ISACA.CISA.v2022-09-15.q220

Exam Code:	CISA
Exam Name:	Certified Information Systems Auditor
Certification Provider:	ISACA
Free Question Number:	220
Version:	v2022-09-15
# of views:	2105
# of Questions views:	2200
https://www.dumpsdb.com/dumps/ISACA/CISA/ISACA.CISA.v2022-09-15.q220	

NEW QUESTION: 1
.Who is responsible for the overall direction, costs, and timetables for systems-development projects?
A. The project sponsor
B. The project steering committee
C. Senior management
D. The project team leader
Answer: B (LEAVE A REPLY)
The project steering committee is responsible for the overall direction, costs, and timetables for systems-development projects.

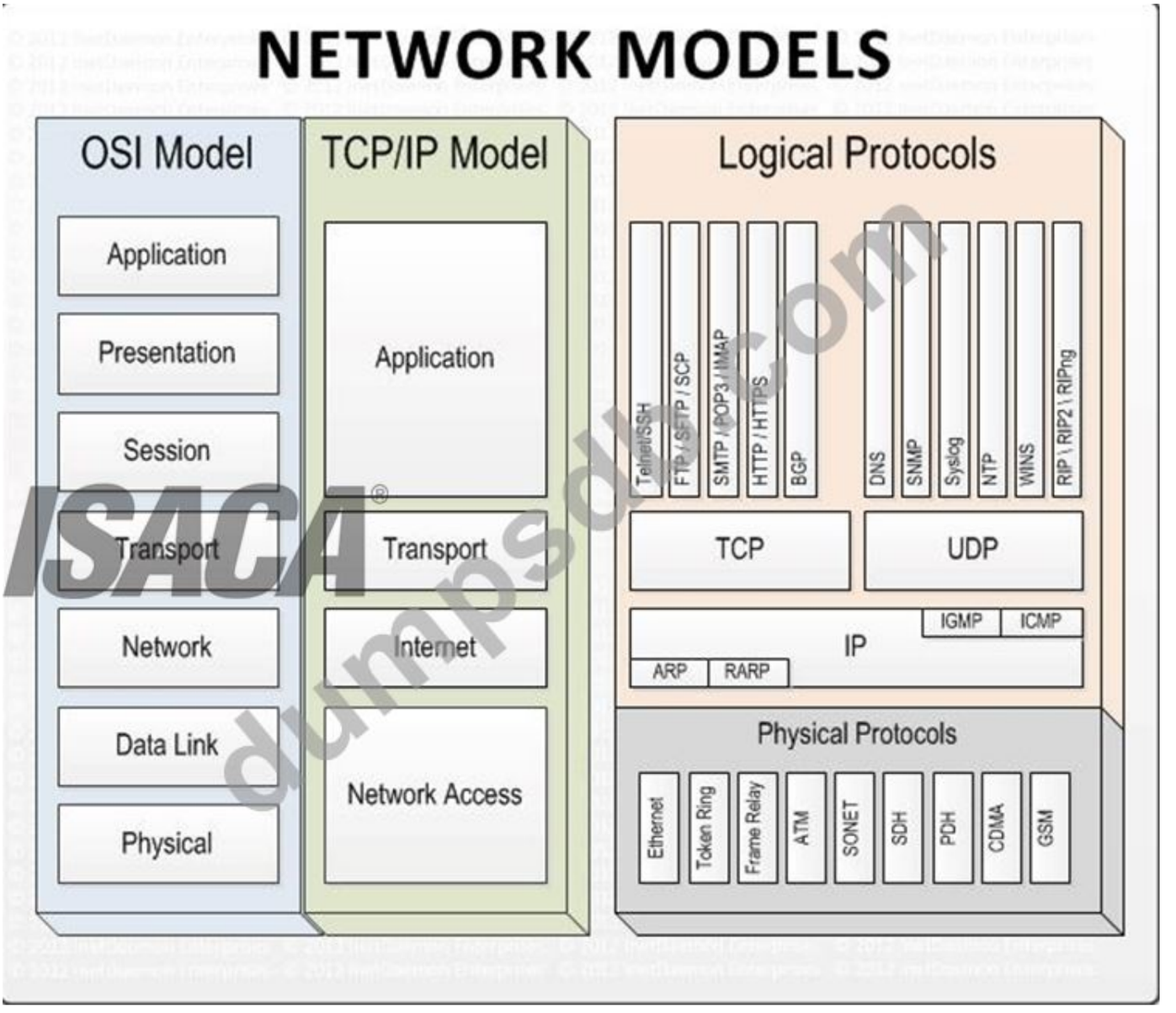
NEW QUESTION: 2
Which of the following fourth generation language is a development tools to generate lower level programming languages?
A. Query and report generator
B. Embedded database 4GLs
C. Relational database 4GL
D. Application generators
Answer: D (LEAVE A REPLY)
Section: Information System Acquisition, Development and Implementation Explanation:
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.
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.
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.
Reference:
CISA review manual 2014 Page number 209

NEW QUESTION: 3
From an IS auditor's perspective, which of the following would be the GREATEST risk associated with an incomplete inventory of deployed software in an organization?
A. Inability to determine the cost of deployed software
B. Inability to close unused ports on critical servers
C. Inability to identify unused licenses within the organization
D. Inability to deploy updated security patches
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
Which of the following is the INCORRECT "layer - protocol" mapping within the TCP/IP model?
A. Application layer - NFS
B. Transport layer - TCP
C. Network layer - UDP
D. LAN or WAN interface layer - point-to-point protocol
Answer: C (LEAVE A REPLY)
Explanation/Reference:

The word INCORRECT is the keyword used in the question.
You need to find out invalid layer-protocol mapping.
The UDP protocol works at 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

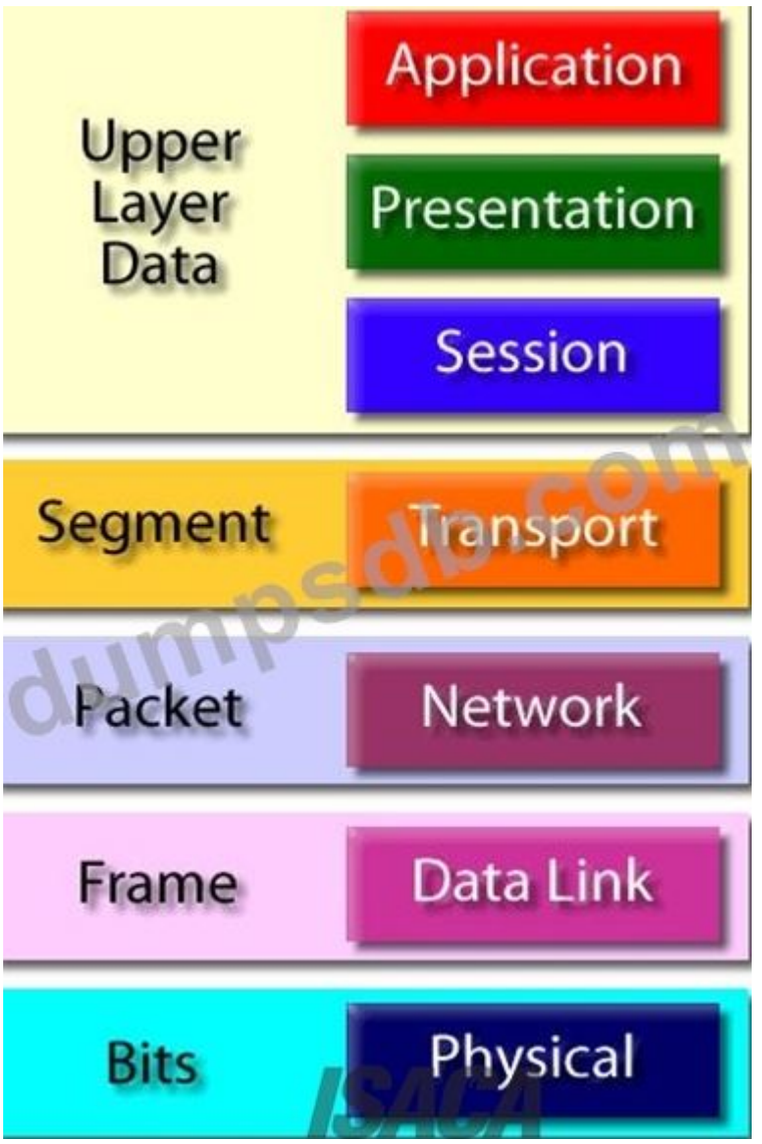
Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information 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 layer-protocol mapping in TCP/IP protocol.

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

CISA review manual 2014 page number 272

NEW QUESTION: 5

An IS auditor should carefully review the functional requirements in a system-development project to ensure that the project is designed to:

A. Meet business objectives

B. Enforce data security

C. Be culturally feasible

D. Be financially feasible

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation:

An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to meet business objectives.

NEW QUESTION: 6
Which of the following should be a concern to an IS auditor reviewing a wireless network?
A. 128-bit static-key WEP (Wired Equivalent Privacy) encryption is enabled.
B. SSID (Service SetIDentifier) broadcasting has been enabled.
C. Antivirus software has been installed in all wireless clients.
D. MAC (Media Access Control) access control filtering has been deployed.
Answer: (SHOW ANSWER)
SSID broadcasting allows a user to browse for available wireless networks and to access them without authorization. Choices A, C and D are used to strengthen a wireless network.

NEW QUESTION: 7
Which of the following is a form of Hybrid Cryptography where the sender encrypts the bulk of the data
using Symmetric Key cryptography and then communicates securely a copy of the session key to the
receiver?
A. Digital Envelope
B. Digital Signature
C. Symmetric key encryption
D. Asymmetric
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation/Reference:
A Digital Envelope is used to send encrypted information using symmetric keys, and the relevant session
key along with it. It is a secure method to send electronic document without compromising the data
integrity, authentication and non-repudiation, which were obtained with the use of symmetric keys.
A Digital envelope mechanism works as follows:
The symmetric key, which is used to encrypt the bulk of the date or message can be referred to as session
key. It is simply a symmetric key picked randomly in the key space.
In order for the receiver to have the ability to decrypt the message, the session key must be sent to the
receiver.
This session key cannot be sent in clear text to the receiver, it must be protected while in transit, else
anyone who have access to the network could have access to the key and confidentiality can easily be

compromised.
Therefore, it is critical to encrypt and protect the session key before sending it to the receiver. The session
key is encrypted using receiver's public key. Thus providing confidentiality of the key.
The encrypted message and the encrypted session key are bundled together and then sent to the receiver
who, in turn opens the session key with the receiver matching private key.
The session key is then applied to the message to get it in plain text.
The process of encrypting bulk data using symmetric key cryptography and encrypting the session key with
a public key algorithm is referred as a digital envelope. Sometimes people refer to it as Hybrid Cryptography as well.
The following were incorrect answers:
Digital-signature - A digital signature is an electronic identification of a person or entity created by using
public key algorithm and intended to verify to recipient the integrity of the data and the identity of the
sender. Applying a digital signature consist of two simple steps, first you create a message digest, then you
encrypt the message digest with the sender's private key. Encrypting the message digest with the private
key is the act of signing the message.
Symmetric Key Encryption - Symmetric encryption is the oldest and best-known technique. A secret key,
which can be a number, a word, or just a string of random letters, is applied to the text of a message to
change the content in a particular way. This might be as simple as shifting each letter by a number of
places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and
decrypt all messages that use this key.
Asymmetric Key Encryption - The term "asymmetric" stems from the use of different keys to perform these
opposite functions, each the inverse of the other - as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both. Public-key algorithms are based on mathematical problems which currently admit no efficient solution that are inherent in certain integer
factorization, discrete logarithm, and elliptic curve relationships. It is computationally easy for a user to
generate their own public and private key-pair and to use them for encryption and decryption. The strength

lies in the fact that it is "impossible" (computationally unfeasible) for a properly generated private key to be
determined from its corresponding public key. Thus the public key may be published without compromising
security, whereas the private key must not be revealed to anyone not authorized to read messages or
perform digital signatures. Public key algorithms, unlike symmetric key algorithms, do not require a secure
initial exchange of one (or more) secret keys between the parties.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 350 and 351
http://en.wikipedia.org/wiki/Public-key_cryptography

NEW QUESTION: 8
Which of the following is an IS auditor's BEST course of action upon learning that preventive controls have been replaced with detective and corrective controls'
A. Report the issue to management as the risk level has increased.
B. Verify the revised controls enhance the efficiency of related business processes.
C. Recommend the implementation of preventive controls in addition to the other controls.
D. Evaluate whether new controls manage the risk at an acceptable level.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 9
Which of the following is the BEST reason to implement a data retention policy?
A. To document business objectives for processing data within the organization
B. To establish a recovery point detective (RPO) for (toaster recovery procedures
C. To limit the liability associated with storing and protecting information
D. To assign responsibility and ownership for data protection outside IT
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Which of the following statement is NOT true about smoke detector?
A. The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised in the computer room floor
B. The smoke detector should produce an audible alarm when activated and be linked to a monitored station
C. The location of the smoke detector should be marked on the tiling for easy identification and access
D. Smoke detector should replace fire suppression system
Answer: D (LEAVE A REPLY)
Explanation/Reference:

The word NOT is the keyword used in the question. You need to find out a statement which is not applicable to smoke detector. Smoke detector should supplement, not replace, fire suppression system.
For CISA exam you should know below information about smoke detector.
The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised computer room floor.
The smoke detector should produce an audible alarm when activated be linked to a monitored station The location of the smoke detector should be marked on the tiling for easy identification and access.
Smoke detector should supplement, not replace, fire suppression system
The following were incorrect answers:
The other presented options are valid statement about smoke detector.
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number373

NEW QUESTION: 11
Which of the following statement is NOT true about smoke detector?
A. The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the
raised in the computer room floor
B. The smoke detector should produce an audible alarm when activated and be linked to a monitored
station
C. The location of the smoke detector should be marked on the tiling for easy identification and access
D. Smoke detector should replace fire suppression system
Answer: D (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation/Reference:
The word NOT is the keyword used in the question. You need to find out a statement which is not applicable to smoke detector. Smoke detector should supplement, not replace, fire suppression system.
For CISA exam you should know below information about smoke detector.
The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the
raised computer room floor.
The smoke detector should produce an audible alarm when activated be linked to a monitored station
The location of the smoke detector should be marked on the tiling for easy identification and access.
Smoke detector should supplement, not replace, fire suppression system

The following were incorrect answers:
The other presented options are valid statement about smoke detector.
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number373

NEW QUESTION: 12
Which of the following is the PRIMARY benefit of implementing configuration management for IT?
A. It establishes the dependency of application systems with various IT assets.
B. It provides visibility to the overall function and technical attributes of IT assets.
C. It helps automate change and release management processes in IT.
D. It helps audit in verifying IT conformance to business requirements.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 13
An IS auditor performing a review of the backup processing facilities should be MOST concerned that:
A. adequate fire insurance exists.
B. regular hardware maintenance is performed.
C. offsite storage of transaction and master files exists.
D. backup processing facilities are fully tested.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.

NEW QUESTION: 14
The most common problem in the operation of an intrusion detection system (IDS) is:
A. the detection of false positives.
B. receiving trap messages.
C. reject-error rates.
D. denial-of-service attacks.
Answer: A (LEAVE A REPLY)
Because of the configuration and the way IDS technology operates, the main problem in operating IDSs is the recognition (detection) of events that are not really security incidents-false positives, the equivalent of a false alarm. An IS auditorneeds to be aware of this and should check for implementation of related controls, such as IDS tuning, and incident handling procedures, such as the screening process to know if an event is a security incident or a false positive. Trap messages aregenerated by the Simple Network Management Protocol (SNMP)

agents when an important event happens, but are not particularly related to security or IDSs. Reject-error rate is related to
biometric technology and is not related to IDSs. Denial-of-service is a type of attack and is not a problem in the operation of IDSs.

NEW QUESTION: 15
Your final audit report should be issued:
A. after an agreement on the observations is reached.
B. before an agreement on the observations is reached.
C. if an agreement on the observations cannot reached.
D. without mentioning the observations.
E. None of the choices.
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Reporting can take the forms of verbal presentation, an issue paper or a written audit report summarizing observations and management's responses. After agreement is reached on the observations, a final report can be issued.

NEW QUESTION: 16
Which of the following incident management practices would BEST facilitate rapid resolution and reduce downtime from unplanned interruptions?
A. Ensuring incidents with unknown root causes are escalated
B. Ensuring the service desk is trained on issue resolution
C. Ensuring IT systems are monitored on a continual basis
D. Ensuring the service desk has access to catalogs of known errors
Answer: D (LEAVE A REPLY)

NEW QUESTION: 17
Which of the following term in business continuity defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences?
A. RPO
B. RTO

C. WRT

D. MTD

Answer: D (LEAVE A REPLY)

Explanation/Reference:

The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual

Business as usual

Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

Disaster Occurs

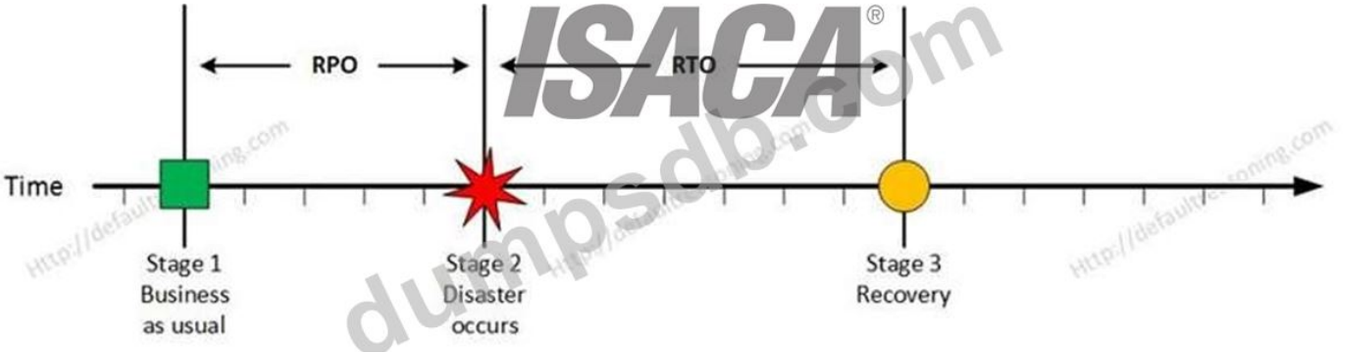


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

Recovery

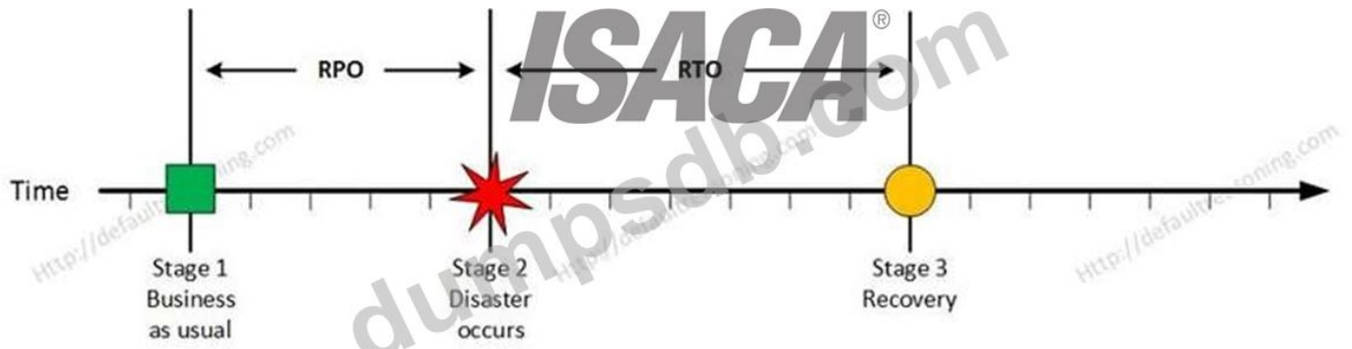


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production

Resume Production

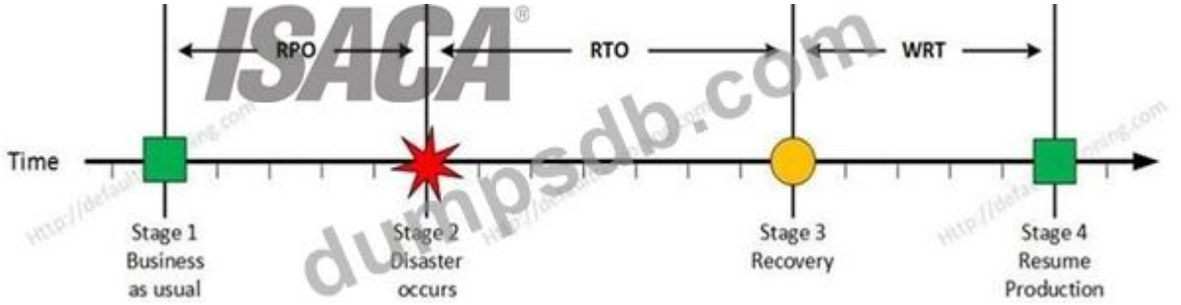


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available.

In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD

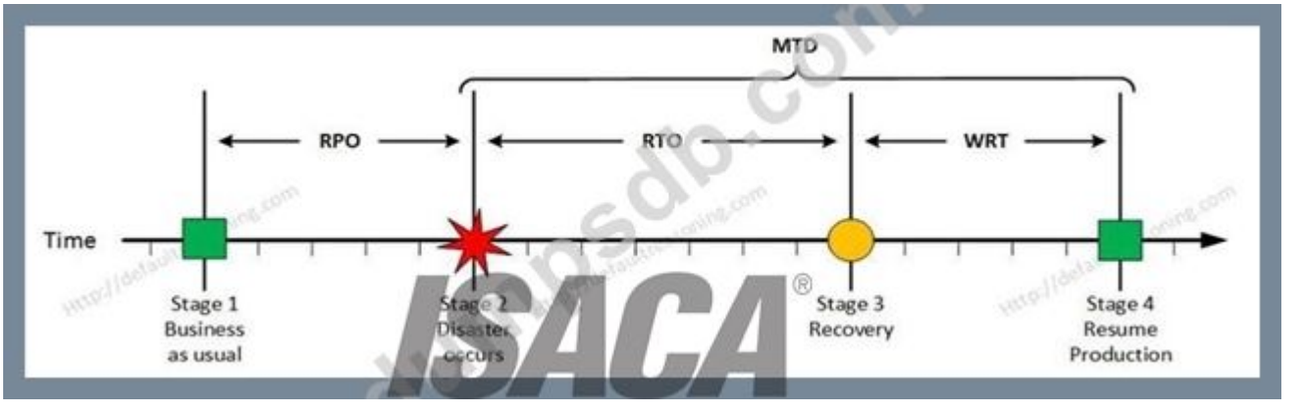


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.
The following answers are incorrect:
RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.
RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure.
In most cases this part is carried out by system administrator, network administrator, storage administrator etc.
WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc.
When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 284
http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

NEW QUESTION: 18
After an employee termination, a network account was removed, but the application account remained active.
To keep this issue from recurring, which of the following is the BEST recommendation?
A. Leverage shared accounts for the application.
B. Perform periodic access reviews.
C. Integrate application accounts with network single sign-on.
D. Retrain system administration staff.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Following significant organizational changes, which of the following is the MOST important consideration when updating the IT policy?
A. The policy is endorsed by senior executives.
B. The policy is integrated into job descriptions.
C. The policy is compliant with relevant laws and regulations.
D. The policy is aligned with industry standards and best practice.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 20
An IS auditor has been asked to audit a complex system with computerized and manual elements. Which of the following should be identified FIRST?
A. System risks
B. Input validation
C. Programmed controls
D. Manual controls
Answer: A (LEAVE A REPLY)

NEW QUESTION: 21
Which of the following is the MOST important action in recovering from a cyberattack?
A. Creation of an incident response team
B. Use of cybenforensic investigators
C. Execution of a business continuity plan
D. Filing an insurance claim
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The most important key step in recovering from cyberattacks is the execution of a business continuity plan to quickly and cost-effectively recover critical systems, processes and datA. The incident response team should exist prior to a cyberattack. When a cyberattack is suspected, cyberforensics investigators should be used to set up alarms, catch intruders within the network, and track and trace them over the Internet.
After taking the above steps, an organization may have a residual risk that needs to be insured and claimed for traditional and electronic exposures.

NEW QUESTION: 22
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: A (LEAVE A REPLY)

NEW QUESTION: 23
In an EDI process, the device which transmits and receives electronic documents is the:
A. communications handler.
B. EDI translator.
C. application interface.
D. EDI interface.

Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
A communications handler transmits and receives electronic documents between trading partners and/or
wide area networks (WANs).

NEW QUESTION: 24
Which of the following is the PRIMARY basis on which audit objectives are established?
A. Consideration of risks
B. Business strategy
C. Assessment of prior audits
D. Audit risk
Answer: (SHOW ANSWER)

NEW QUESTION: 25
During a disaster recovery test, an IS auditor observes that the performance of the disaster recovery site's server is slow. To find the root cause of this, the IS auditor should FIRST review the:
A. event error log generated at the disaster recovery site.
B. disaster recovery test plan.
C. disaster recovery plan (DRP).
D. configurations and alignment of the primary and disaster recovery sites.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Since the configuration of the system is the most probable cause, the IS auditor should review that first. If the issue cannot be clarified, the IS auditor should then review the event error log. The disaster recovery test plan and the disaster recovery plan (DRP) would not contain information about the system configuration.

NEW QUESTION: 26
Which of the following is the MOST important objective of data protection?
A. identifying persons who need access to information
B. Ensuring the integrity of information
C. Denying or authorizing access to the IS system
D. Monitoring logical accesses
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:

Maintaining data integrity is the most important objective of data security. This is a necessity if an organization is to continue as a viable and successful enterprise. The other choices are important techniques for achieving the objective of data integrity.

NEW QUESTION: 27
Which of the following is of greatest concern when performing an IS audit?
A. Users' ability to directly modify the database
B. Users' ability to submit queries to the database
C. Users' ability to indirectly modify the database
D. Users' ability to directly view the database
Answer: A (LEAVE A REPLY)
Explanation/Reference:
A major IS audit concern is users' ability to directly modify the database.

NEW QUESTION: 28
Time constraints and expanded needs have been found by an IS auditor to be the root causes for recent
violations of corporate data definition standards in a new business intelligence project.
Which of the following is the MOST appropriate suggestion for an auditor to make?
A. Achieve standards alignment through an increase of resources devoted to the project
B. Align the data definition standards after completion of the project
C. Delay the project until compliance with standards can be achieved
D. Enforce standard compliance by adopting punitive measures against violators
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Provided that data architecture, technical, and operational requirements are sufficiently documented, the
alignment to standards could be treated as a specific work package assigned to new project resources.
The usage of nonstandard data definitions would lower the efficiency of the new development, and increase
the risk of errors in critical business decisions. To change data definition standards after project conclusion
(choice B) is risky and is not a viable solution. On the other hand, punishing the violators (choice D) or
delaying the project (choice C) would be an inappropriate suggestion because of the likely damage to the
entire project profitability.

NEW QUESTION: 29

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

NEW QUESTION: 30
What is the PRIMARY benefit of an audit approach which requires reported findings to be issued together with related action plans, owners, and target dates?
A. it helps to ensure factual accuracy of findings
B. it establishes accountability for the action plans
C. it enforces action plan consensus between auditors and auditees
D. it facilitates easier audit follow-up
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
.The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a(n):
A. Implementor
B. Facilitator
C. Developer
D. Sponsor
Answer: B (LEAVE A REPLY)
The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a facilitator.

NEW QUESTION: 32
Upon receipt of the initial signed digital certificate the user will decrypt the certificate with the public key of the:
A. registration authority (RA).
B. certificate authority (CA).
C. certificate repository.
D. receiver.

Answer: (SHOW ANSWER)
A certificate authority (CA) is a network authority that issues and manages security credentials and public keys for message encryption. As a part of the public key infrastructure, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can issue a certificate. The CA signs the certificate with its private key for distribution to the user. Upon receipt, the user will decrypt the certificate with the CA's public key.

NEW QUESTION: 33
Which of the following should an IS auditor be MOST concerned with during a post-implementation review?
A. The system does not have a maintenance plan
B. The system contains several minor defects
C. The system was over budget by 15%
D. The system deployment was delayed by three weeks
Answer: A (LEAVE A REPLY)
Section: The process of Auditing Information System

NEW QUESTION: 34
An IT steering committee should review information systems PRIMARILY to assess:
A. whether IT processes support business requirements.
B. if proposed system functionality is adequate.
C. the stability of existing software.
D. the complexity of installed technology.
Answer: A (LEAVE A REPLY)
The role of an IT steering committee is to ensure that the IS department is in harmony with the organization's mission and objectives. To ensure this, the committee must determine whether IS processes support the business requirements. Assessing proposed additional functionality and evaluating software stability and the complexity of technology are too narrow in scope to ensure that IT processes are, in fact, supporting the organization's goals.

NEW QUESTION: 35
When determining whether a project in the design phase will meet organizational objectives, what is BEST to compare against the business case?
A. Project budget provisions
B. plan Project plan
C. Implementation
D. Requirements analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 36

An organization has implemented periodic reviews of logs showing privileged user activity production servers.
Which type of control has been established?
A. Protective
B. Corrective
C. Detective
D. Preventive
Answer: C (LEAVE A REPLY)

NEW QUESTION: 37
A new system is being developed by a vendor for a consumer service organization. The vendor will provide its proprietary software once system development is completed Which of the following is the MOST important requirement to include In the vendor contract to ensure continuity?
A. Source code for the software must be placed in escrow.
B. Continuous 24/7 support must be available.
C. The vendor must have a documented disaster recovery plan (DRP) in place.
D. The vendor must train the organization's staff to manage the new software
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?
A. User acceptance testing (UAT) occur for all reports before release into production
B. Organizational data governance practices be put in place
C. Standard software tools be used for report development
D. Management sign-off on requirements for new reports
Answer: B (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
This choice directly addresses the problem. An organization wide approach is needed to achieve effective management of data assets. This includes enforcing standard definitions of data elements, which is part of a data governance initiative. The other choices, while sound development practices, do not address the root cause of the problem described.

NEW QUESTION: 39
Which of the following BEST enables timely detection of changes in the IT environment to support informed decision making by management?
A. Continuous monitoring
B. Sampling checks on high-risk areas
C. Change management reports

D. Established key risk indicators (KRIs)
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets

NEW QUESTION: 40
Both statistical and nonstatistical sampling techniques:
A. permit the auditor to quantify and fix the level of risk
B. provide each item an equal opportunity of being selected,
C. permit the auditor to quantity the probability of error,
D. require judgment when defining population characteristics
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
Which of the following refers to the act of creating and using an invented scenario to persuade a target to perform an action?
A. Pretexting
B. Backgrounding
C. Check making
D. Bounce checking
E. None of the choices.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Pretexting is the act of creating and using an invented scenario to persuade a target to release information or perform an action and is usually done over the telephone. It is more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information.

NEW QUESTION: 42
Which of the following is the GREATEST benefit of utilizing data analytics?
A. Improved communication with management due to more confidence with data results
B. Higher-quality audit evidence due to more representative audit sampling
C. Expedient audit planning due to early identification of problem areas and incomplete data
D. Better risk assessments due to the identification of anomalies and trends
Answer: D (LEAVE A REPLY)

NEW QUESTION: 43
Which of the following term in business continuity determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity?
A. RPO
B. RTO

C. WRT

D. MTD

Answer: (SHOW ANSWER)

Explanation/Reference:

The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual

Business as usual

Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

Disaster Occurs

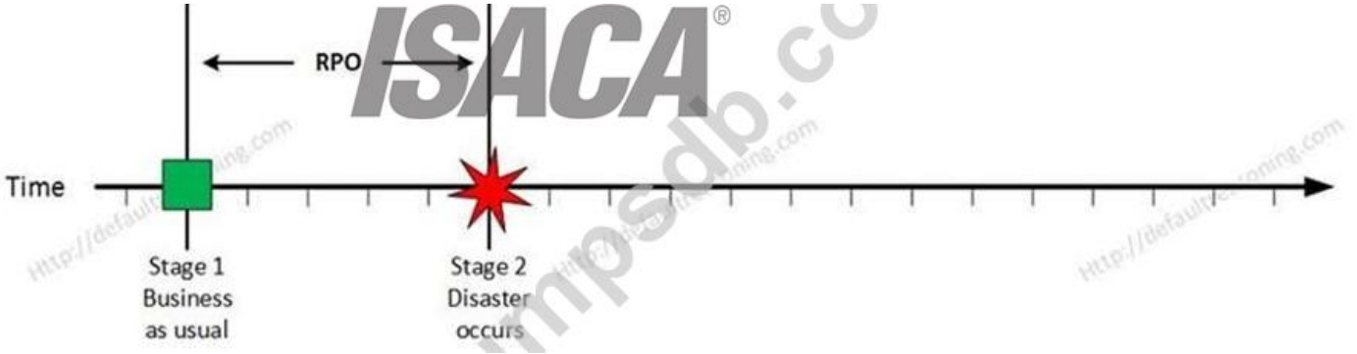


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

Recovery

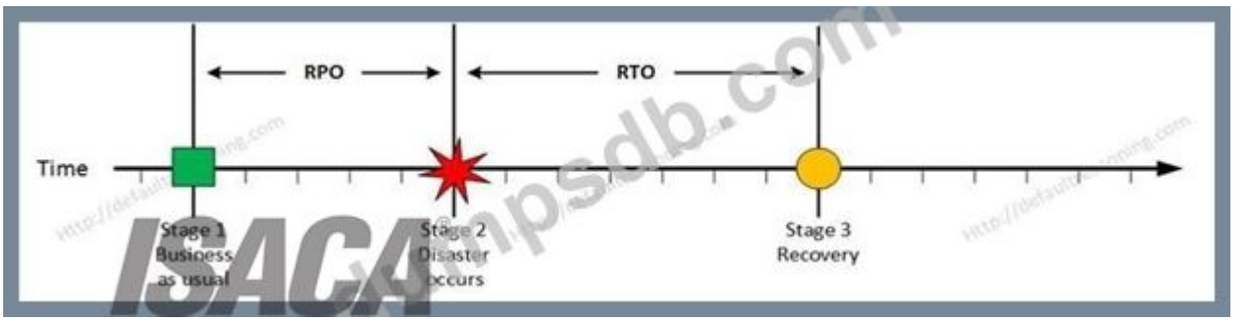


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production

Resume Production

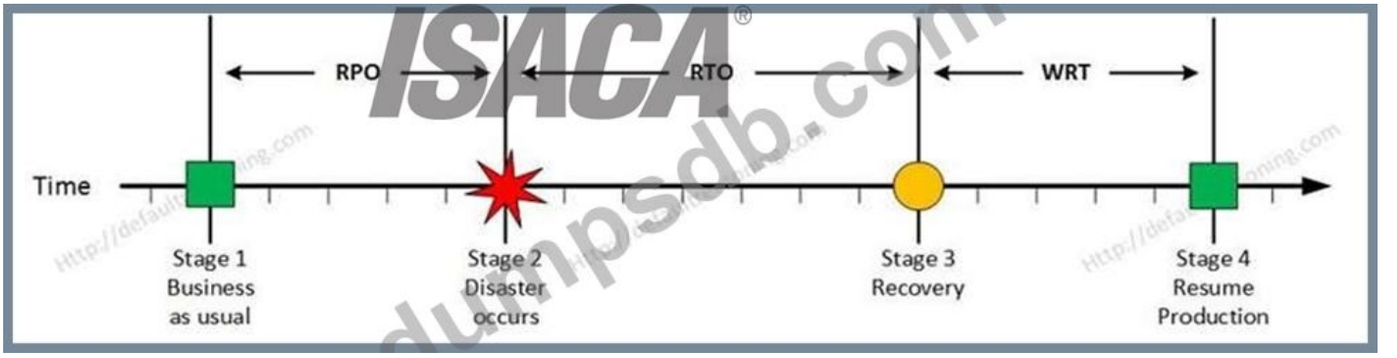


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available.

In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD

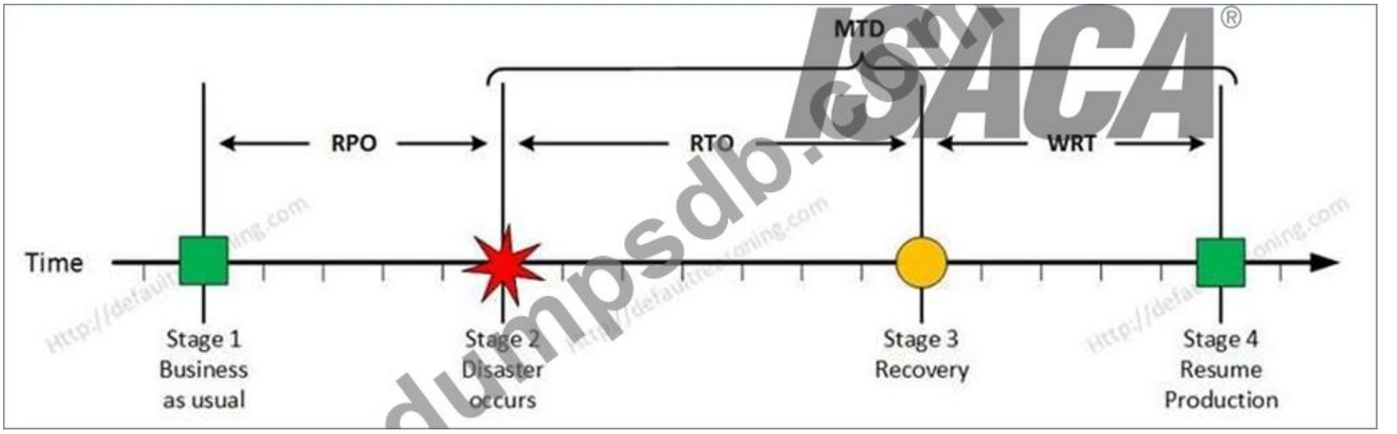


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.
The following answers are incorrect:
RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.
RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure.
In most cases this part is carried out by system administrator, network administrator, storage administrator etc.
MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 284
http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

NEW QUESTION: 44
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

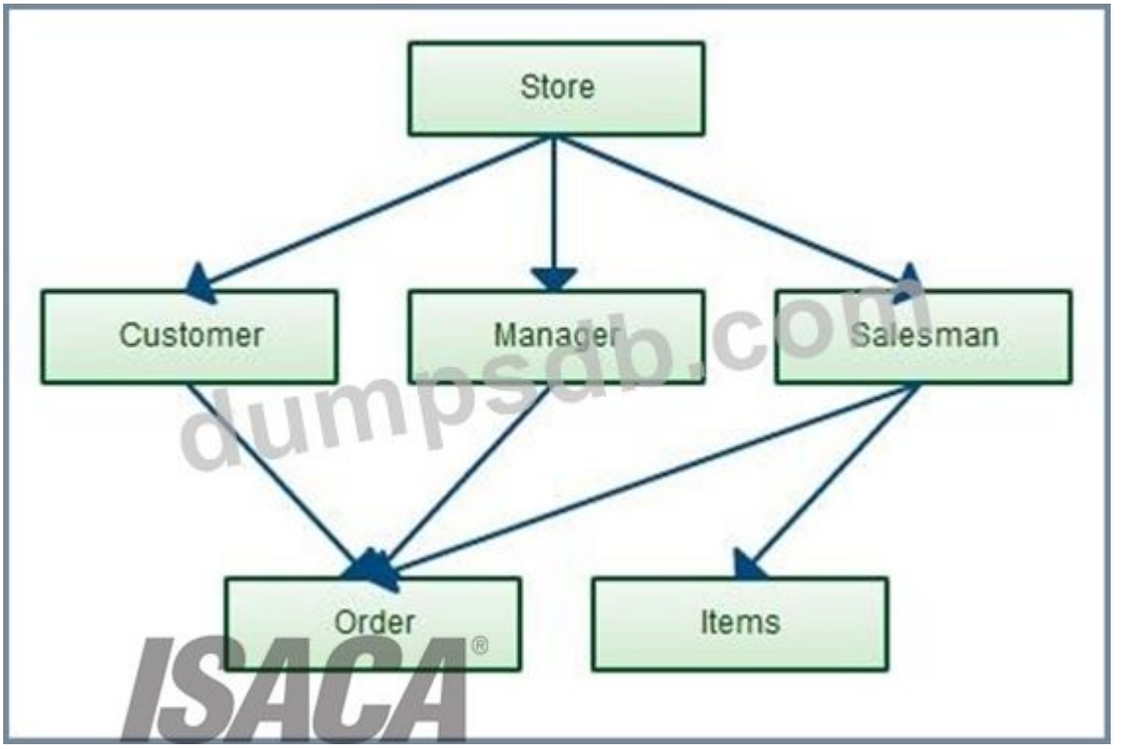
Image source: http://creately.com/blog/wp-content/uploads/2012/06/hierarchical-database-model.png Network database model The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents. It was the most popular before 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

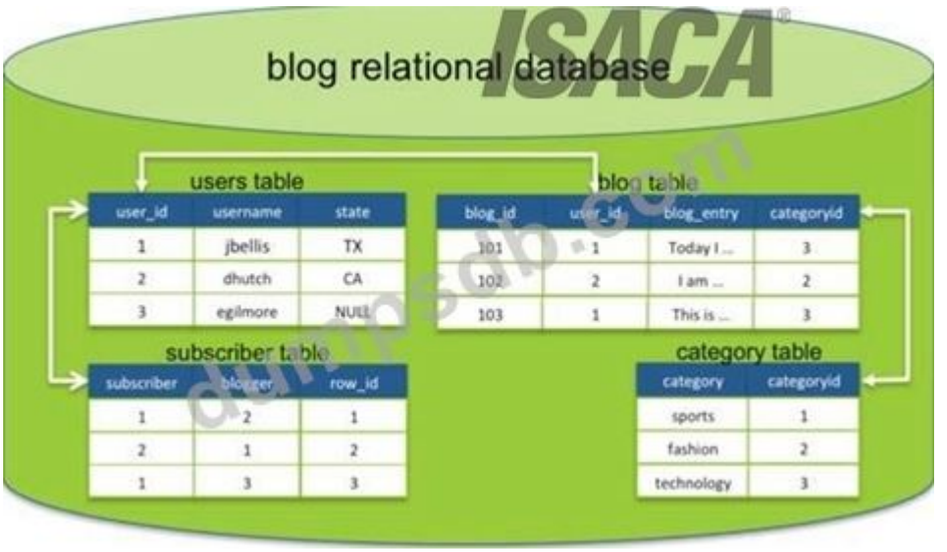


Image Source: http://www.datastax.com/docs/_images/relational_model.png Object-relational database Model An object-relational database (ORD), or object-relational database management system (ORDBMS), is a database management system (DBMS) similar to a relational database, but with an object-oriented 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: 45
Which of the following protocols would be involved in the implementation of a router and an interconnectivity device monitoring system?
A. Simple Network Management Protocol
B. File Transfer Protocol
C. Simple Mail Transfer Protocol
D. Telnet
Answer: A (LEAVE A REPLY)
The Simple Network Management Protocol provides a means to monitor and control network devices and to manage configurations and performance. The File Transfer Protocol (FTP) transfers files from a computer on the Internet to the user's computer and does not have any functionality related to monitoring network devices. Simple Mail Transfer Protocol (SMTP) is a protocol for sending and receiving e-mail messages and does not provide any monitoring or management for network devices. Telnet is a standard terminal emulation protocol used for remote terminal connections, enabling users to log into remote systems and use resources as if they were connected to a local system; it does not provide any monitoring or management of network devices.

NEW QUESTION: 46
Which of the following should an IS auditor use when verifying a three-way match has occurred in an enterprise resource planning (ERP) system?
A. Goods delivery notification
B. Purchase requisition
C. Bank confirmation
D. Purchase order
Answer: D (LEAVE A REPLY)
Section: Governance and Management of IT

NEW QUESTION: 47
Internal audit is conducting an audit of customer transaction risk. Which of the following would be the BEST reason to use data analytics?

A. The audit is being performed to comply with regulations requiring periodic random sample testing
B. The audit focus is on a small number of predefined high-risk transactions
C. Transactional data is contained in multiple discrete systems that have varying levels of reliability
D. Anomalies and risk trends in the data set have yet to be defined
Answer: B (LEAVE A REPLY)

NEW QUESTION: 48
Which of the following metrics would be MOST useful to an IS auditor when assessing the resilience of an application programming interface (API)?
A. Number of defects logged during development compared to other APIs
B. Number of API calls expected versus actually received within a lime interval
C. Number of developers adopting the API for their applications
D. Number of patches released within a time interval for the API
Answer: B (LEAVE A REPLY)

NEW QUESTION: 49
An organization recently experienced a phishing attack that resulted in a breach of confidential information. Which of the following would be MOST relevant for an IS auditor to review when determining the root cause of the incident?
A. Email configurations
B. Browser configurations
C. Simple mail transfer protocol (SMTP) logging
D. Audit logging
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
A change to the scope of an IT project has been formally submitted to the project manager. What should the project manager do NEXT?
A. Discuss the change with the project team and determine if it should be approved
B. Escalate the change to the change advisory board for approval
C. Determine how the change will affect the schedule and budget
D. Update the project plan to reflect the change in scope
Answer: (SHOW ANSWER)

NEW QUESTION: 51
As an outcome of information security governance, strategic alignment provides:
A. security requirements driven by enterprise requirements.
B. baseline security following best practices.
C. institutionalized and commoditized solutions.

D. an understanding of risk exposure.
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Information security governance, when properly implemented, should provide four basic outcomes:
strategic alignment, value delivery, risk management and performance measurement. Strategic alignment
provides input for security requirements driven by enterprise requirements. Value delivery provides a
standard set of security practices, i.e., baseline security following best practices or institutionalized and
commoditized solutions. Risk management provides an understanding of risk exposure.

NEW QUESTION: 52
Which of the following findings should be of GREATEST concern to an IS auditor performing an information security audit of critical server log management activities?
A. Logs are monitored using manual processes.
B. Log records can be overwritten before being reviewed.
C. Logging procedures are insufficiently documented
D. Log records are dynamically dispersed into different servers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 53
Which of lite following components of a risk assessment is MOST helpful to management in determining the level of risk mitigation to apply?
A. Risk classification
B. Risk identification
C. Control self-assessment (CSA)
D. Impact assessment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 54
Which of the following is the MOST significant risk associated with the use of visualization?
A. Insufficient network bandwidth
B. Performance issues of hosts
C. Inadequate configuration
D. Single point of failure
Answer: (SHOW ANSWER)

NEW QUESTION: 55

.Regarding digital signature implementation, which of the following answers is correct?
A. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's private key. Upon receiving the data, the recipient can decrypt the data using the sender's public key.
B. A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's public key.
C. A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value or message digest from the entire message contents. Upon receiving the data, the recipient can independently create it.
D. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's private key.
Answer: C (LEAVE A REPLY)
A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value, or message digest, from the entire message contents. Upon receiving the data, the recipient can independently create its own message digest from the data for comparison and data integrity validation. Public and private are used to enforce confidentiality. Hashing algorithms are used to enforce integrity.

NEW QUESTION: 56
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: 57
Which of the following would BEST demonstrate that an effective disaster recovery plan (DRP) is in place?
A. Full operational test
B. Periodic risk assessment
C. Frequent testing of backups
D. Annual walk-through testing
Answer: (SHOW ANSWER)

NEW QUESTION: 58

An IS auditor is reviewing the remote access methods of a company used to access system remotely.
Which of the following is LEAST preferred remote access method from a security and control point of view?
A. RADIUS
B. TACACS
C. DIAL-UP
D. DIAMETER
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Dial-up connectivity not based on centralize control and least preferred from security and control standpoint.
Remote access user can connect remotely to their organization's networks with the same level of functionality as if they would access from within their office.
In connecting to an organization's network, a common method is to use dial-up lines. Access is granted through the organization's network access server (NAS) working in concert with an organization network firewall and router. The NAS handle user authentication, access control and accounting while maintaining connectivity. The most common protocol for doing this is the Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Controller System (TACACS).
Remote access Controls include:
Policy and standard
Proper authorization
Identification and authentication mechanism
Encryption tool and technique such as use of VPN
System and network management
The following reference(s) were/was used to create this question:
CISA Review Manual 2014 Page number 334

NEW QUESTION: 59
Which of the following is MOST critical for the successful implementation and maintenance of a security
policy?
A. Assimilation of the framework and intent of a written security policy by all appropriate parties
B. Management support and approval for the implementation and maintenance of a security policy
C. Enforcement of security rules by providing punitive actions for any violation of security rules
D. Stringent implementation, monitoring and enforcing of rules by the security officer through access
control software
Answer: (SHOW ANSWER)

Section: Protection of Information Assets
Explanation:
Assimilation of the framework and intent of a written security policy by the users of the system is critical to
the successful implementation and maintenance of the security policy. A good password system may exist,
but if the users of the system keep passwords written on their desk, the password is of little value.
Management support and commitment is no doubt important, but for successful implementation and
maintenance of security policy, educating the users on the importance of security is paramount. The
stringent implementation, monitoring and enforcing of rules by the security officer through access control
software, and provision for punitive actions for violation of security rules, is also required, along with the
user's education on the importance of security.

NEW QUESTION: 60
Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following?
A. IT strategic plan
B. Business continuity plan
C. Business impact analysis
D. Incident response plan
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of a business continuity plan.

NEW QUESTION: 61
Which of the following is MOST likely to be included in computer operating procedures in a large data center?
A. Instructions for job scheduling
B. Procedures for resequencing source code
C. Procedures for utility configuration
D. Guidance on setting security parameters
Answer: A (LEAVE A REPLY)
Section: Governance and Management of IT

NEW QUESTION: 62
Which of the following test approaches would utilize data analytics to validate customer authentication controls for banking transactions?
A. Evaluate configuration settings for transactions requiring customer identification.
B. Review transactions completed for one period that have blank customer identification fields.
C. Attempt to complete a monetary transaction and leave the customer identification fields blank.
D. Review the business requirements document for customer identification requirements.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 63
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)
Section: Protection of Information Assets
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: 64
Which of the following is the MOST secure and economical method for connecting a private network over the Internet in a small- to medium-sized organization?
A. Virtual private network
B. Dedicated line
C. Leased line
D. integrated services digital network
Answer: A (LEAVE A REPLY)

Explanation/Reference:
Explanation:
The most secure method is a virtual private network (VPN), using encryption, authentication and tunneling to allow data to travel securely from a private network to the internet. Choices B, C and D are network connectivity options that are normally too expensive to be practical for small- to medium-sized organizations.

NEW QUESTION: 65
An information systems security officer's PRIMARY responsibility for business process applications is to:
A. ensure access rules agree with policies
B. create role-based rules for each business process
C. authorize secured emergency access,
D. approve the organization's security policy.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 66
In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:
A. implementation.
B. compliance.
C. documentation.
D. sufficiency.
Answer: D (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
An IS auditor should first evaluate the definition of the minimum baseline level by ensuring the sufficiency of
controls. Documentation, implementation and compliance are further steps.

NEW QUESTION: 67
Which of the following access rights presents the GREATEST risk when granted to a new member of the system development staff?
A. Execute access to development program libraries
B. Execute access to production program libraries
C. Write access to development data libraries
D. Write access to production program libraries
Answer: D (LEAVE A REPLY)

NEW QUESTION: 68
A database administrator should be prevented from:

A. using an emergency user ID.
B. accessing sensitive information.
C. having end user responsibilities.
D. having access to production files.
Answer: B (LEAVE A REPLY)
Section: Protection of Information Assets

NEW QUESTION: 69
An IS auditor is evaluating the security of an organization's data backup process which includes the transmission of daily incremental backups to a public cloud provider Which of the following findings poses the GREATEST risk to the organization?
A. Data recovery testing is conducted quarterly
B. Backup transmissions are not encrypted
C. Backup transmissions occasionally fail
D. The archived data log is incomplete
Answer: B (LEAVE A REPLY)

NEW QUESTION: 70
What is an effective control for granting temporary access to vendors and external support personnel?
Choose the BEST answer.
A. Creating user accounts that automatically expire by a predetermined date
B. Creating permanent guest accounts for temporary use
C. Creating user accounts that restrict logon access to certain hours of the day
D. Creating a single shared vendor administrator account on the basis of least-privileged access
Answer: (SHOW ANSWER)
Explanation/Reference:
Creating user accounts that automatically expire by a predetermined date is an effective control for granting temporary access to vendors and external support personnel.

NEW QUESTION: 71
An IS auditor finds that, at certain times of the day, the data warehouse query performance decreases
significantly. Which of the following controls would it be relevant for the IS auditor to review?
A. Permanent table-space allocation
B. Commitment and rollback controls
C. User spool and database limit controls
D. Read/write access log controls
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation:

User spool limits restrict the space available for running user queries. This prevents poorly formed queries
from consuming excessive system resources and impacting general query performance. Limiting the space
available to users in their own databases prevents them from building excessively large tables. This helps
to control space utilization which itself acts to help performance by maintaining a buffer between the actual
data volume stored and the physical device capacity. Additionally, it prevents users from consuming
excessive resources in ad hoc table builds (as opposed to scheduled production loads that often can run
overnight and are optimized for performance purposes), in a data warehouse, since you are not running
online transactions, commitment and rollback does not have an impact on performance. The other choices
are not as likely to be the root cause of this performance issue.

NEW QUESTION: 72
An organization has implemented a control to help ensure databases containing personal information will not be updated with online transactions that are incomplete due to connectivity issues. Which of the following information attributes is PRIMARILY addressed by this control?
A. Compliance
B. Availability
C. integrity
D. Confidentiality
Answer: C (LEAVE A REPLY)

NEW QUESTION: 73
An IS auditor is reviewing the results of a business process improvement project. Which of the following
should be performed FIRST?
A. Evaluate control gaps between the old and the new processes.
B. Develop compensating controls.
C. Document the impact of control weaknesses in the process.
D. Ensure that lessons learned during the change process are documented.
Answer: (SHOW ANSWER)
Section: Protection of Information Assets

NEW QUESTION: 74

Which of the following should be performed immediately after a computet security incident has been detected and analyzed by an incident response team?
A. Categorize the incident
B. Eradicate the component that caused the incident
C. Assess the impact of the incident on critical systems.
D. Contain the incident before it spreads.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
An IS auditor discovers that several desktop computers contain unauthorized software. Which of the following would be the auditor's BEST course of action?
A. Inform the users of the unauthorized software
B. Report the use of the unauthorized software to auditee management
C. Delete the unauthorized software from the computers
D. Report the use of the unauthorized software to the legal department
Answer: B (LEAVE A REPLY)

NEW QUESTION: 76
An IS auditor reviewing an organization's data privacy controls observes that privacy notices do not clearly
state how the organization uses customer data for its processing operations. Which of the following data
protection principles MUST be implemented to address this gap?
A. Maintenance of data integrity
B. Access to collected data
C. Retention of consent documentation
D. Purpose for data collection
Answer: B (LEAVE A REPLY)
Section: The process of Auditing Information System

NEW QUESTION: 77

A new regulation requires organizations to report significant security incidents to the regulator within 24 hours of identification. Which of the following is the IS auditor s BEST recommendation to facilitate compliance with the regulation?

A. Establish key performance indicators (KPIs) for timely identification of security incidents.

B. Engage an external security incident response expert for incident handling.

C. Enhance the alert functionality of the intrusion detection system (IDS).

D. Include the requirement in the incident management response plan.

Answer: (SHOW ANSWER)

NEW QUESTION: 78

Which of the following IS functions can be performed by the same group or individual while still providing

the proper segregation of duties?

A. Computer operations and application programming

B. Database administration and computer operations

C. Security administration and application programming

D. Application programming and systems analysis

Answer: A (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation/Reference:

https://www.isaca.org/Journal/archives/2016/volume-3/Pages/implementing-segregation-of-duties.aspx

NEW QUESTION: 79

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)

Section: Information System Operations, Maintenance and Support

Explanation:

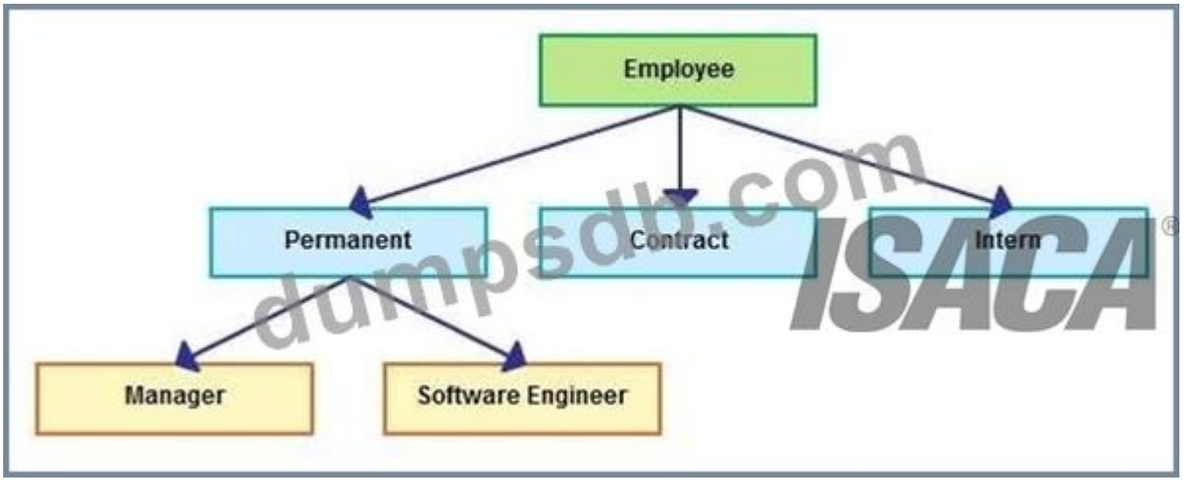
Network database model-The network model expands upon the hierarchical structure, allowing many-to- many relationships in a tree-like structure that allows multiple parents.

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

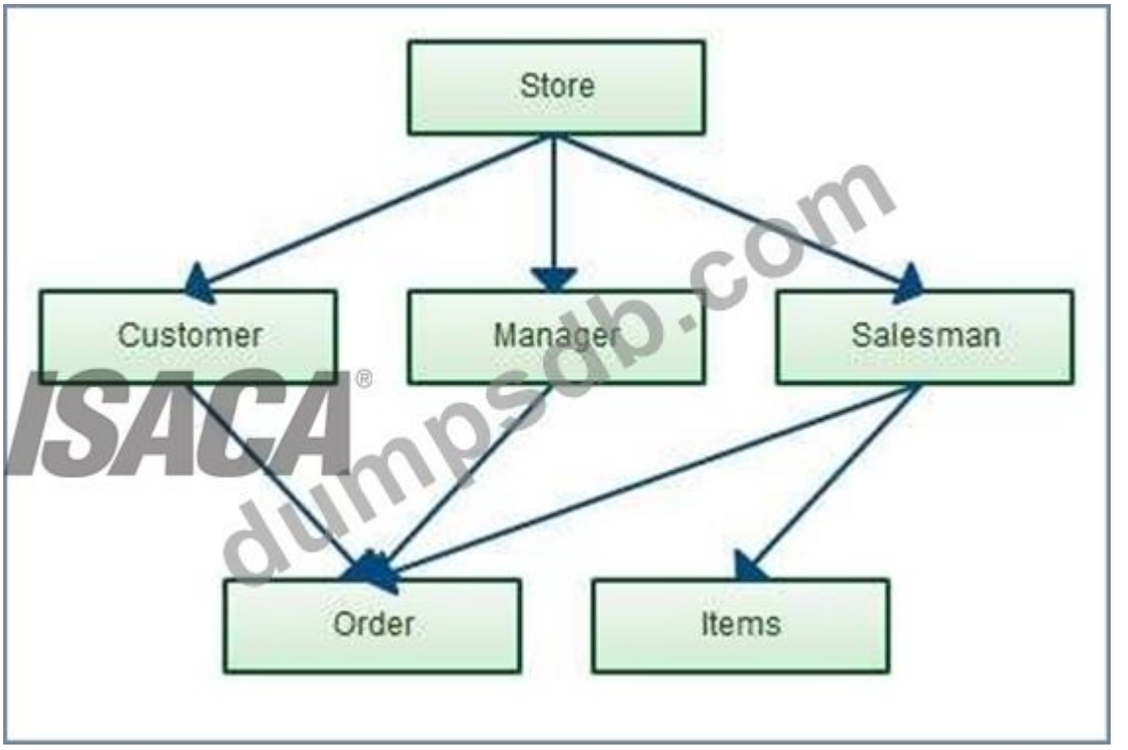


Network database model
The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents. It was the most popular before being replaced by the relational model, and is defined by the CODASYL specification.
The network 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".

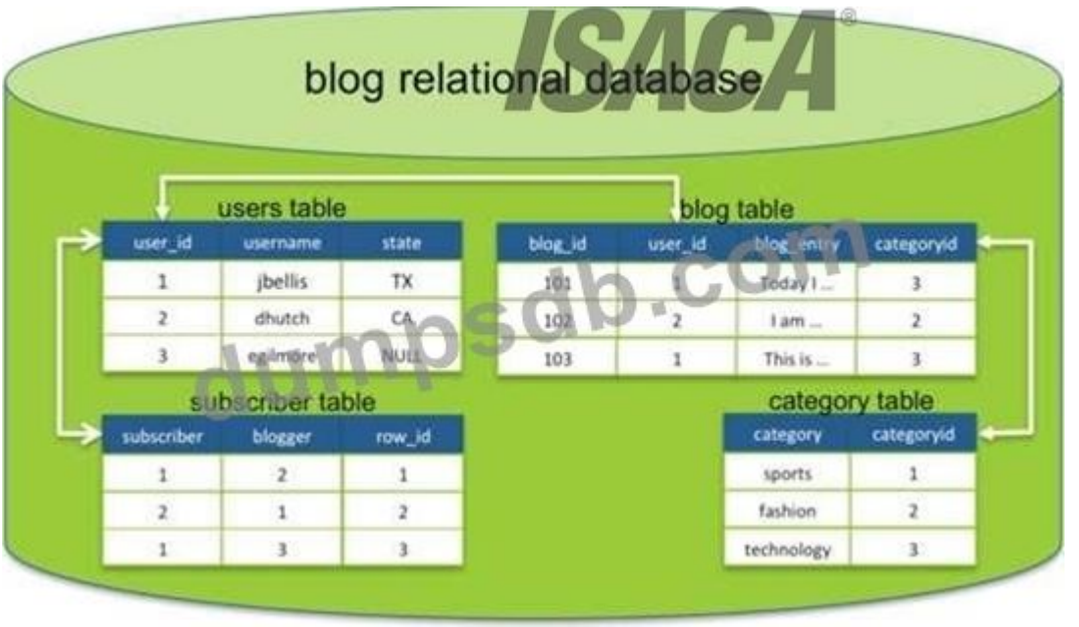
The purpose of the relational model is to provide a declarative method for specifying data and queries:

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.

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.
Reference:
CISA review manual 2014 Page number 254

NEW QUESTION: 80
Which of the following findings should be of GREATEST concern to an IS auditor conducting a forensic analysis following incidents of suspicious activities on a server?
A. Audit logs are not enabled on the server.
B. The server is outside the domain.
C. Most suspicious activities were created by system IDs.
D. The server's operating system is outdated.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 81
Users are issued security tokens to be used in combination with a PIN to access the corporate virtual private network (VPN). Regarding the PIN, what is the MOST important rule to be included in a security policy?
A. Users should not leave tokens where they could be stolen
B. Users must never keep the token in the same bag as their laptop computer
C. Users should select a PIN that is completely random, with no repeating digits
D. Users should never write down their PIN
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
If a user writes their PIN on a slip of paper, an individual with the token, the slip of paper, and the computer could access the corporate network. A token and the PIN is a two-factor authentication method.
Access to the token is of no value without the PIN; one cannot work without the other. The PIN does not need to be random as long as it is secret.

NEW QUESTION: 82
Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting
from normal network activity?
A. Statistical-based
B. Signature-based
C. Neural network
D. Host-based
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets

Explanation:
A statistical-based IDS relies on a definition of known and expected behavior of systems. Since normal
network activity may at times include unexpected behavior (e.g., a sudden massive download by multiple
users), these activities will be flagged as suspicious. A signature-based IDS is limited to its predefined set
of detection rules, just like a virus scanner. A neural network combines the previous two IDSs to create a
hybrid and better system. Host-based is another classification of IDS. Any of the three IDSs above may be
host- or network-based.

NEW QUESTION: 83
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)
Explanation/Reference:
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.

The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 30 (The process of auditing information system)

NEW QUESTION: 84
"Nowadays, computer security comprises mainly "preventive"" measures."
A. True
B. True only for trusted networks
C. True only for untrusted networks
D. False
E. None of the choices.
Answer: (SHOW ANSWER)
"Nowadays, computer security comprises mainly ""preventive"" measures, like firewalls or an Exit Procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network and is normally implemented as software running on the machine or as physical integrated hardware."

NEW QUESTION: 85
The PRIMARY benefit of information asset classification is that it:
A. prevents loss of assets.
B. enables risk management decisions.
C. facilitates budgeting accuracy.
D. helps to align organizational objectives.
Answer: (SHOW ANSWER)

NEW QUESTION: 86
After completing the business impact analysis (BIA), what is the next step in the business continuity planning process?
A. Test and maintain the plan.
B. Develop a specific plan.
C. Develop recovery strategies.
D. implement the plan.
Answer: C (LEAVE A REPLY)
The next phase in the continuity plan development is to identify the various recovery strategies and select the most appropriate strategy for recovering from a disaster. After selecting a strategy, a specific plan can be developed, tested and implemented.

NEW QUESTION: 87
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:

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 Reference:
CISA review manual 2014 Page number 167
Official ISC2 guide to CISSP CBK 3rd Edition Page number 176

NEW QUESTION: 88
Which of the following Is a challenge in developing a service level agreement (SLA) for network services?
A. Establishing a well-designed framework for network services
B. Ensuring that network components are not modified by the client
C. Reducing the number of entry points into the network
D. Finding performance metrics that can be measured property
Answer: D (LEAVE A REPLY)

NEW QUESTION: 89
Which of the following layer of an enterprise data flow architecture represents subsets of information from the core data warehouse?
A. Presentation layer
B. Desktop Access Layer
C. Data Mart layer
D. Data access layer

Answer: C (LEAVE A REPLY)

Section: Information System Acquisition, Development and Implementation Explanation:

Data Mart layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components The enterprise data flow architecture (EDFA) A logical data architecture Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer - This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data - Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data - Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data - Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse - This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down - Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across - Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis - The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer - This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This

layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.
Data Access Layer - This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.
Data Preparation layer - This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to 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 is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.
The following were incorrect answers:
Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.
Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Reference:
CISA review manual 2014 Page number 188

NEW QUESTION: 90
To address issues related to privileged users identified in an IS audit, management implemented a security information and event management (SIEM) system. Which type of control .....
A. Corrective
B. Directive
C. Preventive
D. Detective
Answer: (SHOW ANSWER)

NEW QUESTION: 91
Test and development environments should be separated. True or false?
A. True
B. False
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Test and development environments should be separated, to control the stability of the test environment.

NEW QUESTION: 92
Which of the following is the BEST approach for determining the maturity level of an information security program?
A. Review internal audit results.
B. Engage a third-party review.
C. Perform a self-assessment.
D. Evaluate key performance indicators (KPIs).
Answer: D (LEAVE A REPLY)
Section: Governance and Management of IT

NEW QUESTION: 93

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: 94
Which of the following would BEST assist senior management in evaluating IT performance as well as the alignment between corporate and IT strategic objectives?
A. Balanced scorecard
B. Enterprise architecture
C. IT project value analysis
D. Control self-assessment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 95
During an audit of a business continuity plan (BCP), an IS auditor found that, although all departments were housed in the same building, each department had a separate BCP. The IS auditor recommended that the BCPs be reconciled. Which of the following areas should be reconciled FIRST?
A. Evacuation plan
B. Recovery priorities
C. Backup storages
D. Call tree
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Protecting human resources during a disaster-related event should be addressed first. Having separate BCPs could result in conflicting evacuation plans, thus jeopardizing the safety of staff and clients. Choices B, C and D may be unique to each department and could be addressed separately, but still should be reviewed for possible conflicts and/or the possibility of cost reduction, but only after the issue of human safety has been analyzed.

NEW QUESTION: 96
Which of the following must exist to ensure the viability of a duplicate information processing facility?
A. The site is near the primary site to ensure quick and efficient recovery.

B. The site contains the most advanced hardware available.
C. The workload of the primary site is monitored to ensure adequate backup is available.
D. The hardware is tested when it is installed to ensure it is working properly.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Resource availability must be assured. The workload of the site must be monitored to ensure that availability for emergency backup use is not impaired. The site chosen should not be subject to the same natural disaster as the primary site. In addition, a reasonable compatibility of hardware/software must exist to serve as a basis for backup. The latest or newest hardware may not adequately serve this need. Testing the hardware when the site is established is essential, but regular testing of the actual backup data is necessary to ensure the operation will continue to perform as planned.

NEW QUESTION: 97
An IS auditor conducting a review of disaster recovery planning (DRP) at a financial processing organization has discovered the following:
The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department. The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting their attention.
The plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.
The IS auditor's report should recommend that:
A. the deputy CEO be censured for their failure to approve the plan.
B. a board of senior managers is set up to review the existing plan.
C. the existing plan is approved and circulated to all key management and staff.
D. a manager coordinates the creation of a new or revised plan within a defined time limit.
Answer: (SHOW ANSWER)
The primary concern is to establish a workable disaster recovery plan, which reflects current processing volumes to protect the organization from any disruptive incident. Censuring the deputy CEO will not achieve this and is generally not within the scope of an IS auditor to recommend. Establishing a board to review the plan, which is two years out of date, may achieve an updated plan, but is not likely to be a speedy operation, and issuing the existing plan would be folly without first ensuring that it is workable. The best way to achieve a disaster recovery plan in a short time is to make an experienced manager responsible for coordinating the knowledge of other managers into a single, formal document within a defined time limit.

NEW QUESTION: 98

When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

A. establishment of a review board.

B. creation of a security unit.

C. effective support of an executive sponsor.

D. selection of a security process owner.

Answer: (SHOW ANSWER)

The executive sponsor would be in charge of supporting the organization's strategic security program, and would aid in directing the organization's overall security management activities. Therefore, support by the executive level of management is themost critical success factor (CSF). None of the other choices are effective without visible sponsorship of top management.

NEW QUESTION: 99

_____ (fill in the blank) is/are ultimately accountable for the functionality, reliability, and security within IT governance.

A. Data custodians

B. The board of directors and executive officers

C. IT security administration

D. Business unit managers

Answer: B (LEAVE A REPLY)

Section: Protection of Information Assets

Explanation:

The board of directors and executive officers are ultimately accountable for the functionality, reliability, and security within IT governance.

NEW QUESTION: 100

An IS auditor notes that several employees are spending an excessive amount of time using social media sites for personal reasons. Which of the following should the auditor recommend be performed FIRST?

A. Use data loss prevention (DLP) tools on endpoints.

B. Implement a process to actively monitor postings on social networking sites.

C. Adjust budget for network usage to include social media usage.

D. implement policies addressing acceptable usage of social media during working hours.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 101

The Federal Information Processing Standards (FIPS) are primarily for use by (Choose two.):

A. all non-military government agencies

B. US government contractors

C. all military government agencies

D. all private and public colleges in the US

E. None of the choices.
Answer: A,B (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Federal Information Processing Standards (FIPS) are publicly announced standards developed by the
United States Federal government for use by all nonmilitary government agencies and by government
contractors. Many FIPS standards are modified versions of standards used in the wider community.

NEW QUESTION: 102
Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?
A. A substantive test of program library controls
B. A compliance test of program library controls
C. A compliance test of the program compiler controls
D. A substantive test of the program compiler controls
Answer: B (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
A compliance test determines if controls are operating as designed and are being applied in a manner that
complies with management policies and procedures. For example, if the IS auditor is concerned whether
program library controls are working properly, the IS auditor might select a sample of programs to determine if the source and object versions are the same. In other words, the broad objective of any
compliance test is to provide auditors with reasonable assurance that a particular control on which the
auditor plans to rely is operating as the auditor perceived it in the preliminary evaluation.

NEW QUESTION: 103
Which of the following IS functions can be performed by the same group or individual while still providing the proper segregation of duties?
A. Computer operations and application programming
B. Application programming and systems analysis
C. Security administration and application programming
D. Database administration and computer operations
Answer: A (LEAVE A REPLY)

NEW QUESTION: 104
Sam is the security Manager of a financial institute. Senior management has requested he performs a risk
analysis on all critical vulnerabilities reported by an IS auditor. After completing the risk analysis, Sam has
observed that for a few of the risks, the cost benefit analysis shows that risk mitigation cost (countermeasures, controls, or safeguard) is more than the potential lost that could be incurred. What kind
of a strategy should Sam recommend to the senior management to treat these risks?
A. Risk Mitigation
B. Risk Acceptance
C. Risk Avoidance
D. Risk transfer
Answer: (SHOW ANSWER)
Section: The process of Auditing Information System
Explanation/Reference:
Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may
also weigh the cost versus the benefit of dealing with the risk in another way.
For your exam you should know below information about risk assessment and treatment:
A risk assessment, which is a tool for risk management, is a method of identifying vulnerabilities and
threats and assessing the possible impacts to determine where to implement security controls. A risk
assessment is carried out, and the results are analyzed. Risk analysis is used to ensure that security is
cost-effective, relevant, timely, and responsive to threats. Security can be quite complex, even for well-
versed security professionals, and it is easy to apply too much security, not enough security, or the wrong
security controls, and to spend too much money in the process without attaining the necessary objectives.
Risk analysis helps companies prioritize their risks and shows
management the amount of resources that should be applied to protecting against those risks in a sensible
manner.
A risk analysis has four main goals:
Identify assets and their value to the organization.
Identify vulnerabilities and threats.
Quantify the probability and business impact of these potential threats.
Provide an economic balance between the impact of the threat and the cost

of the countermeasure.

Treating Risk

Risk Mitigation

Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented.

Examples of risk mitigation can be seen in everyday life and are readily apparent in the information technology world. Risk Mitigation involves applying appropriate control to reduce risk. For example, to lessen the risk of exposing personal and financial information that is highly sensitive and confidential organizations put countermeasures in place, such as firewalls, intrusion detection/prevention systems, and other mechanisms, to deter malicious outsiders from accessing this highly sensitive information. In the underage driver example, risk mitigation could take the form of driver education for the youth or establishing a policy not allowing the young driver to use a cell phone while driving, or not letting youth of a certain age have more than one friend in the car as a passenger at any given time.

Risk Transfer

Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way. The family is evaluating whether to permit an underage driver to use the family car. The family decides that it is important for the youth to be mobile, so it transfers the financial risk of a youth being in an accident to the insurance company, which provides the family with auto insurance.

It is important to note that the transfer of risk may be accompanied by a cost. This is certainly true for the insurance example presented earlier, and can be seen in other insurance instances, such as liability insurance for a vendor or the insurance taken out by companies to protect against hardware and software theft or destruction. This may also be true if an organization must purchase and implement security controls in order to make their organization less desirable to attack. It is important to remember that not all risk can be transferred. While financial risk is simple to transfer through insurance, reputational risk may almost never be fully transferred.

Risk Avoidance

Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized. For example, have you ever heard a friend, or parents of a friend, complain about the costs of insuring an underage driver? How about the risks that many of these children face as they become mobile? Some of these families will decide that the child in question will not be allowed to drive the family car, but will rather wait until he or she is of legal age (i.e., 18 years of age) before committing to owning, insuring, and driving a motor vehicle.

In this case, the family has chosen to avoid the risks (and any associated benefits) associated with an underage driver, such as poor driving performance or the cost of insurance for the child. Although this choice may be available for some situations, it is not available for all. Imagine a global retailer who, knowing the risks associated with doing business on the Internet, decides to avoid the practice. This decision will likely cost the company a significant amount of its revenue (if, indeed, the company has products or services that consumers wish to purchase). In addition, the decision may require the company to build or lease a site in each of the locations, globally, for which it wishes to continue business. This could have a catastrophic effect on the company's ability to continue business operations

Risk Acceptance

In some cases, it may be prudent for an organization to simply accept the risk that is presented in certain scenarios. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way. For example, an executive may be confronted with risks identified during the course of a risk assessment for their organization. These risks have been prioritized by high, medium, and low impact to the organization. The executive notes that in order to mitigate or transfer the low-level risks, significant costs could be involved. Mitigation might involve the hiring of additional highly skilled personnel and the purchase

of new hardware, software, and office equipment, while transference of the risk to an insurance company
would require premium payments. The
executive then further notes that minimal impact to the organization would occur if any of the reported low-
level threats were realized. Therefore, he or she (rightly) concludes that it is wiser for the organization to
forgo the costs and accept the risk. In the young driver example, risk acceptance could be based on the
observation that the youngster has demonstrated the responsibility and maturity to warrant the parent's
trust in his or her judgment.
The following answers are incorrect:
Risk Transfer - Risk transfer is the practice of passing on the risk in question to another entity, such as an
insurance company. Let us look at one of the examples that were presented above in a different way.
Risk Avoidance - Risk avoidance is the practice of coming up with alternatives so that the risk in question is
not realized.
Risk Mitigation -Risk mitigation is the practice of the elimination of, or the significant decrease in the level of
risk presented.
The following reference(s) were/was used to create this question:
CISA Review Manual 2014 Page number 51
and
Official ISC2 guide to CISSP CBK 3rd edition page number 534-539

NEW QUESTION: 105
When reviewing an organization's data protection practices, an IS auditor should be MOST concerned with a lack of:
A. a security team.
B. data classification.
C. training manuals.
D. data encryption.
Answer: (SHOW ANSWER)
Section: Protection of Information Assets

NEW QUESTION: 106
Which of the following may be deployed in a network as lower cost surveillance and early-warning tools?

A. Honeypots
B. Hardware IPSs
C. Hardware IDSs
D. Botnets
E. Stateful inspection firewalls
F. Stateful logging facilities
G. None of the choices.
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
Honeypots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools. Techniques used by the attackers that attempt to compromise these
decoy resources are studied during and after an attack to keep an eye on new exploitation techniques.

NEW QUESTION: 107
Which of the following is a management technique that enables organizations to develop strategically
important systems faster, while reducing development costs and maintaining quality?
A. Function point analysis
B. Critical path methodology
C. Rapid application development
D. Program evaluation review technique
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation:
Rapid application development is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality. The
program evaluation review technique (PERT) and critical path methodology (CPM) are both planning and

control techniques, while function point analysis is used for estimating the complexity of developing
business applications.

NEW QUESTION: 108
An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to:
A. Meet business objectives
B. Enforce data security
C. Be culturally feasible
D. Be financially feasible
Answer: A (LEAVE A REPLY)
Explanation/Reference:
An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to meet business objectives.

NEW QUESTION: 109
Following a security breach, in which a hacker exploited a well-known vulnerability in the domain controller, an IS auditor has been asked to conduct a control assessment. The auditor's BEST course of action would be to determine it:
A. The logs were monitored
B. The patches were updated
C. The domain controller was classified for high availability
D. The network traffic was being monitored
Answer: B (LEAVE A REPLY)

NEW QUESTION: 110
An organization has made a strategic decision to split into separate operating entities to improve profitability. However, the IT infrastructure remains shared between the entities. Which of the following
would BEST help to ensure that IS audit still covers key risk areas within the IT environment as part of its
annual plan?
A. Increasing the frequency of risk-based IS audits for each business entity
B. Revising IS audit plans to focus on IT changes introduced after the split
C. Conducting an audit of newly introduced IT policies and procedures
D. Developing a risk-based plan considering each entity's business processes
Answer: (SHOW ANSWER)
Section: Governance and Management of IT

NEW QUESTION: 111

Which of the following is the BEST reason to utilize blockchain technology to record accounting transactions?

A. Integrity of records

B. Distribution of records

C. Availability of records

D. Confidentiality of records

Answer: A (LEAVE A REPLY)

NEW QUESTION: 112

Which of the following procedures for testing a disaster recovery plan (DRP) is MOST effective?

A. Testing at a secondary site using offsite data backups

B. Reviewing documented backup and recovery procedures

C. Performing a quarterly tabletop exercise

D. Performing an unannounced shutdown of the computing facility after hours

Answer: A (LEAVE A REPLY)

NEW QUESTION: 113

Which of the following are BEST suited for continuous auditing?

A. Low-value transactions

B. Irregular transactions

C. Manual transactions

D. Real-time transactions

Answer: D (LEAVE A REPLY)

NEW QUESTION: 114

Which of the following is the GREATEST advantage of implementing an IT enterprise architecture framework within an organization?

A. It helps to identify security issues in systems across the organization.

B. It reduces the overlap of infrastructure technologies within the organization.

C. It improves the organization's ability to meet service level agreements (SLAs).

D. It better equips an organization to adopt innovative and emerging technologies.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 115

A 5 year audit plan provides for general audits every year and application audits on alternating years. To achieve higher efficiency, the IS audit manager would MOST likely:

A. Alternate between control self-assessment (CSA) and general audits every year.

B. Proceed with the plan and integrate all new applications

C. Have control self-assessments (CSAs) and formal audits of application on alternating years

D. Implement risk assessment criteria to determine audit priorities

Answer: (SHOW ANSWER)

NEW QUESTION: 116
Which of the following fire-suppression methods is considered to be the most environmentally friendly?
A. Halon gas
B. Deluge sprinklers
C. Dry-pipe sprinklers
D. Wet-pipe sprinklers
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Although many methods of fire suppression exist, dry-pipe sprinklers are considered to be the most environmentally friendly.

NEW QUESTION: 117
An IS auditor should expect the responsibility for authorizing access rights to production data and systems to be entrusted to the:
A. process owners.
B. system administrators.
C. security administrator.
D. data owners.
Answer: D (LEAVE A REPLY)
Data owners are primarily responsible for safeguarding the data and authorizing access to production data on a need-to-know basis.

NEW QUESTION: 118
Which of the following would MOST likely impair the independence of the IS auditor when performing a post-implementation review of an application system?
A. The IS auditor designed an embedded audit module exclusively for auditing the application system.
B. The IS auditor participated as a member of the application system project team, but did not have operational responsibilities.
C. The IS auditor implemented a specific control during the development of the application system.
D. The IS auditor provided consulting advice concerning application system best practices.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 119
Which of the following is the MOST important element when developing an information security strategy?
A. Identifying applicable laws and regulations
B. Identifying information assets

C. Determining the risk management methodology
D. Aligning security activities with organizational goals
Answer: D (LEAVE A REPLY)
Section: Governance and Management of IT

NEW QUESTION: 120
An IS auditor notes that nightly hatch processing is frequently incomplete for an application. The auditor should FIRST review controls over which of the following?
A. Backup procedures
B. Job scheduling
C. Job notification
D. Application logs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 121
A legacy application is running on an operating system that is no longer supported by vendor, if the organization continues to use the current application, which of the application should be the IS auditor's GREATEST concern?
A. Potential exploitation of zero-day vulnerabilities in the system
B. Inability to use the operating system due to potential licence issues
C. Increased cost of maintaining the system
D. Inability to update the legacy application database
Answer: D (LEAVE A REPLY)

NEW QUESTION: 122
Which of the following is an effective method for controlling downloading of files via FTP?
A. An application-layer gateway, or proxy firewall, but not stateful inspection firewalls
B. An application-layer gateway, or proxy firewall
C. A circuit-level gateway
D. A first-generation packet-filtering firewall
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation:

Application-layer gateways, or proxy firewalls, are an effective method for controlling downloading of files via FTP. Because FTP is an OSI application-layer protocol, the most effective firewall needs to be capable of inspecting through the application layer.

NEW QUESTION: 123
A firewall has been installed on the company's web server. Which concern does the firewall address?
A. Availability of the information
B. Unauthorized modification of information by internal users
C. Accessing information by the outside world
D. Connectivity to the Internet
Answer: C (LEAVE A REPLY)
Section: Information System Operations, Maintenance and Support
Explanation/Reference:

NEW QUESTION: 124
Which of the following should an IS auditor recommend to BEST enforce alignment of an IT project portfolio with strategic organizational priorities?
A. Define a balanced scorecard (BSC) for measuring performance
B. Consider user satisfaction in the key performance indicators (KPIs)
C. Select projects according to business benefits and risks
D. Modify the yearly process of defining the project portfolio
Answer: (SHOW ANSWER)
Prioritization of projects on the basis of their expected benefit(s) to business, and the related risks, is the best measure for achieving alignment of the project portfolio to an organization's strategic priorities. Modifying the yearly process of the projects portfolio definition might improve the situation, but only if the portfolio definition process is currently not tied to the definition of corporate strategies; however, this is unlikely since the difficulties are in maintaining the alignment, and not in setting it up initially. Measures such as balanced scorecard (BSC) and key performance indicators (KPIs) are helpful, but they do not guarantee that the projects are aligned with business strategy.

NEW QUESTION: 125
Which of the following term in business continuity determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity?
A. RPO
B. RTO
C. WRT
D. MTD
Answer: C (LEAVE A REPLY)
Explanation/Reference:

The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual

Business as usual

Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

Disaster Occurs

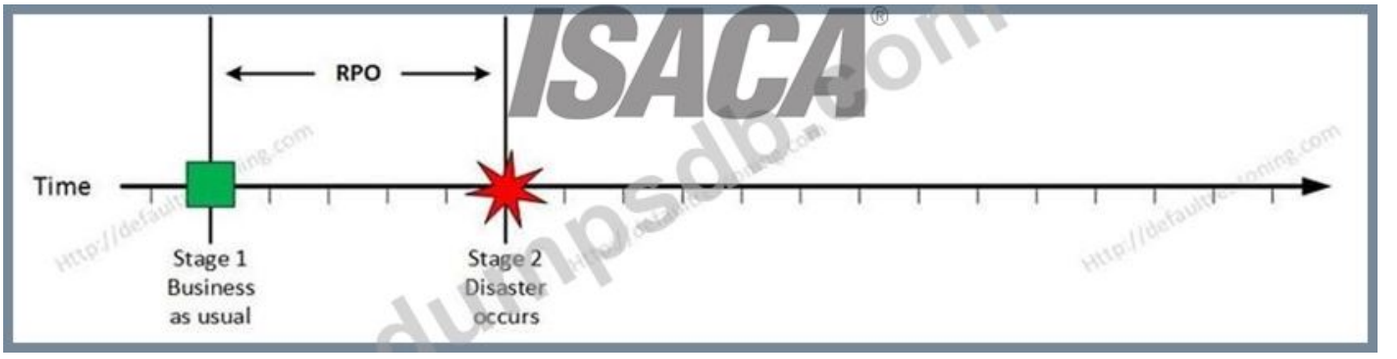


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

Recovery

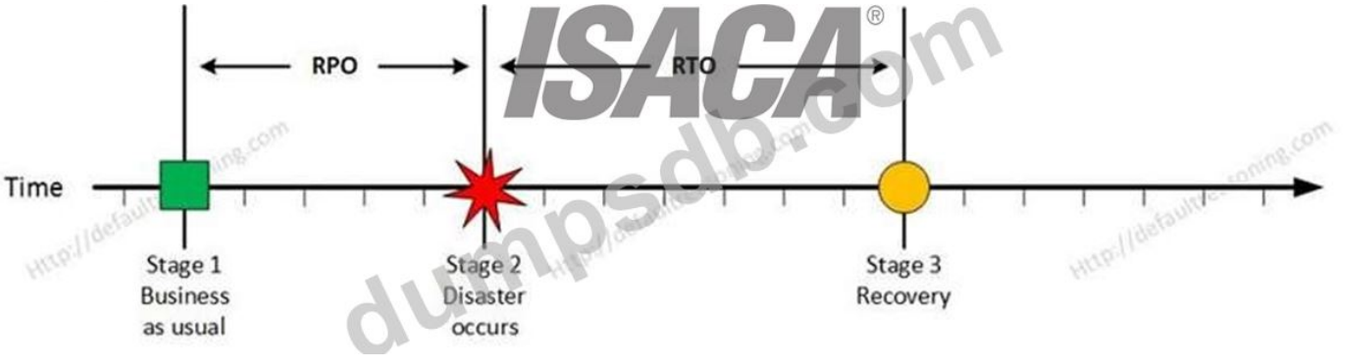


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production

Resume Production

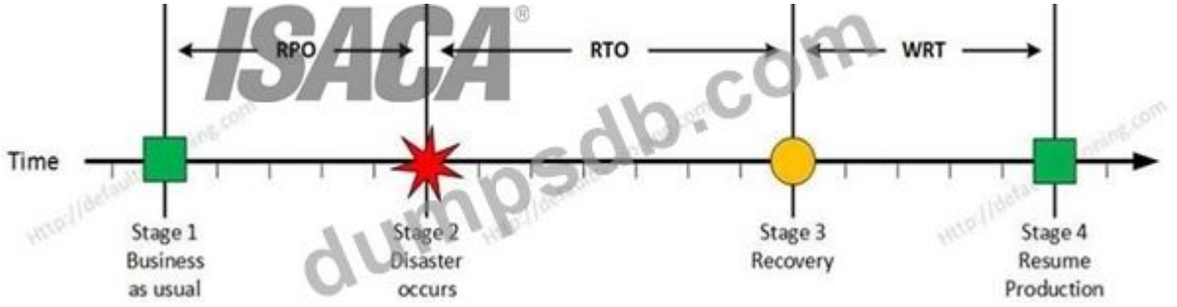


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available.

In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD

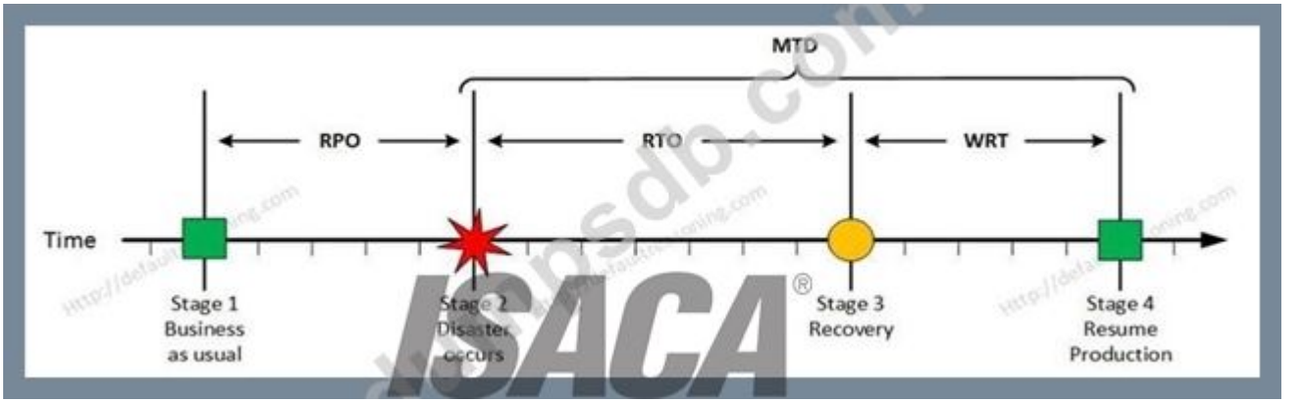


Image Reference - http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure.
In most cases this part is carried out by system administrator, network administrator, storage administrator etc.
MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 284
http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

NEW QUESTION: 126
If inadequate, which of the following would be the MOST likely contributor to a denial-of-service attack?
A. Router configuration and rules
B. Design of the internal network
C. Updates to the router system software
D. Audit testing and review techniques
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Inadequate router configuration and rules would lead to an exposure to denial-of-service attacks. Choices B and C would be lesser contributors. Choice D is incorrect because audit testing and review techniques are applied after the fact.

NEW QUESTION: 127
During an exit interview, senior management disagrees with some of the facts presented in the draft audit report and wants them removed from tie report. Which of the blowing would be the auditor's BEST course of action?
A. Finalize tie draft audit report without changes
B. Escalate the issue to audit management
C. Gather evidence to analyze senior management's objections
D. Revise the assessment based on senior management's objections
Answer: (SHOW ANSWER)

NEW QUESTION: 128
To confirm integrity for a hashed message, the receiver should use
A. a different hashing algorithm from me sender s to create a binary image of the file
B. the same hashing algorithm as the tender s to create a numerical representation of the file.

C. the same hashing algorithm as the sender's to create a binary image of the file.
D. a different hashing algorithm from the sender s to create a numerical representation of the file
Answer: (SHOW ANSWER)

NEW QUESTION: 129
An IS auditor conducts a review of a third-party vendor's reporting of key performance indicators (KPI). Which of the following findings should be of MOST concern to the audition?
A. Some KPIs are not documented
B. KPIs are not clearly defined
C. KPI data is not being analysed
D. KPIs have never been updated
Answer: D (LEAVE A REPLY)

NEW QUESTION: 130
During an audit of identity and access management, an IS auditory finds that the engagement audit plan does not include the testing of controls that regulate access by third parties. Which of the following would be the auditor's BEST course of action?
A. Determine whether the risk has been identified in the planning documents
B. Escalate the deficiency to audit management.
C. Add testing of third-party access controls to the scope of the audit.
D. Plan to test these controls in another audit
Answer: C (LEAVE A REPLY)

NEW QUESTION: 131
Which of the following is the PRIMARY objective of using a capability maturity model as a tool to communicate audit results to senior management?
A. To evaluate management's action plan
B. To confirm audit findings
C. To illustrate improvement opportunities
D. To prioritize remediation efforts
Answer: A (LEAVE A REPLY)
Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 132
Which of the following cloud computing service model provides a way to rent operating systems, storage
and network capacity over the Internet?
A. Software as a service
B. Data as a service
C. Platform as a service
D. Infrastructure as a service

Answer: C (LEAVE A REPLY)

Section: Governance and Management of IT

Explanation

Explanation/Reference:

Platform as a Service (Peas) is a way to rent operating systems, storage and network capacity over the

Internet. The service delivery model allows the customer to rent virtualized servers and associated services

for running existing applications or developing and testing new ones.

For your exam you should know below information about Cloud Computing:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared

pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that

can be rapidly provisioned and released with minimal management effort or service provider interaction.

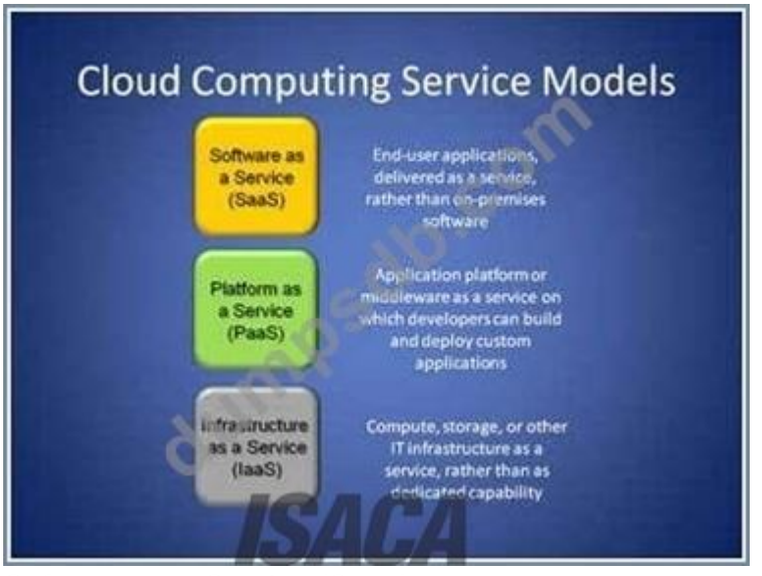
This cloud model promotes availability and is composed of five essential characteristics, three service

models, and four deployment models.

Cloud Computing

Cloud computing service models:

Cloud computing service models



Software as a Service (Seas)

Software as a Service (Seas) is a software distribution model in which applications are hosted by a vendor

or service provider and made available to customers over a network, typically the Internet. SaaS is closely

related to the ASP (application service provider) and on demand computing software delivery models. IDC

identifies two slightly different delivery models for Seas. The hosted application management (hosted AM)
model is similar to ASP: a provider hosts commercially available software for customers and delivers it over
the Web. In the software on demand model, the provider gives customers network-based access to a
single copy of an application created specifically for Seas distribution.
Provider gives users access to specific application software (CRM, e-mail, games). The provider gives the
customers network based access to a single copy of an application created specifically for Seas distribution
and use.
Benefits of the Seas model include:
easier administration
automatic updates and patch management
compatibility: All users will have the same version of software.
easier collaboration, for the same reason
global accessibility.
Platform as a Service (Peas)
Platform as a Service (Peas) is a way to rent operating systems, storage and network capacity over the
Internet. The service delivery model allows the customer to rent virtualized servers and associated services
for running existing applications or developing and testing new ones.
Cloud providers deliver a computing platform, which can include an operating system, database, and web
server as a holistic execution environment. Where Iasi is the "raw IT network," Peas is the software
environment that runs on top of the IT network.
Platform as a Service (Peas) is an outgrowth of Software as a Service (Seas), a software distribution model
in which hosted software applications are made available to customers over the Internet. Peas has several
advantages for developers. With Peas, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development
projects. Services can be obtained from diverse sources that cross international boundaries. Initial and
ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than

maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility
problems. Overall expenses can also be minimized by unification of programming development efforts.
On the downside, Peas involves some risk of "lock-in" if offerings require proprietary service interfaces or
development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of
some users whose requirements rapidly evolve.
Infrastructure as a Service (Iasi)
Cloud providers offer the infrastructure environment of a traditional data center in an on-demand delivery
method. Companies deploy their own operating systems, applications, and software onto this provided
infrastructure and are responsible for maintaining them.
Infrastructure as a Service is a provision model in which an organization outsources the equipment used to
support operations, including storage, hardware, servers and networking components. The service provider
owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on
a per-use basis.
Characteristics and components of Iasi include:
Utility computing service and billing model.
Automation of administrative tasks.
Dynamic scaling.
Desktop virtualization.
Policy-based services.
Internet connectivity.
Infrastructure as a Service is sometimes referred to as Hardware as a Service (HaaS).
The following answers are incorrect:
Data as a service - Data Provided as a service rather than needing to be loaded and prepared on premises.
Software as a service - Software as a Service (Seas) is a software distribution model in which applications
are hosted by a vendor or service provider and made available to customers over a network, typically the
Internet. Seas is closely related to the ASP (application service provider) and on demand computing
software delivery models.

Infrastructure as a service - Infrastructure as a Service is a provision model in which an organization
outsources the equipment used to support operations, including storage, hardware, servers and networking
components. The service provider owns the equipment and is responsible for housing, running and
maintaining it. The client typically pays on a per-use basis.
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 102
Official ISC2 guide to CISSP 3rd edition Page number 689
http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service
http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS
http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

NEW QUESTION: 133
Which of the following is the BEST use of a balanced scorecard when evaluating IT performance?
A. Determining compliance with relevant regulatory requirements
B. Evaluating implementation of the business strategy
C. Monitoring alignment of the IT project portfolio to budget
D. Monitoring alignment of IT with the rest of the organization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 134
Which of the following is the FIRST step in initiating a data classification program?
A. Inventory of data assets
B. Assignment of data ownership
C. Assignment of sensitivity levels
D. Risk appetite assessment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 135
Which of the following is the BEST reason to perform root cause analysis after a critical server failure?
A. To enable appropriate corrective measures
B. To enable the gathering of system availability data
C. To enable timely follow-up audits
D. To enable the optimization of IT investments
Answer: (SHOW ANSWER)
Section: Protection of Information Assets

NEW QUESTION: 136

An IS auditor is asked to provide feedback on the systems options analysis for a new project. The BEST course of action for the IS auditor would be to:
A. identify the best alternative.
B. request at least one other alternative.
C. comment on the criteria used to assess the alternatives.
D. retain comments as findings for the audit report.
Answer: (SHOW ANSWER)
Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 137
When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:
A. incorporates state of the art technology.
B. addresses the required operational controls.
C. articulates the IT mission and vision.
D. specifies project management practices.
Answer: C (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not
address the technology, operational controls or project management practices.

NEW QUESTION: 138
An organization is moving its on-site application servers to a service provider that operates a virtualized environment shared by multiple customers. Which of the following is the MOST significant risk to the organization?
A. Competing workloads from other clients
B. Account hacking from other clients
C. Service provider access to organizational data
D. Service provider limiting the right to audit
Answer: A (LEAVE A REPLY)

NEW QUESTION: 139

An organization has a recovery time objective (RTO) equal to zero and a recovery point objective (RPO)
close to 1 minute for a critical system. This implies that the system can tolerate:
A. a data loss of up to 1 minute, but the processing must be continuous.
B. a 1-minute processing interruption but cannot tolerate any data loss.
C. a processing interruption of 1 minute or more.
D. both a data less and processing interruption longer than 1 minute.
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
The recovery time objective (RTO) measures an organization's tolerance for downtime and the recovery
point objective (RPO) measures how much data loss can be accepted. Choices B, C and D are incorrect
since they exceed the RTO limits set by the scenario.

NEW QUESTION: 140
Performance of a biometric measure is usually referred to in terms of (choose all that apply):
A. failure to reject rate
B. false accept rate
C. false reject rate
D. failure to enroll rate
E. None of the choices.
Answer: B,C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Performance of a biometric measure is usually referred to in terms of the false accept rate (FAR), the false non match or reject rate (FRR), and the failure to enroll rate (FTE or FER). The FAR measures the percent of invalid users who are incorrectly accepted in, while the FRR measures the percent of valid users who are wrongly rejected.

NEW QUESTION: 141
Which of the following is the BEST way to determine if IT is delivering value to the business?
A. Distribute surveys to various end users of IT services.
B. Interview key IT managers and service providers.
C. Review IT service level agreement (SLA) metrics.
D. Analyze downtime frequency and duration.
Answer: C (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:

A service level agreement (SLA) is a written document, which officially describe the details of services, in non-technical terms, provided by the IT department (internal or external) to its customers. The aim of SLA is to maintain and improve the customer satisfaction to an agreed level.

NEW QUESTION: 142
A trojan horse simply cannot operate autonomously.
A. true
B. false
Answer: A (LEAVE A REPLY)
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: 143
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 achievenonrepudiation of the signed message.
D. registers signed messages to protect them from future repudiation.
Answer: A (LEAVE A REPLY)
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: 144
To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:
A. schedule the audits and monitor the time spent on each audit.
B. train the IS audit staff on current technology used in the company.
C. develop the audit plan on the basis of a detailed risk assessment.
D. monitor progress of audits and initiate cost control measures.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

Monitoring the time (choice A) and audit programs {choice D), as well as adequate training (choice B), will improve the IS audit staff's productivity (efficiency and performance), but that which delivers value to the organization are the resources and efforts being dedicated to, and focused on, the higher-risk areas.

NEW QUESTION: 145
Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would MOST likely focus on a review of:
A. pre-BPR process flowcharts.
B. post-BPR process flowcharts.
C. BPR project plans.
D. continuous improvement and monitoring plans.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
An IS auditor's task is to identify and ensure that key controls have been incorporated into the reengineered process. Choice A is incorrect because an IS auditor must review the process as it is today, not as it was in the past. Choices C and D are incorrect because they are steps within a BPR project.

NEW QUESTION: 146
Which of the following refers to the proving of mathematical theorems by a computer program?
A. Analytical theorem proving
B. Automated technology proving
C. Automated theorem processing
D. Automated theorem proving
E. None of the choices.
Answer: (SHOW ANSWER)
Automated theorem proving (ATP) is the proving of mathematical theorems by a computer program. Depending on the underlying logic, the problem of deciding the validity of a theorem varies from trivial to impossible. Commercial use of automated theorem proving is mostly concentrated in integrated circuit design and verification.

NEW QUESTION: 147
Which of the following procedures would BEST contribute to the reliability of information in a data warehouse?
A. Retaining only current data
B. Storing only a single type of data
C. Maintaining archive data
D. Maintaining current metadata
Answer: C (LEAVE A REPLY)

Section: Information System Operations, Maintenance and Support

NEW QUESTION: 148
In a small organization, an IS auditor finds that security administration and system analysis functions are performed by the same employee. Which of the following is the MOST significant finding?
A. The security policy has not been updated to reflect the situation.
B. The employee's formal job description has not been updated.
C. The employee has not signed the security policy.
D. The employee's activities are not independently reviewed.
Answer: D (LEAVE A REPLY)
Section: The process of Auditing Information System

NEW QUESTION: 149
During an audit of a financial application, it was determined that many terminated users' accounts were not disabled. Which of the following should be the IS auditors NEXT step?
A. Perform a review of terminated users' account activity.
B. Communicate risks to the application owner.
C. Perform substantive testing of terminated users' access rights.
D. Conclude that IT general controls are ineffective.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 150
An IS auditor should ensure that an application's audit trail:
A. logs ail database records.
B. does not impact operational efficiency
C. Is accessible online
D. has adequate security.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 151
An IS auditor performing a telecommunication access control review should be concerned PRIMARILY with the:
A. maintenance of access logs of usage of various system resources.
B. authorization and authentication of the user prior to granting access to system resources.
C. adequate protection of stored data on servers by encryption or other means.
D. accountability system and the ability to identify any terminal accessing system resources.
Answer: B (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:

The authorization and authentication of users is the most significant aspect in a telecommunications access control review, as it is a preventive control. Weak controls at this level can affect all other aspects.
The maintenance of access logs of usage of system resources is a detective control. The adequate protection of data being transmitted to and from servers by encryption or other means is a method of protecting information during transmission and is not an access issue. The accountability system and the ability to identify any terminal accessing system resources deal with controlling access through the identification of a terminal.

NEW QUESTION: 152
Which of the following will BEST ensure the successful offshore development of business applications?
A. Stringent contract management practices
B. Detailed and correctly applied specifications
C. Awareness of cultural and political differences
D. Postimplementation reviews
Answer: B (LEAVE A REPLY)
When dealing with offshore operations, it is essential that detailed specifications be created. Language differences and a lack of interaction between developers and physically remote end users could create gaps in communication in which assumptionsand modifications may not be adequately communicated. Contract management practices, cultural and political differences, and postimplementation reviews, although important, are not as pivotal to the success of the project.

NEW QUESTION: 153
Which of the following would MOST likely impair the independence of the IS auditor when performing a post-implementation review of an application system?
A. The IS auditor implemented a specific control during the development of the application system.
B. The IS auditor designed an embedded audit module exclusively for auditing the application system.
C. The IS auditor provided consulting advice concerning application system best practices.
D. The IS auditor participated as a member of the application system pro)ecl team.
but did not have operational responsibilities.

Answer: (SHOW ANSWER)

NEW QUESTION: 154
When reviewing the configuration of network devices, an IS auditor should FIRST identify:
A. the best practices for the type of network devices deployed.
B. whether components of the network are missing.
C. the importance of the network device in the topology.
D. whether subcomponents of the network are being used appropriately.
Answer: (SHOW ANSWER)
The first step is to understand the importance and role of the network device within the organization's network topology. After understanding the devices in the network, the best practice for using the device should be reviewed to ensure that there are no anomalies within the configuration. Identification of which component or subcomponent is missing or being used inappropriately can only be known upon reviewing and understanding the topology and the best practice for deployment of the device in the network.
Topic 6, PROTECTION OF INFORMATION ASSETS (251 PRACTICE QUESTIONS)

NEW QUESTION: 155
Users are issued security tokens to be used in combination with a PIN to access the corporate virtual private network (VPN). Regarding the PIN, what is the MOST important rule to be included in a security policy?
A. Users should not leave tokens where they could be stolen
B. Users must never keep the token in the same bag as their laptop computer
C. Users should select a PIN that is completely random, with no repeating digits
D. Users should never write down their PIN
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
If a user writes their PIN on a slip of paper, an individual with the token, the slip of paper, and the computer could access the corporate network. A token and the PIN is a two-factor authentication method. Access to the token is of no value with out the PIN; one cannot work without the other. The PIN does not need to be random as long as it is secret.

NEW QUESTION: 156
Which of the following is NOT a disadvantage of Single Sign On (SSO)?
A. Support for all major operating system environment is difficult
B. The cost associated with SSO development can be significant
C. SSO could be single point of failure and total compromise of an organization asset
D. SSO improves an administrator's ability to manage user's account and authorization to all associated system
Answer: D (LEAVE A REPLY)

Explanation/Reference:
Single sign-on (SSO)is a Session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.
SSO Advantages include
Multiple passwords are no longer required
It improves an administrator's ability to manage user's accounts and authorization to all associated systems It reduces administrative overhead in resetting forgotten password over multiple platforms and applications It reduces time taken by users to logon into multiple application and platform SSO Disadvantages include Support for all major operating system is difficult
The cost associated with SSO development can be significant when considering the nature and extent of interface development and maintenance that may be necessary The centralize nature of SSO presents the possibility of a single point of failure and total compromise of an organization's information asset.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 332

NEW QUESTION: 157
Management receives information indicating a high level of risk associated with potential flooding near the organization's data center within the next few years. As a result, a decision has been made to move data center operations to another facility on higher ground. Which approach has been adopted?
A. Risk reduction
B. Risk transfer
C. Risk acceptance
D. Risk avoidance
Answer: (SHOW ANSWER)

NEW QUESTION: 158
An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?
A. A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewall.
B. Firewall policies are updated on the basis of changing requirements.
C. inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
D. The firewall is placed on top of the commercial operating system with all installation options.
Answer: (SHOW ANSWER)

The greatest concern when implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that could undermine the security posture of the firewall platform itself. In most circumstances, when commercial firewalls are breached that breach is facilitated by vulnerabilities in the underlying operating system. Keeping all installation options available on the system further increases the risks of vulnerabilities and exploits. Using SSL for firewall administration (choice A) is important, because changes in user and supply chain partners' roles and profiles will be dynamic. Therefore, it is appropriate to maintain the firewall policies daily (choice B), and prudent to block all inbound traffic unless permitted (choice C).

NEW QUESTION: 159
When identifying an earlier project completion time, which is to be obtained by paying a premium for early
completion, the activities that should be selected are those:
A. whose sum of activity time is the shortest.
B. that have zero slack time.
C. that give the longest possible completion time.
D. whose sum of slack time is the shortest.
Answer: B (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
A critical path's activity time is longer than that for any other path through the network. This path is
important because if everything goes as scheduled, its length gives the shortest possible completion time
for the overall project. Activities on the critical path become candidates for crashing, i.e., for reduction in
their time by payment of a premium for early completion. Activities on the critical path have zero slack time
and conversely, activities with zero slack time are on a critical path. By successively relaxing activities on a
critical path, a curve showing total project costs vs. time can be obtained.

NEW QUESTION: 160
Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?
A. Intrusion detection systems
B. Data mining techniques
C. Firewalls
D. Packet filtering routers
Answer: B (LEAVE A REPLY)
Explanation/Reference:

Explanation:
Data mining is a technique used to detect trends or patterns of transactions or datA. If the historical pattern of charges against a credit card account is changed, then it is a flag that the transaction may have resulted from a fraudulent use of the card.

NEW QUESTION: 161
Which of the following is MOST important when planning a network audit?
A. Analysts of traffic content
B. Isolation of rogue access points
C. Determination of IP range in use
D. Identification of existing nodes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 162
When developing a business continuity plan (BCP), which of the following tools should be used to gain an understanding of the organization's business processes?
A. Business continuity self-audit
B. Resource recovery analysis
C. Risk assessment
D. Gap analysis
Answer: C (LEAVE A REPLY)
Risk assessment and business impact assessment are tools for understanding business-forbusiness continuity planning. Business continuity self-audit is a tool for evaluating the adequacy of the BCP, resource recovery analysis is a tool for identifying a business resumption strategy, while the role gap analysis can play in business continuity planning is to identify deficiencies in a plan. Neither of these is used for gaining an understanding of the business.

NEW QUESTION: 163
Which of the following hardware upgrades would BEST enhance the capability of a web server to accommodate a significant increase in web traffic?
A. Multicore CPUs
B. Solid state drives
C. Additional flash memory
D. Cloud architecture
Answer: A (LEAVE A REPLY)
Section: Information System Operations, Maintenance and Support

NEW QUESTION: 164
Which of the following BEST helps to ensure that all relevant data within an organization is added to a data warehouse during deployment?
A. Data migration

B. Architecture review
C. Project planning
D. Data mining
Answer: A (LEAVE A REPLY)
Section: Information System Operations, Maintenance and Support

NEW QUESTION: 165
The initial step in establishing an information security program is the:
A. development and implementation of an information security standards manual.
B. performance of a comprehensive security control review by the IS auditor.
C. adoption of a corporate information security policy statement.
D. purchase of security access control software.
Answer: C (LEAVE A REPLY)
A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

NEW QUESTION: 166
When reviewing the configuration of network devices, an IS auditor should FIRST identify:
A. the best practices for the type of network devices deployed.
B. whether components of the network are missing.
C. the importance of the network device in the topology.
D. whether subcomponents of the network are being used appropriately.
Answer: C (LEAVE A REPLY)
The first step is to understand the importance and role of the network device within the organization's network topology. After understanding the devices in the network, the best practice for using the device should be reviewed to ensure that there are no anomalies within the configuration. Identification of which component or subcomponent is missing or being used inappropriately can only be known upon reviewing and understanding the topology and the best practice for deployment of the device in the network.

NEW QUESTION: 167
Which of the following is the GREATEST advantage of application penetration testing over vulnerability

scanning?
A. Penetration testing does not require a special skill set to be executed.
B. Penetration testing provides a more accurate picture of gaps in application controls.
C. Penetration testing can be conducted in a relatively short time period.
D. Penetration testing creates relatively smaller risks to application availability and integrity.
Answer: (SHOW ANSWER)
Section: Protection of Information Assets

NEW QUESTION: 168
An IS auditor has completed a review of an outsourcing agreement and has communicating the issues at a meeting with senior management?
A. Provide a plan of action and milestones.
B. Present an overview highlighting the key findings.
C. Provide a detailed report in advance and open the floor to questions.
D. Present a completed report and discuss the details.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 169
The application systems quality assurance (QA) function should:
A. assist programmers in designing and developing applications.
B. compare programs to approved system changes.
C. design and develop quality applications by employing system development methodology.
D. ensure adherence of programs to standards.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 170
Which of the following hardware devices relieves the central computer from performing network control,
format conversion and message handling tasks?
A. Spool
B. Cluster controller
C. Protocol converter
D. Front end processor
Answer: D (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
A front-end processor is a hardware device that connects all communication lines to a central computer to
relieve the central computer.

NEW QUESTION: 171

Which of the following activities should the business continuity manager perform FIRST after the replacement of hardware at the primary information processing facility?
A. verify compatibility with the hot site.
B. Review the implementation report.
C. Perform a walk-through of the disaster recovery plan.
D. Update the IS assets inventory.
Answer: D (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
An IS assets inventory is the basic input for the business continuity/disaster recovery plan, and the plan
must be updated to reflect changes in the IS infrastructure. The other choices are procedures required to
update the disaster recovery plan after having updated the required assets inventory.

NEW QUESTION: 172
When would an IS auditor expect to see testing completed for a protect using agile methodology?
A. At the end of development
B. Just before a major release
C. Parallel to the development activity
D. After the requirements phase
Answer: C (LEAVE A REPLY)

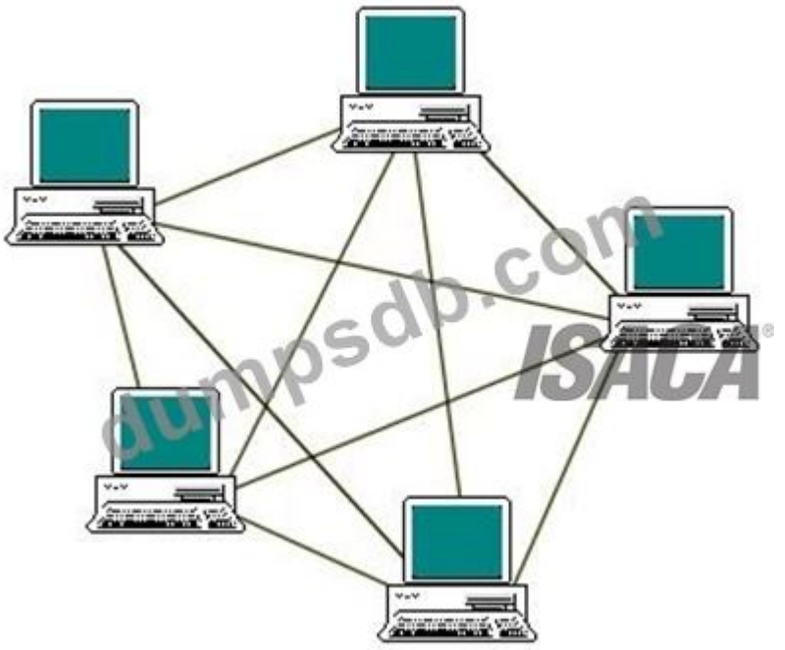
NEW QUESTION: 173
Which of the following methods of encryption has been proven to be almost unbreakable when correctly used?
A. key pair
B. Oakley
C. certificate
D. 3-DES
E. one-time pad
F. None of the choices.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
It's possible to protect messages in transit by means of cryptography.
One method of encryption --the one-time pad --has been proven to be unbreakable when correctly used.
This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

NEW QUESTION: 174
A risk analysis for a new system is being performed. For which of the following is business knowledge MORE important than IT knowledge?
A. Vulnerability analysis
B. Cost-benefit analysis
C. Impact analysis
D. Balanced scorecard
Answer: (SHOW ANSWER)
Section: Information System Acquisition, Development and Implementation

NEW QUESTION: 175
A certificate authority (CA) can delegate the processes of:
A. revocation and suspension of a subscriber's certificate.
B. generation and distribution of the CA public key.
C. establishing a link between the requesting entity and its public key.
D. issuing and distributing subscriber certificates.,
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Establishing a link between the requesting entity and its public key is a function of a registration authority.
This may or may not be performed by a CA; therefore, this function can be delegated. Revocation and suspension and issuance and distribution of the subscriber certificate are functions of the subscriber certificate life cycle management, which the CA must perform. Generation and distribution of the CA public key is a part of the CA key life cycle management process and, as such, cannot be delegated.

NEW QUESTION: 176
Which of the following sampling methods is the BEST approach for drawing conclusions based on frequency of occurrence?
A. Difference estimation sampling
B. Stratified sampling
C. Monetary estimation sampling
D. Attribute sampling
Answer: (SHOW ANSWER)

NEW QUESTION: 177
Identify the network topology from below diagram presented below:



Network Topology

A. Bus

B. Star

C. Ring

D. Mesh

Answer: (SHOW ANSWER)

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.

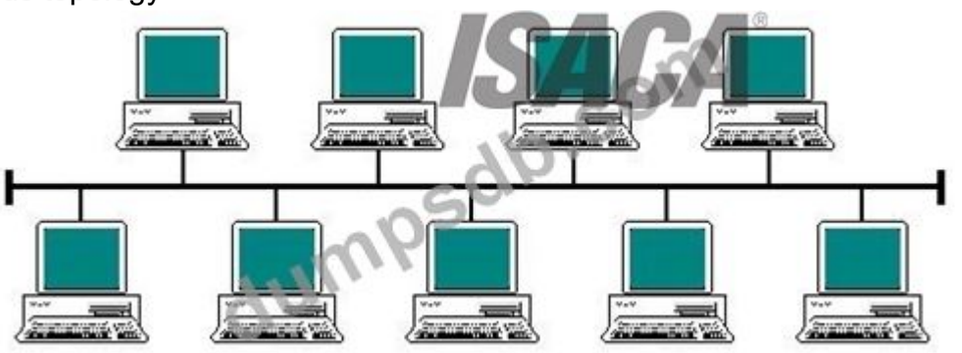
Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

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

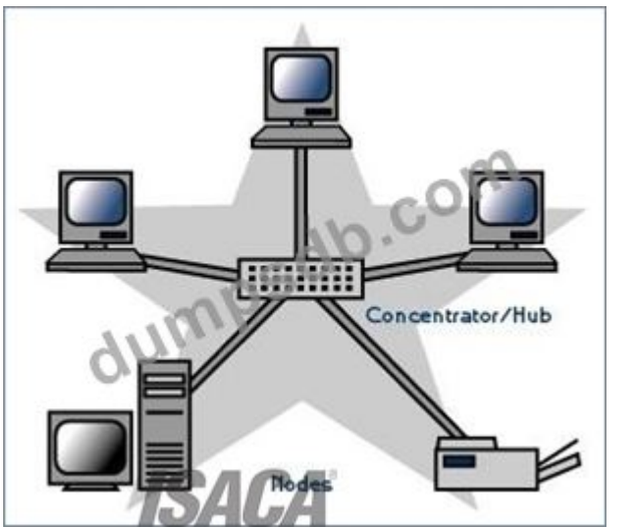


Image from: http://fcit.usf.edu/network/chap5/pics/star.gif

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

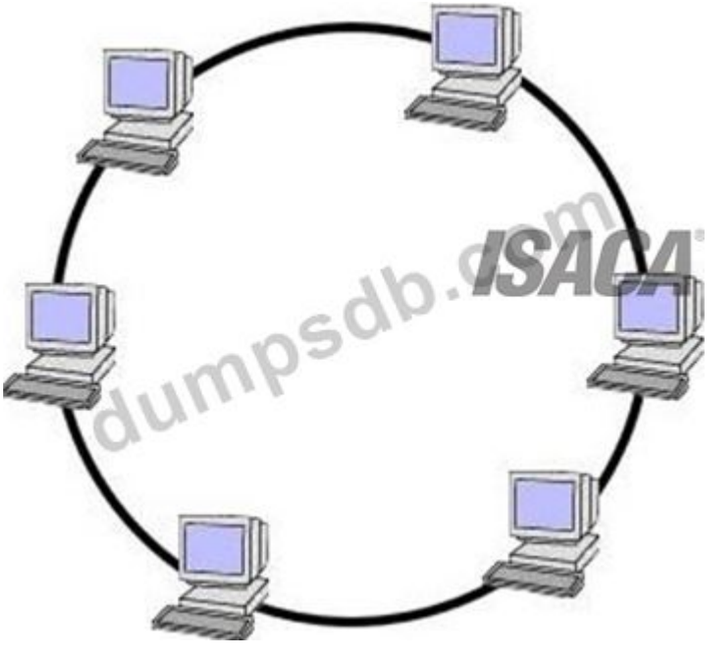


Image from: https://forrester-infosystems.wikispaces.com/

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

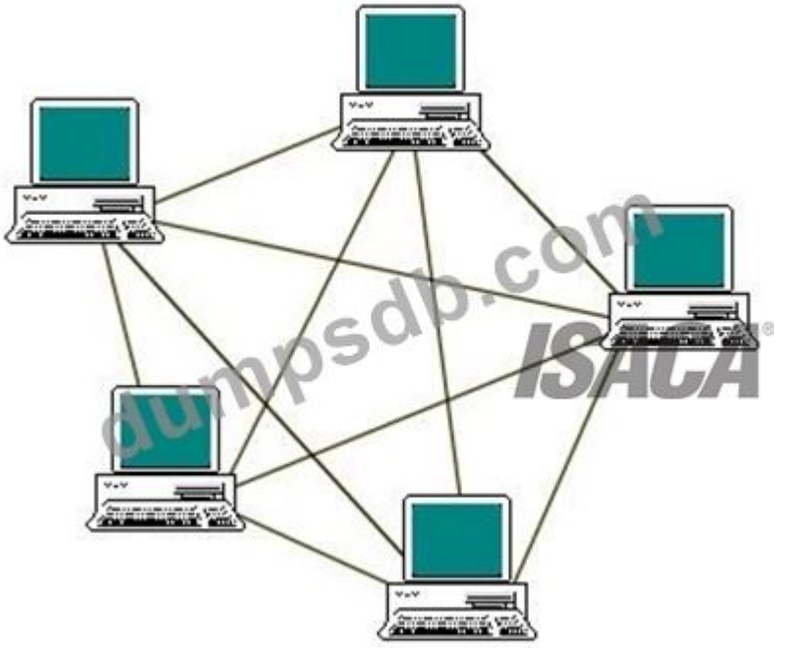


Image from:
http://www.technologyuk.net/telecommunications/networks/images/mesh_topology.gif Fully connected mesh topology
A fully connected network is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network 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: 178
Which of the following should an IS auditor be MOST concerned with during a post-implementation review?
A. The system does not have a maintenance plan
B. The system contains several minor defects

C. The system was over budget by 15%
D. The system deployment was delayed by three weeks
Answer: (SHOW ANSWER)
Section: The process of Auditing Information System
Explanation

NEW QUESTION: 179
The IS auditor learns that when equipment was brought into the data center by a vendor, the emergency power shutoff switch was accidentally pressed and the UPS was engaged. Which of the following audit recommendations should the IS auditor suggest?
A. Relocate the shut off switch.
B. Install protective covers.
C. Escort visitors.
D. Log environmental failures.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A protective cover over the switch would allow it to be accessible and visible, but would prevent accidental activation.
Incorrect Answers:
A. Relocating the shut off switch would defeat the purpose of having it readily accessible.
C. Escorting the personnel moving the equipment may not have prevented this incident.
D. Logging of environmental failures would provide management with a report of incidents, but reporting alone would not prevent a reoccurrence.

NEW QUESTION: 180
In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?
A. Automated logging of changes to development libraries
B. Additional staff to provide separation of duties
C. Procedures that verify that only approved program changes are implemented
D. Access controls to prevent the operator from making program modifications
Answer: C (LEAVE A REPLY)
While it would be preferred that strict separation of duties be adhered to and that additional staff is recruited as suggested in choice B, this practice is not always possible in small organizations. An IS auditor must look at recommended alternative processes. Of the choices, C is the only practical one that has an impact. An IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed on a regular basis by a third party. This would be a compensating control process. Choice A, involving logging of changes to development libraries, would not detect changes to

production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

NEW QUESTION: 181
A typical network architecture used for e-commerce, a load balancer is normally found between the:
A. users and the external gateways.
B. routers and the web servers.
C. mail servers and the mail repositories
D. databases and the external gateways,
Answer: B (LEAVE A REPLY)

NEW QUESTION: 182
When auditing the effectiveness of a biometric system, which of the following indicators would be MOST
important to review?
A. False negatives
B. False acceptance rate
C. Failure to enroll rate
D. System response time
Answer: B (LEAVE A REPLY)
Section: The process of Auditing Information System

NEW QUESTION: 183
When segregation of duties concerns exist between IT support staff and end users, what would be a suitable compensating control?
A. Restricting physical access to computing equipment
B. Reviewing transaction and application logs
C. Performing background checks prior to hiring IT staff
D. Locking user sessions after a specified period of inactivity
Answer: B (LEAVE A REPLY)
Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also

discourages abuse, because people who may otherwise be tempted to exploit the situation are aware of the likelihood of being caught. Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure ITstaff are trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to prevent unauthorized users from gaining system access, but the issue of a lack of segregation of duties is more the misuse (deliberately or inadvertently} of access privileges that have officially been granted.

NEW QUESTION: 184
Overall responsibility for approving logical access rights to information assets should reside with the:
A. data and systems owners.
B. systems delivery and operations group.
C. security administrator.
D. systems administrator.
Answer: (SHOW ANSWER)
Section: Information System Operations, Maintenance and Support

NEW QUESTION: 185
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)
Explanation/Reference:
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: 186
A call-back system requires that a user with an id and password call a remote server through a dial-up line,
then the server disconnects and:
A. dials back to the user machine based on the user id and password using a telephone number from its

database.
B. dials back to the user machine based on the user id and password using a telephone number provided
by the user during this connection.
C. waits for a redial back from the user machine for reconfirmation and then verifies the user id and
password using its database.
D. waits for a redial back from the user machine for reconfirmation and then verifies the user id and
password using the sender's database.
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation:
A call-back system in a net centric environment would mean that a user with an id and password calls a
remote server through a dial-up line first, and then the server disconnects and dials back to the user
machine based on the user id and password using a telephone number from its database. Although the
server can depend upon its own database, it cannot know the authenticity of the dialer when the user dials
again. The server cannot depend upon the sender's database to dial back as the same could be manipulated.

NEW QUESTION: 187
An IS auditor observes a weakness in the tape management system at a data center in that some parameters are set to bypass or ignore tape header records. Which of the following is the MOST effective
compensating control for this weakness?
A. Staging and job set up
B. Supervisory review of logs
C. Regular back-up of tapes
D. Offsite storage of tapes
Answer: A (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
If the IS auditor finds that there are effective staging and job set up processes, this can be accepted as a
compensating control. Choice B is a detective control while choices C and D are corrective controls, none
of which would serve as good compensating controls.

NEW QUESTION: 188
Which of the following is the PRIMARY benefit of using an integrated audit approach?
A. Higher acceptance of the findings from the audited business areas
B. The avoidance of duplicated work and redundant recommendations
C. Enhanced allocation of resources and reduced audit costs
D. A holistic perspective of overall risk and a better understanding of controls
Answer: D (LEAVE A REPLY)
Section: The process of Auditing Information System

NEW QUESTION: 189
When reviewing the configuration of network devices, an IS auditor should FIRST identify:
A. the best practices for the type of network devices deployed.
B. whether components of the network are missing.
C. the importance of the network device in the topology.
D. whether subcomponents of the network are being used appropriately.
Answer: C (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
The first step is to understand the importance and role of the network device within the organization's network topology. After understanding the devices in the network, the best practice for using the device should be reviewed to ensure that there are no anomalies within the configuration. Identification of which component or subcomponent is missing or being used inappropriately can only be known upon reviewing and understanding the topology and the best practice for deployment of the device in the network.

NEW QUESTION: 190
An IS auditor is reviewing security controls related to collaboration tools for a business unit responsible for intellectual property and patents. Which of the following observations should be of MOST concern to the auditor?
A. Logging and monitoring for content filtering is not enabled.
B. Training was not provided to the department that handles intellectual property and patents
C. Employees can share files with users outside the company through collaboration tools.
D. The collaboration tool is hosted and can only be accessed via an Internet browser.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 191
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: (SHOW ANSWER)
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

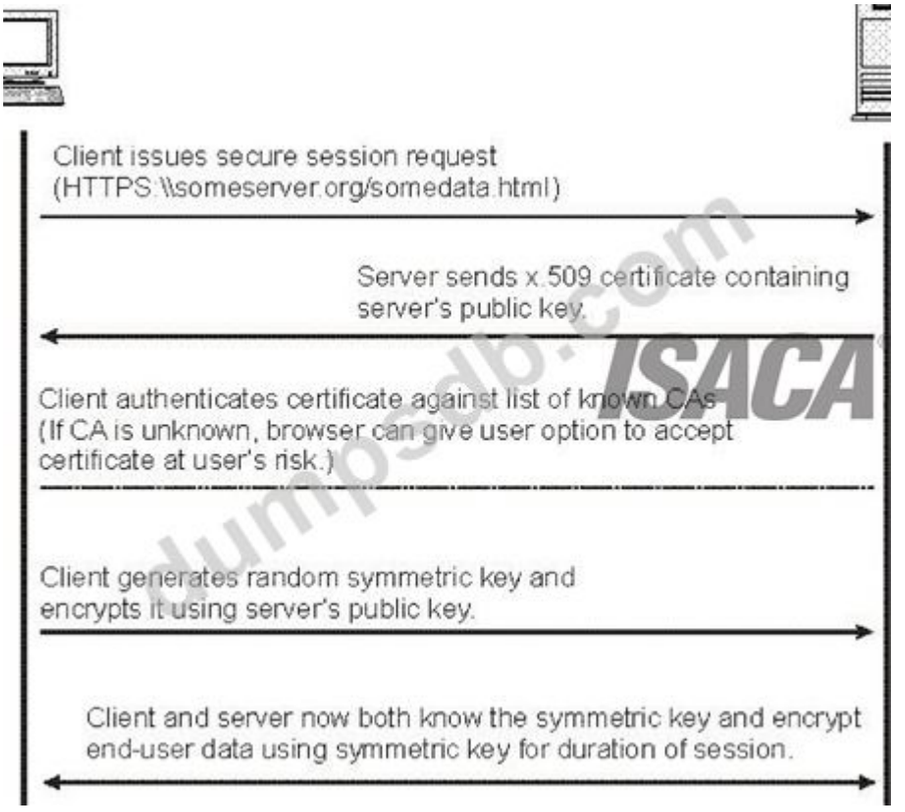


Image Reference - http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1363-00/en_US/HTML/handshak.gif

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: 192

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: (SHOW ANSWER)

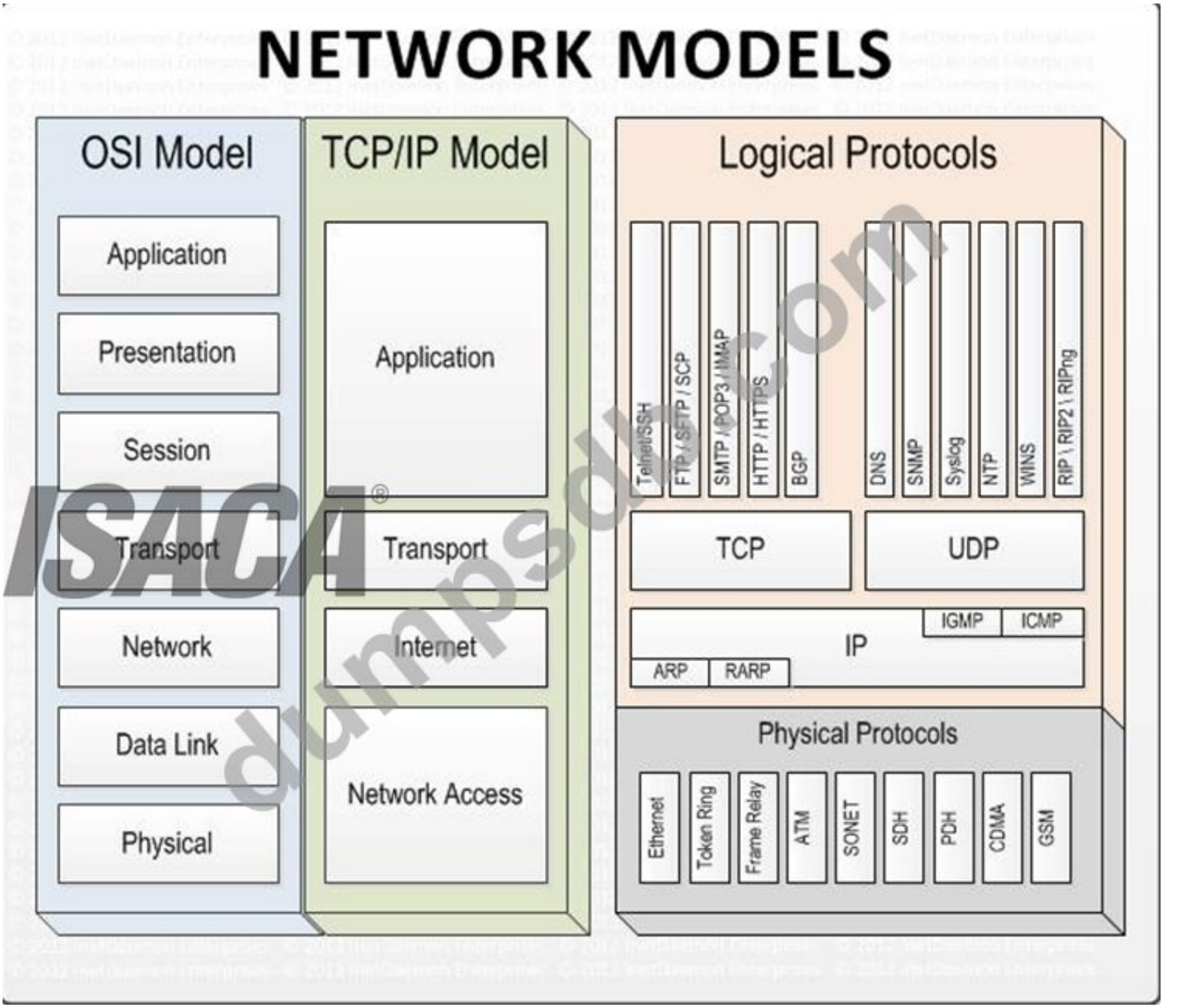
Explanation/Reference:

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.

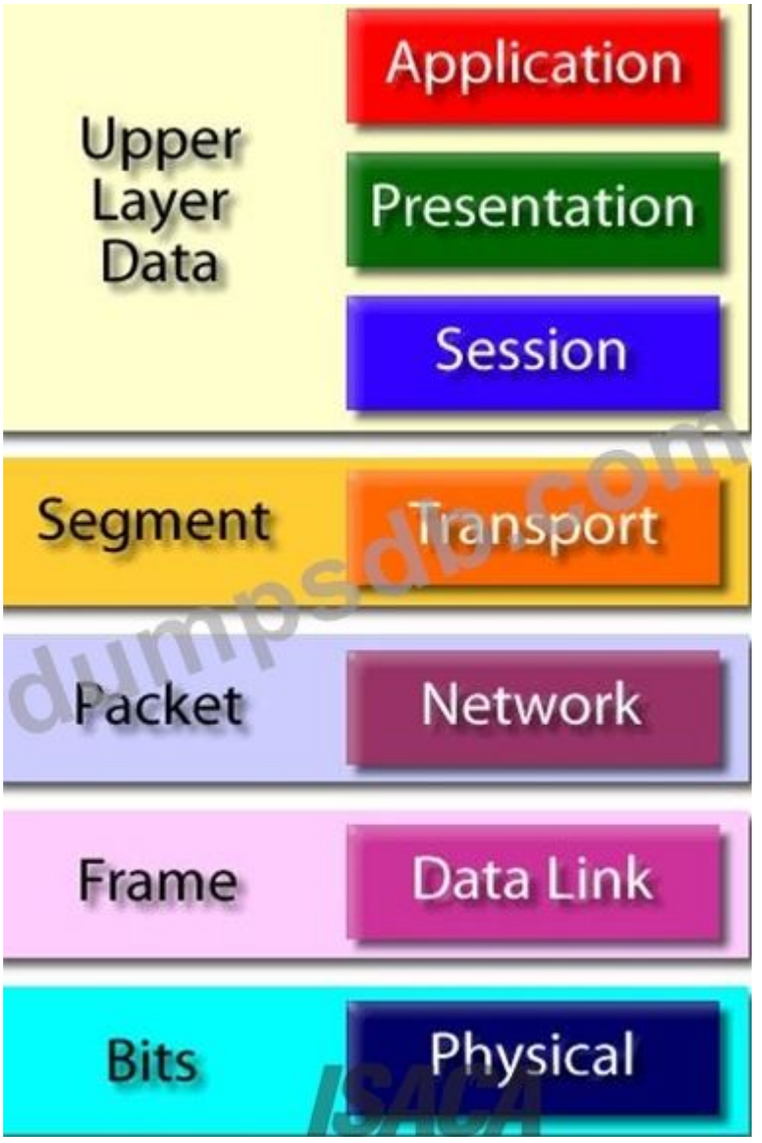
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

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: 193

For which of the following applications would rapid recovery be MOST crucial?

A. Point-of-sale system
B. Corporate planning
C. Regulatory reporting
D. Departmental chargeback
Answer: A (LEAVE A REPLY)
A point-of-sale system is a critical online system that when inoperable will jeopardize the ability of Company.com to generate revenue and track inventory properly.

NEW QUESTION: 194
In what way is a common gateway interface (CGI) MOST often used on a webserver?
A. Consistent way for transferring data to the application program and back to the user
B. Computer graphics imaging method for movies and TV
C. Graphic user interface for web design
D. interface to access the private gateway domain
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation:
The common gateway interface (CGI) is a standard way for a web server to pass a user's request to an
application program and to move data back and forth to the user. When the user requests a web page (for
example, by clicking on a highlighted word orienteering a web site address), the server sends back the
requested page. However, when a user fills out a form on a web page and submits it, it usually needs to be
processed by an application program. The web server typically passes the form information to a small
application program that processes the data and may send back a confirmation message. This method, or
convention, for passing data back and forth between the server and the application is called the common
gateway interface (CGI). It is part of the web's HTTP protocol.

NEW QUESTION: 195
Which of the following is the BEST indicator of the effectiveness of signature-based intrusion detection systems (IDSs)?
A. An increase in the number of internally reported critical incidents
B. An increase in the number of unfamiliar sources of intruders
C. An increase in the number of detected incidents not previously identified
D. An increase in the number of identified false positives
Answer: (SHOW ANSWER)

NEW QUESTION: 196
When an organization introduces virtualization into its architecture, which of the following should be an IS auditor's PRIMARY area of focus to verify adequate protection?
A. Host operating system configuration
B. Shared storage space
C. Maintenance cycles
D. Multiple versions of the same operating system
Answer: A (LEAVE A REPLY)

NEW QUESTION: 197
An IS auditor is reviewing a small organization's business continuity and disaster recovery plans Which of the following findings would pose the GREATEST concern?
A. Data backup and storage is not performed every day
B. The organization's hardware is near end-of-the
C. Practice drills related to the plans are conducted infrequently
D. The plans are not periodically reviewed and updated
Answer: D (LEAVE A REPLY)

NEW QUESTION: 198
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)
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: 199
Which of the following types of data validation editing checks is used to determine if a field contains data,
and not zeros or blanks?
A. Check digit
B. Existence check
C. Completeness check
D. Reasonableness check
Answer: C (LEAVE A REPLY)
Section: Protection of Information Assets
Explanation:
A completeness check is used to determine if a field contains data and not zeros or blanks.

NEW QUESTION: 200
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)
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: 201
Which of the following is MOST critical to the success of an information security program?
A. Integration of business and information security
B. Alignment of information security with IT objectives
C. Management's commitment to information security
D. User accountability for information security
Answer: (SHOW ANSWER)
Section: Governance and Management of IT

NEW QUESTION: 202
The use of statistical sampling procedures helps minimize:
A. Detection risk
B. Business risk
C. Controls risk
D. Compliance risk
Answer: (SHOW ANSWER)
Section: Protection of Information Assets
Explanation:
The use of statistical sampling procedures helps minimize detection risk.

NEW QUESTION: 203
The PRIMARY purpose of implementing Redundant Array of Inexpensive Disks (RAID) level 1 in a file server is to:
A. achieve performance improvement.
B. provide user authentication.
C. ensure availability of data.
D. ensure the confidentiality of data.
Answer: (SHOW ANSWER)
RAID level 1 provides disk mirroring. Data written to one disk are also written to another disk. Users in the network access data in the first disk; if disk one fails, the second disk takes over. This redundancy ensures the availability of datA . RAID level 1 does not improve performance, has no relevance to authentication and does nothing to provide for data confidentiality.

NEW QUESTION: 204
The PRIMARY role of a control self-assessment (CSA) facilitator is lo:
A. conduct interviews to gain background information.
B. report on the internal control weaknesses
C. focus the team on internal controls.
D. provide solutions (or control weaknesses
Answer: C (LEAVE A REPLY)

NEW QUESTION: 205
An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST cost-effective test of the DRP?
A. Full operational test
B. Preparedness test
C. Paper test
D. Regression test
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 206
Which of the following BEST ensures the confidentiality of sensitive data during transmission?
A. Sending data over public networks using Transport Layer Security (TLS)
B. Sending data through proxy servers
C. Password protecting data over virtual local area networks (VLAN)
D. Restricting the recipient through destination IP addresses
Answer: A (LEAVE A REPLY)

NEW QUESTION: 207
The recovery point objective (RPO) is required in which of the following?
A. Information security plan
B. Incident response plan
C. Disaster recovery plan
D. Business continuity plan
Answer: (SHOW ANSWER)
Section: Protection of Information Assets

NEW QUESTION: 208
When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:
A. not be concerned since there may be other compensating controls to mitigate the risks.
B. ensure that overrides are automatically logged and subject to review.
C. verify whether all such overrides are referred to senior management for approval.
D. recommend that overrides not be permitted.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
If input procedures allow overrides of data validation and editing, automatic logging should occur. A management individual who did not initiate the override should review this log. An IS auditor should not assume that compensating controls exist. Aslong as the overrides are policy-compliant, there is no need for senior management approval or a blanket prohibition.

NEW QUESTION: 209

An organization has recently implemented a Voice-over IP (VoIP) communication system. Which ot the following should be the IS auditor's PRIMARY concern?
A. Voice quality degradation due to packet toss
B. A single point of failure for both voice and data communications
C. Lack of integration of voice and data communications
D. Inability to use virtual private networks (VPNs) for internal traffic
Answer: B (LEAVE A REPLY)

NEW QUESTION: 210
Which of the following is an example of a preventive control?
A. Regular assessments of the sales department to identify the most profitable sales strategies used by sales staff
B. Purchase orders in the system being checked by a supervisor prior to execution to identify errors during entry
C. An online retailer's daily review of transactions processed to identify trends and changes in customer demand
D. Continuous operation of a screening system to identify fraudulent patterns in recent transactions
Answer: B (LEAVE A REPLY)

NEW QUESTION: 211
Which of the following would be of MOST concern for an IS auditor evaluating the design of an organization's incident management processes?
A. Expected time to resolve incidents is not specified.
B. Service management standards are not followed.
C. Metrics are not reported to senior management.
D. Prioritization criteria are not defined.
Answer: (SHOW ANSWER)

NEW QUESTION: 212
During a post-implementation review, an IS auditor learns that while benefits were realized according to the business case, complications during implementation added to the cost of the solution. Which of the following is the auditor's BEST course of action?

A. Design controls that will prevent future added costs.
B. Ensure costs related to the complications were subtracted from realized benefits.
C. Verify that lessons learned were documented for future projects.
D. Determine if project deliverables were provided on time
Answer: C (LEAVE A REPLY)

NEW QUESTION: 213
A retirement system verifies that the field for employee status has either a value of A (for active) or R (for retired). This is an example of which type of check?
A. Completeness
B. Existence
C. Validity
D. Limit
Answer: (SHOW ANSWER)

NEW QUESTION: 214
As part of a mergers and acquisitions activity, an acquiring organization wants to consolidate data and
system from the organization being acquired into existing systems. To ensure the data is relevant, the
acquiring organization should:
A. obtain data quality software.
B. define data quality requirements based on business needs.
C. automate the process of data collection and cleaning.
D. implement a data warehouse solution.
Answer: B (LEAVE A REPLY)
Section: Protection of Information Assets

NEW QUESTION: 215
An organization needs to comply with data privacy regulations forbidding the display of personally identifiable information (PII) on customer bills or receipts However it is a business requirement to display at least one attribute so that customers can verify the bills or receipts are intended for them What is the BEST recommendation?
A. Data sanitization
B. Data encryption
C. Data tokenization
D. Data masking
Answer: D (LEAVE A REPLY)

NEW QUESTION: 216

An IS auditor reviewing digital rights management (DRM) applications should expect to find an extensive use for which of the following technologies?
A. Digitalized signatures
B. Hashing
C. Parsing
D. Steganography
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Steganography is a technique for concealing the existence of messages or information. An increasingly important stenographical technique is digital watermarking, which hides data within data, e.g., by encoding rights information in a picture or music file without altering the picture or music's perceivable aesthetic qualities. Digitalized signatures are not related to digital rights management. Hashing creates a message hash or digest, which is used to ensure the integrity of the message; it is usually considered a part of cryptography. Parsing is the process of splitting up a continuous stream of characters for analytical purposes, and is widely applied in the design of programming languages or in data entry editing.

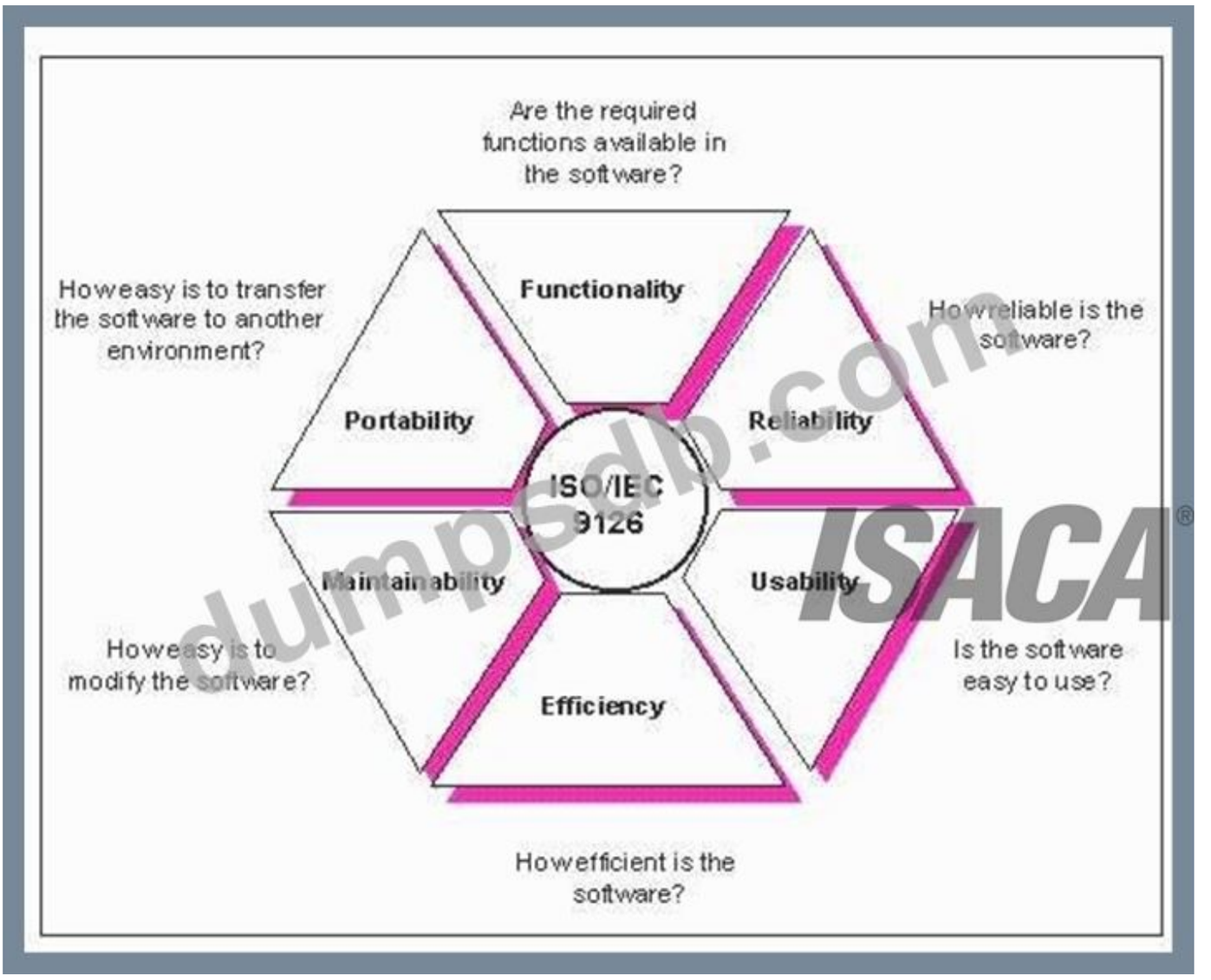
NEW QUESTION: 217
Which of the following is a practice that should be incorporated into the plan for testing disaster recovery procedures?
A. Invite client participation.
B. involve all technical staff.
C. Rotate recovery managers.
D. install locally-stored backup.
Answer: (SHOW ANSWER)
Recovery managers should be rotated to ensure the experience of the recovery plan is spread among the managers. Clients may be involved but not necessarily in every case. Not all technical staff should be involved in each test. Remote or offsite backup should always be used.

NEW QUESTION: 218
A complex IS environment which of the following tasks should be performed by the data owner?
A. Perform technical database maintenance.
B. Perform data restoration when necessary.
C. Review data classifications periodically
D. Test the validity of backup data
Answer: C (LEAVE A REPLY)

NEW QUESTION: 219
Which of the following should be of MOST concern to an IS auditor evaluating a forensics program?

A. Forensic images are stored on removable media with encryption.
B. Forensic images are only stored for involuntarily terminated employees.
C. Forensic images are only maintained for 12 months.
D. Forensic images are stored on shared disks.
Answer: D (LEAVE A REPLY)
Section: The process of Auditing Information System

NEW QUESTION: 220
ISO 9126 is a standard to assist in evaluating the quality of a product. Which of the following is defined as a set of attributes that bear on the existence of a set of functions and their specified properties?
A. Reliability
B. Usability
C. Functionality
D. Maintainability
Answer: (SHOW ANSWER)
Section: Information System Acquisition, Development and Implementation Explanation:
Functionality - A set of attributes that bear on the existence of a set of functions and their specified properties.
The functions are those that satisfy stated or implied needs.
Suitability
Accuracy
Interoperability
Security
Functionality Compliance
For CISA Exam you should know below information about ISO 9126 model:
ISO/IEC 9126 Software engineering - Product quality was an international standard for the evaluation of software quality. It has been replaced by ISO/IEC 25010:2011.[1] The fundamental objective of the ISO/IEC
9126 standard is to address some of the well-known human biases that can adversely affect the delivery and perception of a software development project. These biases include changing priorities after the start of a project or not having any clear definitions of "success." By clarifying, then agreeing on the project priorities and subsequently converting abstract priorities (compliance) to measurable values (output data can be validated against schema X with zero intervention), ISO/IEC 9126 tries to develop a common understanding of the project's objectives and goals.
ISO 9126



The standard is divided into four parts:

Quality model

External metrics

Internal metrics

Quality in use metrics.

Quality Model

The quality model presented in the first part of the standard, ISO/IEC 9126-1,[2] classifies software quality in a structured set of characteristics and sub-characteristics as follows:

Functionality - A set of attributes that bear on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs.

Suitability

Accuracy

Interoperability

Security

Functionality Compliance

Reliability - A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.

Maturity
Fault Tolerance
Recoverability
Reliability Compliance
Usability - A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users.
Understandability
Learn ability
Operability
Attractiveness
Usability Compliance
Efficiency - A set of attributes that bear on the relationship between the level of performance of the software and the amount of resources used, under stated conditions.
Time Behavior
Resource Utilization
Efficiency Compliance
Maintainability - A set of attributes that bear on the effort needed to make specified modifications.
Analyzability
Changeability
Stability
Testability
Maintainability Compliance
Portability - A set of attributes that bear on the ability of software to be transferred from one environment to another.
Adaptability
Install ability
Co-Existence
Replace ability
Portability Compliance
Each quality sub-characteristic (e.g. adaptability) is further divided into attributes. An attribute is an entity which can be verified or measured in the software product. Attributes are not defined in the standard, as they vary between different software products.
Software product is defined in a broad sense: it encompasses executables, source code, architecture descriptions, and so on. As a result, the notion of user extends to operators as well as to programmers, which are users of components such as software libraries.
The standard provides a framework for organizations to define a quality model for a software product. On doing so, however, it leaves up to each organization the task of specifying precisely its own model. This may be done, for example, by specifying target values for quality metrics which evaluates the degree of presence of quality attributes.
Internal Metrics

Internal metrics are those which do not rely on software execution (static measure) External Metrics External metrics are applicable to running software.
Quality in Use Metrics
Quality in use metrics are only available when the final product is used in real conditions.
Ideally, the internal quality determines the external quality and external quality determines quality in use.
This standard stems from the GE model for describing software quality, presented in 1977 by McCall et al., which is organized around three types of Quality Characteristics:
Factors (To specify): They describe the external view of the software, as viewed by the users.
Criteria (To build): They describe the internal view of the software, as seen by the developer.
Metrics (To control): They are defined and used to provide a scale and method for measurement.
ISO/IEC 9126 distinguishes between a defect and a nonconformity, a defect being The nonfulfillment of intended usage requirements, whereas a nonconformity is The nonfulfillment of specified requirements. A similar distinction is made between validation and verification, known as V&V in the testing trade.
The following were incorrect answers:
Reliability - A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.
Usability - A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users.
Maintainability - A set of attributes that bear on the effort needed to make specified modifications.
Reference:
CISA review manual 2014 Page number 188