risk management is a shared responsibility.
* Metrics Dashboard Approved by Management (Incorrect - C)
* A useful tool, but does not indicate effective risk management.
* Regular Updates to the Risk Register (Incorrect - D)
* Keeping records updated is necessary but not a strong indicator of maturity.
References:
* ISACA CISA Review Manual
* COBIT 2019: Risk Governance
* ISO 31000 (Risk Management Framework)

NEW QUESTION: 168
Which of the following is the MOST important action to ensure timely detection and triage for potential security incidents within an organization?
A. Install an agent to forward logs to a security information and event management (SIEM) solution for real-time analysis.
B. Train help desk staff to identify potential symptoms of security incidents when users initiate service tickets.
C. Ensure all network components and endpoints are hardened.
D. Engage a third-party service provider for incident response and forensic investigation.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 169
When auditing the IT governance of an organization planning to outsource a critical financial application to a cloud vendor, the MOST important consideration for the auditor should be:
A. the cost of the outsourced system.
B. alignment with business requirements.
C. alignment with industry standards.
D. the inclusion of a service termination clause.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 170
Which of the following provides nonrepudiation services for e-commerce transactions?
A. Public key infrastructure (PKI)
B. Data Encryption Standard (DES)
C. Message authentication code (MAC)
D. Personal identification number (PIN)
Answer: A (LEAVE A REPLY)
PKI is the administrative infrastructure for digital certificates and encryption key pairs. The qualities of an acceptable digital signature are: it is unique to the person using it; it is capable of verification; it is under the sole control of theperson using it; and it is linked to data in such a manner that if data are changed, the digital signature is invalidated. PKI meets these tests. The Data Encryption Standard (DES) is the most common private key cryptographic system. DES does not address nonrepudiation . A MAC is a cryptographic value calculated by passing an entire message through a cipher system. The sender attaches the MAC before transmission and the receiver recalculates the MAC and compares it to the sent MAC. If the two MACs are not equal, this indicates that the message has been altered during transmission; it has nothing to do with nonrepudiation . A PIN is a type of password, a secret number assigned to an individual that, in conjunction with some other means of identification, serves to verify the authenticity of the individual.

NEW QUESTION: 171
.What kind of protocols does the OSI Transport Layer of the TCP/IP protocol suite provide to ensure reliable communication?
A. Nonconnection-oriented protocols
B. Connection-oriented protocols
C. Session-oriented protocols
D. Nonsession-oriented protocols
Answer: B (LEAVE A REPLY)
The transport layer of the TCP/IP protocol suite provides for connection-oriented protocols to ensure reliable communication.

NEW QUESTION: 172

Which of the following is the BEST indication that a software development project is on track to meet its completion deadline?
A. The planned software go-live date has been communicated in advance to end users and stakeholders.
B. Technical specifications and development requirements have been agreed upon and formally recorded.
C. Project plan due dates have been documented for each phase of the software development life cycle.
D. Issues identified during user acceptance testing (UAT) have been addressed prior to the original implementation date.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 173
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: 174
An IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could an IS auditor use to estimate the size of the development effort?
A. Program evaluation review technique (PERT)
B. Counting source lines of code (SLOC)
C. Function point analysis
D. White box testing
Answer: C (LEAVE A REPLY)
Explanation/Reference:

Explanation:
Function point analysis is an indirect method of measuring the size of an application by considering the number and complexity of its inputs, outputs and files. It is useful for evaluating complex applications.
PERT is a project management technique that helps with both planning and control. SLOC gives a direct measure of program size, but does not allow for the complexity that may be caused by having multiple, linked modules and a variety of inputs and outputs. White box testing involves a detailed review of the behavior of program code, and is a quality assurance technique suited to simpler applications during the design and build stage of development.

NEW QUESTION: 175
Which of the following would BEST detect logic bombs in the new programs?
A. Final acceptance testing by users
B. Parallel/pilot testing
C. Regression testing
D. Independent program review
Answer: C (LEAVE A REPLY)
Section: Protection of Information Assets

NEW QUESTION: 176
The quality of the metadata produced from a data warehouse is _____ in the warehouse's design.
A. Often hard to determine because the data is derived from a heterogeneous data environment
B. The most important consideration
C. Independent of the quality of the warehoused databases
D. Of secondary importance to data warehouse content
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The quality of the metadata produced from a data warehouse is the most important consideration in the warehouse's design.

NEW QUESTION: 177
Which of the following BEST enables an IS auditor to combine and compare access control lists from various applications and devices?
A. Data analytics
B. Integrated test facility (ITF)
C. Audit hooks
D. Snapshots
Answer: A (LEAVE A REPLY)

NEW QUESTION: 178
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: B (LEAVE A REPLY)
Explanation/Reference:
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: 179
An organization maintains an inventory of the IT applications used by its staff Which of me following would pose the GREATEST concern with regard to tie quality inventory data?
A. Inventory data is available on and downloadable from the corporate intranet
B. The organization has not established a formal recertification process for the inventory data.
C. The application owner and contact information fields are not required to be completed
D. The inventory does not contain a formal risk ranking for all the IT applications.
Answer: (SHOW ANSWER)

NEW QUESTION: 180
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. Limit check
B. Parity check
C. Reasonableness check
D. Validity check
Answer: D (LEAVE A REPLY)

NEW QUESTION: 181
Which of the following is MOST important to have in place before developing a disaster recovery plan (DRP)?
A. A duplicate processing facility
B. Defined acceptable downtime
C. System restoration procedures

D. Appropriate insurance coverage
Answer: B (LEAVE A REPLY)

NEW QUESTION: 182
Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?
A. Time zone differences could impede communications between IT teams.
B. Telecommunications cost could be much higher in the first year.
C. Privacy laws could prevent cross-border flow of information.
D. Software development may require more detailed specifications.
Answer: C (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Privacy laws prohibiting the cross-border flow of personally identifiable information would make it impossible to locate a data warehouse containing customer information in another country. Time zone differences and higher telecommunications costs are more manageable. Software development typically requires more detailed specifications when dealing with offshore operations.

NEW QUESTION: 183
Winch of the following is MOST impen controls in a web application have been moved from the server side into the browser to boost performance. This
A. Acceptance test criteria have been developed
B. The design has been approved by senior management
C. Program coding standards have been tallowed
D. Data conversion procedures have been established
Answer: (SHOW ANSWER)

NEW QUESTION: 184
Which of the following is the BEST way to ensure that an application is performing according to its specifications?
A. Unit testing
B. Integration testing

C. Pilot testing
D. System testing
Answer: (SHOW ANSWER)

NEW QUESTION: 185
What is the MOST difficult aspect of access control in a multiplatform, multiple-site client/server environment?
A. Maintaining consistency throughout all platforms
B. Restricting a local user to necessary resources on the host server
C. Creating new user IDs valid only on a few hosts
D. Restricting a local user to necessary resources on a local platform
Answer: (SHOW ANSWER)

NEW QUESTION: 186
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: 187
What should be an IS auditor's MOST important consideration when assessing whether an organization's IT project portfolio is appropriately prioritized?
A. Business impact analysis (BIA)
B. The organization's IT budget
C. Cost-benefit analysis results
D. The organization's business plan
Answer: D (LEAVE A REPLY)

NEW QUESTION: 188
Which of following areas is MOST important for an IS auditor to focus on when reviewing the maturity model for a technology organization?
A. Standard operating procedures
B. Service level agreements (SLAs)
C. Roles and responsibility matrix

D. Business resiliency

Answer: (SHOW ANSWER)

A maturity model for a technology organization is a tool that measures the progress and capability of the IT function in relation to its goals, processes, and practices. A maturity model can help identify gaps and areas for improvement, as well as benchmark the IT function against industry standards or best practices. One of the key aspects of a maturity model is the definition and clarity of roles and responsibilities for the IT function and its stakeholders. A roles and responsibility matrix, such as a RACI matrix, is a document that clarifies who is responsible, accountable, consulted, and informed for each task or deliverable in a project or process.

A roles and responsibility matrix can help avoid confusion, duplication, or omission of work, as well as ensure accountability and communication among the IT function and its customers, partners, and suppliers.

Therefore, an IS auditor should focus on reviewing the roles and responsibility matrix when evaluating the maturity model for a technology organization.

A standard operating procedure (SOP) is a document that describes the steps and instructions for performing a routine or repetitive task or process. SOPs are important for ensuring consistency, quality, and compliance in the IT function, but they are not directly related to the maturity model. A service level agreement (SLA) is a contract that defines the expectations and obligations between an IT service provider and its customers. SLAs are important for ensuring customer satisfaction, performance measurement, and dispute resolution in the IT function, but they are not directly related to the maturity model. A business resiliency plan is a document that outlines how an IT function will continue to operate or recover from a disruption or disaster. Business resiliency is important for ensuring availability, reliability, and security in the IT function, but it is not directly related to the maturity model. References: 1: Maturity Models for IT & Technology | Splunk 2: Responsibility assignment matrix - Wikipedia 3: Roles and Responsibilities Matrix - SDLCforms

NEW QUESTION: 189

A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual's experience and:

A. length of service, since this will help ensure technical competence.

B. age, as training in audit techniques may be impractical.

C. IS knowledge, since this will bring enhanced credibility to the audit function.

D. ability, as an IS auditor, to be independent of existing IS relationships.

Answer: D (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

Independence should be continually assessed by the auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests, and prior job assignments and responsibilities. The fact that the employee has worked in IS for many years may not in itself ensure credibility. The audit department's needs should be defined and any

candidate should be evaluated against those requirements. The length of service will not ensure technical competency. Evaluating an individual's qualifications based on the age of the individual is not a good criterion and is illegal in many parts of the world.

NEW QUESTION: 190
Assessing IT risks is BEST achieved by:
A. evaluating threats associated with existing IT assets and IT projects.
B. using the firm's past actual loss experience to determine current exposure.
C. reviewing published loss statistics from comparable organizations.
D. reviewing IT control weaknesses identified in audit reports.
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk
assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process,
but by themselves are not sufficient. Basing an assessment on past losses will not adequately reflect
inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also
likely to be problems with the scope and quality of the loss data available to be assessed. Comparable
organizations will have differences in their IT assets, control environment and strategic circumstances.
Therefore, their loss experience cannot be used to directly assess organizational IT risk. Control weaknesses identified during audits will be relevant in assessing threat exposure and further analysis may
be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not
all of the critical IT assets and projects will have recently been audited, and there may not be a sufficient
assessment of strategic IT risks.

NEW QUESTION: 191
The application systems of an organization using open-source software have no single recognized developer producing patches. Which of the following would be the MOST secure way of updating open- source software?
A. Rewrite the patches and apply them
B. Code review and application of available patches
C. Develop in-house patches

D. identify and test suitable patches before applying them

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Suitable patches from the existing developers should be selected and tested before applying them.

Rewriting the patches and applying them is not a correct answer because it would require skilled resources and time to rewrite the patches. Code review could be possible but tests need to be performed before applying the patches. Since the system was developed outside the organization, the IT department may not have the necessary skills and resources to develop patches.

NEW QUESTION: 192

In which of the following database models is the data represented in terms of tulles and grouped into

relations?

A. Hierarchical database model

B. Network database model

C. Relational database model

D. Object-relational database model

Answer: (SHOW ANSWER)

Section: Information System Operations, Maintenance and Support

Explanation/Reference:

In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A

database organized in terms of the relational model is a relational database.

For your exam you should know below information about database models:

A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized, and manipulated. The most

popular example of a database model is the relational model, which uses a table-based format.

Common logical data models for databases include:

Hierarchical database model

Network model

Relational model

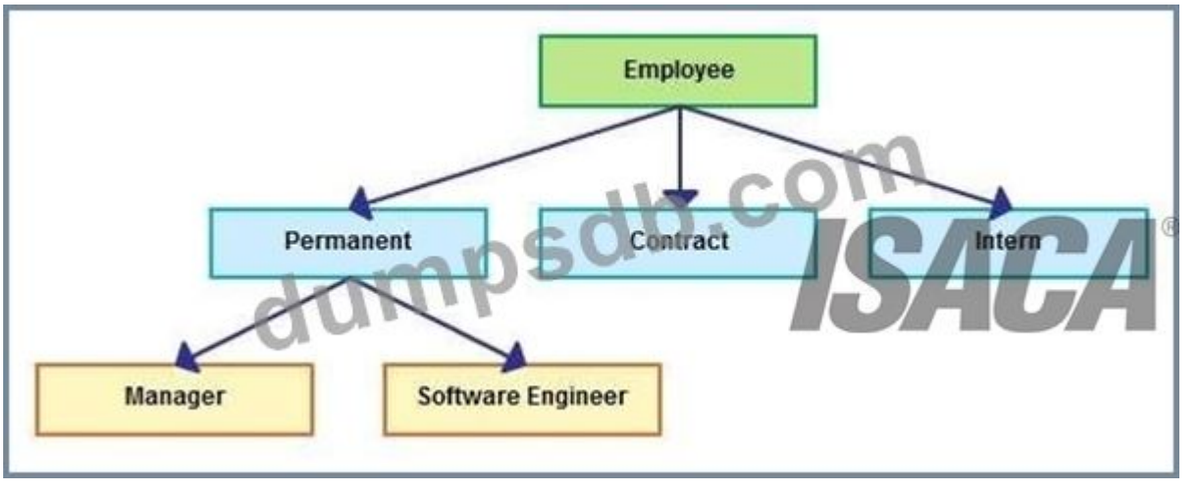
Object-relational database models

Hierarchical database model

In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record.

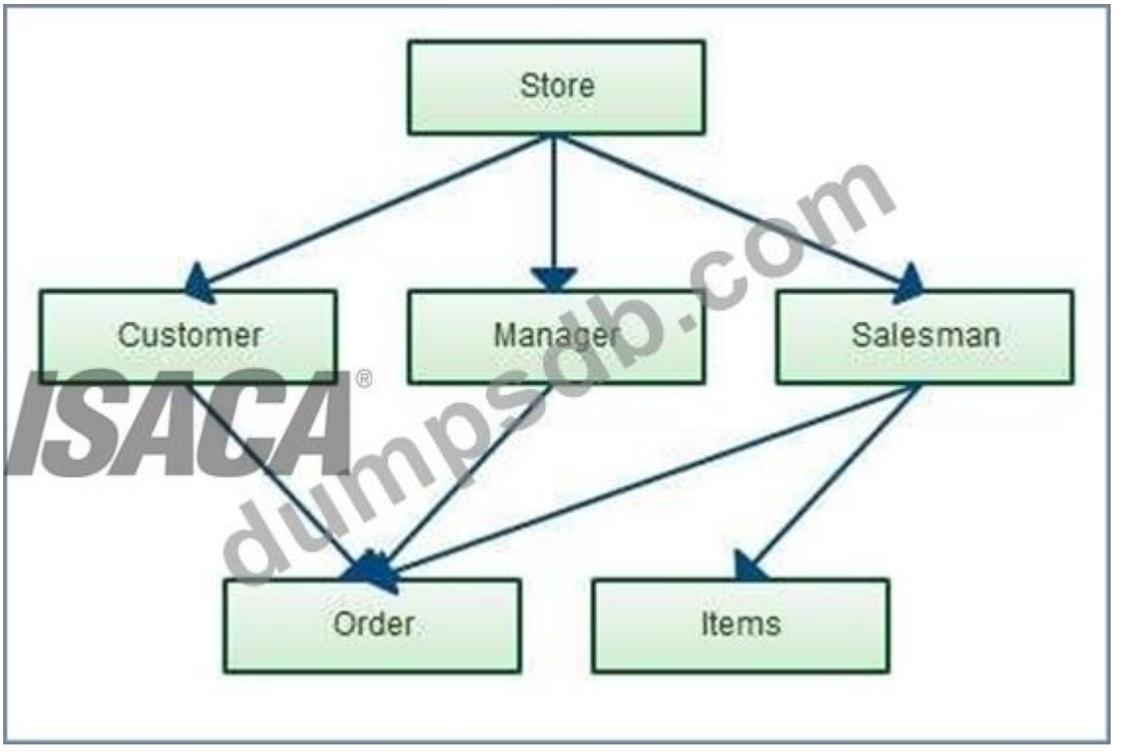
A sort field keeps sibling records in a particular order. Hierarchical structures were widely used in the early

mainframe database management systems, such as the Information Management System (IMS) by IBM,
and now describe the structure of XML documents. This structure allows one one-to-many relationship
between two types of data. This structure is very efficient to describe many relationships in the real world;
recipes, table of contents, ordering of paragraphs/verses, any nested and sorted information.
This hierarchy is used as the physical order of records in storage. Record access is done by navigating
through the data structure using pointers combined with sequential accessing. Because of this, the
hierarchical structure is inefficient for certain database operations when a full path (as opposed to upward
link and sort field) is not also included for each record. Such limitations have been compensated for in later
IMS versions by additional logical hierarchies imposed on the base physical hierarchy.
Hierarchical database model



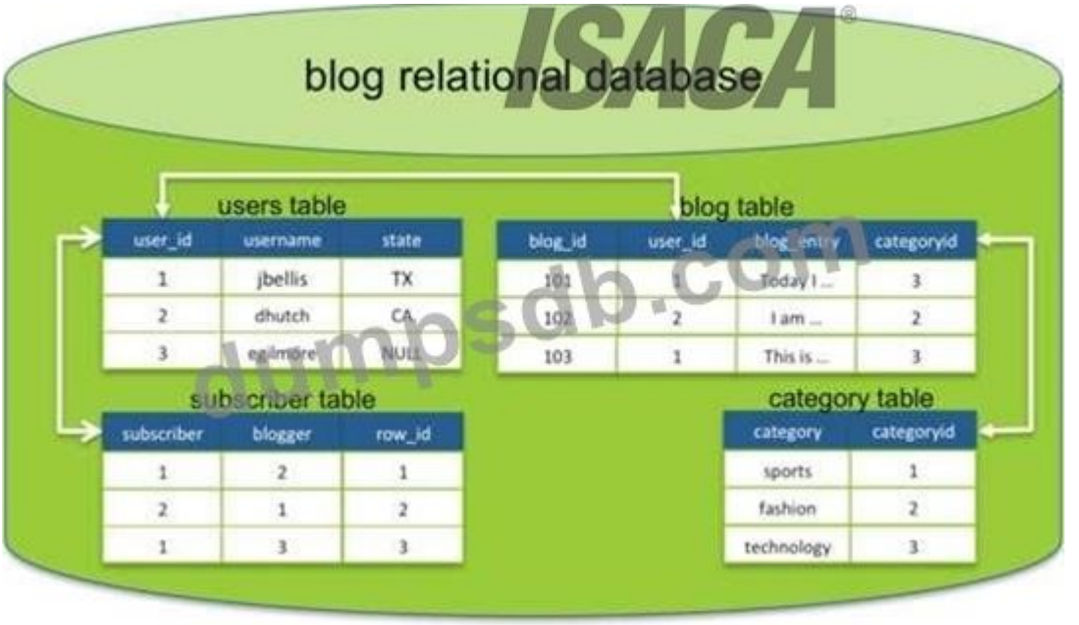
Network database model
The network model expands upon the hierarchical structure, allowing many-to-many relationships in a
tree-like structure that allows multiple parents. It was the most popular before being replaced by the
relational model, and is defined by the CODASYL specification.
The network model organizes data using two fundamental concepts, called records and sets. Records
contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not
to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between
records: one owner, many members. A record may be an owner in any number of sets, and a member in

any number of sets.
A set consists of circular linked lists where one record type, the set owner or parent, appears once in each
circle, and a second record type, the subordinate or child, may appear multiple times in each circle. In this
way a hierarchy may be established between any two record types, e.g., type A is the owner of B. At the
same time another set may be defined where B is the owner of
A. Thus all the sets comprise a general
directed graph (ownership defines a direction), or network construct. Access to records is either sequential
(usually in each record type) or by navigation in the circular linked lists.
The network model is able to represent redundancy in data more efficiently than in the hierarchical model,
and there can be more than one path from an ancestor node to a descendant. The operations of the
network model are navigational in style: a program maintains a current position, and navigates from one
record to another by following the relationships in which the record participates. Records can also be
located by supplying key values.
Network Database model



Relational database model
In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A

database organized in terms of the relational model is a relational database.
In the relational model, related records are linked together with a "key".
The purpose of the relational model is to provide a declarative method for specifying data and queries:
users directly state what information the database contains and what information they want from it, and let
the database management system software take care of describing data structures for storing the data and
retrieval procedures for answering queries.
Most relational databases use the SQL data definition and query language; these systems implement what
can be regarded as an engineering approximation to the relational model. A table in an SQL database
schema corresponds to a predicate variable; the contents of a table to a relation; key constraints, other
constraints, and SQL queries correspond to predicates. However, SQL databases, including DB2, deviate
from the relational model in many details, and Cod fiercely argued against deviations that compromise the
original principles.
Relational database model



Object-relational database Model
An object-relational database (ORD), or object-relational database management system (ORDBMS), is a
database management system (DBMS) similar to a relational database, but with an object-oriented
database model: objects, classes and inheritance are directly supported in database schemas and in the

query language. In addition, just as with pure relational systems, it supports extension of the data model
with custom data-types and methods.
Example of an object-oriented database model
An object-relational database can be said to provide a middle ground between relational databases and
object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of
relational databases: the data resides in the database and is manipulated collectively with queries in a
query language; at the other extreme are OODBMSes in which the database is essentially a persistent
object store for software written in an object-oriented programming language, with a programming API for
storing and retrieving objects, and little or no specific support for querying.
The following were incorrect answers:
Hierarchical database model - In a hierarchical model, data is organized into a tree-like structure, implying
a single parent for each record. A sort field keeps sibling records in a particular order.
Network database model-The network model expands upon the hierarchical structure, allowing many-to-
many relationships in a tree-like structure that allows multiple parents.
Object-relational database models- An object-relational database can be said to provide a middle ground
between relational databases and object-oriented databases (OODBMS). In object-relational databases,
the approach is essentially that of relational databases: the data resides in the database and is manipulated
collectively with queries in a query language; at the other extreme are OODBMSes in which the database is
essentially a persistent object store for software written in an object-oriented programming language, with a
programming API for storing and retrieving objects, and little or no specific support for querying.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 254

NEW QUESTION: 193
Which of the following would be MOST critical for an IS auditor to look for when evaluating fire precautions in a manned data center located in the upper floor of a multi-story building?
A. Existence of handheld fire extinguishers in highly visible locations
B. Adequacy of the HVAC system throughout the facility

C. Documentations of regular inspections by the local fire department
D. Documentation of tested emergency evacuation plans
Answer: A (LEAVE A REPLY)

NEW QUESTION: 194
Which of the following access rights presents the GREATEST risk when granted to a new member of the system development staff?
A. Write access to development data libraries
B. Execute access to development program libraries
C. Write access to production program libraries
D. Execute access to production program libraries
Answer: C (LEAVE A REPLY)

NEW QUESTION: 195
Which of the following backup techniques is the MOST appropriate when an organization requires extremely granular data restore points, as defined in the recovery point objective (RPO)?
A. Virtual tape libraries
B. Disk-based snapshots
C. Continuous data backup
D. Disk-to-tape backup
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The recovery point objective (RPO) is based on the acceptable data loss in the case of a disruption. In this scenario the organization needs a short RPO. Virtual tape libraries, disk-based snapshots and disk-to-tape backup would require time to complete the backup, while continuous data backup happens online (in real time).

NEW QUESTION: 196
Which of the following is the MOST effective way for internal audit management to ensure the quality of IS audits is maintained?
A. Include quality metrics in audit staff annual performance evaluations.
B. Introduce a balanced scorecard for internal audit.
C. Conduct control self-assessments (CSA) with IT management.
D. Engage a third party to conduct regular quality assurance (QA) reviews.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 197
During a review of an insurance company's claims system, the IS auditor learns that claims for specific medical procedures are acceptable only from females. This is an example of a:
A. key verification.
B. completeness check.
C. reasonableness check.
D. logical relationship check.
Answer: (SHOW ANSWER)
Section: The process of Auditing Information System

NEW QUESTION: 198
Which of the following would provide the BEST protection against the hacking of a computer connected to the Internet?
A. A remote access server
B. A proxy server
C. A personal firewall
D. A password-generating token
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A personal firewall is the best way to protect against hacking, because it can be defined with rules that describe the type of user or connection that is or is not permitted. A remote access server can be mapped or scanned from the Internet, creating security exposures. Proxy servers can provide protection based on the IP address and ports; however, an individual would need to have in-depth knowledge to do this, and applications can use different ports for the different sections of their program. A password-generating token may help to encrypt the session but does not protect a computer against hacking.

NEW QUESTION: 199
Which of the following user profiles should be of MOST concern to an IS auditor when performing an audit of an EFT system?
A. Three users with the ability to capture and verify their own messages
B. Five users with the ability to capture and send their own messages
C. Five users with the ability to verify other users and to send their own messages
D. Three users with the ability to capture and verify the messages of other users and to send their own messages
Answer: (SHOW ANSWER)

Explanation/Reference:
Explanation:
The ability of one individual to capture and verify messages represents an inadequate segregation, since messages can be taken as correct and as if they had already been verified.

NEW QUESTION: 200
Which of the following provides the BEST assurance that vendor-supported software remains up to date?
A. Version management
B. Software asset management
C. Licensing agreement and escrow
D. Release and patch management
Answer: (SHOW ANSWER)

NEW QUESTION: 201
What type of BCP test uses actual resources to simulate a system crash and validate the plan's effectiveness?
A. Paper
B. Preparedness
C. Walk-through
D. Parallel
Answer: B (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Of the three major types of BCP tests (paper, walk-through, and preparedness), only the preparedness test
uses actual resources to simulate a system crash and validate the plan's effectiveness.

NEW QUESTION: 202
Which of the following technique is used for speeding up network traffic flow and making it easier to manage?
A. Point-to-point protocol
B. X.25
C. MPLS
D. ISDN
Answer: C (LEAVE A REPLY)
Explanation/Reference:
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.

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

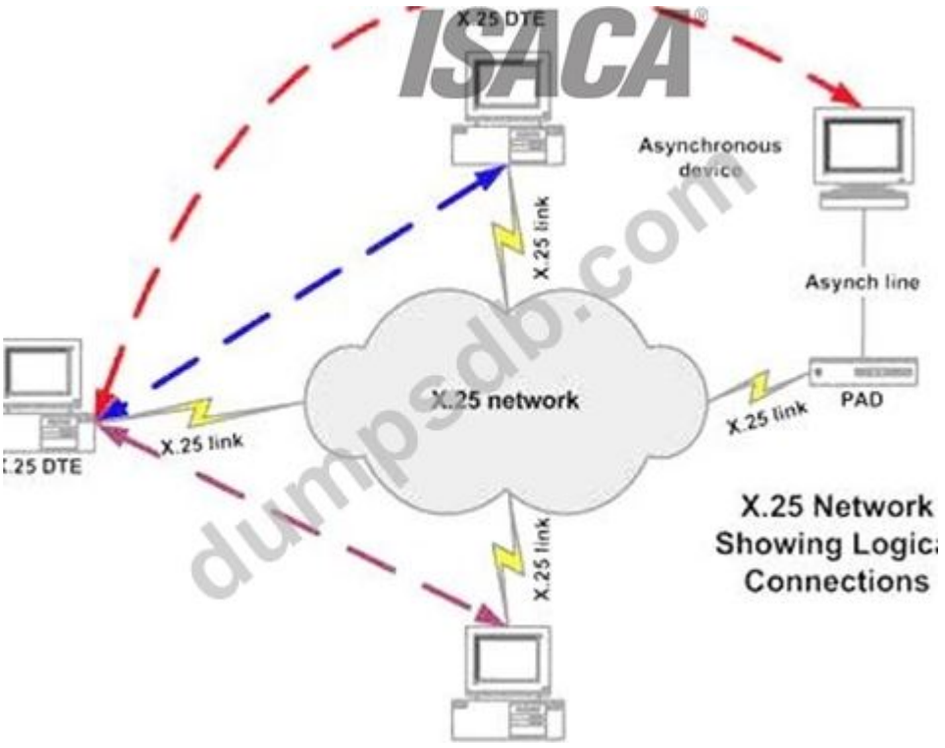
X.25

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

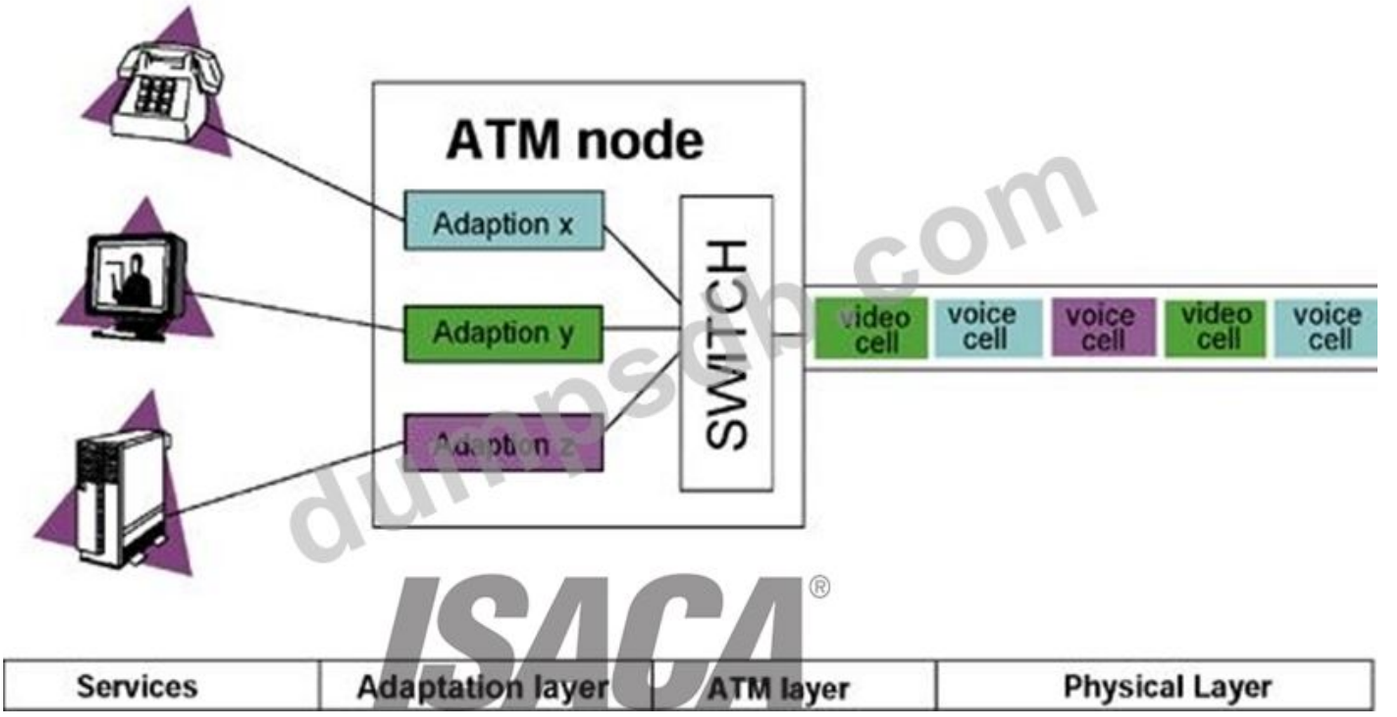
Asynchronous Transfer Mode (ATM)

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

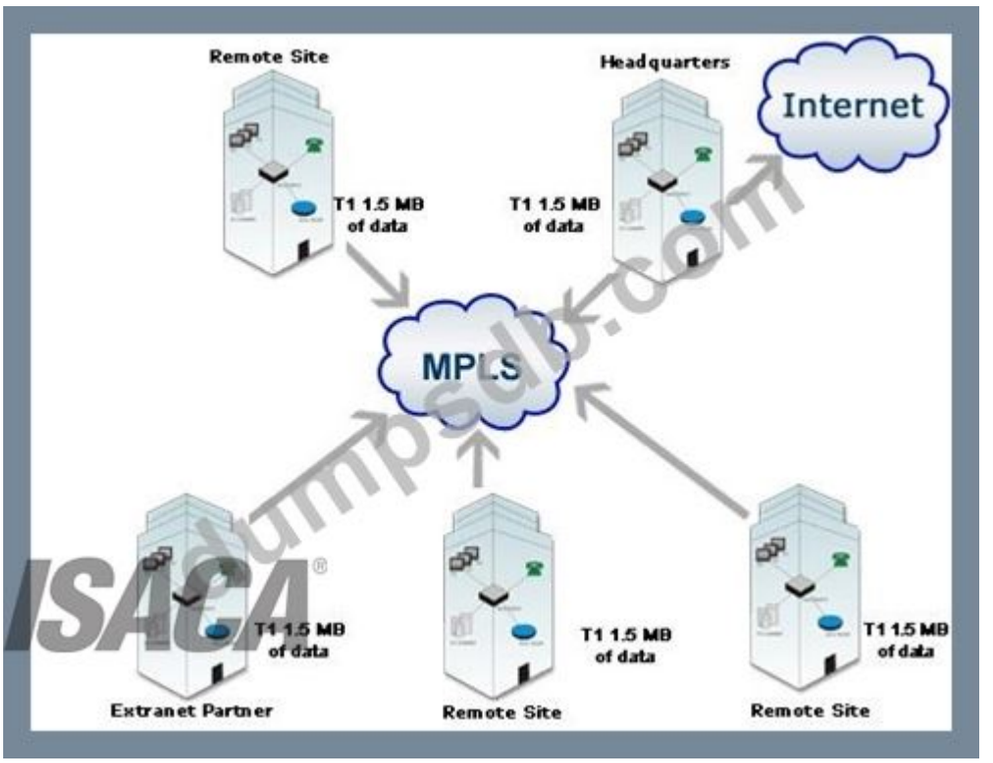
Asynchronous Transfer Mode



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.
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.
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.
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 266

NEW QUESTION: 203
An organization developed a comprehensive three-year IT strategic plan. Halfway into the plan, a major
legislative change impacting the organization is enacted. Which of the following should be management's
NEXT course of action?
A. Develop specific procedural documentation related to the changed legislation.
B. Assess the legislation to determine whether are required to the strategic IT plan.
C. Perform a risk management of the legislative changes.
D. Develop a new IT strategic plan that encompasses the new legislation.
Answer: B (LEAVE A REPLY)
Section: Governance and Management of IT

NEW QUESTION: 204
To protect a VoIP infrastructure against a denial-of-service (DoS) attack, it is MOST important to secure the:
A. access control servers.
B. session border controllers.
C. backbone gateways.
D. intrusion detection system (IDS).
Answer: (SHOW ANSWER)
Session border controllers enhance the security in the access network and in the core. In the access network, they hide a user's real address and provide a managed public address. This public address can be monitored, minimizing the opportunities forscanning and denial-of-service (DoS) attacks. Session border controllers permit access to clients behind firewalls while maintaining the firewall's effectiveness. In the core, session border controllers protect the users and the network. They hide network topology and users' real addresses. They can also monitor bandwidth and quality of service. Securing the access control server, backbone gateways and intrusion detection systems (IDSs) does not effectively protect against DoS attacks.

NEW QUESTION: 205
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: (SHOW ANSWER)
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: 206
Human error is being HEAVILY relied upon on by which of the following types of attack?
A. DDoS
B. Eavedropping
C. Social Engineering
D. None of the choices.
E. ATP
F. DoS

Answer: (SHOW ANSWER)

NEW QUESTION: 207
A review of an organization's IT portfolio revealed several applications that are not in use. The BEST way to prevent this situation from recurring would be to implement.
A. Asset life cycle management.
B. Business case development procedures
C. An information asset acquisition policy
D. A formal request for proposal (RFP) process
Answer: C (LEAVE A REPLY)

NEW QUESTION: 208
Who is PRIMARILY responsible for the design of IT controls to meet control objectives?
A. Risk management
B. Internal auditor
C. IT manager
D. Business management
Answer: A (LEAVE A REPLY)

NEW QUESTION: 209
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: B (LEAVE A REPLY)
Explanation
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: 210
Which of the following uses a prototype that can be updated continually to meet changing user or business requirements?
A. PERT
B. Rapid application development (RAD)
C. Function point analysis (FPA)
D. GANTT
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Rapid application development (RAD) uses a prototype that can be updated continually to meet changing user or business requirements.

NEW QUESTION: 211
Which of the following measures BEST mitigates the risk of data exfiltration during a cyberattack?
A. Perimeter firewall
B. Network access controls (NAC)
C. Data loss prevention (DLP) system
D. Hashing of sensitive data
Answer: (SHOW ANSWER)

NEW QUESTION: 212
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 number361

NEW QUESTION: 213

An IS auditor is reviewing a project to implement a payment system between a parent bank and a subsidiary. The IS auditor should FIRST verify that the:

A. technical platforms between the two companies are interoperable.

B. parent bank is authorized to serve as a service provider.

C. security features are in place to segregate subsidiary trades.

D. subsidiary can join as a co-owner of this payment system.

Answer: (SHOW ANSWER)

Section: Protection of Information Assets

Explanation:

Even between parent and subsidiary companies, contractual agreement(s) should be in place to conduct shared services. This is particularly important in highly regulated organizations such as

banking. Unless granted to serve as a service provider, it may not be legal for the bank to extend business to the subsidiary companies. Technical aspects should always be considered; however, this can be initiated after confirming that the parent bank can serve as a service provider. Security aspects are another important factor; however, this should be considered after confirming that the parent bank can serve as a service provider.
The ownership of the payment system is not as important as the legal authorization to operate the system.

NEW QUESTION: 214
The reason a certification and accreditation process is performed on critical systems is to ensure that:
A. security compliance has been technically evaluated.
B. data have been encrypted and are ready to be stored.
C. the systems have been tested to run on different platforms.
D. the systems have followed the phases of a waterfall model.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Certified and accredited systems are systems that have had their security compliance technically evaluated for running on a specific production server. Choice B is incorrect because not all data of certified systems are encrypted. Choice C is incorrect because certified systems are evaluated to run in a specific environment. A waterfall model is a software development methodology and not a reason for performing a certification and accrediting process.

NEW QUESTION: 215
The PRIMARY objective of an audit of IT security policies is to ensure that:
A. they are distributed and available to all staff.
B. security and control policies support business and IT objectives.
C. there is a published organizational chart with functional descriptions.
D. duties are appropriately segregated.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives. Reviewing whether policies are available to all is an objective, but distribution does not ensure compliance. Availability of organizational charts with functional descriptions and segregation of duties might be included in the review, but are not the primary objective of an audit of security policies.

NEW QUESTION: 216

An organization has contracted with a third party to implement and configure a new accounting application.
Once the application is implemented, in-house staff will provide all application support and maintenance.
Which of the following is MOST important to the success of this initiative?
A. Establishing a knowledge transfer plan
B. Ensuring the third party completed testing
C. Documenting an implementation plan
D. Conducting a post-implementation review
Answer: A (LEAVE A REPLY)

NEW QUESTION: 217
After observing suspicious activities in a server, a manager requests a forensic analysis.
Which of the following findings should be of MOST concern to the investigator?
A. Server is a member of a workgroup and not part of the server domain
B. Guest account is enabled on the server
C. Recently, 100 users were created in the server
D. Audit logs are not enabled for the server
Answer: D (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Audit logs can provide evidence which is required to proceed with an investigation and should not be
disabled. For business needs, a server can be a member of a workgroup and, therefore, not a concern.
Having a guest account enabled on a system is a poor security practice but not a forensic investigation
concern. Recently creating 100 users in the server may have been required to meet business needs and
should not be a concern.

NEW QUESTION: 218
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: A (LEAVE A REPLY)
Explanation/Reference:

Programmers should perform unit, module, and full regression testing following any changes to an application or system.

NEW QUESTION: 219
.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: 220
A business application system accesses a corporate database using a single ID and password embedded in a program. Which of the following would provide efficient access control over the organization's data?
A. Introduce a secondary authentication method such as card swipe
B. Apply role-based permissions within the application system
C. Have users input the ID and password for each database transaction
D. Set an expiration period for the database password embedded in the program
Answer: B (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
When a single ID and password are embedded in a program, the best compensating control would be a sound access control over the application layer and procedures to ensure access to data is granted based on a user's role. The issue is user permissions, not authentication, therefore adding a stronger authentication does not improve the situation. Having a user input the ID and password for access would provide a better control because a database log would identify the initiator of the activity. However, this may not be efficient because each transaction would require a separate authentication process. It is a good practice to set an expiration date for a password. However, this might not be practical for an ID automatically logged in from the program. Often, this type of password is set not to expire.

NEW QUESTION: 221
Which of the following is one most common way that spyware is distributed?
A. as a trojan horse.
B. as a virus.
C. as an Adware.
D. as a device driver.
E. as a macro.

F. None of the choices.

Answer: (SHOW ANSWER)

Explanation/Reference:

One of the most common ways that spyware is distributed is as a Trojan horse, bundled with a piece of desirable software that the user downloads off the Web or a peer-to-peer file-trading network. When the user installs the software, the spyware is installed alongside.

NEW QUESTION: 222

An IS auditor is assigned to review the development of a specific application. Which of the following would be the MOST significant step following the feasibility study?

A. Attend project progress meetings to monitor timely implementation of the application.

B. Assist users in the design of proper acceptance-testing procedures.

C. Follow up with project sponsor for project's budgets and actual costs.

D. Review functional design to determine that appropriate controls are planned.

Answer: (SHOW ANSWER)

Section: The process of Auditing Information System

NEW QUESTION: 223

Which of the following INCORRECTLY describes the layer functions of the LAN or WAN Layer of the TCP/ IP model?

A. Combines packets into bytes and bytes into frame

B. Providers logical addressing which routers use for path determination

C. Provide address to media using MAC address

D. Performs only error detection

Answer: B (LEAVE A REPLY)

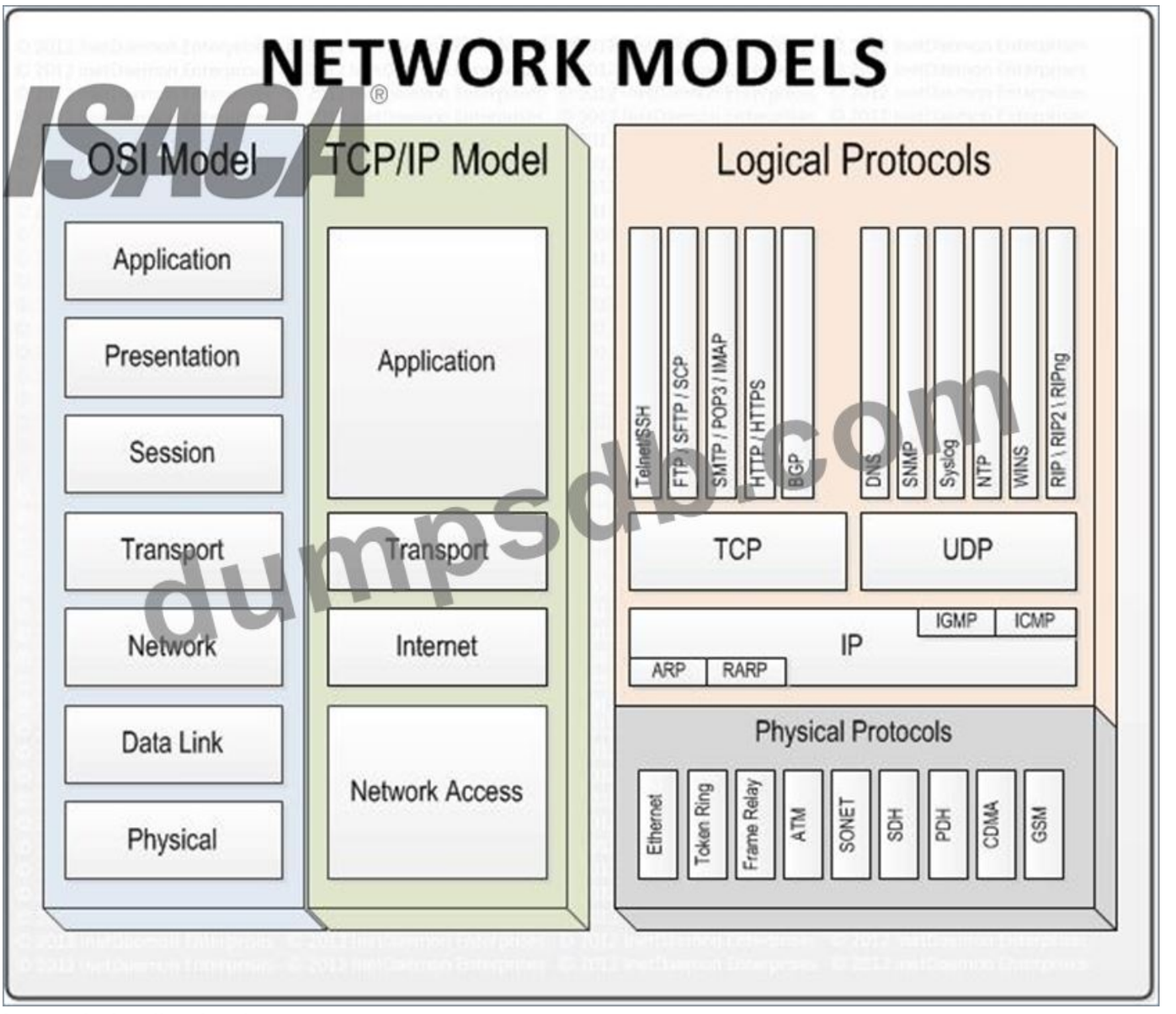
Explanation/Reference:

The word INCORRECTLY is the keyword used in the question. You need to find out the functionality that is not performed by LAN or WAN layer in TCP/IP model.

The Network layer of a TCP/IP model provides logical addressing which routers use for path determination.

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.

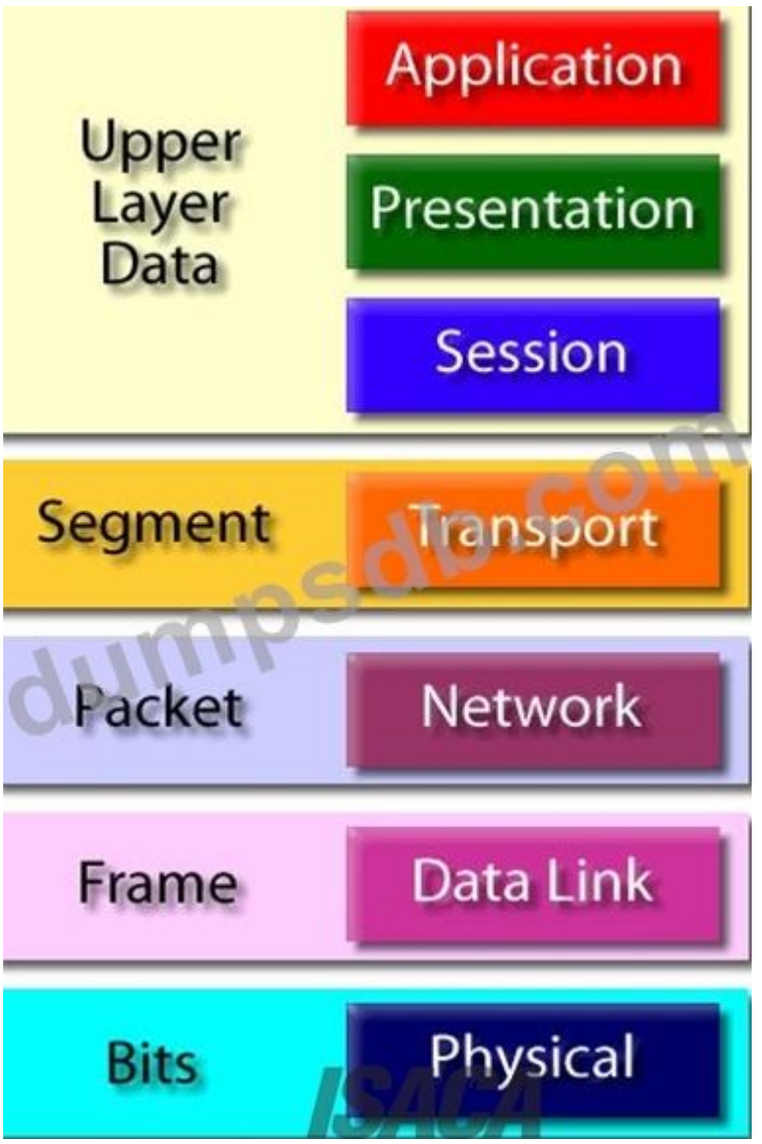
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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 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: 224

When initiating an IT project, which of the following should be completed FIRST?

A. IT resource plan

B. Milestone plan

C. Feasibility study

D. Request for proposal (RFP)

Answer: C (LEAVE A REPLY)

NEW QUESTION: 225

During the extraction and transfer process of data from an application database to an enterprise data warehouse, some of the fields were not picked up in the extraction process and therefore did

not end up in the data warehouse. Which of the following is the GREATEST concern with this situation?

A. Management decisions may be based on incorrect data.

B. Management reporting could be delayed.

C. Transaction errors may occur within the application.

D. Costs associated with correcting the process may exceed budget.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 226

Upon completion of audit work, an IS auditor should:

A. distribute a summary of general findings to the members of the auditing team.

B. review the working papers with the auditee.

C. provide a report to the auditee stating the initial findings.

D. provide a report to senior management prior to discussion with the auditee.

Answer: (SHOW ANSWER)

NEW QUESTION: 227

Which of the following types of testing would determine whether a new or modifies system can operate in its target environment without adversely impacting other existing systems?

A. Parallel testing

B. Pilot testing

C. Interface/integration testing

D. Sociability testing

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

The purpose of sociability testing is to confirm that a new or modified system can operate in its target environment without adversely impacting existing systems. This should cover the platform that will perform primary application processing and interfaces with other systems, as well as changes to the desktop in a client-server or web development. Parallel testing is the process of feeding data into two systems-the modified system and an alternate system- and comparing the results. In this approach, the old and new systems operate concurrently for a period of time and perform the same processing functions. Pilot testing takes place first at one location and is then

extended to other locations. The purpose is to see if the new system operates satisfactorily in one place before implementing it at other locations. Interface/integration testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective is to take unit-tested modules and build an integrated structure.

NEW QUESTION: 228
When engaging services from external auditors, which of the following should be established FIRST?
A. Termination conditions agreements
B. Nondisclosure agreements
C. Service level agreements
D. Operational level agreements
Answer: B (LEAVE A REPLY)
Section: The process of Auditing Information System

NEW QUESTION: 229
Following Pie last external review, the audit client implemented an advanced data storage solution Which of the following is MOST important to include in the audit scope?
A. Reviewing procedures to ensure administrators are managing data storage appropriately
B. Determining whether management has adequate off-site storage of operational procedures and manuals
C. Reviewing the implemented storage options and architectures for critical applications
D. Ensuring management has completed a cost-benefits analysis and documented results
Answer: D (LEAVE A REPLY)

NEW QUESTION: 230
Which of the following is necessary for the effective risk management in IT governance?
A. Risk evaluation is embedded in management processes
B. Risk management strategy is approved by the audit committee
C. Local managers are solely responsible for risk evaluation
D. IT risk management is separate from corporate risk management
Answer: A (LEAVE A REPLY)
Section: Governance and Management of IT

NEW QUESTION: 231
Which of the following provides an IS auditor assurance that the interface between a point-of-sale (POS) system and the general ledger is transferring sales data completely and accurately?
A. Electronic copies of customer sales receipts are maintained.
B. Monthly bank statements are reconciled without exception.
C. Nightly batch processing has been replaced with real-time processing.

D. The data transferred over the POS interface is encrypted.

Answer: A (LEAVE A REPLY)

The best option to provide an IS auditor assurance that the interface between a point-of-sale (POS) system and the general ledger is transferring sales data completely and accurately is A. Electronic copies of customer sales receipts are maintained. Electronic copies of customer sales receipts are records of the transactions that occurred at the POS system, which can be compared with the data transferred to the general ledger. This can help detect any errors, omissions, or discrepancies in the data transfer process and ensure that the sales data is complete and accurate.

The other options are not as effective as A in providing assurance that the interface between the POS system and the general ledger is transferring sales data completely and accurately. B. Monthly bank statements are reconciled without exception. Monthly bank statements are records of the cash inflows and outflows of the organization, which may not match with the sales data recorded by the POS system and the general ledger. For example, there may be delays, discounts, returns, or refunds that affect the cash flow but not the sales revenue.

Therefore, reconciling monthly bank statements without exception does not necessarily mean that the sales data is complete and accurate. C. Nightly batch processing has been replaced with real-time processing.

Nightly batch processing is a method of transferring data from the POS system to the general ledger in batches at a scheduled time, usually at night. Real-time processing is a method of transferring data from the POS system to the general ledger as soon as the transactions occur. Real-time processing may improve the timeliness and efficiency of the data transfer process, but it does not guarantee that the sales data is complete and accurate. There may still be errors, omissions, or discrepancies in the data transfer process that need to be detected and corrected.

D. The data transferred over the POS interface is encrypted. Encryption is a process of transforming data into an unreadable form using a secret key or algorithm, so that only authorized parties can access the original data. Encryption protects the confidentiality and security of the data transferred over the POS interface, but it does not ensure that the sales data is complete and accurate. There may still be errors, omissions, or discrepancies in the data transfer process that need to be detected and corrected.

References:

* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2
* Sales Audit Overview - Oracle3
* Notes on Audit of Ledgers - Guidelines to Auditors - Accountlearning

NEW QUESTION: 232

External experts were used on a recent IT audit engagement. While assessing the external experts' work, the internal audit team found some gaps in the evidence mat may have impacted their conclusions. What is the internal audit team's BEST course of action?

A. Recommend the external experts conduct additional testing.

B. Report a scope limitation in their conclusions.
C. Engage another expert to conduct the same testing.
D. Escalate to senior management.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 233
Which of the following is the PRIMARY reason to perform user acceptance testing (UAT) prior to production release for a new system?
A. It validates that users are trained on the system before moving to production.
B. It provides assurance that that all initial requirements have been developed and implemented.
C. It demonstrates that developed functions are operating effectively according to requirements.
D. It demonstrates that hot fixes meet expected results before moving to production.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 234
An organization's software develops need access to personally identifiable information (PII) stored in a
particular data format. Which of the following would be the BEST way to protect this sensitive information
while allowing the developers to use it in development and test environments?
A. Data masking
B. Data encryption
C. Data tokenization
D. Data abstraction
Answer: (SHOW ANSWER)
Section: Protection of Information Assets

NEW QUESTION: 235
When auditing the feasibility study of a system development project, the IS auditor should:
A. review qualifications of key members of the project team.
B. review the request for proposal (RFP) to ensure that it covers the scope of work.
C. review cost-benefit documentation for reasonableness.
D. ensure that vendor contracts are reviewed by legal counsel.
Answer: C (LEAVE A REPLY)
Explanation
A feasibility study is an assessment that determines the likelihood of a proposed project being successful, such as a new system development1. A feasibility study typically covers various aspects of the project, such as technical, economic, operational and legal feasibility2. The IS auditor's role is to audit the feasibility study and ensure that it is objective, realistic and reliable3. One of the most important aspects of a feasibility study is the economic feasibility, which analyzes the costs and benefits of the proposed system and compares them with alternative solutions2.

The economic feasibility study should include a detailed breakdown of the development, implementation and operational costs, as well as the expected revenues, savings and intangible benefits of the system3. The IS auditor should review the cost-benefit documentation for reasonableness and accuracy, and verify that the assumptions and calculations are valid and supported by evidence3.
The other options are not directly related to auditing the feasibility study of a system development project.
Reviewing qualifications of key members of the project team (option A) is more relevant to auditing the project management and human resources aspects of the project. Reviewing the request for proposal (RFP) to ensure that it covers the scope of work (option B) is more relevant to auditing the procurement and vendor selection process of the project. Ensuring that vendor contracts are reviewed by legal counsel (option D) is more relevant to auditing the legal and contractual aspects of the project.
References: 3: Types of Feasibility Study in Software Project Development 2: Feasibility Analysis in System Development Process 1: What Is a Feasibility Study? Definition, Benefits and Types

NEW QUESTION: 236
For several years, a vendor has been providing offsite backup media and record storage for a bank. Due to
familiarity with bank employees, the vendor does not consistently require authorization forms from them to
retrieve media. Which of the following is the GREATEST risk from this situation?
A. Bank employees can inappropriately obtain sensitive records
B. Backup tapes may not be available
C. Chain of custody could not be validated
D. The vendor provides the incorrect media to employees
Answer: C (LEAVE A REPLY)
Section: Information System Operations, Maintenance and Support

NEW QUESTION: 237
Which of the following would MOST effectively reduce social engineering incidents?
A. Security awareness training
B. increased physical security measures
C. E-mail monitoring policy
D. intrusion detection systems
Answer: (SHOW ANSWER)
Social engineering exploits human nature and weaknesses to obtain information and access privileges. By increasing employee awareness of security issues, it is possible to reduce the number of successful social engineering incidents. In most cases, social engineering incidents do not require the physical presence of the intruder. Therefore, increased physical security measures would not prevent the intrusion. An e-mail monitoring policy informs users that all e-mail in the

organization is subject to monitoring; it does not protect the users from potential security incidents and intruders. Intrusion detection systems are used to detect irregular or abnormal traffic patterns.

NEW QUESTION: 238
An IS auditor Is reviewing a complete population of incidents to assess an organization's incident management process. Which of the following observations should be the IS auditor's GREATEST concern?
A. Some incidents were not subject to secondary review
B. All incidents were initially assigned to the queue manager
C. Some incidents do not have a root cause defined.
D. All incidents are assigned the same priority.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 239
Which of the following is the MOST important element for the successful implementation of IT governance?
A. Implementing an IT scorecard
B. Identifying organizational strategies
C. Performing a risk assessment
D. Creating a formal security policy
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The key objective of an IT governance program is to support the business, thus the identification of organizational strategies is necessary to ensure alignment between IT and corporate governance. Without identification of organizational strategies,the remaining choices-even if implemented-would be ineffective.

NEW QUESTION: 240
Functional acknowledgements are used:
A. as an audit trail for EDI transactions.
B. to functionally describe the IS department.
C. to document user roles and responsibilities.
D. as a functional description of application software.
Answer: (SHOW ANSWER)
Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and, therefore, can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

NEW QUESTION: 241

To enable the alignment of IT staff development plans with IT strategy, which of the following should be done FIRST?

A. Develop quarterly training for each IT staff member.

B. Identify required IT skill sets that support key business processes

C. Include strategic objectives m IT staff performance objectives

D. Review IT staff job descriptions for alignment

Answer: B (LEAVE A REPLY)

NEW QUESTION: 242

When determining whether a project in the design phase will meet organizational objectives, what is BEST to compare against the business case?

A. Implementation plan

B. Project budget provisions

C. Requirements analysis

D. Project plan

Answer: C (LEAVE A REPLY)

Requirements analysis should be the best thing to compare against the business case when determining whether a project in the design phase will meet organizational objectives, because it defines the functional and non-functional specifications of the project deliverables that should satisfy the business needs and expectations. Requirements analysis can help evaluate whether the project design is aligned with the business case and whether it can achieve the desired outcomes and benefits. Implementation plan, project budget provisions, and project plan are also important aspects of a project in the design phase, but they are not as relevant as requirements analysis for comparing against the business case. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.1

NEW QUESTION: 243

The performance of an order-processing system can be measured MOST reliably by monitoring:

A. turnaround time of completed transactions.

B. application and database servers' CPU load.

C. input/request queue length.

D. heartbeats between server systems.

Answer: (SHOW ANSWER)

NEW QUESTION: 244
During a review of an organization's network threat response process. The IS auditor noticed that the majority of alerts were closed without resolution. Management responded that those alerts were unworkable due to lack of actionable intelligence, and therefore the support team is allowed to close them. What is the best way for the auditor to address the situation?
A. Further review closed unactioned alerts to identify mishandling of threats
B. Omit the finding from the report as this practice is in compliance with the current policy
C. Reopen unactioned alerts and report to the audit committee
D. Recommend that management enhance the policy and improve threat awareness training
Answer: (SHOW ANSWER)

NEW QUESTION: 245
An IS auditor is reviewing a project that is using an Agile software development approach. Which of the following should the IS auditor expect to find?
A. Use a process-based maturity model such as the capability maturity model (CMM)
B. Regular monitoring of task-level progress against schedule
C. Extensive use of software development tools to maximize team productivity
D. Postiteration reviews that identify lessons learned for future use in the project
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A key tenet of the Agile approach to software project management is team learning and the use of team learning to refine project management and software development processes as the project progresses.
One of the best ways to achieve this is that, at the end of each iteration, the team considers and documents what worked well and what could have worked better, and identifies improvements to be implemented in subsequent iterations. CMM and Agile really sit at opposite poles. CMM places heavy emphasis on predefined formal processes and formal project management and software development deliverables. Agile projects, by contrast, rely on refinement of process as dictated by the particular needs of the project and team dynamics.
Additionally, less importance is placed on formal paper- based deliverables, with the preference being effective informal communication within the team and with key outside contributors. Agile projects produce releasable software in short iterations, typically ranging from 4 to 8 weeks. This, in itself, instills considerable performance discipline within the team. This, combined with short daily meetings to agree on what the team is doing and the identification of any impediments, renders task-level tracking against a schedule redundant. Agile projects do make use of suitable development tools; however, tools are not seen as the primary means of achieving productivity. Team harmony, effective communications and collective ability to solve challenges are of greater importance.

NEW QUESTION: 246
As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?
A. The same value.
B. Greater value.
C. Lesser value.
D. Prior audit reports are not relevant.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Prior audit reports are considered of lesser value to an IS auditor attempting to gain an understanding of an organization's IT process than evidence directly collected.

NEW QUESTION: 247
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: (SHOW ANSWER)
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 (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 248
Which of the following should be the GREATEST concern to an IS auditor reviewing an organization's job scheduling practices?
A. Job dependencies are undefined.
B. Job processing procedures are missing.

C. Most jobs are run manually.
D. Jobs are executed during working hours.
Answer: (SHOW ANSWER)

NEW QUESTION: 249
When testing the accuracy of transaction data, which of the following situations BEST justifies the use of a smaller sample size?
A. The IS audit staff has a high level of experience.
B. It is expected that the population is error-free.
C. Proper segregation of duties is in place.
D. The data can be directly changed by users.
Answer: B (LEAVE A REPLY)
The best situation that justifies the use of a smaller sample size when testing the accuracy of transaction data is B: It is expected that the population is error-free. The sample size is the number of items selected from the population for testing. The sample size depends on various factors, such as the level of confidence, the tolerable error rate, the expected error rate, and the variability of the population. A smaller sample size means that fewer items are tested, which reduces the cost and time of testing, but also increases the sampling risk (the risk that the sample is not representative of the population).
One of the factors that affects the sample size is the expected error rate, which is the auditor's best estimate of the proportion of errors in the population before testing. A higher expected error rate means that more errors are likely to be found in the population, which requires a larger sample size to provide sufficient evidence for the auditor's conclusion. A lower expected error rate means that fewer errors are likely to be found in the population, which allows a smaller sample size to provide sufficient evidence for the auditor's conclusion.
Therefore, if it is expected that the population is error-free (i.e., the expected error rate is zero or very low), a smaller sample size can be justified.
The other situations do not justify the use of a smaller sample size when testing the accuracy of transaction data. A. The IS audit staff has a high level of experience. The IS audit staff's level of experience does not affect the sample size, but rather their ability to design and execute the sampling procedures and evaluate the results. The IS audit staff's level of experience may affect their judgment in selecting and applying sampling methods, but it does not change the statistical or mathematical principles that determine the sample size. B.
Proper segregation of duties is in place. Proper segregation of duties is an internal control that helps prevent or detect errors or fraud in transaction processing, but it does not affect the sample size. The sample size is based on the characteristics of the population and the objectives of testing, not on the controls in place. Proper segregation of duties may reduce the likelihood or impact of errors or fraud in transaction processing, but it does not eliminate them completely. Therefore, proper segregation of duties does not justify a smaller sample size when testing the accuracy of transaction data. C. The data can be directly changed by users. The data's ability to be directly changed by users does not justify a smaller sample size, but rather a larger one. The

data's ability to be directly changed by users increases the risk of errors or fraud in transaction processing, which requires a larger sample size to provide sufficient evidence for the auditor's conclusion. The data's ability to be directly changed by users also increases the variability of the population, which affects the sample size.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2
* Audit Sampling - AICPA3
* How to choose a sample size (for the statistically challenged)

NEW QUESTION: 250
A malicious code that changes itself with each file it infects is called a:
A. logic bomb.
B. stealth virus.
C. trojan horse.
D. polymorphic virus.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A polymorphic virus has the capability of changing its own code, enabling it to have many different variants. Since they have no consistent binary pattern, such viruses are hard to identify.

NEW QUESTION: 251
In a RACI modal, which of the following roles must be assigned to only one individual?
A. Responsible
B. Consuited
C. Accountable
D. Informed
Answer: C (LEAVE A REPLY)

NEW QUESTION: 252
Which of the following would be MOST useful when analyzing computer performance?
A. Tuning of system software to optimize resource usage
B. statiscal metrics measuring capacity utilization
C. Report of off-peal utilization and response time
D. Operations report of user dissatisfaction with response time
Answer: B (LEAVE A REPLY)

NEW QUESTION: 253
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: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation/Reference:
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 mix-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: 254
Doing which of the following during peak production hours could result in unexpected downtime?
A. Performing data migration or tape backup
B. Performing preventive maintenance on electrical systems
C. Promoting applications from development to the staging environment
D. Replacing a failed power supply in the core router of the data center
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Choices A and C are processing events which may impact performance, but would not cause downtime.
Enterprise-class routers have redundant hot-swappable power supplies, so replacing a failed power supply should not be an issue. Preventive maintenance activities should be scheduled for non-peak times of the day, and preferably during a maintenance window time period. A mishap or incident caused by a maintenance worker could result in unplanned downtime.

NEW QUESTION: 255
The FIRST step in auditing a data communication system is to determine:
A. traffic volumes and response-time criteria
B. physical security for network equipment
C. the level of redundancy in the various communication paths
D. business use and types of messages to be transmitted
Answer: D (LEAVE A REPLY)
The first step in auditing a data communication system is to determine the business use and types of messages to be transmitted. This is because the auditor needs to understand the purpose, scope, and objectives of the data communication system, as well as the nature, volume, and sensitivity of the data being transmitted. This will help the auditor to identify the risks, controls, and audit criteria for the data communication system.
Traffic volumes and response-time criteria, physical security for network equipment, and the level of redundancy in the various communication paths are important aspects of a data communication system, but they are not the first step in auditing it. They depend on the business use and types of messages to be transmitted, and they may vary according to different scenarios

and requirements. References: CISA Review Manual (Digital Version), [ISACA Auditing Standards]

NEW QUESTION: 256
In an online transaction processing system, data integrity is maintained by ensuring that a transaction is either completed in its entirety or not at all. This principle of data integrity is known as:
A. isolation.
B. consistency.
C. atomicity.
D. durability.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The principle of atomicity requires that a transaction be completed in its entirety or not at all. If an error or interruption occurs, all changes made up to that point are backed out. Consistency ensures that all integrity conditions in the database be maintained with each transaction. Isolation ensures that each transaction is isolated from other transactions; hence, each transaction only accesses data that are part of a consistent database state. Durability ensures that, when a transaction has been reported back to a user as complete, the resultant changes to the database will survive subsequent hardware or software failures.

NEW QUESTION: 257
During a follow-up audit, an IS auditor discovers that a recommendation has not been implemented.
However, the auditee has implemented a manual workaround that addresses the identified risk, through far
less efficiency than the recommended action would. Which of the following would be the auditor's BEST
course of action?
A. Notify management that the risk has been addressed and take no further action.
B. Escalate the remaining issue for further discussion and resolution.
C. Note that the risk has been addressed and notify management of the inefficiency.

D. Insist to management that the original recommendation be implemented.
Answer: D (LEAVE A REPLY)
Section: Protection of Information Assets

NEW QUESTION: 258
Which of the following is MOST helpful for understanding an organization's key driver to modernize application platforms?
A. Vendor software inventories
B. System-wide incident reports
C. Network architecture diagrams
D. Inventory of end-of-life software
Answer: (SHOW ANSWER)

NEW QUESTION: 259
Which is MOST important when contracting an external party to perform a penetration test?
A. Obtain approval from IT management.
B. Define the project scope.
C. Increase the frequency of log reviews.
D. Provide network documentation.
Answer: B (LEAVE A REPLY)
Section: Protection of Information Assets

NEW QUESTION: 260
Which of the following is the MOST important control for virtualized environments?
A. Regular updates of policies for the operation of the virtualized environment
B. Hardening for the hypervisor and guest machines
C. Redundancy of hardware resources and network components
D. Monitoring utilization of resources at the guest operating system level
Answer: B (LEAVE A REPLY)
Explanation
The most important control for virtualized environments is hardening for the hypervisor and guest machines.
Hardening is the process of applying security measures and configurations to reduce the vulnerabilities and risks of a system or device. Hardening for the hypervisor and guest machines is essential for protecting the virtualized environments from attacks, as they are exposed to various threats from both the physical and virtual layers. Hardening for the hypervisor and guest machines involves the following steps:
Applying the latest patches and updates for the hypervisor and guest operating systems, as well as the applications and drivers running on them.
Configuring the firewall and network settings for the hypervisor and guest machines, to restrict and monitor the network traffic and prevent unauthorized access or communication.

Disabling or removing any unnecessary or unused features, services, accounts, or ports on the hypervisor and guest machines, to minimize the attack surface and reduce the potential entry points for attackers.
Enforcing strong authentication and authorization policies for the hypervisor and guest machines, to ensure that only authorized users or administrators can access or manage them.
Encrypting the data and communication for the hypervisor and guest machines, to protect the confidentiality and integrity of the information stored or transmitted on them.
Implementing logging and auditing mechanisms for the hypervisor and guest machines, to record and track any activities or events that occur on them, and enable detection and investigation of any incidents or anomalies.
Hardening for the hypervisor and guest machines can help prevent or mitigate common attacks on virtualized environments, such as:
Hypervisor escape: An attack where a malicious guest machine breaks out of its isolated environment and gains access to the hypervisor or other guest machines.
Hypervisor compromise: An attack where an attacker exploits a vulnerability or misconfiguration in the hypervisor to gain control over it or its resources.
Guest compromise: An attack where an attacker exploits a vulnerability or misconfiguration in a guest machine to gain access to its data or applications.
Guest impersonation: An attack where an attacker creates a fake or cloned guest machine to trick other guests or users into interacting with it.
Guest denial-of-service: An attack where an attacker consumes or exhausts the resources of a guest machine to disrupt its availability or performance.
Therefore, hardening for the hypervisor and guest machines is the most important control for virtualized environments, as it can enhance their security, reliability, and performance. For more information about hardening for virtualized environments, you can refer to some of these web sources:
Hypervisor security on the Azure fleet
Chapter 2: Hardening the Hyper-V host
Plan for Hyper-V security in Windows Server

NEW QUESTION: 261
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.

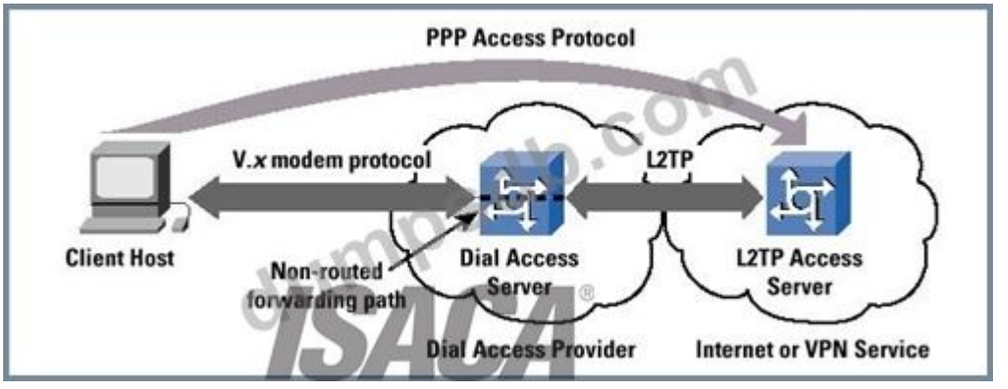
For your exam you should know below information about WAN Technologies:

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

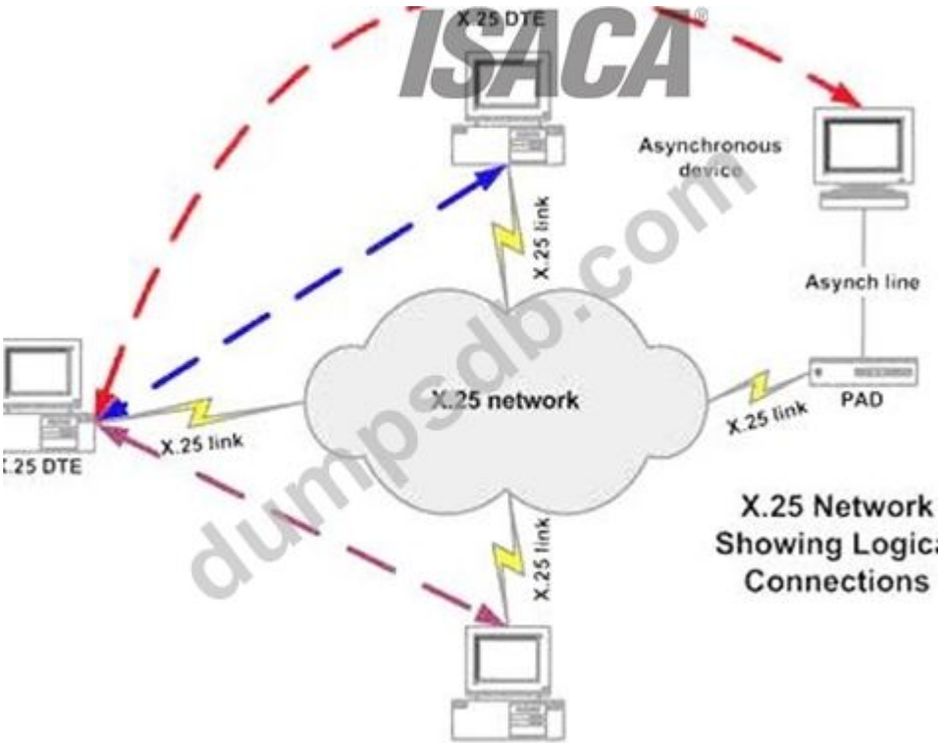
X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

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)

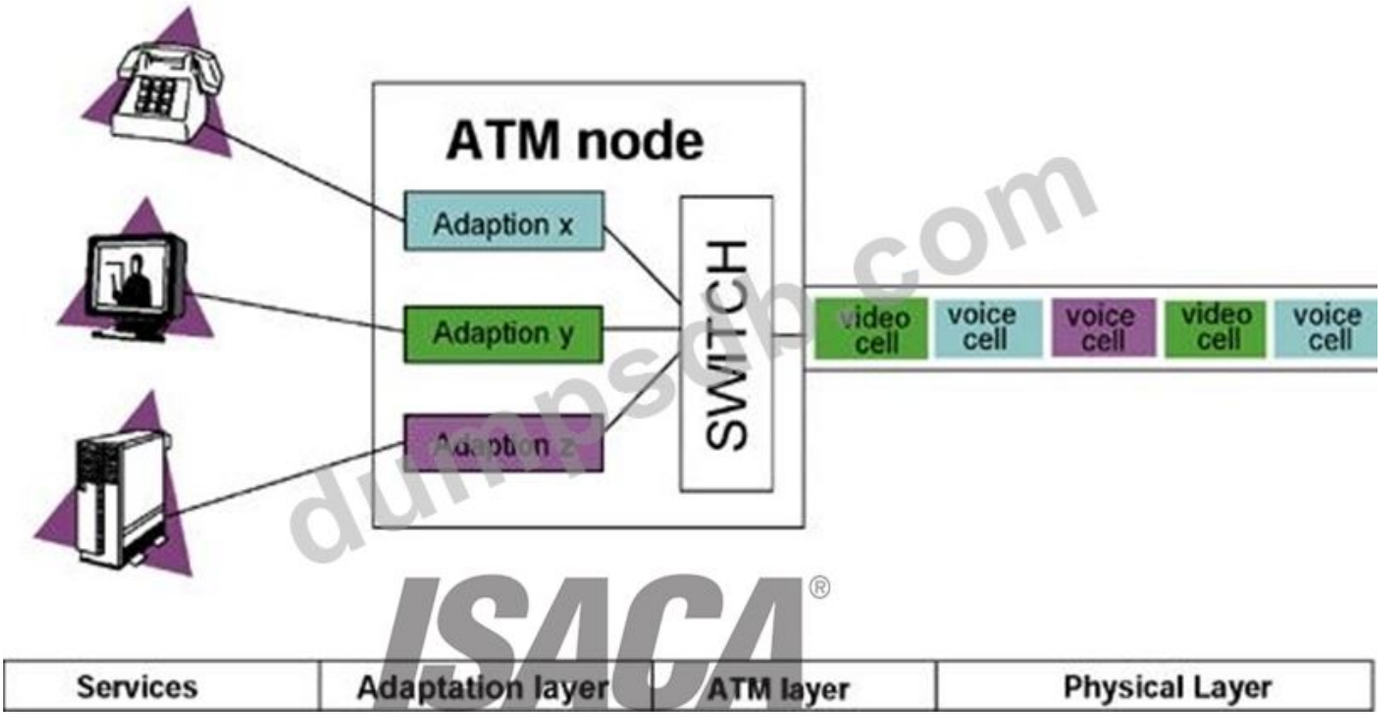
Uses Cell switching method

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

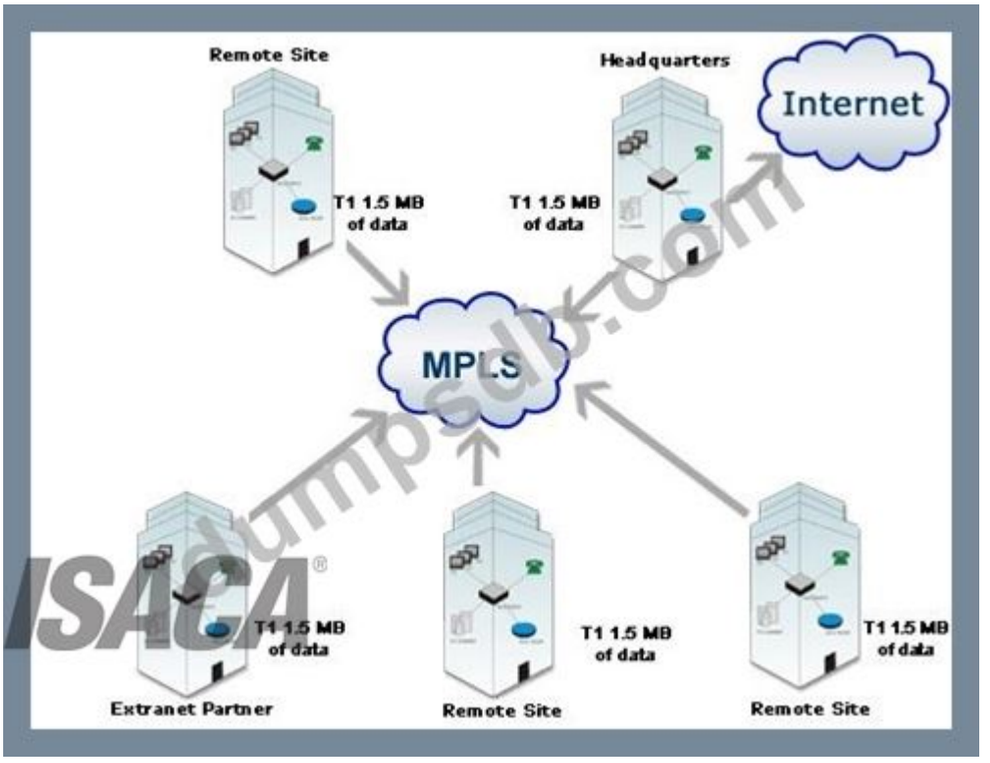


Multiprotocol Label Switching (MPLS)

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: 262

The PRIMARY purpose of a precedence diagramming method in managing IT projects is to:

A. monitor project scope creep.

B. identify the critical path.

C. identify key milestones.

D. minimize delays and overruns.

Answer: (SHOW ANSWER)

Section: Governance and Management of IT

NEW QUESTION: 263

Which of the following layer of an enterprise data flow architecture is responsible for data copying, transformation in Data Warehouse (DW) format and quality control?

A. Data Staging and quality layer

B. Desktop Access Layer

C. Data Mart layer

D. Data access layer

Answer: (SHOW ANSWER)

Explanation/Reference:

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.

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 per-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 are 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 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 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: 264
A national bank recently migrated a large number of business-critical applications to the cloud. Which of the following is MOST important to ensuring the resiliency of the applications?
A. Conducting periodic system stress testing
B. Creating restore points for critical applications
C. Negotiating a nondisclosure agreement (NDA) with the provider
D. Using a monitoring tool to assess uptime
Answer: (SHOW ANSWER)

NEW QUESTION: 265
Which of the following is the MOST important consideration for an organization when strategizing to comply
with privacy regulations?
A. Ensuring there are staff members with in-depth knowledge of the privacy regulations
B. Ensuring up-to-date knowledge of where customer data is saved
C. Ensuring regularly updated contracts with third parties that process customer data
D. Ensuring appropriate access to information systems containing privacy information.
Answer: (SHOW ANSWER)
Section: Governance and Management of IT

NEW QUESTION: 266
The drives of a tile 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. Replicate the server's volatile data to another drive.
D18912E1457D5D1DDCBD40AB3BF70D5D
B. Run forensic analysis software on the backup drive.
C. Create a logical copy of the file server's drives.
D. Capture a bit-by-bit image of the file server's drives.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 267
A company has implemented a new client-server enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following would BEST ensure that the orders are entered accurately and the corresponding products are produced?
A. Verifying production to customer orders
B. Logging all customer orders in the ERP system
C. Using hash totals in the order transmitting process
D. Approving (production supervisor) orders prior to production
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Verification will ensure that production orders match customer orders. Logging can be used to detect inaccuracies, but does not in itself guarantee accurate processing. Hash totals will ensure accurate order transmission, but not accurate processing centrally. Production supervisory approval is a time consuming, manual process that does not guarantee proper control.

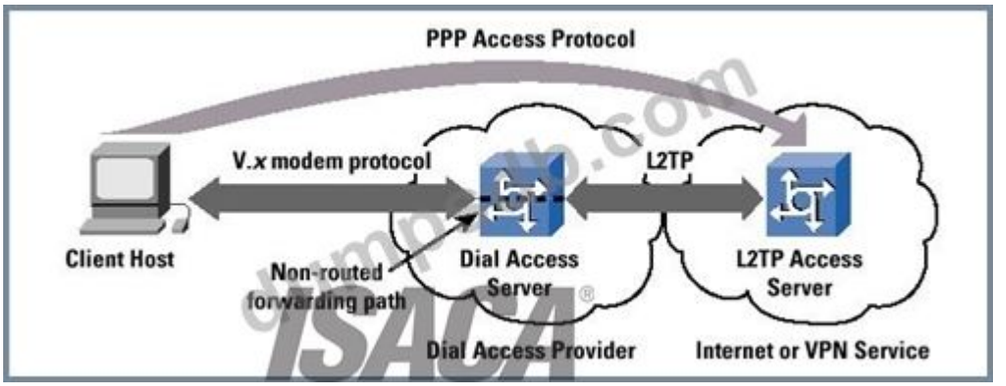
NEW QUESTION: 268
What should be an IS auditor s NEXT course of action when a review of an IT organizational structure reveals IT staff members have duties in other departments?
A. Immediately report a potential finding to the audit committee.
B. Report the issue to human resources (HR) management
C. Recommend that segregation of duties controls be implemented.
D. Determine whether any segregation of duties conflicts exist.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 269
Which of the following is the GREATEST risk of cloud computing?
A. Lack of scalability
B. Disclosure of data
C. Inflexibility
D. Reduced performance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 270
The PRIMARY benefit of automating application testing is to:
A. provide more flexibility.
B. replace all manual test processes.
C. provide test consistency.
D. reduce the time to review code.

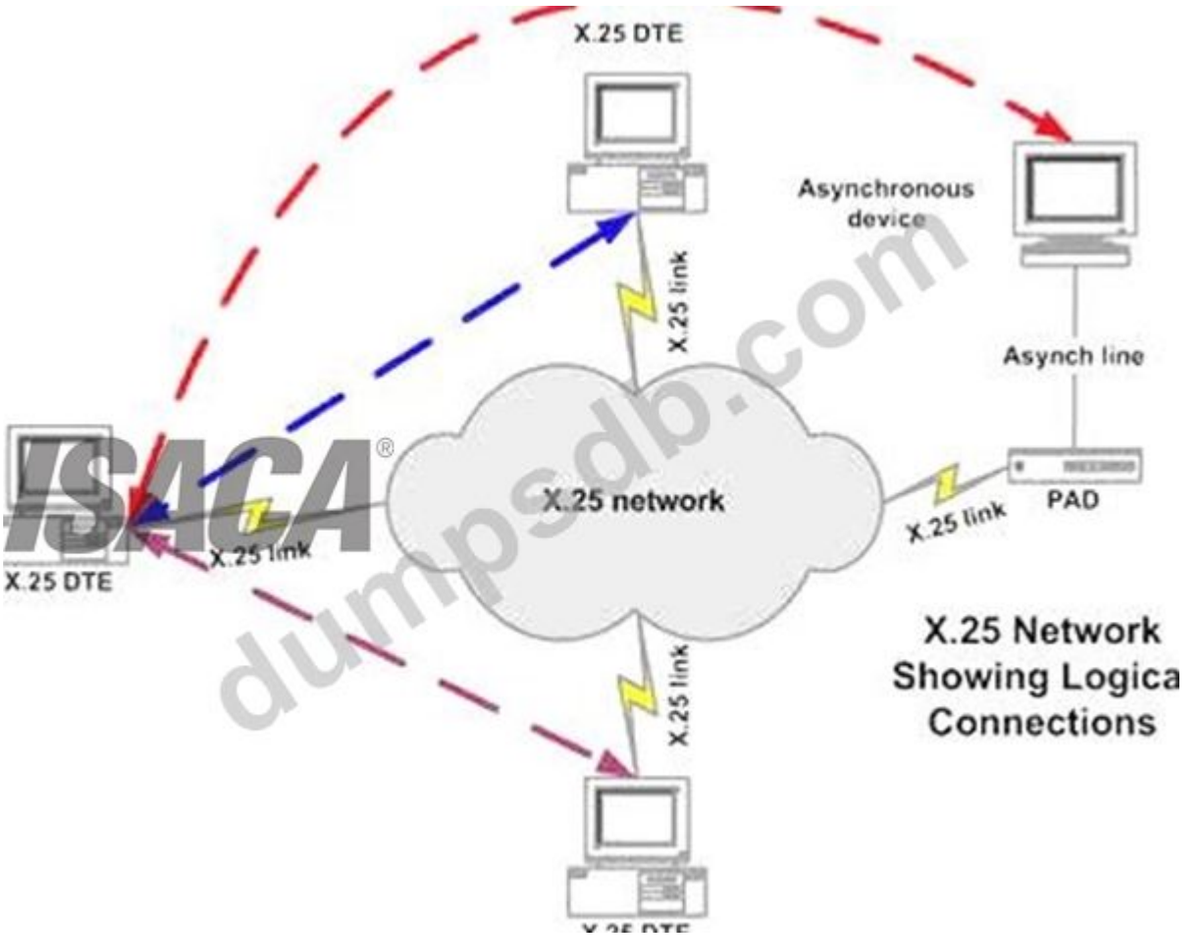
Answer: D (LEAVE A REPLY)

NEW QUESTION: 271
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

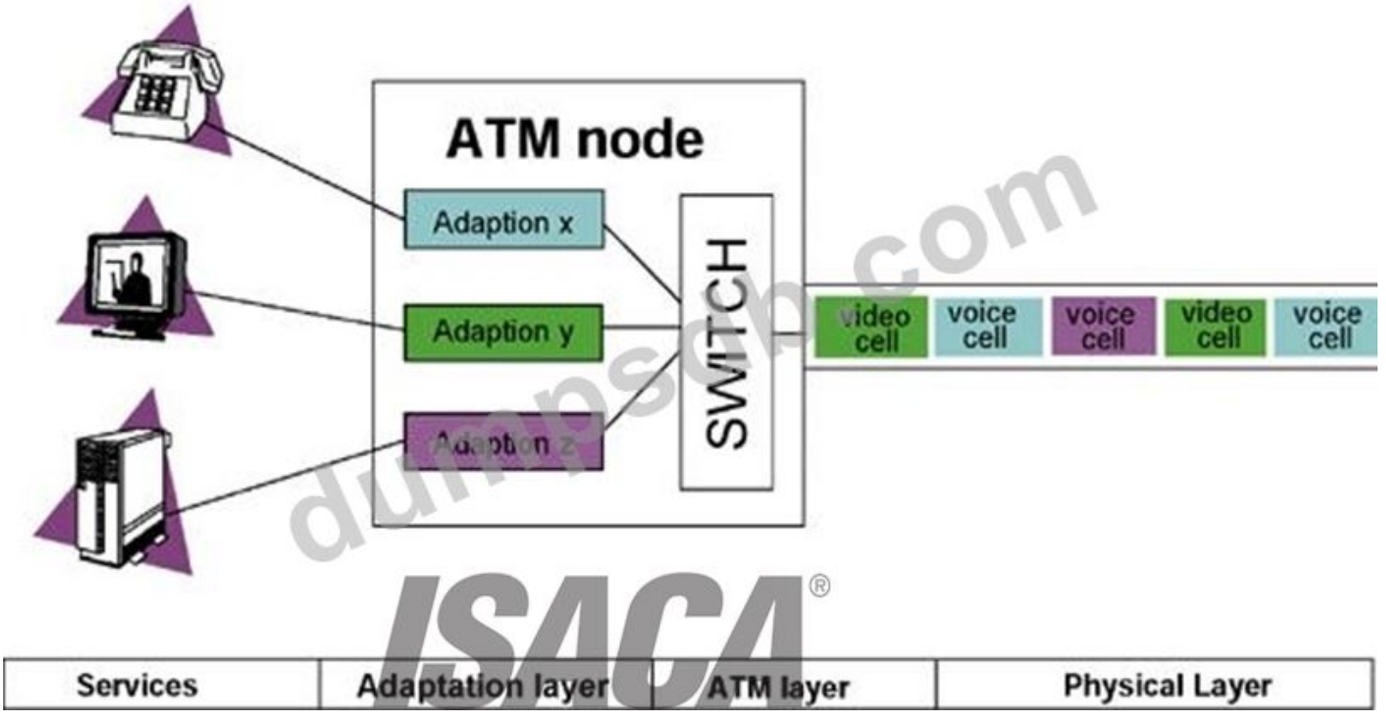
X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.
X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.
Subscribers are charged based on amount of bandwidth they use. Data are divided into 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

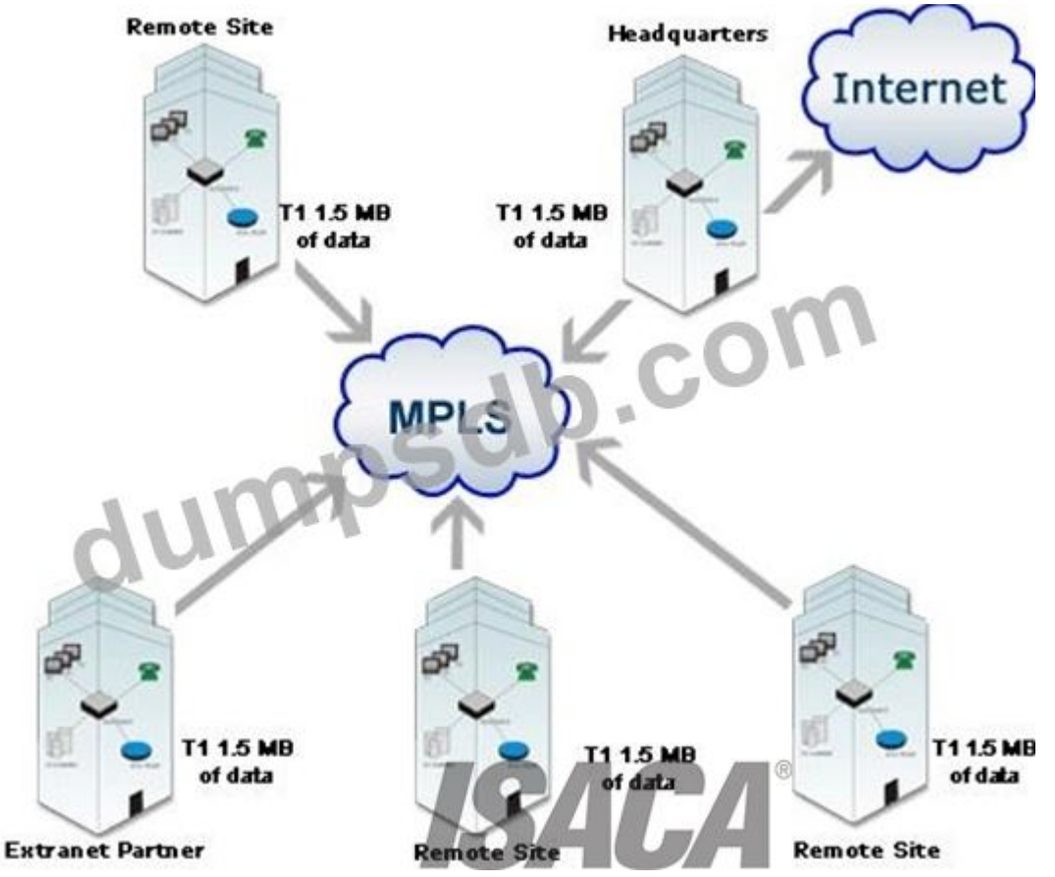
Asynchronous Transfer Mode (ATM)
Uses Cell switching method
High speed network technology used for LAN, MAN and WAN
Like a frame relay it is connection oriented technology which creates and uses fixed channel Data are segmented into fixed size cell of 53 bytes Some companies have replaces FDDI back-end with ATM Asynchronous Transfer Mode



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: 272
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: 273
A review of IT interface controls finds an organization does not have a process to identify and correct records that do not get transferred to the receiving system Which of the following is the IS auditors BEST recommendation?
A. Enable automatic encryption decryption and electronic signing of data files
B. implement software to perform automatic reconciliations of data between systems
C. Have coders perform manual reconciliation of data between systems
D. Automate the transfer of data between systems as much as feasible
Answer: (SHOW ANSWER)
Explanation
The best recommendation for an organization that does not have a process to identify and correct records that do not get transferred to the receiving system is to implement software to perform automatic reconciliations of data between systems. This will ensure that the data integrity and completeness are maintained and that any errors or discrepancies are detected and resolved in a timely manner. Enabling encryption, decryption, and electronic signing of data files may enhance the data security and authenticity, but not the data accuracy or consistency. Having coders perform manual reconciliation of data between systems may be prone to human errors and inefficiencies. Automating the transfer of data between systems as much as feasible may reduce

the chances of data loss or corruption, but not eliminate them completely. References: IS Audit and Assurance Standards, section "Standard 1202: Risk Assessment in Planning"

NEW QUESTION: 274
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)
Section: Protection of Information Assets
Explanation:
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: 275
An employee loses a mobile device resulting in loss of sensitive corporate data. Which of the following would have BEST prevented data leakage?
A. Awareness training for mobile device users
B. Data encryption on the mobile device
C. The triggering of remote data wipe capabilities
D. Complex password policy for mobile devices
Answer: C (LEAVE A REPLY)
Section: Protection of Information Assets

NEW QUESTION: 276
Which of the following would BEST detect that a distributed denial of service (DDoS) attack is occurring?
A. Customer service complaints
B. Server crashes
C. Automated monitoring of logs
D. Penetration testing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 277

Which of the following is a general operating system access control function?
A. Creating database profiles
B. Verifying user authorization at a field level
C. Creating individual accountability
D. Logging database access activities for monitoring access violation
Answer: C (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Creating individual accountability is the function of the general operating system. Creating database
profiles, verifying user authorization at a field level and logging database access activities for monitoring
access violations are all database-level access control functions.

NEW QUESTION: 278
When should reviewing an audit client's business plan be performed relative to reviewing an organization's
IT strategic plan?
A. Reviewing an audit client's business plan should be performed before reviewing an organization's IT
strategic plan.
B. Reviewing an audit client's business plan should be performed after reviewing an organization's IT
strategic plan.
C. Reviewing an audit client's business plan should be performed during the review of an organization's IT
strategic plan.
D. Reviewing an audit client's business plan should be performed without regard to an organization's IT
strategic plan.
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation:
Reviewing an audit client's business plan should be performed before reviewing an organization's IT
strategic plan.

NEW QUESTION: 279
An IS auditor is analyzing a sample of accounts payable transactions for a specific vendor and identifies one transaction with a value five times as high as the average transaction. Which of the following should the auditor do NEXT?

A. Report the variance immediately to the audit committee
B. Request an explanation of the variance from the auditee
C. Increase the sample size to 100% of the population
D. Exclude the transaction from the sample population
Answer: (SHOW ANSWER)
An IS auditor is analyzing a sample of accounts payable transactions for a specific vendor and identifies one transaction with a value five times as high as the average transaction. The next step that the auditor should do is to request an explanation of the variance from the auditee. This is because the variance may indicate an error, fraud, or an unusual but legitimate transaction that requires further investigation. The auditor should not report the variance immediately to the audit committee without verifying its cause and significance. The auditor should not increase the sample size to 100% of the population without considering the cost-benefit analysis and the sampling methodology. The auditor should not exclude the transaction from the sample population without justification, as itmay affect the validity and reliability of the audit results.
References: CISA Review Manual (Digital Version), [ISACA Auditing Standards]

NEW QUESTION: 280
When planning an audit to assess application controls of a cloud-based system, it is MOST important for the IS auditor to understand the:
A. policies and procedures of the business area being audited.
B. architecture and cloud environment of the system.
C. availability reports associated with the cloud-based system.
D. business process supported by the system.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 281
A purpose of project closure is to determine the:
A. potential risks affecting the quality of deliverables.
B. lessons learned for use in future projects.
C. project feasibility requirements
D. professional expertise of the project manager.
Answer: B (LEAVE A REPLY)
Section: Protection of Information Assets

NEW QUESTION: 282
An organization has purchased a replacement mainframe computer to cope with the demands of increased business. Which of the following should be the PRIMARY concern of an IS auditor?
A. Appropriate tender evaluation processes have been followed.
B. Application access controls are adequate.
C. The disaster recovery plan has been reviewed and updated.
D. The procurement is within the planned budget for the year.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 283
Which of the following is the PRIMARY advantage of using visualization technology for corporate applications?
A. Improved disaster recovery
B. Better utilization of resources
C. Stronger data security
D. Increased application performance
Answer: B (LEAVE A REPLY)
Visualization technology is the use of software and hardware to create graphical representations of data, such as charts, graphs, maps, images, etc. Visualization technology can help users to understand, analyze, and communicate complex and large amounts of data in an intuitive and engaging way1.
One of the primary advantages of using visualization technology for corporate applications is that it can improve the utilization of resources, such as time, money, human capital, and physical assets. Some of the ways that visualization technology can achieve this are:
* Visualization technology can help users to quickly and easily explore, filter, and interact with data, reducing the need for manual data processing and analysis1. This can save time and effort for both data producers and consumers, and allow them to focus on more value-added tasks.
* Visualization technology can help users to discover patterns, trends, outliers, correlations, and causations in data that may otherwise be hidden or overlooked in traditional reports or tables1. This can enable users to make better and faster decisions based on data-driven insights, and optimize their strategies and actions accordingly.
* Visualization technology can help users to communicate and share data more effectively and persuasively with different audiences, such as customers, partners, investors, regulators, etc1. This can enhance the reputation and credibility of the organization, and foster collaboration and innovation among stakeholders.
* Visualization technology can help users to monitor and measure the performance and impact of their activities, products, services, or processes1. This can help users to identify problems or opportunities for improvement, and adjust their plans or actions accordingly.
* Visualization technology can help users to create engaging and interactive experiences for their customers or end-users1. This can increase customer satisfaction and loyalty, and generate more revenue or value for the organization.
Therefore, using visualization technology for corporate applications can help organizations to better utilize their resources and achieve their goals.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
* TechRadar Blog, Best data visualization tools of 20232
* IBM Blog, What is Data Visualization?3

* TDWI Blog, Data Visualization Technology4
* Tableau Blog, What are the advantages and disadvantages of data visualization?

NEW QUESTION: 284
An organization's IT security policy states that user ID's must uniquely identify individual's and that user should not disclose their passwords. An IS auditor discovers that several generic user ID's are being used.
Which of the following is the MOST appropriate course of action for the auditor?
A. Recommend a change in security policy.
B. Investigate the noncompliance.
C. Recommend disciplinary action.
D. Include the finding in the final audit report.
Answer: (SHOW ANSWER)

NEW QUESTION: 285
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: 286
An IS auditor reviewing a proposed application software acquisition should ensure that the:
A. operating system (OS) being used is compatible with the existing hardware platform.
B. planned OS updates have been scheduled to minimize negative impacts on company needs.
C. OS has the latest versions and updates.

D. products are compatible with the current or planned OS.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Choices A, B and C are incorrect because none of them are related to the area being audited. In reviewing the proposed application the auditor should ensure that the products to be purchased are compatible with the current or planned OS. Regarding choice A, if the OS is currently being used, it is compatible with the existing hardware platform, because if it is not it would not operate properly. In choice B, the planned OS updates should be scheduled to minimize negative impacts on the organization. For choice C, the installed OS should be equipped with the most recent versions and updates (with sufficient history and stability).

NEW QUESTION: 287
Which of the following will provide the GREATEST assurance to IT management that a quality management system (QMS) is effective?
A. A high percentage of stakeholders satisfied with the quality of IT
B. A high percentage of IT employees attending quality training
C. A high percentage of IT processes reviewed by quality assurance (QA)
D. A high percentage of incidents being quickly resolved
Answer: A (LEAVE A REPLY)

NEW QUESTION: 288
During an audit, an IS auditor notes that an organization's business continuity plan (BCP) does not
adequately address information confidentiality during a recovery process. The IS auditor should recommend that the plan be modified to include:
A. the level of information security required when business recovery procedures are invoked.
B. information security roles and responsibilities in the crisis management structure.
C. information security resource requirements.
D. change management procedures for information security that could affect business continuity arrangements.
Answer: (SHOW ANSWER)
Section: Protection of Information Assets

Explanation:
Business should consider whether information security levels required during recovery should be the same,
lower or higher than when business is operating normally. In particular, any special rules for access to
confidential data during a crisis need to be identified. The other choices do not directly address the
information confidentiality issue.

NEW QUESTION: 289
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: B (LEAVE A REPLY)
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: 290
In which phase of the audit life cycle process are audit observations initially discussed with the client?
A. Reporting phase
B. Planning phase
C. Follow-up phase
D. Execution phase
Answer: (SHOW ANSWER)

NEW QUESTION: 291
When developing a risk-based audit strategy, an IS auditor should conduct a risk assessment to ensure that:

A. controls needed to mitigate risks are in place.
B. vulnerabilities and threats are identified.
C. audit risks are considered.
D. a gap analysis is appropriate.
Answer: B (LEAVE A REPLY)
In developing a risk-based audit strategy, it is critical that the risks and vulnerabilities be understood. This will determine the areas to be audited and the extent of coverage. Understanding whether appropriate controls required to mitigate risksare in place is a resultant effect of an audit. Audit risks are inherent aspects of auditing, are directly related to the audit process and are not relevant to the risk analysis of the environment to be audited. A gap analysis would normally be doneto compare the actual state to an expected or desirable state.

NEW QUESTION: 292
Management has agreed to perform multiple remediation actions in response to an audit issue, including the implementation of a new control. Which of the following is the BEST time for an IS auditor to perform an audit follow-up of this issue?
A. After the new control has been in place for one year
B. When management resources are available
C. When audit resources are available
D. After management has completed the required actions
Answer: D (LEAVE A REPLY)

NEW QUESTION: 293
Which of the following would be the PRIMARY benefit of replacing physical keys with an electronic badge system for access to a data center?
A. Increasing accountability
B. Maintaining compliance
C. Tracking employee work hours
D. Increasing reliability
Answer: (SHOW ANSWER)
Section: Information System Operations, Maintenance and Support

NEW QUESTION: 294
Which of the following is the GREATEST risk associated with lack of IT involvement in the organization's strategic planning initiatives?
A. Business strategies may not align with IT capabilities.
B. Business strategies may not consider emerging technologies.
C. IT strategies may not align with business strategies.
D. IT strategic goals may not be considered by the business.
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:

IfIT is not involvedinstrategic planning,IT strategy may diverge from business needs, leading to misalignment and inefficiencies.
* Option A (Incorrect):Business strategy alignmentis important, but the greater risk is thatIT investments do not support business goals.
* Option B (Incorrect):Lack of emerging technology awareness is a risk, butIT-business misalignment has broader consequences.
* Option C (Correct):Thegreatest riskis when IT strategyfails to align with business objectives, leading towasted investments, inefficiencies, and competitive disadvantages.
* Option D (Incorrect):IT goals being overlooked is a concern, butmisalignment of IT and business strategies is a more critical risk.
Reference:ISACA CISA Review Manual -Domain 2: Governance and Management of IT- Covers strategic IT alignment and governance best practices.

NEW QUESTION: 295
A company has implemented an IT segregation of duties policy. In a role-based environment, which of the
following roles may be assigned to an approach developer?
A. IT operator
B. Database administration
C. System administration
D. Emergency support
Answer: (SHOW ANSWER)
Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 296
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)
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:
1.

ISACA. "Technical Guide on IT Migration Audit."
1(http://kb.icai.org/pdfs/PDFFile5b278a12a66758.
27269499.pdf)
2. Zapier. "IT audit: The ultimate guide [with checklist]." 2(https://zapier.com/blog/it-audit/)
3. ISACA. "CISA Certification | Certified Information Systems Auditor." 3(https://www.isaca.org
/credentialing/cisa)

NEW QUESTION: 297
When developing a risk management program, what is the FIRST activity to be performed?
A. Threat assessment
B. Classification of data
C. Inventory of assets
D. Criticality analysis
Answer: C (LEAVE A REPLY)
Identification of the assets to be protected is the first step in the development of a risk management program. A listing of the threats that can affect the performance of these assets and criticality analysis are later steps in the process. Data classification is required for defining access controls and in criticality analysis.

NEW QUESTION: 298
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: (SHOW ANSWER)
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.

NEW QUESTION: 299
The information security function in a large organization is MOST effective when:

A. partnered with the IS development team to determine access rights
B. decentralized as close to the user as possible
C. established at a corporate-wide level.
D. the function reports directly to the IS operations manager.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 300
While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern shouldbe that the:
A. requirement for protecting confidentiality of information could be compromised.
B. contract may be terminated because prior permission from the outsourcer was not obtained.
C. other service provider to whom work has been outsourced is not subject to audit.
D. outsourcer will approach the other service provider directly for further work.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Many countries have enacted regulations to protect the confidentiality of information maintained in their countries and/or exchanged with other countries. Where a service provider outsources part of its services to another service provider, there is a potential risk that the confidentiality of the information will be compromised. Choices B and C could be concerns but are not related to ensuring the confidentiality of information. There is no reason why an IS auditor should be concerned with choice D.

NEW QUESTION: 301
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)
Section: Protection of Information Assets
Explanation:
The project sponsor is ultimately responsible for providing requirement specifications to the software- development team.

NEW QUESTION: 302
The waterfall life cycle model of software development is BEST suited for which of the following situations?
A. The protect requirements are wall understood.
B. The project is subject to time pressures.
C. The project intends to apply an object-oriented design approach.
D. The project will involve the use of new technology.
Answer: A (LEAVE A REPLY)
Explanation
The waterfall life cycle model of software development is best suited for situations where the project requirements are well understood. The waterfall life cycle model is a sequential and linear approach to software development that consists of several phases, such as planning, analysis, design, implementation, testing, and maintenance. Each phase depends on the completion and approval of the previous phase before proceeding to the next phase. The waterfall life cycle model is best suited for situations where the project requirements are well understood, as it assumes that the requirements are clear, stable, and fixed at the beginning of the project, and do not change significantly throughout the project. The project is subject to time pressures is not a situation where the waterfall life cycle model of software development is best suited, as it may not be flexible or agile enough to accommodate changes or adjustments in the project schedule or timeline. The waterfall life cycle model may involve long delays or dependencies between phases, and may not allow for early feedback or delivery of software products. The project intends to apply an object-oriented design approach is not a situation where the waterfall life cycle model of software development is best suited, as it may not be compatible or effective with the object-oriented design approach. The object-oriented design approach is a technique that models software as a collection of interacting objects that have attributes and behaviors. The object-oriented design approach may require iterative and incremental development methods that allow for dynamic and adaptive changes in software design and functionality. The project will involve the use of new technology is not a situation where the waterfall life cycle model of software development is best suited, as it may not be able to cope with the uncertainty or complexity of new technology. The waterfall life cycle model may not allow for sufficient exploration or experimentation with new technology, and may not be able to handle changes or issues that arise from new technology.

NEW QUESTION: 303
Which of the following is the BEST reason for an organization to develop a business continuity plan?
A. To avoid the costs resulting from the failure of key systems and processes

B. To identify the users of information systems and processes
C. To establish business un prioritization of systems projects, and strategies
D. To develop a detailed desertion of information systems and processes
Answer: C (LEAVE A REPLY)

NEW QUESTION: 304
Which of the following BEST protects evidence in a forensic investigation?
A. imaging the affected system
B. Powering down the affected system
C. Protecting the hardware of the affected system
D. Rebooting the affected system
Answer: A (LEAVE A REPLY)
Imaging the affected system is the best way to protect evidence in a forensic investigation, because it creates a bit-by-bit copy of the original data that can be analyzed without altering or compromising the original source. Imaging preserves the integrity and authenticity of the evidence and allows for verification and validation of the results34. Powering down or rebooting the affected system can cause data loss or corruption, while protecting the hardware does not prevent unauthorized access or tampering with the software or data. References: 3: CISA Review Manual (Digital Version), Chapter 6, Section 6.4.1 4: CISA Online Review Course, Module 6, Lesson 4

NEW QUESTION: 305
Which of the following is MOST helpful when establishing the authenticity of digital evidence collected from a hard disk?
A. Mash of the files on the hard disk
B. Confirmation by witnesses
C. Bit-by-bit image of the hard disk
D. Chain of custody documentation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 306
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. Deviation detection
B. Cluster sampling
C. Random sampling
D. Classification
Answer: D (LEAVE A REPLY)
The most useful analytical method when trying to identify groups with similar behavior or characteristics in a large population is classification. Classification is a technique that assigns data points to predefined categories or classes based on their features or attributes. Classification

can help to discover patterns, trends, and relationships among the data and reveal the similarities or differences among the groups. Classification can also help to support decision making, prediction, or recommendation based on the data analysis. References:
* CISA Review Manual (Digital Version), Chapter 3, Section 3.4.21
* CISA Online Review Course, Domain 2, Module 3, Lesson 12

NEW QUESTION: 307
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: (SHOW ANSWER)
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: 308
Which of the following is the GREATEST benefit related to disaster recovery for an organization that has converted its infrastructure to a virtualized environment?
A. Virtual servers can be recreated on similar hardware faster than restoring from backups.
B. Virtual servers decrease the recovery time objective (RTO).
C. Virtual servers reduce the time and complexity associated with backup procedures.
D. Virtual servers eliminate the need to verify backups.
Answer: (SHOW ANSWER)

NEW QUESTION: 309
Which of the following is the GREATEST concern when consolidating several applications from two outdated servers onto one new server?
A. System maintenance may require more coordination.
B. Power usage will increase.
C. Network traffic may increase.

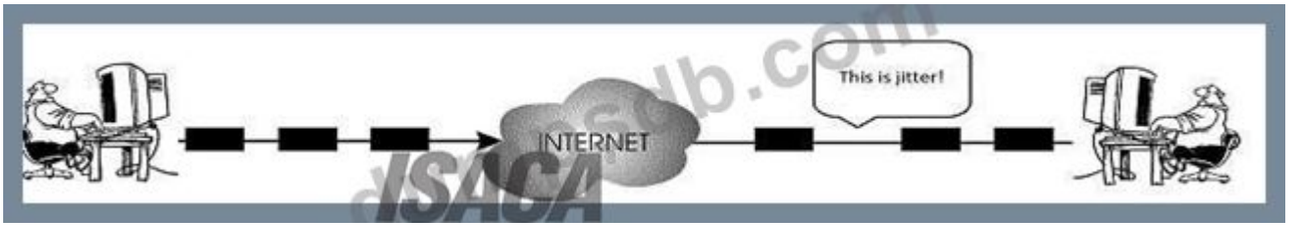
D. The new server will not be fully utilized after migration.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 310
An IS auditor reviews an organizational chart PRIMARILY for:
A. an understanding of workflows.
B. investigating various communication channels.
C. understanding the responsibilities and authority of individuals.
D. investigating the network connected to different employees.
Answer: C (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation: An organizational chart provides information about the responsibilities and authority of
individuals in the organization. This helps an IS auditor to know if there is a proper segregation of functions.
A workflow chart would provide information about the roles of different employees. A network diagram will
provide information about the usage of various communication channels and will indicate the connection of
users to the network.

NEW QUESTION: 311
When performing an audit of a third-party provider, it is MOST important to ensure:
A. a vendor relationship manager is assigned.
B. items identified in the risk assessment have been addressed.
C. a vendor monitoring process has been implemented.
D. the service level agreement (SLA) is monitored.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 312
IT disaster recovery time objectives (RTOs) should be based on the:
A. maximum tolerable loss of data.
B. nature of the outage
C. maximum tolerable downtime (MTD).
D. business-defined criticality of the systems.
Answer: D (LEAVE A REPLY)
IT disaster recovery time objectives (RTOs) are the maximum acceptable time that an IT system can be unavailable after a disaster before it causes unacceptable consequences for the business. IT RTOs should be based on the business-defined criticality of the systems, which reflects how important they are for supporting the business processes and functions. The maximum tolerable

loss of data, the nature of the outage, and the maximum tolerable downtime (MTD) are also factors that affect the IT RTOs, but they are not the primary basis for determining them.

NEW QUESTION: 313
Which of the following term related to network performance refers to the variation in the time of arrival of packets on the receiver of the information?
A. Bandwidth
B. Throughput
C. Latency
D. Jitter
Answer: (SHOW ANSWER)
Section: Information System Operations, Maintenance and Support
Explanation:
Simply said, the time difference in packet inter-arrival time to their destination can be called jitter. Jitter is specific issue that normally exists in packet switched networks and this phenomenon is usually not causing any communication problems. TCP/IP is responsible for dealing with the jitter impact on communication.
On the other hand, in VoIP network environment, or better say in any bigger environment today where we use IP phones on our network this can be a bigger problem. When someone is sending VoIP communication at a normal interval (let's say one frame every 10 ms) those packets can stuck somewhere in between inside the packet network and not arrive at expected regular peace to the destined station.
That's the whole jitter phenomenon all about so we can say that the anomaly in tempo with which packet is expected and when it is in reality received is jitter.
jitter


In this image above, you can notice that the time it takes for packets to be send is not the same as the period in which the will arrive on the receiver side. One of the packets encounters some delay on his way and it is received little later than it was asumed. Here are the jitter buffers entering the story. They will mitigate packet delay if required. VoIP packets in networks have very changeable packet inter-arrival intervals because they are usually smaller than normal data packets and are therefore more numerous with bigger chance to get some delay along the way.
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 sen 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 Reference:
CISA review manual 2014 page number 275
and
http://howdoesinternetwork.com/2013/jitter

NEW QUESTION: 314
Which of the following comparisons are used for identification and authentication in a biometric system?
A. One-to-many for identification and authentication
B. One-to-one for identification and authentication
C. One-to-many for identification and one-to-one for authentication
D. One-to-one for identification and one-to-many for authentication
Answer: C (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
In identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in

identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person
"where the system establishes whether the person is who she (implicitly or explicitly) denies to be" In verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.
Management of Biometrics
Management of biometrics should address effective security for the collection, distribution and processing of biometrics data encompassing:
Data integrity, authenticity and non-repudiation
Management of biometric data across its life cycle - compromised of the enrollment, transmission and storage, verification, identification, and termination process Usage of biometric technology, including one-to-one and one-to-many matching, for identification and authentication Application of biometric technology for internal and external, as well as logical and physical access control Encapsulation of biometric data Security of the physical hardware used throughout the biometric data life cycle Techniques for integrity and privacy protection of biometric data.
The following were incorrect answers:
All other choices presented were incorrectly describing identification and authentication mapping.
Reference:
CISA review manual 2014 Page number 331
http://en.wikipedia.org/wiki/Biometrics

NEW QUESTION: 315
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)
Explanation
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: 316
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: 317
Which of the following controls is MOST important for ensuring the integrity of system interfaces?
A. Periodic audits
B. File counts

C. File checksums
D. IT operator monitoring
Answer: C (LEAVE A REPLY)
Explanation
File checksums are values that are calculated from the contents of a file and can detect any changes or corruption in the file. They are used to verify that the files that are transferred or processed through system interfaces are not altered in any way. File checksums are more effective than periodic audits, file counts, or IT operator monitoring, which are other types of controls that can help ensure the integrity of system interfaces, but they are not as reliable or timely as file checksums.

NEW QUESTION: 318
What should be the PRIMARY objective of performing a risk assessment when planning for an IS audit engagement?
A. To minimize the number of resources allocated to the engagement
B. To identify high-risk business processes
C. To reduce risk to an acceptable level
D. To minimize the level of substantive testing required
Answer: B (LEAVE A REPLY)

NEW QUESTION: 319
As part of a mergers and acquisitions activity, an acquiring organization wants to consolidate data and systems from the organization being acquired into existing systems. To ensure the data is relevant the acquiring organization should:
A. automate the process of data collection and cleaning.
B. obtain data quality software.
C. define data quality requirements based on business needs.
D. implement a data warehouse solution.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 320
Which of the following E-commerce model covers all the transactions between companies and government
organization?
A. B-to-C relationships
B. B-to-B relationships
C. B-to-E relationships
D. B-to-G relationships
Answer: (SHOW ANSWER)
Section: Information System Acquisition, Development and Implementation
Explanation/Reference:

Business-to-Government(B-to-G) relationships covers all the transactions between companies and
government organizations. Currently this category is infancy, but it could expand quit rapidly as government
use their own operations to promote awareness and growth of e-commerce. In addition to public procurement, administrations may also offer the option of electronic interchange for such transactions as
VAT returns and the payment of corporate taxes.
For CISA exam you should know below E-commerce models:
Business-to-Consumer (B-to-C) relationships - The greatest potential power of E-commerce comes from
its ability to redefine relationship with customers in creating a new convenient, low-cost channel to transact
business. Companies can tailor their marketing strategies to an individual customer's needs and wants. As
more of its business shifts on-line, a company will have an enhanced ability to track how its customer
interact with it.
Business-to-Business (B-to-B) relationships -The relationship among the selling services of two or more
business opens up the possibility of re-engineering business process across the boundaries that have
traditionally separated external entities from each other. Because of the ease of access and the ubiquity of
the Internet, for example companies can build business process that combine previously separated
activities. The result is faster, higher quality and lower-cost set of transactions. The market has ever
created to subdivision of B-to-B called business-to-small business(B-to-SB) relationships
Business-to-employee(B-to-E) relationships -Web technologies also assist in the dissemination of information to and among an organization employees.
Business-to-Government(B-to-G) relationships - covers all the transactions between companies and
government organizations. Currently this category is infancy, but it could expand quit rapidly as government
use their own operations to promote awareness and growth of e-commerce. In addition to public procurement, administrations may also offer the option of electronic interchange for such transactions as
VAT returns and the payment of corporate taxes.
The following were incorrect answers:

The other options presented does not covers all transactions between companies and government
organizations.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 175

NEW QUESTION: 321
An IS auditor is reviewing the installation of a new server. The IS auditor's PRIMARY objective is to ensure that
A. the procurement project invited lenders from at least three different suppliers.
B. security parameters are set in accordance with the organization's policies.
C. security parameters are set in accordance with the manufacturer s standards.
D. a detailed business case was formally approved prior to the purchase.
Answer: (SHOW ANSWER)

NEW QUESTION: 322
.What is a primary high-level goal for an auditor who is reviewing a system development project?
A. To ensure that programming and processing environments are segregated
B. To ensure that proper approval for the project has been obtained
C. To ensure that business objectives are achieved
D. To ensure that projects are monitored and administrated effectively
Answer: (SHOW ANSWER)
A primary high-level goal for an auditor who is reviewing a systems-development project is to ensure that business objectives are achieved. This objective guides all other systems development objectives.

NEW QUESTION: 323
During a follow-up audit, it was found that a complex security vulnerability of low risk was not resolved within the agreed-upon timeframe. IT has stated that the system with the identified vulnerability is being replaced and is expected to be fully functional in two months Which of the following is the BEST course of action?
A. Require documentation that the finding will be addressed within the new system
B. Schedule a meeting to discuss the issue with senior management
C. Perform an ad hoc audit to determine if the vulnerability has been exploited
D. Recommend the finding be resolved prior to implementing the new system
Answer: A (LEAVE A REPLY)
Requiring documentation that the finding will be addressed within the new system is the best course of action for a follow-up audit. An IS auditor should obtain evidence that the complex security vulnerability of low risk will be resolved in the new system and that there is a reasonable timeline for its implementation. The other options are not appropriate courses of action, as they may be too costly, time-consuming, or impractical for a low-risk finding. References:

* CISA Review Manual (Digital Version), Chapter 2, Section 2.5.31
* CISA Review Questions, Answers & Explanations Database, Question ID 209

NEW QUESTION: 324
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. Reviewing quality assurance (QA) procedures
B. Running historical transactions through the new system
C. Comparing code between old and new systems
D. Loading balance and transaction data to the new system
Answer: D (LEAVE A REPLY)

NEW QUESTION: 325
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 penetration tests are not performed.
C. Network firewall rules have not been documented.
D. The network firewall policy has not been approved by the information security officer.
Answer: (SHOW ANSWER)

NEW QUESTION: 326
Which of the following is a PRIMARY responsibility of an IT steering committee?
A. Prioritizing IT projects in accordance with business requirements
B. Reviewing periodic IT risk assessments
C. Validating and monitoring the skill sets of IT department staff
D. Establishing IT budgets for the business
Answer: A (LEAVE A REPLY)
A primary responsibility of an IT steering committee is prioritizing IT projects in accordance with business requirements, as this ensures that IT resources are allocated to support the strategic objectives and needs of the organization. Reviewing periodic IT risk assessments, validating and monitoring the skill sets of IT department staff, and establishing IT budgets for the business are important activities, but they are not the primary responsibility of an IT steering committee. They may be delegated to other IT governance bodies or functions within the organization. References: CISA Review Manual (Digital Version), Chapter 1:
Information Systems Auditing Process, Section 1.2: IT Governance

NEW QUESTION: 327

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: (SHOW ANSWER)

The answer D is correct because the greatest concern for an IS auditor with the situation of business owners being removed from the project initiation phase is that the requirements may be incomplete. The project initiation phase is the first step in starting a new project, where the project's purpose, scope, objectives, and deliverables are defined and documented. The project initiation phase also involves identifying and engaging the key stakeholders who have an interest or influence in the project, such as sponsors, customers, users, or business owners.

Business owners are the individuals or entities who have the authority and responsibility to define the business needs and expectations for the project. They are also the primary beneficiaries of the project outcomes and benefits. Business owners play a crucial role in the project initiation phase, as they provide valuable input and feedback on the requirements and specifications of the project. Requirements are the statements that describe what the project should accomplish or deliver to meet the business needs and expectations. Requirements are essential for guiding the project planning, execution, monitoring, and closure phases.

If business owners are removed from the project initiation phase, it can result in incomplete or inaccurate requirements, which can have negative impacts on the project's quality, scope, time, cost, and risk. Some of the possible consequences of incomplete requirements are:

* Misalignment: The project may not align with the business strategy, vision, or goals, which can reduce its value or relevance.
* Confusion: The project team may not have a clear understanding of what the project should achieve or deliver, which can affect their performance or productivity.
* Rework: The project may need to undergo frequent changes or revisions to accommodate new or modified requirements, which can increase the time and cost of the project.
* Dissatisfaction: The project may not meet the expectations or satisfaction of the business owners or other stakeholders, which can affect their acceptance or support of the project.
* Failure: The project may not deliver the expected outcomes or benefits, which can affect its success or viability.

Therefore, an IS auditor should be concerned about the involvement and participation of business owners in the project initiation phase, as it affects the completeness and quality of requirements. An IS auditor should review the policies and procedures for stakeholder identification and engagement, verify that the business owners have adequate knowledge and skills to define their requirements, and test that the requirements are well-defined, documented, approved, and communicated.

References:

* Project Initiation: The First Step to Project Management [2023] * Asana
* Everything you need to know about the project initiation phase
* Project Initiation Phase - The Business Professor
* Project Initiation: A Guide to Starting a Project Right Way - Kissflow

NEW QUESTION: 328
An IS auditor notes that not all security tests were completed for an online sales system recently promoted to production. Which of the following is the auditor's BEST course of action?
A. Hire a third party to perform security testing.
B. Increase monitoring for security incidents.
C. Determine exposure to the business.
D. Adjust future testing activities accordingly.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 329
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: 330
Which of the following ensures a sender's authenticity and an e-mail's confidentiality?
A. Encrypting the hash of the message with the sender's private key and thereafter encrypting the hash of the message with the receiver's public key
B. The sender digitally signing the message and thereafter encrypting the hash of the message with the sender's private key
C. Encrypting the hash of the message with the sender's private key and thereafter encrypting the message with the receiver's public key
D. Encrypting the message with the sender's private key and encrypting the message hash with the receiver's public key.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
To ensure authenticity and confidentiality, a message must be encrypted twice: first with the sender's private key, and then with the receiver's public key. The receiver can decrypt the message, thus ensuring confidentiality of the message. Thereafter, the decrypted message can

be decrypted with the public key of the sender, ensuring authenticity of the message. Encrypting the message with the sender's private key enables anyone to decrypt it.

NEW QUESTION: 331
Naming conventions for system resources are important for access control because they:
A. ensure that resource names are not ambiguous.
B. reduce the number of rules required to adequately protect resources.
C. ensure that user access to resources is clearly and uniquely identified.
D. ensure that internationally recognized names are used to protect resources.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Naming conventions for system resources are important for the efficient administration of security controls.
The conventions can be structured, so resources beginning with the same high-level qualifier can be governed by one or more generic rules. This reduces the number of rules required to adequately protect resources, which in turn facilitates security administration and maintenance efforts. Reducing the number of rules required to protect resources allows for the grouping of resources and files by application, which makes it easier to provide access. Ensuring that resource names are not ambiguous cannot be achieved through the use of naming conventions. Ensuring the clear and unique identification of user access to resources is handled by access control rules, not naming conventions. Internationally recognized names are not required to control access to resources. Naming conventions tend to be based on how each organization wants to identify its resources.

NEW QUESTION: 332
When using a universal storage bus (USB) flash drive to transport confidential corporate data to an offsite location, an effective control would be to:
A. carry the flash drive in a portable safe.
B. assure management that you will not lose the flash drive.
C. request that management deliver the flash drive by courier.
D. encrypt the folder containing the data with a strong key.
Answer: D (LEAVE A REPLY)

Explanation/Reference:
Explanation:
Encryption, with a strong key, is the most secure method for protecting the information on the flash drive.
Carrying the flash drive in a portable safe does not guarantee the safety of the information in the event that the safe is stolen or lost. No matter what measures you take, the chance of losing the flash drive still exists. It is possible that a courier might lose the flash drive or that it might be stolen.

NEW QUESTION: 333
Which of the following is the BEST way to address ongoing concerns with the quality and accuracy of internal audits?
A. Engage an independent review of the audit function.
B. Require peer reviews of audit workpapers.
C. Implement performance management for IS auditors.
D. Require IS audit management to lead exit meetings.
Answer: A (LEAVE A REPLY)
Section: The process of Auditing Information System

NEW QUESTION: 334
Which of the following is the MOST effective control to restrict the use of instant messaging (IM) within an organization?
A. Packet filtering firewall
B. Antivirus software
C. Intrusion detection system (IDS)
D. Application-based firewall
Answer: A (LEAVE A REPLY)

NEW QUESTION: 335
.Why is the WAP gateway a component warranting critical concern and review for the IS auditor when auditing and testing controls enforcing message confidentiality?
A. WAP is often configured by default settings and is thus insecure.
B. WAP provides weak encryption for wireless traffic.
C. WAP functions as a protocol-conversion gateway for wireless TLS to Internet SSL.
D. WAP often interfaces critical IT systems.
Answer: C (LEAVE A REPLY)
Functioning as a protocol-conversion gateway for wireless TLS to Internet SSL, the WAP gateway is a component warranting critical concern and review for the IS auditor when auditing and testing controls that enforce message confidentiality.

NEW QUESTION: 336

An organization is currently replacing its accounting system. Which of the following strategies will BEST minimize risk associated with the loss of data integrity from the upgrade?
A. Fallback contingency
B. Functional integration testing
C. Parallel implementation
D. Pilot implementation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 337
Which of the following is the MOST important responsibility of data owners when implementing a data classification process?
A. Reviewing emergency changes to data
B. Authorizing application code changes
C. Determining appropriate user access levels
D. Implementing access rules over database tables
Answer: C (LEAVE A REPLY)

NEW QUESTION: 338
When reviewing an organization's approved software product list, which of the following is the MOST
important thing to verify?
A. The risks associated with the use of the products are periodically assessed
B. The latest version of software is listed for each product
C. Due to licensing issues the list does not contain open source software
D. After hours' support is offered
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Since the business conditions surrounding vendors may change, it is important for an organization to
conduct periodic risk assessments of the vendor software list. This might be best incorporated into the IT
risk management process. Choices B, C and D are possible considerations but would not be the most
important.

NEW QUESTION: 339
John has been hired to fill a new position in one of the well-known financial institute. The position is for IS auditor. He has been assigned to complete IS audit of one of critical financial system. Which of the following should be the first step for John to be perform during IS audit planning?
A. Perform risk assessment

B. Determine the objective of the audit
C. Gain an understanding of the business process
D. Assign the personnel resource to audit
Answer: (SHOW ANSWER)
Section: Information System Operations, Maintenance and Support
Explanation:
Determine the objective of audit should be the first step in the audit planning process. Depending upon the objective of an audit, auditor can gather the information about business process.
For CISA exam you should know the information below:
Steps to perform audit planning
Gain an understanding of the business mission, objectives, purpose and processes which includes information and processing requirement such as availability, integrity, security and business technology and information confidentiality.
Understand changes in the business environment audited.
Review prior work papers
Identify stated contents such as policies, standards and required guidelines, procedure and organization structures.
Perform a risk analysis to help in designing the audit plan.
Set the audit scope and audit objectives.
Develop the audit approach or audit strategy
Assign personnel resources to audit
Address engagement logistics.
The following answers are incorrect:
The other options specified should be completed once we finalize on the objective of audit.
Reference:
CISA review manual 2014 page number 30 (The process of auditing information system)

NEW QUESTION: 340
Which of the following would MOST effectively help to reduce the number of repealed incidents in an organization?
A. Testing incident response plans with a wide range of scenarios
B. Prioritizing incidents after impact assessment.
C. Linking incidents to problem management activities
D. Training incident management teams on current incident trends
Answer: C (LEAVE A REPLY)
Explanation
Linking incidents to problem management activities would most effectively help to reduce the number of repeated incidents in an organization, because problem management aims to identify and eliminate the root causes of incidents and prevent their recurrence. Testing incident response plans, prioritizing incidents, and training incident management teams are all good practices, but

they do not directly address the issue of repeated incidents. References: ISACA ITAF 3rd Edition Section 3600

NEW QUESTION: 341
An organization has replaced all of the storage devices at its primary data center with new higher-capacity units The replaced devices have been installed at the disaster recovery site to replace older units An IS auditor s PRIMARY concern would be whether
A. the recovery site devices can handle the storage requirements
B. hardware maintenance contract is in place for both old and new storage devices
C. the procurement was in accordance with corporate policies and procedures
D. the relocation plan has been communicated to all concerned parties
Answer: A (LEAVE A REPLY)
Explanation
An IS auditor's primary concern would be whether the recovery site devices can handle the storage requirements. The storage requirements are determined by the amount and type of data that needs to be backed up and restored in case of a disaster at the primary data center. The recovery site devices should have enough capacity, performance, reliability, and compatibility to meet these requirements.
If the recovery site devices cannot handle the storage requirements, then there is a risk that some data may not be backed up properly or may not be available for recovery when needed. This could result in data loss, corruption, or inconsistency, which could affect the business continuity and integrity of the organization.
Therefore, an IS auditor should verify that:
The recovery site devices have sufficient storage space to accommodate all the data that needs to be backed up from the primary data center.
The recovery site devices have adequate bandwidth and speed to transfer and access data efficiently and effectively.
The recovery site devices have appropriate security features and controls to protect data from unauthorized access or modification.
The recovery site devices are compatible with the primary data center devices in terms of hardware, software, format, and protocol.
References:
10: What Is a Disaster Recovery Site? Hot, Cold & Warm Site
11: Disaster recovery site - What is the ideal distance to mitigate risks? - Advisera
12: Offsite Data Backup Storage vs Disaster Recovery (DR) - LINBIT

NEW QUESTION: 342
Which of the following non-audit activities may impair an IS auditor's independence and objectivity?
A. Providing advice on an IT project management framework
B. Evaluating a third-party customer satisfaction survey

C. Designing security controls for a new cloud-based workforce management system
D. Reviewing secure software development guidelines adopted by an organization
Answer: C (LEAVE A REPLY)

NEW QUESTION: 343
A banking organization has outsourced its customer data processing facilities to an external service provider.
Which of the following roles is accountable for ensuring the security of customer data?
A. The service provider's data privacy officer
B. The bank's vendor risk manager
C. The bank's senior management
D. The service provider's data processor
Answer: (SHOW ANSWER)

NEW QUESTION: 344
Which of the following is the BEST method to maintain an audit trail of changes made to the source code of a program?
A. Embed details within source code.
B. Standardize file naming conventions.
C. Utilize automated version control.
D. Document details on a change register.
Answer: C (LEAVE A REPLY)
Explanation
Automated version control systems are the best method to maintain an audit trail of changes made to the source code of a program. They automatically track and manage changes to the source code over time, allowing you to see what changes were made, when they were made, and who made them1. This provides a clear and detailed audit trail that can be invaluable for debugging, understanding the evolution of the code, and ensuring accountability23.

NEW QUESTION: 345
An organization has virtualized its server environment without making any other changes to the network or security infrastructure. Which of the following is the MOST significant risk?
A. Data center environmental controls not aligning with new configuration
B. System documentation not being updated to reflect changes in the environment
C. Inability of the network intrusion detection system (IDS) to monitor virtual server-lo-server communications
D. Vulnerability in the virtualization platform affecting multiple hosts
Answer: B (LEAVE A REPLY)

NEW QUESTION: 346
Which of the following is the BEST indicator for measuring performance of IT help desk function?

A. Percentage of problems raised from incidents
B. Mean time to categorize tickets
C. Number 0t incidents reported
D. Number of reopened tickets
Answer: (SHOW ANSWER)
The answer D is correct because the number of reopened tickets is the best indicator for measuring the performance of IT help desk function. Reopened tickets are tickets that have been marked as resolved by the help desk agents, but the customers are not satisfied with the resolution and reopen them for further assistance.
Reopened tickets reflect the quality and effectiveness of the help desk service, as well as the customer satisfaction level. A high number of reopened tickets indicates that the help desk agents are not resolving the issues properly, or that they are not communicating well with the customers. This can lead to customer frustration, dissatisfaction, and churn. Therefore, minimizing the number of reopened tickets is a key goal for any help desk function.
The other options are not as good as option D. Percentage of problems raised from incidents (option A) is a metric that shows how many incidents are escalated to problems, which are more complex and require root cause analysis and long-term solutions. This metric reflects the complexity and severity of the issues faced by the customers, but it does not directly measure the performance of the help desk function. Mean time to categorize tickets (option B) is a metric that shows how long it takes for the help desk agents to assign a category to each ticket, such as technical, billing, or feedback. This metric reflects the efficiency and accuracy of the help desk agents, but it does not measure the quality or effectiveness of the resolution. Number of incidents reported (option C) is a metric that shows how many issues are reported by the customers to the help desk function. This metric reflects the demand and workload of the help desk function, but it does not measure how well the issues are resolved or how satisfied the customers are.
References:
* Key Metrics to Measure Help Desk Performance
* 8 service desk KPIs and performance metrics for IT support
* 13 Most Important Help Desk KPIs to Track and Measure Help Desk Performance

NEW QUESTION: 347
Which of the following is the BEST indication of effective governance over IT infrastructure?
A. The ability to deliver continuous, reliable performance

B. A requirement for annual security awareness programs
C. An increase in the number of IT infrastructure servers
D. A decrease in the number of information security incidents
Answer: A (LEAVE A REPLY)
Effective governance over IT infrastructure is indicated by the ability to deliver continuous, reliable performance12. This is because good governance ensures that IT investments support business objectives and produce measurable results towards achieving their strategies2. It involves implementing management and internal controls, strengthening security, financial controls, risk mitigation, and inspection and compliance obligations3. While security awareness programs, the number of servers, and the number of security incidents can be aspects of IT governance, they are not the best indicators of its effectiveness.
References:
The Value of IT Governance - ISACA
What is IT governance? A formal way to align IT & business strategy | CIO Robust Governance - KPMG Global

NEW QUESTION: 348
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)
Explanation
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: 349
Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?
A. Sensitive data can be read by operators.
B. Data can be amended without authorization.

C. Unauthorized report copies can be printed.
D. Output can be lost in the event of system failure.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Unless controlled, spooling for offline printing may enable additional copies to be printed. Print files are unlikely to be available for online reading by operators. Data on spool files are no easier to amend without authority than any other file. There is usually a lesser threat of unauthorized access to sensitive reports in the event of a system failure.

NEW QUESTION: 350
Which of the following is the PRIMARY purpose of conducting a business impact analysis (BIA)?
A. Identifying risk mitigation options
B. Identifying key business risks
C. Identifying critical business processes
D. Identifying the threat environment
Answer: (SHOW ANSWER)
Section: Governance and Management of IT

NEW QUESTION: 351
Which of the following is an IS auditor's BEST recommendation to protect an organization from attacks when its file server needs to be accessible to external users?
A. Enforce a secure tunnel connection.
B. Enhance internal firewalls.
C. Set up a demilitarized zone (DMZ).
D. Implement a secure protocol.
Answer: C (LEAVE A REPLY)
A demilitarized zone (DMZ) is a network segment that is separated from the internal network and the external network, such as the internet, by firewalls or other security devices. A DMZ provides an extra layer of security for the organization's internal network by isolating the servers and services that need to be accessible to external users, such as a file server, from the rest of the network. A DMZ also prevents external users from accessing the internal network directly, as they have to go through two firewalls to reach it. Therefore, setting up a DMZ is an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users12.
The other possible options are:
* Enforce a secure tunnel connection: This means that the organization requires external users to establish a secure and encrypted connection, such as a virtual private network (VPN), to access its file server.
This can provide some level of security and privacy for the data transmission, but it does not protect the file server or the internal network from attacks if the connection is compromised or if

the external users are malicious. Therefore, enforcing a secure tunnel connection is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users3.
* Enhance internal firewalls: This means that the organization improves the security and performance of its internal firewalls, which are devices that filter and control the network traffic between different segments of the network. This can provide some level of protection for the internal network from unauthorized or malicious access, but it does not protect the file server or the external network from attacks if the file server is exposed to the internet or if the external network is compromised. Therefore, enhancing internal firewalls is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users4.
* Implement a secure protocol: This means that the organization uses a secure and standardized protocol, such as Secure File Transfer Protocol (SFTP) or Secure Shell (SSH), to transfer files between its file server and external users. This can provide some level of security and integrity for the data transmission, but it does not protect the file server or the internal network from attacks if the protocol is exploited or if the external users are malicious. Therefore, implementing a secure protocol is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users5. References: 1: What Is a DMZ Network and Why Would You Use It? | Fortinet 2:
Demilitarised zone (DMZ) | Cyber.gov.au 3: What Is VPN Tunneling? | Fortinet 4: Firewall - Wikipedia 5: Secure Shell - Wikipedia

NEW QUESTION: 352
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: (SHOW ANSWER)
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: 353
An IS auditor concludes that logging and monitoring mechanisms within an organization are ineffective because central servers are not included within the central log repository. Which of the following audit procedures would have MOST likely identified this exception?

A. Inspecting a sample of alerts generated from the central log repository
B. Inspecting a sample of alert settings configured in the central log repository
C. Comparing a list of all servers from the directory server against a list of all servers present in the central log repository
D. Comparing all servers included in the current central log repository with the listing used for the prior-year audit
Answer: C (LEAVE A REPLY)

NEW QUESTION: 354
An IS auditor is reviewing security policies and finds no mention of the return of corporate-owned smartphones upon termination of employment. The GREATEST risk arising from this situation is that unreturned devices:
A. have access to corporate resources
B. cause the asset inventory to be inaccurate.
C. generate excessive telecommunication costs.
D. result in loss of customer contact details
Answer: (SHOW ANSWER)

NEW QUESTION: 355
Critical processes are not defined in an organization's business continuity plan (BCP). Which of the following would have MOST likely identified the gap?
A. Testing the incident response plan
B. Reviewing the business continuity strategy
C. Reviewing the business impact analysis (BIA)
D. Updating the risk register
Answer: C (LEAVE A REPLY)

NEW QUESTION: 356
Code changes are compiled and placed in a change folder by the developer. An implementation team migrates changes to production from the change folder.
Which of the following BEST indicates separation of duties is in place during the migration process?
A. The developer approves changes prior to moving them to the change folder.
B. A second individual performs code review before the change is released to production.
C. The implementation team does not have access to change the source code.
D. The implementation team does not have experience writing code.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 357

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 is 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)
Section: Protection of Information Assets
Explanation:
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: 358
When an organization is developing data classification standards, it is MOST important to ensure the standards:
A. are based on the business requirements for authentication of the information.
B. align with the organization's segregation of duties requirements.
C. are based on the business requirements for confidentiality of the information.
D. align with the organization's IT capability maturity framework.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 359
The GREATEST benefit of using a prototyping approach in software development is that it helps to:
A. improve efficiency of quality assurance (QA) testing.
B. conceptualize and clarify requirements
C. minimize scope changes to the system
D. decrease the time allocated for user testing and review
Answer: B (LEAVE A REPLY)

NEW QUESTION: 360
Which of the following is the BEST justification for deferring remediation testing until the next audit?
A. The audit environment has changed significantly
B. Auditee management has accepted all observations reported by the auditor.
C. The auditor who conducted the audit
D. Management's planned actions are sufficient given the relative importance of the observations
Answer: B (LEAVE A REPLY)

NEW QUESTION: 361
Which of the following should the IS auditor do FIRST to ensure data transfer integrity for Internet of Things (IoT) devices?
A. Verify access control lists to the database where collected data is stored.
B. Confirm that acceptable limits of data bandwidth are defined for each device.
C. Ensure that message queue telemetry transport (MQTT) is used.
D. Determine how devices are connected to the local network.
Answer: D (LEAVE A REPLY)
Section: The process of Auditing Information System

NEW QUESTION: 362
Which of the following is an indication of possible hacker activity involving voice communications?
A. A significant percentage of lines are busy during early morning and late afternoon hours.
B. Outbound calls are found to significantly increase in frequency during non-business hours.
C. Inbound calls experience significant fluctuations based on time-of-day and day-of-week.
D. Direct inward system access (OISA) is found to be disabled on the company's exchange.
Answer: (SHOW ANSWER)

NEW QUESTION: 363
Which of the following is the BEST compensating control against segregation of duties conflicts in new code development?
A. A small number of people have access to deploy code
B. Creation of staging environments
C. Adding the developers to the change approval board

D. Post-implementation change review
Answer: D (LEAVE A REPLY)

NEW QUESTION: 364
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. Identity alternatives to critical applications.
C. Review the business continuity insurance policy.
D. Carry out a risk assessment.
Answer: D (LEAVE A REPLY)
Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 365
For a discretionary access control to be effective, it must:
A. operate within the context of mandatory access controls.
B. operate independently of mandatory access controls.
C. enable users to override mandatory access controls when necessary.
D. be specifically permitted by the security policy.
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Mandatory access controls are prohibitive; anything that is not expressly permitted is forbidden. Only within this context do discretionary controls operate, prohibiting still more access with the same exclusionary principle. When systems enforce mandatory access control policies, they must distinguish between these and the mandatory access policies that offer more flexibility. Discretionary controls do not override access controls and they do not have to be permitted in the security policy to be effective.

NEW QUESTION: 366
Which of the following should be identified FIRST during the risk assessment process?
A. Vulnerability to threats
B. Existing controls
C. Information assets
D. Legal requirements
Answer: (SHOW ANSWER)
The risk assessment process involves identifying the information assets that are at risk, analyzing the threats and vulnerabilities that could affect them, evaluating the impact and likelihood of a risk event, and determining the appropriate controls to mitigate the risk. The first step is to identify the information assets, as they are the objects of protection and the basis for the rest of the process.

Without knowing what assets are at risk, it is not possible to assess their value, exposure, or protection level. References: ISACA Frameworks:
Blueprints for Success

NEW QUESTION: 367
Which of the following is found in an audit charter?
A. The process of developing the annual audit plan
B. The authority given to the audit function
C. Required training for audit staff
D. Audit objectives and scope
Answer: B (LEAVE A REPLY)
The authority given to the audit function is one of the components that is found in an audit charter. According to the IIA, the audit charter is a formal document that defines internal audit's purpose, authority, responsibility and position within the organization1. The authority given to the audit function includes the scope of its activities, the access to records, personnel and physical properties relevant to its work, and the independence and objectivity of its staff2. The authority given to the audit function helps to ensure that internal auditors can perform their duties effectively and efficiently, and that they can provide assurance and consulting services that add value and improve the organization's operations3.
The other options are not found in an audit charter. The process of developing the annual audit plan is not part of the audit charter, but rather a separate document that outlines the methodology, criteria and resources for selecting and prioritizing audit engagements based on a risk assessment4. Required training for audit staff is not part of the audit charter, but rather a component of the quality assurance and improvement program that evaluates the competence and performance of internal auditors and provides them with opportunities for professional development5. Audit objectives and scope are not part of the audit charter, but rather specific elements of each individual audit engagement that define the expected outcomes and the boundaries of the audit work.

NEW QUESTION: 368
Which of the following should be of GREATEST concern to an IS auditor who is assessing an organization's configuration and release management process?
A. The organization does not use an industry-recognized methodology
B. All changes require middle and senior management approval
C. There is no centralized configuration management database (CMDB)
D. Changes and change approvals are not documented
Answer: D (LEAVE A REPLY)

NEW QUESTION: 369
Which of the following methods BEST ensures that a comprehensive approach is used to direct information security activities?

A. Creating communication channels
B. Promoting security training
C. Establishing a steering committee
D. Holding periodic meetings with business owners
Answer: B (LEAVE A REPLY)
Section: Information System Operations, Maintenance and Support

NEW QUESTION: 370
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)
Section: Protection of Information Assets
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 DDS.

NEW QUESTION: 371
Which of the following is MOST important to consider when assessing the scope of privacy concerns for an
IT project?
A. Applicable laws and regulations
B. End user access rights
C. Business requirements
D. Classification of data
Answer: (SHOW ANSWER)
Section: Governance and Management of IT

NEW QUESTION: 372
The source code of an application has just been debugged. Which type of testing should be performed to help ensure that new errors are not been introduced by the debugging process?
A. Validation
B. Black-box
C. Sociability
D. Regression
Answer: D (LEAVE A REPLY)

NEW QUESTION: 373

Which of the following is the BEST way to detect potentially fraudulent purchases where an employee can approve a receipt of an item or service that the employee also procured?
A. Require purchase orders to originate from the same individual with designated authority.
B. Require trial invoices can only be paid when matched with purchase orders.
C. Require receipts to be entered against purchase orders by someone other than the buyer.
D. Require staff training on entering purchase orders into the enterprise resource planning (ERP) system.
Answer: (SHOW ANSWER)

NEW QUESTION: 374
What is an IS auditor's BEST recommendation for management if a network vulnerability assessment confirms that critical patches have not been applied since the last assessment?
A. Implement a process to test and apply appropriate patches.
B. Apply available patches and continue periodic monitoring.
C. Configure servers to automatically apply available patches.
D. Remove unpatched devices from the network.
Answer: A (LEAVE A REPLY)
Section: The process of Auditing Information System

NEW QUESTION: 375
Which of the following is the BEST indicator of an effective employee information security program?
A. Increased management support for security
B. More efficient and effective incident handling
C. Increased detection and reporting of incidents
D. Reduced operational cost of security
Answer: (SHOW ANSWER)
Section: Information System Operations, Maintenance and Support
Explanation

NEW QUESTION: 376
Which of the following is a PRIMARY responsibility of a quality assurance (QA) team?
A. Creating test data to facilitate the user acceptance testing (IJAT) process
B. Managing employee onboarding processes and background checks
C. Advising the steering committee on quality management issues and remediation efforts
D. Implementing procedures to facilitate adoption of quality management best practices
Answer: (SHOW ANSWER)
A quality assurance (QA) team is a group of professionals who are responsible for ensuring that the products or services of an organization meet the quality standards and expectations of customers and stakeholders1. A QA team performs various activities, such as:

Planning, designing, and executing quality tests and audits to verify the quality of the products or services1 Identifying, analyzing, and reporting quality issues, defects, or non-conformities1 Recommending and implementing corrective and preventive actions to resolve quality problems and prevent recurrence1 Monitoring and measuring the effectiveness and efficiency of the quality processes and improvements1 Establishing and maintaining quality documentation, records, and reports1 Providing quality training, guidance, and support to the staff and management1 One of the primary responsibilities of a QA team is to implement procedures to facilitate adoption of quality management best practices. Quality management best practices are the methods, techniques, or tools that have been proven to be effective in achieving and maintaining high-quality standards in an organization2. Some examples of quality management best practices are: Adopting a customer-focused approach that aims to meet or exceed customer requirements and satisfaction2 Implementing a process approach that manages the interrelated activities as a coherent system2 Applying continuous improvement methods that seek to enhance the performance and value of the products or services2 Using evidence-based decision making that relies on factual data and information2 Developing a culture of engagement and empowerment that involves and motivates the people in the organization2 By implementing procedures to facilitate adoption of quality management best practices, a QA team can help the organization achieve the following benefits:
Improve the quality and reliability of the products or services2
Reduce the costs and risks associated with poor quality or non-compliance2 Increase the customer loyalty and retention2 Enhance the reputation and competitiveness of the organization2 Foster a culture of excellence and innovation in the organization2 The other options are not primary responsibilities of a QA team. Creating test data to facilitate the user acceptance testing (UAT) process is a task that can be performed by a QA team, but it is not their main duty. UAT is a process in which the end users test the product or service to ensure that it meets their needs and expectations before it is released or deployed3. A QA team can create test data to simulate real-world scenarios and conditions for UAT, but they are not directly involved in conducting UAT. Managing employee onboarding processes and background checks is not a responsibility of a QA team. Employee onboarding is a process in which new hires are integrated into the organization, while background checks are screenings that verify the identity, credentials, and history of potential employees4. These processes are usually handled by the human resources department or an external agency, not by a QA team. Advising the steering committee on quality management issues and remediation efforts is not a primary responsibility of a QA team. A steering committee is a group of senior executives or managers who provide strategic direction, oversight, and support for a project or program5. A QA team can advise the steering committee on quality management issues and remediation efforts, but they are not accountable for making decisions or implementing actions. Therefore, option D is the correct answer.
References:
Quality Assurance Team: Roles & Responsibilities
What are the Best Practices in Quality Management?
User Acceptance Testing (UAT): A Complete Guide

Employee Onboarding Process: Definition & Best Practices
What Is A Steering Committee? - The Basics

NEW QUESTION: 377
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: (SHOW ANSWER)
Explanation
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: 378
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. Privacy legislation in other countries that may contain similar requirements
C. Operational plan for achieving compliance with the legislation
D. Analysis of systems that contain privacy components
Answer: D (LEAVE A REPLY)
The first thing that an IS auditor should evaluate when reviewing an organization's response to new privacy legislation is the analysis of systems that contain privacy components. Privacy components are elements of a system that collect, process, store, or transmit personal information that is subject to privacy legislation. An analysis of systems that contain privacy components should identify what types of personal information are involved, where they are located, how they are used, who has access to them, and what risks or threats they face. An analysis of systems that contain privacy components is essential for determining the scope and impact of the new privacy legislation on the organization's systems and processes.
The other options are not as important as option D. An implementation plan for restricting the collection of personal information is a possible action, but not the first thing to evaluate, when reviewing an organization's response to new privacy legislation. An implementation plan for restricting the collection of personal information is a document that outlines how an organization will comply with the principle of data minimization, which states that personal information should be collected only for specific and legitimate purposes and only to the extent necessary for those purposes. An implementation plan for restricting the collection of personal information should be based on an analysis of systems that contain privacy components. Privacy legislation in other countries that may contain similar requirements is a possible source of reference, but not the first thing to evaluate, when reviewing an organization's response to new privacy legislation. Privacy legislation in other countries that may contain similar requirements is a set of laws or regulations that governs the protection of personal information in other jurisdictions that may have

comparable or compatible standards or expectations as the new privacy legislation. Privacy legislation in other countries that may contain similar requirements may provide guidance or best practices for complying with the new privacy legislation. However, privacy legislation in other countries that may contain similar requirements should not be used as a substitute for an analysis of systems that contain privacy components.
An operational plan for achieving compliance with the legislation is a possible deliverable, but not the first thing to evaluate, when reviewing an organization's response to new privacy legislation. An operational plan for achieving compliance with the legislation is a document that describes how an organization will implement and maintain the necessary policies, procedures, controls, and measures to comply with the new privacy legislation. An operational plan for achieving compliance with the legislation should be derived from an analysis of systems that contain privacy components. References: Privacy law - Wikipedia, Data Protect ion and Privacy Legislation Worldwide | UNCTAD, Data minimization - Wikipedia

NEW QUESTION: 379
Which of the following testing method examines internal structure or working of an application?
A. White-box testing
B. Parallel Test
C. Regression Testing
D. Pilot Testing
Answer: (SHOW ANSWER)
Section: Information System Acquisition, Development and Implementation
Explanation/Reference:
White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application,
as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the
system, as well as programming skills, are used to design test cases. The tester chooses inputs to
exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes
in a circuit, e.g. in-circuit testing (ICT).
White-box testing can be applied at the unit, integration and system levels of the software testing process.
Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for
integration and system testing more frequently today. It can test paths within a unit, paths between units
during integration, and between subsystems during a system-level test. Though this method of test design

can uncover many errors or problems, it has the potential to miss unimplemented parts of the specification
or missing requirements.
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
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 167
Official ISC2 guide to CISSP CBK 3rd Edition Page number 176

NEW QUESTION: 380

An IS auditor discovers that due to resource constraints a database administrator (DBA) is responsible for developing and executing changes into the production environment Which of the following should the auditor do FIRST?

A. Report a potential segregation of duties (SoD) violation

B. Ensure a change management process is followed prior to implementation

C. Identify whether any compensating controls exist

D. Determine whether another database administrator (DBA) could make the changes

Answer: B (LEAVE A REPLY)

NEW QUESTION: 381

A manager identifies active privileged accounts belonging to staff who have left the organization. Which of the following is the threat actor In this scenario?

A. Terminated staff

B. Unauthorized access

C. Deleted log data

D. Hacktivists

Answer: B (LEAVE A REPLY)

NEW QUESTION: 382

Which of the following would BEST indicate the effectiveness of a security awareness training program?

A. Results of third-party social engineering tests

B. Employee satisfaction with training

C. Increased number of employees completing training

D. Reduced unintentional violations

Answer: D (LEAVE A REPLY)

Explanation

The effectiveness of a security awareness training program is best indicated by a reduction in unintentional violations. When employees are well-trained and aware of security practices, they are less likely to inadvertently violate security policies or make mistakes that could lead to breaches. While other factors (such as third-party social engineering tests, employee satisfaction, and completion rates) provide valuable insights, the ultimate goal of security awareness training is to minimize unintentional errors and improve overall security posture12. References: 1(https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for

NEW QUESTION: 383

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 cost-effective.

C. The scanning will be performed during non-peak hours.

D. The scanning will be followed by penetration testing.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 384
An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?
A. References from other customers
B. Service level agreement (SLA) template
C. Maintenance agreement
D. Conversion plan
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
An IS auditor should look for an independent verification that the ISP can perform the tasks being contracted for. References from other customers would provide an independent, external review and verification of procedures and processes the ISP follows-issues which would be of concern to an IS auditor. Checking references is a means of obtaining an independent verification that the vendor can perform the services it says it can. A maintenance agreement relates more to equipment than to services, and a conversion plan, while important, is less important than verification that the ISP can provide the services they propose.

NEW QUESTION: 385
During a security access review, an IS auditor identifies a segregation of duties issue involving financial reporting for which there are no mitigating controls. Which of the following stakeholders should be notified of this finding FIRST?
A. External auditors
B. The board of directors
C. The audit committee
D. Operational management
Answer: D (LEAVE A REPLY)

NEW QUESTION: 386
.Business process re-engineering often results in _____ automation, which results in _____ number of people using technology. Fill in the blanks.
A. Increased; a greater
B. Increased; a fewer
C. Less; a fewer
D. Increased; the same
Answer: (SHOW ANSWER)
Business process re-engineering often results in increased automation, which results in a greater number of people using technology.

NEW QUESTION: 387
Data anonymizabon helps to prevent which types of attacks in a big data environment?
A. Spoofing
B. Correlation
C. Denial of service (DoS)
D. Man-in-the-middle
Answer: (SHOW ANSWER)

NEW QUESTION: 388
What does PKI use to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions?
A. A combination of public-key cryptography and digital certificates and two-factor authentication
B. A combination of public-key cryptography and two-factor authentication
C. A combination of public-key cryptography and digital certificates
D. A combination of digital certificates and two-factor authentication
Answer: (SHOW ANSWER)
Explanation/Reference:
PKI uses a combination of public-key cryptography and digital certificates to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions.

NEW QUESTION: 389
Which of the following is the MOST important consideration when defining recovery point objectives (RPOs)?
A. Minimum operating requirements
B. Acceptable data loss
C. Mean time between failures
D. Acceptable time for recovery
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation:
Recovery time objectives (RTOs) are the acceptable time delay in availability of business operations, while recovery point objectives (RPOs) are the level of data loss/reworking an organization is willing to accept.
Mean time between failures and minimum operating requirements help in defining recovery strategies.

NEW QUESTION: 390
Which of the following is the BEST reason to perform root cause analysis after a critical server failure?
A. To enable timely follow-up audits

B. To enable the optimization of IT investments
C. To enable the gathering of system availability data
D. To enable appropriate corrective measures
Answer: D (LEAVE A REPLY)

NEW QUESTION: 391
Which of the following would be of GREATEST concern to an IS auditor receiving an organization's
security incident handling procedures?
A. Annual tabletop exercises are performed instead of functional incident response exercises.
B. Roles for computer emergency response team (CERT) members have not been formally documented.
C. Guidelines for prioritizing incidents have not been identified.
D. Workstation antivirus software alerts are not regularly reviewed.
Answer: D (LEAVE A REPLY)
Section: Information System Operations, Maintenance and Support

NEW QUESTION: 392
Which of the following is the unique identifier within and IPSec packet that enables the sending host to reference the security parameter to apply?
A. SPI
B. SA
C. ESP
D. AH
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The Security Parameter Index (SPI) is the unique identifier that enables the sending host to reference the security parameter to apply in order to decrypt the packet.
For you exam you should know the information below about the IPSec protocol:
The IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods.

For the transport method, the data portion of each packet is encrypted, encryption within IPSEC is referred to as the encapsulation security payload (ESP), it is ESP that provides confidentiality over the process.
In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied.
In establishing IPSec sessions in either mode, Security Associations (SAs) are established. SAs defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAs is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host.
IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows automated key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and the cryptographic keys.
The following were incorrect answers:
SA - Security Association (SA) defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc.
ESP - Encapsulation Security Payload (ESP) is used to support authentication of sender and encryption of data
AH - Authentication Header allows authentication of a sender of a data.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number353

NEW QUESTION: 393
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:
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 shave 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: 394
An organization has just completed their annual risk assessment. Regarding the business continuity plan, what should an IS auditor recommend as the next step for the organization?
A. Review and evaluate the business continuity plan for adequacy
B. Perform a full simulation of the business continuity plan
C. Train and educate employees regarding the business continuity plan
D. Notify critical contacts in the business continuity plan
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation:
The business continuity plan should be reviewed every time a risk assessment is completed for the organization. Training of the employees and a simulation should be performed after the business continuity plan has been deemed adequate for the organization. There is no reason to notify the business continuity plan contacts at this time.

NEW QUESTION: 395
Private Branch Exchange(PBX) environment involves many security risks, one of which is the people both internal and external to an organization. Which of the following risks are NOT associated with Private Branch Exchange?
1. Theft of service
2. Disclosure of information
3. Data Modifications
4. Denial of service
5. Traffic Analysis
A. 3 and 4
B. 4 and 5
C. 1-4
D. They are ALL risks associated with PBX
Answer: D (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:

The NOT is a keyword used in the question. You need to find out the risks which are NOT associated with PBX. All the risk listed within the options are associated with PBX.
The threat of the PBX telephone system is many, depending on the goals of these attackers, and include:
Theft of service - Toll fraud, probably the most common of motives for attacker.
Disclosure of Information - Data disclosed without authorization, either by deliberate actionably accident.
Examples includes eavesdropping on conversation and unauthorized access to routing and address data.
Data Modification - Data altered in some meaningful way by recording, deleting or modifying it. For example, an intruder may change billing information or modify system table to gain additional services.
Unauthorized access - Actions that permit an unauthorized user to gain access to system resources or privileges.
Denial of service - Actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.
Traffic Analysis - A form of passive attack in which an intruder observes information about calls and make inferences, e.g. from the source and destination number or frequency and length of messages. For example, an intruder observes a high volume of calls between a company's legal department and patent office, and conclude that a patent is being filed.
The following were incorrect answers:
All the risks presented in options are associated with PBX. So other options are not valid.
Reference:
CISA review manual 2014 Page number356

NEW QUESTION: 396
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. testing only the authorizations to implement the new program.
C. reviewing only the actual lines of source code changed in the program.
D. tracing modifications from the executable program back to the original request for change.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 397
Which of the following procedures would BEST contribute to the reliability of information in a data warehouse?
A. Storing only a single type of data
B. Maintain archive data
C. Maintaining current metadata
D. Retaining only current data.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 398
Which of the following protocol is PRIMARILY used to provide confidentiality in a web based application thus protecting data sent across a client machine and a server?
A. SSL
B. FTP
C. SSH
D. S/MIME
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The Secure Socket Layer (SSL) Protocol is primarily used to provide confidentiality to the information sent across clients and servers.
For your exam you should know the information below:
The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmitted over a public network such as the Internet.
SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.
SSL is included as part of both the Microsoft and Netscape browsers and most Web server products.
Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security.
The
"sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer.SSL uses the public-and- private key encryption system from RSA, which also includes the use of a digital certificate. Later on SSL uses a Session Key along a Symmetric Cipher for the bulk of the data.
TLS and SSL are an integral part of most Web browsers (clients) and Web servers. If a Web site is on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access. Any Web server can be enabled by using Netscape's SSLRef program library which can be downloaded for noncommercial use or licensed for commercial use.
TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.
The SSL handshake
A HTTP-based SSL connection is always initiated by the client using a URL starting with https:// instead of with http://. At the beginning of an SSL session, an SSL handshake is performed. This handshake produces the cryptographic parameters of the session. A simplified overview of how the SSL handshake is processed is shown in the diagram below.
SSL Handshake

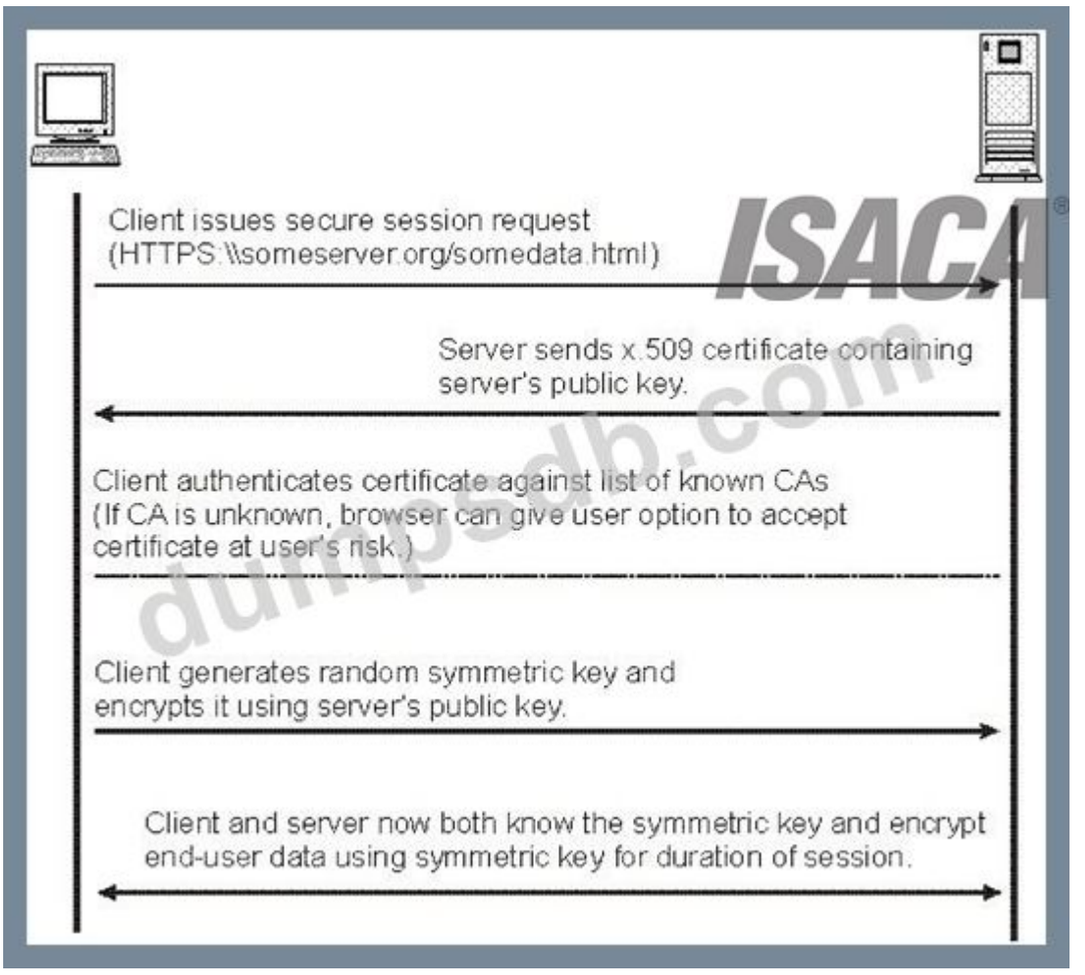


Image Reference - http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1363-00/en_US/HTML/handshak.gif The client sends a client "hello" message that lists the cryptographic capabilities of the client (sorted in client preference order), such as the version of SSL, the cipher suites supported by the client, and the data compression methods supported by the client. The message also contains a 28-byte random number.

The server responds with a server "hello" message that contains the cryptographic method (cipher suite) and the data compression method selected by the server, the session ID, and another random number.

Note:

The client and the server must support at least one common cipher suite, or else the handshake fails. The server generally chooses the strongest common cipher suite.

The server sends its digital certificate. (In this example, the server uses X.509 V3 digital certificates with SSL.) If the server uses SSL V3, and if the server application (for example, the Web server) requires a digital certificate for client authentication, the server sends a "digital certificate request" message. In the "digital certificate request" message, the server sends a list of the types of digital certificates supported and the distinguished names of acceptable certificate authorities.

The server sends a server "hello done" message and waits for a client response. Upon receipt of the server "hello done" message, the client (the Web browser) verifies the validity of the server's digital certificate and checks that the server's "hello" parameters are acceptable.

If the server requested a client digital certificate, the client sends a digital certificate, or if no suitable digital certificate is available, the client sends a "no digital certificate" alert. This alert is only a warning, but the server application can fail the session if client authentication is mandatory.
The client sends a "client key exchange" message. This message contains the pre-master secret, a 46- byte random number used in the generation of the symmetric encryption keys and the message authentication code (MAC) keys, encrypted with the public key of the server.
If the client sent a digital certificate to the server, the client sends a "digital certificate verify" message signed with the client's private key. By verifying the signature of this message, the server can explicitly verify the ownership of the client digital certificate.
Note:
An additional process to verify the server digital certificate is not necessary. If the server does not have the private key that belongs to the digital certificate, it cannot decrypt the pre-master secret and create the correct keys for the symmetric encryption algorithm, and the handshake fails.
The client uses a series of cryptographic operations to convert the pre-master secret into a master secret, from which all key material required for encryption and message authentication is derived. Then the client sends a "change cipher spec" message to make the server switch to the newly negotiated cipher suite.
The next message sent by the client (the "finished" message) is the first message encrypted with this cipher method and keys.
The server responds with a "change cipher spec" and a "finished" message of its own.
The SSL handshake ends, and encrypted application data can be sent.
The following answers are incorrect:
FTP - File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.
SSH - Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers. It connects, via a secure channel over an insecure network, a server and a client running SSH server and SSH client programs, respectively.
S/MIME - S/MIME (Secure Multi-Purpose Internet Mail Extensions) is a secure method of sending e-mail that uses the Rivets-Shamir-Adelman encryption system. S/MIME is included in the latest versions of the Web browsers from Microsoft and Netscape and has also been endorsed by other vendors that make messaging products. RSA has proposed S/MIME as a standard to the Internet Engineering Task Force (IETF).
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 352
Official ISC2 guide to CISSP CBK 3rd Edition Page number 256

http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1363-00/en_US/HTML/ss7aumst18.htm

NEW QUESTION: 399
Which of the following is the BEST control to ensure data entered into a calculation program is accurate?
A. Manual recalculation of data
B. Reasonableness checks with a data entry range
C. Programmed edit checks to prevent entry of invalid data
D. Visual verification of data entered
Answer: C (LEAVE A REPLY)

NEW QUESTION: 400
Which of the following is the BEST security control to validate the integrity of data communicated between production databases and a big data analytics system?
A. Hashing in-scope data sets
B. Encrypting in-scope data sets
C. Running and comparing the count function within the in-scope data sets
D. Hosting a digital certificate for in-scope data sets
Answer: A (LEAVE A REPLY)
Hashing is a technique that transforms data into a fixed-length value, called a hash or a digest, that uniquely represents the original data. Hashing can be used to validate the integrity of data communicated between production databases and a big data analytics system by comparing the hash values of the data before and after the communication. If the hash values match, the data has not been altered; if they differ, the data has been tampered with or corrupted. Hashing is a better security control than encrypting, running and comparing the count function, or hosting a digital certificate for this purpose because:
* Encrypting in-scope data sets can protect the confidentiality of the data, but not necessarily the integrity.
Encryption algorithms can be broken or bypassed by malicious actors, or encryption keys can be compromised or lost. Moreover, encryption adds overhead to the communication process and may affect the performance of the big data analytics system.
* Running and comparing the count function within the in-scope data sets can only verify the number of records or elements in the data sets, but not the content or quality of the data. The count function cannot detect any changes or errors in the data values, such as missing, duplicated, corrupted, or manipulated data.
* Hosting a digital certificate for in-scope data sets can provide authentication and non-repudiation for the data sources, but not integrity for the data itself. A digital certificate is a document that contains information about the identity and public key of an entity, such as a person, organization, or device. A digital certificate does not contain or verify the actual data that is communicated between production databases and a big data analytics system.
References:

* Ensuring Data Integrity with Hash Codes
* Database Security: An Essential Guide
* Control methods of Database Security

NEW QUESTION: 401
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)
Explanation/Reference:
Explanation:
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: 402
Which of the following controls is MOST important for ensuring the integrity of system interfaces?
A. IT operator monitoring
B. Periodic audits
C. File counts
D. File checksums
Answer: (SHOW ANSWER)

NEW QUESTION: 403
Which of the following should be done FIRST when planning a penetration test?
A. Obtain management consent for the testing
B. Define the testing scope.

C. Execute nondisclosure agreements (NDAs).
D. Determine reporting requirements for vulnerabilities
Answer: C (LEAVE A REPLY)

NEW QUESTION: 404
Which of the following is an analytical review procedure for a payroll system?
A. Performing penetration attempts on the payroll system
B. Testing hours reported on time sheets
C. Performing reasonableness tests by multiplying the number of employees by the average wage rate
D. Evaluating the performance of the payroll system using benchmarking software
Answer: C (LEAVE A REPLY)

NEW QUESTION: 405
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. Some KPIs are not documented
B. KPI data is not being analyzed
C. KPIs are not clearly defined
D. KPIs have never been updated
Answer: (SHOW ANSWER)

NEW QUESTION: 406
An IS audit manager is reviewing workpapers for a recently completed audit of the corporate disaster recovery test. Which of the following should the IS audit manager specifically review to substantiate the conclusions?
A. Prior audit reports involving other corporate disaster recovery audits
B. Summary memos reflecting audit opinions regarding noted weaknesses
C. Overviews of interviews between data center personnel and the auditor
D. Detailed evidence of the successes and weaknesses of all contingency testing
Answer: (SHOW ANSWER)

NEW QUESTION: 407

The BEST way to evaluate the effectiveness of a newly developed application is to:
A. perform a post-implementation review,
B. analyze load-testing results,
C. review acceptance-testing results
D. perform a pre-implementation renew.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 408
A database administrator is responsible for:
A. defining data ownership.
B. establishing operational standards for the data dictionary.
C. creating the logical and physical database.
D. establishing ground rules for ensuring data integrity and security.
Answer: C (LEAVE A REPLY)
A database administrator is responsible for creating and controlling the logical and physical database. Defining data ownership resides with the head of the user department or top management if the data is common to the organization. IS management and the data administrator are responsible for establishing operational standards for the data dictionary. Establishing ground rules for ensuring data integrity and security in line with the corporate security policy is a function of the security administrator.

NEW QUESTION: 409
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 identify unusual fluctuations or changes in any employee's monthly pay
B. To collect statistical information in preparation for future pay scale reviews
C. To evaluate gaps between employee performance and salary adjustments
D. To verify the accuracy of bank account information for payroll deposit
Answer: A (LEAVE A REPLY)

NEW QUESTION: 410
The PRIMARY purpose of a configuration management system is to:
A. track software updates.
B. define baselines for software.
C. support the release procedure.
D. standardize change approval.
Answer: (SHOW ANSWER)
Explanation
A configuration management system is a process that establishes and maintains the consistency of a product's attributes throughout its life cycle. It helps to identify and control the functional and

physical characteristics of a product, and to record and report any changes to those characteristics. A configuration management system also supports the audit of the product to verify its conformance to requirements.
One of the key activities of a configuration management system is to define baselines for software. A baseline is a fixed reference point that serves as a basis for comparison and measurement. A baseline can be established for any configuration item, such as a requirement, a design document, a test plan, or a software component. A baseline helps to ensure that the software product meets its intended purpose and quality standards, and that any changes to the software are controlled and documented.
A configuration management system also supports other activities, such as tracking software updates, supporting the release procedure, and standardizing change approval, but these are not its primary purpose.
Therefore, the other options are incorrect.
References: : What is configuration management - Red Hat : Configuration Management | Definition, Importance & Benefits - ServerWatch

NEW QUESTION: 411
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)
Section: Protection of Information Assets
Explanation:
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: 412
Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:
A. meets or exceeds industry security standards.
B. agrees to be subject to external security reviews.
C. has a good market reputation for service and experience.
D. complies with security policies of the organization.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
It is critical that an independent security review of an outsourcing vendor be obtained because customer credit information will be kept there. Compliance with security standards or organization

policies is important, but there is no way to verify or prove that that is the case without an independent review.
Though long experience in business and good reputation is an important factor to assess service quality, the business cannot outsource to a provider whose security control is weak.

NEW QUESTION: 413
The MOST likely effect of the lack of senior management commitment to IT strategic planning is:
A. a lack of investment in technology.
B. a lack of a methodology for systems development.
C. technology not aligning with the organization's objectives.
D. an absence of control over technology contracts.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

NEW QUESTION: 414
Stress testing should ideally be earned out under a:
A. test environment with production workloads.
B. production environment with production workloads.
C. production environment with test data.
D. test environment with test data.
Answer: A (LEAVE A REPLY)
Stress testing is a type of performance testing that evaluates the behavior and reliability of a system under extreme conditions, such as high workload, limited resources, or concurrent users. Stress testing should ideally be carried out under a test environment with production workloads, as this would simulate the most realistic and demanding scenario for the system without affecting the actual production environment. A production environment with production workloads is not suitable for stress testing, as it could cause disruption or damage to the system and its users. A production environment with test data is not suitable for stress testing, as it could compromise the integrity and security of the production data. A test environment with test data is not suitable for stress testing, as it could underestimate the potential issues and risks that could occur in the production environment. References:
* CISA Review Manual, 27th Edition, pages 471-4721
* CISA Review Questions, Answers & Explanations Database, Question ID: 261

NEW QUESTION: 415

Which of the following methods would BEST ensure that IT strategy is in line with business strategy?
A. Break-even point analysis
B. IT value analysis
C. Business impact analysis (BIA)
D. Critical path analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 416
A company has decided to implement an electronic signature scheme based on public key infrastructure.
The user's private key will be stored on the computer's hard drive and protected by a password.
The MOST significant risk of this approach is:
A. use of the user's electronic signature by another person if the password is compromised.
B. forgery by using another user's private key to sign a message with an electronic signature.
C. impersonation of a user by substitution of the user's public key with another person's public key.
D. forgery by substitution of another person's private key on the computer.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The user's digital signature is only protected by a password. Compromise of the password would enable access to the signature. This is the most significant risk. Choice B would require subversion of the public key infrastructure mechanism, which is very difficult and least likely. Choice C would require that the message appear to have come from a different person and therefore the true user's credentials would not be forged. Choice D has the same consequence as choice C.

NEW QUESTION: 417
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)
Section: Information System Operations, Maintenance and Support
Explanation:
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.
Reference:
CISA review manual 2014 page number 265

NEW QUESTION: 418
An IS auditor has been asked to audit the proposed acquisition of new computer hardware. The auditor's PRIMARY concern Is that:
A. the implementation plan meets user requirements.
B. a full, visible audit trail will be Included.
C. a dear business case has been established.
D. the new hardware meets established security standards
Answer: C (LEAVE A REPLY)
Explanation
The IS auditor's primary concern when auditing the proposed acquisition of new computer hardware is that a clear business case has been established. A business case is a document that justifies the need, feasibility, and benefits of a proposed project or investment. A clear business case can help to ensure that the acquisition of new computer hardware is aligned with the organization's goals, objectives, and requirements, and that it provides value for money and return on investment. The other options are not as important as establishing a clear business case, as they do not address the rationale or justification for acquiring new computer hardware.
References: CISA Review Manual, 27th Edition, page 467

NEW QUESTION: 419
Following significant business model changes, which of the following is the MOST important consideration when updating the IT policy?
A. The policy is integrated into job descriptions.
B. The policy is aligned with industry standards and best practice.
C. The policy is endorsed by IT leadership.
D. The policy is compliant with relevant laws and regulations.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 420
An incorrect version of the source code was amended by a development team. This MOST likely indicates a weakness in:
A. incident management.
B. quality assurance (QA).
C. change management.
D. project management.
Answer: C (LEAVE A REPLY)
Explanation

A weakness in change management is the most likely cause of an incorrect version of source code being amended by a development team. Change management is the process of controlling and documenting changes to IT systems and software. It ensures that changes are authorized, tested, and implemented in a controlled manner. If change management is weak, there is a risk of using outdated or incorrect versions of source code, which can lead to errors, defects, or security vulnerabilities in the software.

NEW QUESTION: 421
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. Industry standards
B. The business impact analysis (BIA)
C. The business objectives
D. Previous audit recommendations
Answer: (SHOW ANSWER)
Section: Governance and Management of IT

NEW QUESTION: 422
When reviewing a contract for a disaster recovery hot site, which of the following would be the MOST significant omission?
A. Audit rights
B. Testing procedures
C. Exposure coverage
D. Equipment provided
Answer: (SHOW ANSWER)
Section: Protection of Information Assets

NEW QUESTION: 423
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: 424
The PRIMARY role of an IS auditor in the remediation of problems found during an audit engagement is to:
A. help auditee management by providing the solution.
B. take ownership of the problems and oversee remediation efforts.
C. present updated policies to management for approval.
D. explain the findings and provide general advice.
Answer: (SHOW ANSWER)

NEW QUESTION: 425
Which of the following would BEST support a business case to implement a data leakage prevention (DLP) solution?
A. An unusual upward trend in outbound email volume
B. Lack of visibility into previous data leakage incidents
C. Industry benchmark of DLP investments
D. A risk assessment on the threat of data leakage
Answer: D (LEAVE A REPLY)
Section: Protection of Information Assets

NEW QUESTION: 426
Which of the following attack involves slicing small amount of money from a computerize transaction or account?
A. Eavesdropping
B. Traffic Analysis
C. Salami
D. Masquerading
Answer: C (LEAVE A REPLY)
Explanation/Reference:

Salami slicing or Salami attack refers to a series of many small actions, often performed by clandestine means, that as an accumulated whole produces a much larger action or result that would be difficult or unlawful to perform all at once. The term is typically used pejoratively. Although salami slicing is often used to carry out illegal activities, it is only a strategy for gaining an advantage over time by accumulating it in small increments, so it can be used in perfectly legal ways as well.

An example of salami slicing, also known as penny shaving, is the fraudulent practice of stealing money repeatedly in extremely small quantities, usually by taking advantage of rounding to the nearest cent (or other monetary unit) in financial transactions. It would be done by always rounding down, and putting the fractions of a cent into another account. The idea is to make the change small enough that any single transaction will go undetected.

In information security, a salami attack is a series of minor attacks that together results in a larger attack.

Computers are ideally suited to automating this type of attack.

The following answers are incorrect:

Eavesdropping - is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them." 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.

Masquerading - A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.

Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network. The amount of access masquerade attackers get depends on the level of authorization they've managed to attain. As such, masquerade attackers can have a full smorgasbord of cybercrime opportunities if they've gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

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

http://searchfinancialsecurity.techtarget.com/definition/eavesdropping

http://en.wikipedia.org/wiki/Salami_slicing

http://en.wikipedia.org/wiki/Eavesdropping

http://en.wikipedia.org/wiki/Traffic_analysis

http://www.techopedia.com/definition/4020/masquerade-attack

NEW QUESTION: 427
The use of statistical sampling procedures helps minimize:
A. Detection risk
B. Business risk
C. Controls risk
D. Compliance risk
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The use of statistical sampling procedures helps minimize detection risk.

NEW QUESTION: 428
What can be implemented to provide the highest level of protection from external attack?
A. Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
B. Configuring the firewall as a screened host behind a router
C. Configuring the firewall as the protecting bastion host
D. Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host provides a higher level of protection from external attack than all other answers.

NEW QUESTION: 429
Structured programming is BEST described as a technique that:
A. provides knowledge of program functions to other programmers via peer reviews.
B. reduces the maintenance time of programs by the use of small-scale program modules.
C. makes the readable coding reflect as closely as possible the dynamic execution of the program.
D. controls the coding and testing of the high-level functions of the program in the development process.
Answer: (SHOW ANSWER)
A characteristic of structured programming is smaller, workable units. Structured programming has evolved because smaller, workable units are easier to maintain. Structured programming is a style of programming which restricts the kinds of control structures. This limitation is not crippling. Any program can be written with allowed control structures. Structured programming is sometimes referred to as go-to-less programming, since a go-to statement is not allowed. This is perhaps the most well known restriction of the style, since go-to statements were common at the

time structured programming was becoming more popular. Statement labels also become unnecessary, except in languages where subroutines are identified by labels.

NEW QUESTION: 430
Which of the following is the MOST appropriate and effective fire suppression method for an unstaffed computer room?
A. Fire extinguishers
B. Water sprinkler
C. Carbon dioxide (CO2)
D. Dry pipe
Answer: C (LEAVE A REPLY)

NEW QUESTION: 431
During an integrated audit at a retail bank, an IS auditor is evaluating whether monthly service fees are appropriately charged for business accounts and waived for individual consumer accounts. Which of the following test approaches would utilize data analytics to facilitate the testing?
A. Attempt to charge a monthly service fee to an individual consumer account.
B. Compare the system configuration settings with the business requirements document.
C. Evaluate whether user acceptance testing plans were designed and executed appropriately.
D. Review customer accounts over the last year to determine whether appropriate charges were applied.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 432
Which of the following BEST describes the role of a document owner when implementing a data classification policy in an organization?
A. Classifies documents to correctly reflect the level of sensitivity of information they contain
B. Classifies documents in accordance with industry standards and best practices
C. Defines the conditions under which documents containing sensitive information may be transmitted
D. Ensures documents are handled in accordance with the sensitivity of information they contain
Answer: A (LEAVE A REPLY)

NEW QUESTION: 433
An IS auditor is evaluating the security of an organization's data backup process, which includes the
transmission of daily incremental backups to a dedicated offsite server. Which of the following findings
poses the GREATEST risk to the organization?
A. Backup transmissions are not encrypted

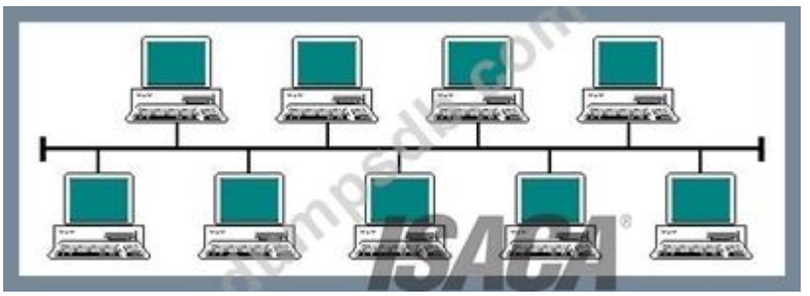
B. Backup transmissions occasionally fail
C. Data recovery testing is conducted once per year
D. The archived data log is incomplete
Answer: A (LEAVE A REPLY)
Section: The process of Auditing Information System
Explanation

NEW QUESTION: 434
Which of the following functionality is NOT supported by SSL protocol?
A. Confidentiality
B. Integrity
C. Authentication
D. Availability
Answer: D (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation/Reference:
The NOT is a keyword used in this question. You need to find out the functionality which is NOT provided
by SSL protocol. The SSL protocol provides:
Confidentiality
Integrity
Authentication, e.g. between client and server
Non-repudiation
For CISA exam you should know the information below about Secure Socket Layer (SSL) and Transport
Layer Security (TLS)
These are cryptographic protocols which provide secure communication on Internet. There are only slight
difference between SSL 3.0 and TLS 1.0. For general concept both are called SSL.
SSL is session-connection layer protocol widely used on Internet for communication between browser and
web servers, where any amount of data is securely transmitted while a session is established. SSL
provides end point authentication and communication privacy over the Internet using cryptography. In
typical use, only the server is authenticated while client remains unauthenticated. Mutual authentication
requires PKI development to clients. The protocol allows application to communicate in a way designed to
prevent eavesdropping, tampering and message forging.
SSL involves a number of basic phases

Peer negotiation for algorithm support
Public-key, encryption based key exchange and certificate based authentication
Symmetric cipher based traffic encryption.
SSL runs on a layer beneath application protocol such as HTTP, SMTP and Network News Transport
Protocol (NNTP) and above the TCP transport protocol, which forms part of TCP/IP suite.
SSL uses a hybrid hashed, private and public key cryptographic processes to secure transmission over the
INTERNET through a PKI.
The SSL handshake protocol is based on the application layer but provides for the security of the communication session too. It negotiates the security parameter for each communication section. Multiple
session can belong to one SSL session and the participating in one session can take part in multiple
simultaneous sessions.
The following were incorrect answers:
Confidentiality - It is supported by the SSL Protocol
Integrity -It is supported by the SSL Protocol
Authentication - It is supported by the SSL protocol
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 352

NEW QUESTION: 435
What should be the GREATEST concern to an IS auditor when employees use portable media (MP3 players, flash drives)?
A. The copying of sensitive data on them
B. The copying of songs and videos on them
C. The cost of these devices multiplied by all the employees could be high
D. They facilitate the spread of malicious code through the corporate network
Answer: A (LEAVE A REPLY)
The MAIN concern with MP3 players and flash drives is data leakage, especially sensitive information. This could occur if the devices were lost or stolen. The risk when copying songs and videos is copyright infringement, but this is normally aless important risk than information leakage. Choice C is hardly an issue because employees normally buy the portable media with their own funds. Choice D is a possible risk, but not as important as information leakage and can be reduced by other controls.

NEW QUESTION: 436
Identify the LAN topology from below diagram presented below:



bus topology

A. Bus

B. Star

C. Ring

D. Mesh

Answer: A (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.

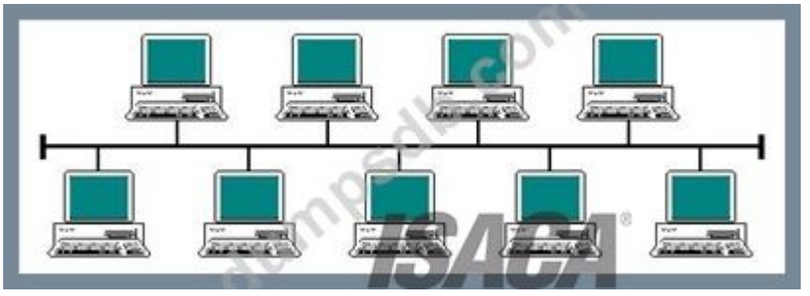
Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless 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

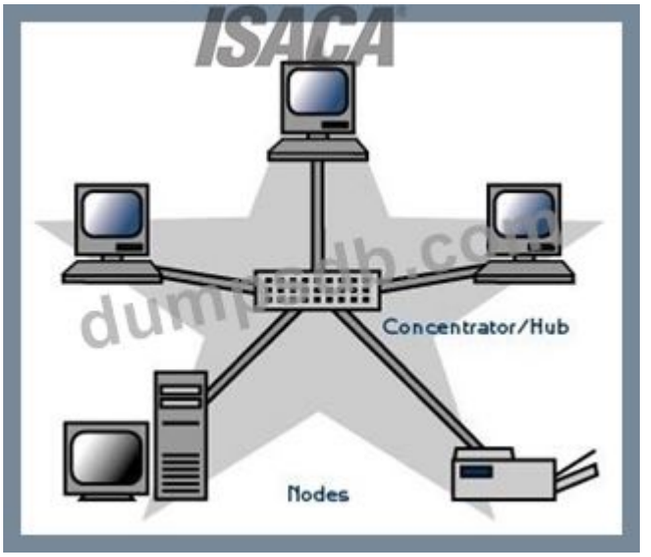


Image from: http://fcit.usf.edu/network/chap5/pics/star.gif
Ring

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

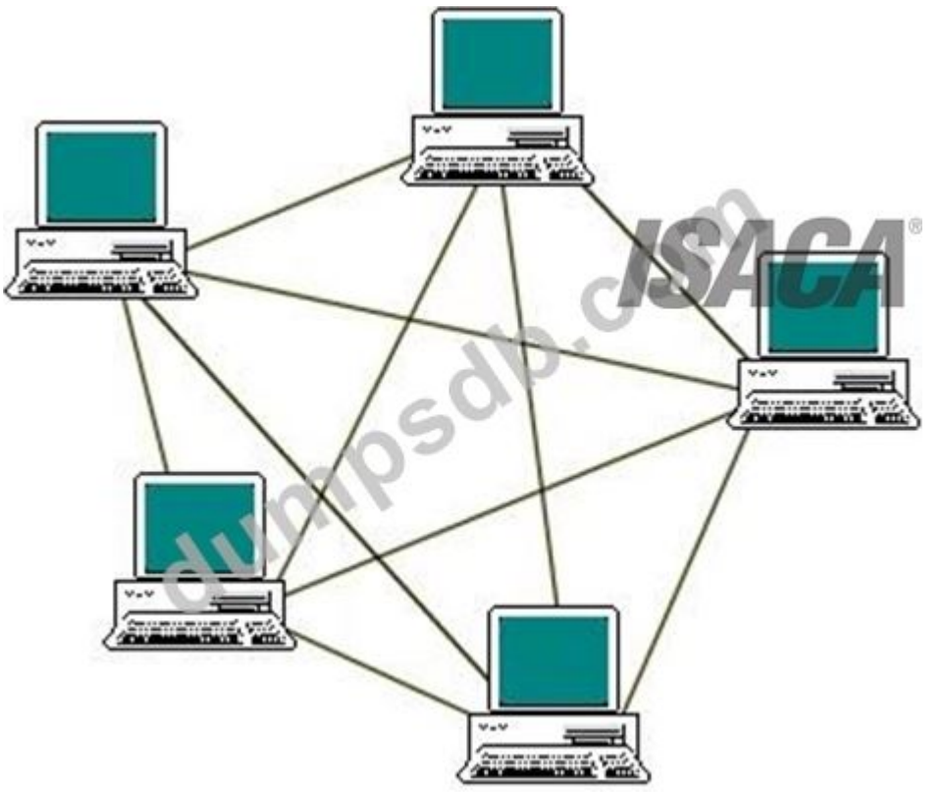


Image from:
http://www.technologyuk.net/telecommunications/networks/images/mesh_topology.gif Fully connected mesh topology A fully connected network is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network 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: 437
Which of the following should an IS auditor expect to see in a network vulnerability assessment?
A. Malicious software and spyware
B. Misconfiguration and missing updates
C. Zero-day vulnerabilities
D. Security design flaws
Answer: B (LEAVE A REPLY)

NEW QUESTION: 438
An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:
A. hardware configuration.
B. access control software.
C. ownership of intellectual property.
D. application development methodology.
Answer: (SHOW ANSWER)
Of the choices, the hardware and access control software is generally irrelevant as long as the functionality, availability and security can be affected, which are specific contractual obligations. Similarly, the development methodology should be ofno real concern. The contract must, however, specify who owns the intellectual property (i.e., information being processed, application programs). Ownership of intellectual property will have a significant cost and is a key aspect to be defined in an outsourcing contract.

NEW QUESTION: 439
An IS auditor identified hard-coded credentials within the source code of recently developed software when evaluating its readiness for implementation. Which of following would be the auditor's BEST recommendation?
A. Ensure source code reviews and debugging are performed and documented
B. Ensure revisions of source code can be tracked and rollback can be performed.
C. Ensure log reports are retained of all persons updating software source code.
D. Ensure documented evidence of source code being kept in escrow is retained.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 440
The BEST access strategy while configuring a firewall would be to:
A. permit access to all and log the activity.
B. permit access to all but deny selected.
C. deny access to all except authorized programs.
D. deny access to all but permit selected.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 441
Which of the following provides re BEST evidence that outsourced provider services are being properly managed?
A. Internal performance standards align with corporate strategy.
B. The service level agreement (SLA) includes penalties tor non-performance.
C. The vendor provides historical data to demonstrate its performance.
D. Adequate action is taken for noncompilance with the service level agreement (SLA).
Answer: D (LEAVE A REPLY)

NEW QUESTION: 442
An organization's enterprise architecture (EA) department decides to change a legacy system's components while maintaining its original functionality. Which of the following is MOST important for an IS auditor to understand when reviewing this decision?
A. The current business capabilities delivered by the legacy system
B. The proposed network topology to be used by the redesigned system
C. The data flows between the components to be used by the redesigned system
D. The database entity relationships within the legacy system
Answer: A (LEAVE A REPLY)
When reviewing an enterprise architecture (EA) department's decision to change a legacy system's components while maintaining its original functionality, an IS auditor should understand the current business capabilities delivered by the legacy system, as this would help to evaluate whether the change is justified, feasible, and aligned with the business goals and needs. The proposed network topology to be used by the redesigned system, the data flows between the components to be used by the redesigned system, and the database entity relationships within the legacy system are technical details that are less relevant for an IS auditor to understand when reviewing this decision. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 443
Which of the following BEST facilitates compliance with requirements mandating the security of confidential data?
A. Standardized escalation protocols for breaches
B. Encryption of external data transmissions
C. Signed acknowledgment of security policies
D. Classification of data
Answer: D (LEAVE A REPLY)

NEW QUESTION: 444

Which of the following control testing approaches is BEST used to evaluate a control's ongoing effectiveness by comparing processing results to independently calculated data?
A. Integrated test facility (ITF)
B. Embedded audit modules
C. Statistical sampling
D. Sample-based re-performance
Answer: C (LEAVE A REPLY)

NEW QUESTION: 445
An IS auditor will be testing accounts payable controls by performing data analytics on the entire population transactions. Which of the following is MOST important for the auditor to confirm when sourcing the population data?
A. There is no privacy information in the data.
B. The data analysis tools have been recently updated.
C. The data can be obtained in a timely manner.
D. The data is taken directly from the system.
Answer: A (LEAVE A REPLY)
Section: The process of Auditing Information System

NEW QUESTION: 446
Which of the following is MOST important for an IS auditor to determine during the detailed design phase of a system development project?
A. Acceptance test criteria have been developed.
B. Program coding standards have been followed.
C. Data conversion procedures have been established.
D. The design has been approved by senior management.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 447
Which of the following is the BEST way to evaluate the effectiveness of access controls to an internal
network?
A. Perform a system penetration test
B. Test compliance with operating procedures
C. Review access rights
D. Review router configuration tables
Answer: A (LEAVE A REPLY)
Section: The process of Auditing Information System

NEW QUESTION: 448

An internal audit department recently established a quality assurance (QA) program. Which of the following activities Is MOST important to include as part of the QA program requirements?
A. Long-term Internal audit resource planning
B. Ongoing monitoring of the audit activities
C. Analysis of user satisfaction reports from business lines
D. Feedback from Internal audit staff
Answer: B (LEAVE A REPLY)
Explanation
Ongoing monitoring of the audit activities is the most important activity to include as part of the quality assurance (QA) program requirements for an internal audit department. An IS auditor should perform regular reviews and evaluations of the audit processes, methods, standards, and outcomes to ensure that they comply with the QA program objectives and criteria. This will help to maintain and improve the quality and consistency of the audit services and deliverables. The other options are less important activities to include as part of the QA program requirements, as they may involve long-term resource planning, user satisfaction reports, or feedback from internal audit staff. References:
CISA Review Manual (Digital Version), Chapter 2, Section 2.61
CISA Review Questions, Answers & Explanations Database, Question ID 224

NEW QUESTION: 449
An IS auditor learns that an in-house system development life cycle (SDLC) project has not met user specifications. The auditor should FIRST examine requirements from which of the following phases?
A. Configuration phase
B. User training phase
C. Quality assurance (QA) phase
D. Development phase
Answer: (SHOW ANSWER)
Explanation
The quality assurance (QA) phase is the phase where the IS auditor should first examine requirements from an in-house SDLC project that has not met user specifications. This is because the QA phase is the phase where the system is tested and verified against the user specifications and the design specifications to ensure that it meets the functional and non-functional requirements, as well as the quality standards and expectations. The QA phase involves various testing activities, such as unit testing, integration testing, system testing, acceptance testing, performance testing, security testing, etc., to identify and resolve any defects, errors, or deviations from the specifications12.
The configuration phase is not the phase where the IS auditor should first examine requirements from an in-house SDLC project that has not met user specifications. The configuration phase is the phase where the system is installed and configured on the target environment, such as hardware, software, network, etc., to prepare it for deployment and operation. The configuration

phase may involve activities such as installation, customization, migration, integration, etc., to ensure that the system is compatible and interoperable with the existing infrastructure and systems34.
The user training phase is not the phase where the IS auditor should first examine requirements from an in-house SDLC project that has not met user specifications. The user training phase is the phase where the end-users are trained and educated on how to use the system effectively and efficiently. The user training phase may involve activities such as developing training materials, conducting training sessions, providing feedback and support, etc., to ensure that the users are familiar and comfortable with the system features and functions56.
The development phase is not the phase where the IS auditor should first examine requirements from an in-house SDLC project that has not met user specifications. The development phase is the phase where the system is coded and built based on the design specifications and the user specifications. The development phase may involve activities such as programming, debugging, documenting, etc., to create a working prototype or a final product of the system

NEW QUESTION: 450
The PRIMARY objective of Secure Sockets Layer (SSL) is to ensure:
A. only the sender and receiver are able to encrypt/decrypt the data.
B. the sender and receiver can authenticate their respective identities.
C. the alteration of transmitted data can be detected.
D. the ability to identify the sender by generating a one-time session key.
Answer: A (LEAVE A REPLY)
SSL generates a session key used to encrypt/decrypt the transmitted data, thus ensuring its confidentiality. Although SSL allows the exchange of X509 certificates to provide for identification and authentication, this feature along with choices C and D are not the primary objectives.

NEW QUESTION: 451
An IS auditor has completed the fieldwork phase of a network security review and is preparing the initial following findings should be ranked as the HIGHEST risk?
A. Network penetration tests are not performed
B. The network firewall policy has not been approved by the information security officer.
C. Network firewall rules have not been documented.
D. The network device inventory is incomplete.
Answer: (SHOW ANSWER)
The finding that should be ranked as the highest risk is that network penetration tests are not performed.
Network penetration tests are simulated cyberattacks that aim to identify and exploit the vulnerabilities and weaknesses of the network security controls, such as firewalls, routers, switches, servers, and devices.
Network penetration tests are essential for assessing the effectiveness and resilience of the network security posture, and for providing recommendations for improvement and remediation. If

network penetration tests are not performed, the organization may not be aware of the existing or potential threats and risks to its network, and may not be able to prevent or respond to real cyberattacks, which can result in data breaches, service disruptions, financial losses, reputational damage, and legal or regulatory penalties. The other findings are also important, but not as risky as the lack of network penetration tests, because they either do not directly affect the network security controls, or they can be addressed by documentation or approval processes.
References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

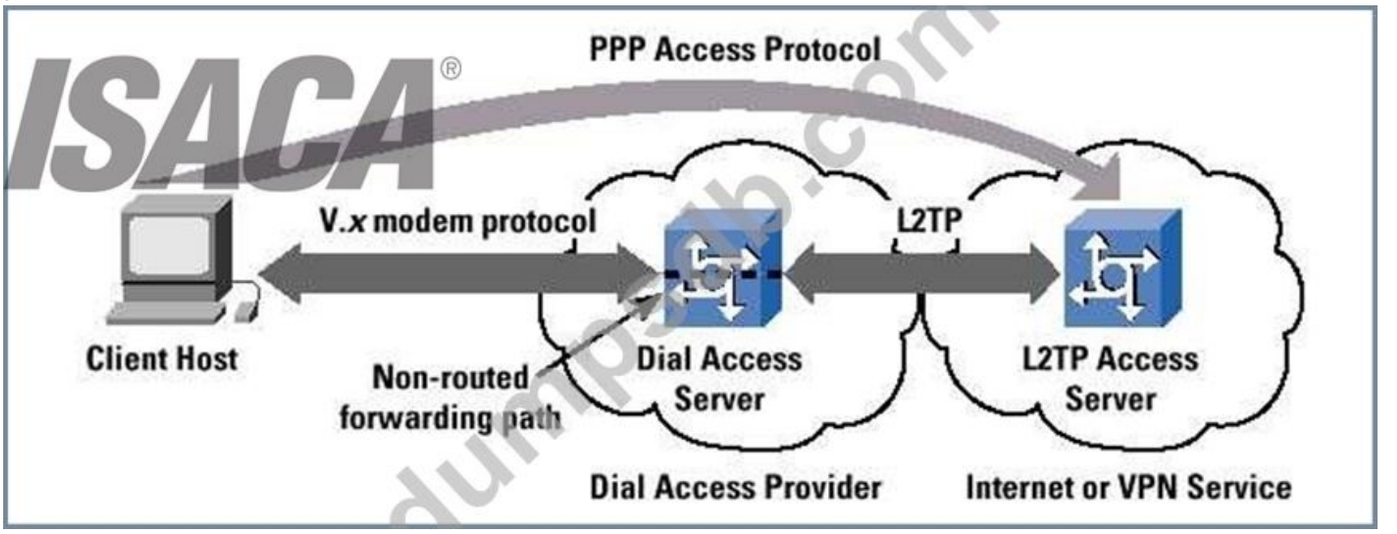
NEW QUESTION: 452
Following a security breach in which a hacker exploited a well-known vulnerability in the domain controller, an IS audit has been asked to conduct a control assessment. the auditor's BEST course of action would be to determine if:
A. The network traffic was being monitored.
B. the patches were updated.
C. The domain controller was classified for high availability.
D. The logs were monitored.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 453
Which of the following is the MOST important advantage of participating in beta testing of software products?
A. It increases an organization's ability to retain staff who prefer to work with new technology.
B. It improves vendor support and training.
C. It enhances security and confidentiality.
D. It enables an organization to gain familiarity with new products and their functionality.
Answer: (SHOW ANSWER)
Beta testing is the process of releasing a near-final version of a software product to a group of external users, known as beta testers, who provide feedback and report bugs based on their real-world experiences. Beta testingoffers various benefits for both the developers and the users of the software product. Some of these benefits are:
It reduces product failure risk via customer validation12.
It helps to test post-launch infrastructure1.
It helps to improve product quality via customer feedback12.

It allows for thorough bug detection and issue resolution3.
It enhances usability and user experience3.
It increases customer satisfaction and loyalty3.
Based on these benefits, the most important advantage of participating in beta testing of software products is
D). It enables an organization to gain familiarity with new products and their functionality. By being involved in beta testing, an organization can learn how to use the new product effectively, discover its features and benefits, and provide suggestions for improvement. This can help the organization to adopt the new product faster, easier, and more efficiently when it is officially released. It can also give the organization a competitive edge over other users who are not familiar with the new product.

NEW QUESTION: 454
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)
Section: Information System Operations, Maintenance and Support
Explanation:
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

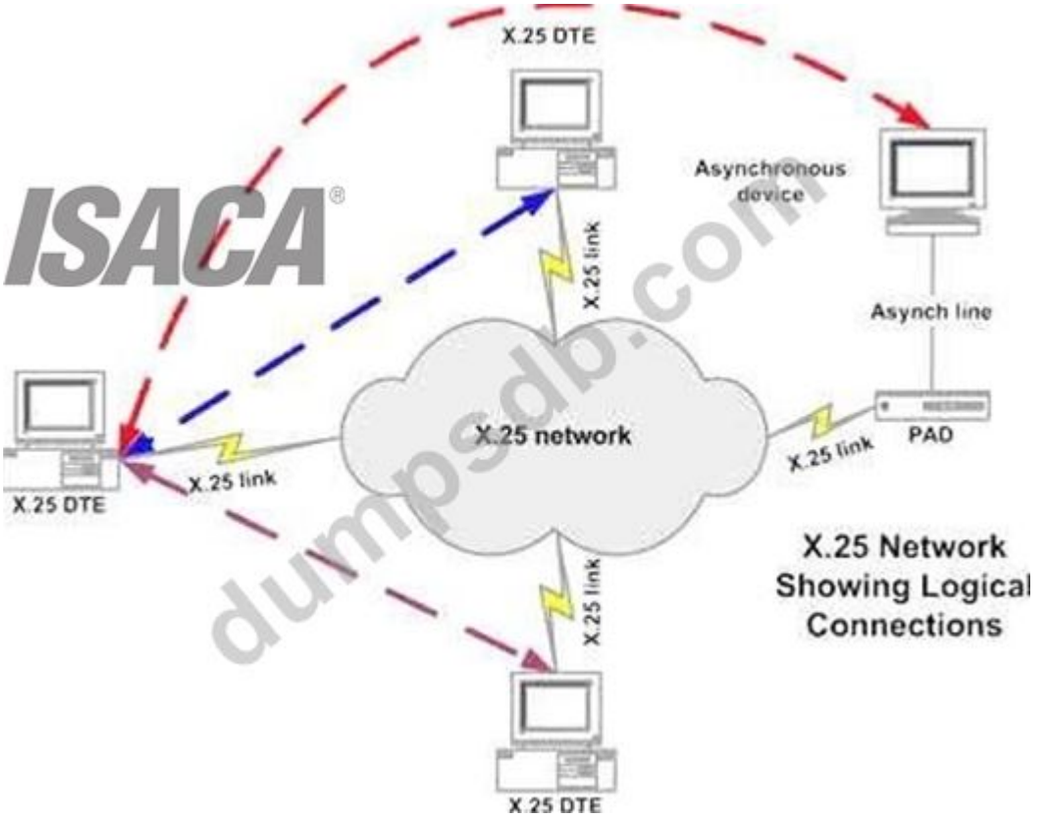
X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

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).

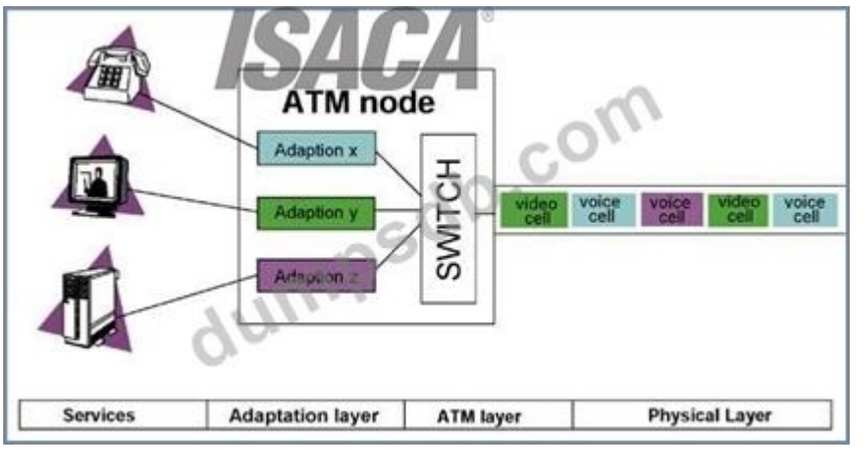
X.25 works at network and data link layer of an OSI model.

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

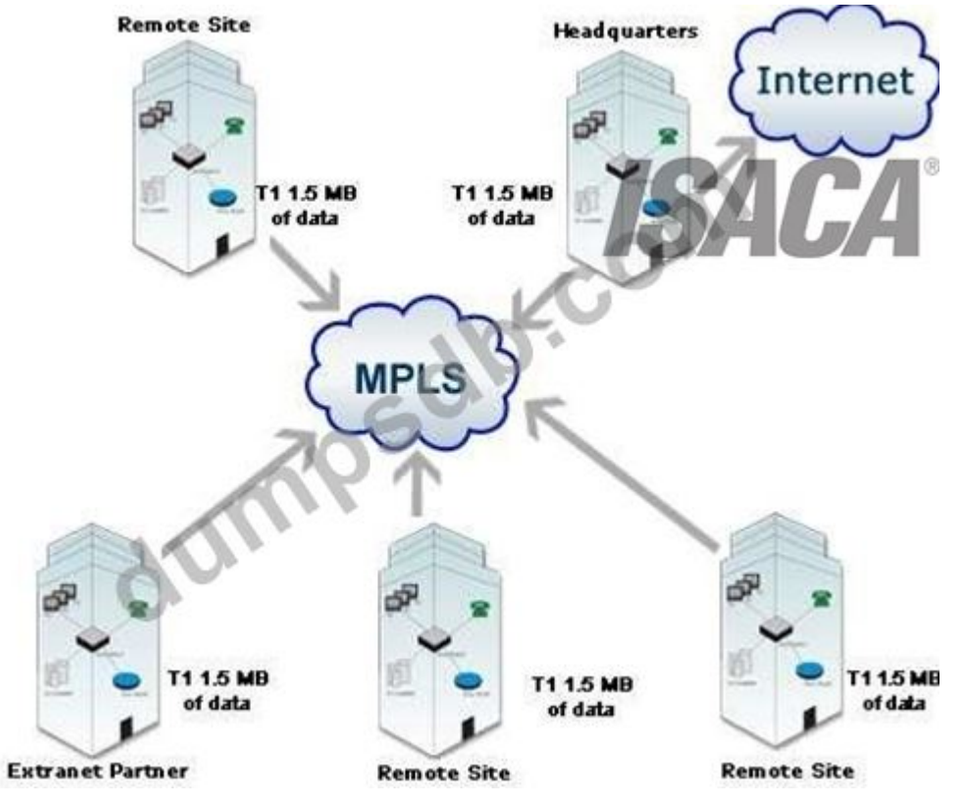
Asynchronous Transfer Mode (ATM)
Uses Cell switching method
High speed network technology used for LAN, MAN and WAN
Like a frame relay it is connection oriented technology which creates and uses fixed channel Data are segmented into fixed size cell of 53 bytes Some companies have replaces FDDI back-end with ATM Asynchronous Transfer Mode



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
Reference:
CISA review manual 2014 page number 266