ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

NEW QUESTION 1
- (Exam Topic 1)
Which of the following represents the GREATEST risk to data confidentiality?

A. Network redundancies are not implemented
B. Security awareness training is not completed
C. Backup tapes are generated unencrypted
D. Users have administrative privileges

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
Which of the following types of technologies would be the MOST cost-effective method to provide a reactive control for protecting personnel in public areas?

A. Install mantraps at the building entrances
B. Enclose the personnel entry area with polycarbonate plastic
C. Supply a duress alarm for personnel exposed to the public
D. Hire a guard to protect the public area

Answer: D

NEW QUESTION 3
- (Exam Topic 2)
In a data classification scheme, the data is owned by the

A. system security managers
B. business managers
C. Information Technology (IT) managers
D. end users

Answer: B

NEW QUESTION 4
- (Exam Topic 3)
Which security service is served by the process of encryption plaintext with the sender’s private key and decrypting cipher text with the sender’s public key?

A. Confidentiality
B. Integrity
C. Identification
D. Availability

Answer: A

NEW QUESTION 5
- (Exam Topic 3)
Which component of the Security Content Automation Protocol (SCAP) specification contains the data required to estimate the severity of vulnerabilities identified automated vulnerability assessments?

A. Common Vulnerabilities and Exposures (CVE)
B. Common Vulnerability Scoring System (CVSS)
C. Asset Reporting Format (ARF)
D. Open Vulnerability and Assessment Language (OVAL)

Answer: B

NEW QUESTION 6
- (Exam Topic 3)
The use of private and public encryption keys is fundamental in the implementation of which of the following?

A. Diffie-Hellman algorithm
B. Secure Sockets Layer (SSL)
C. Advanced Encryption Standard (AES)
D. Message Digest 5 (MD5)

Answer: A

NEW QUESTION 7
- (Exam Topic 4)
An external attacker has compromised an organization’s network security perimeter and installed a sniffer onto an inside computer. Which of the following is the MOST effective layer of security the organization could have implemented to mitigate the attacker’s ability to gain further information?

A. Implement packet filtering on the network firewalls
B. Install Host Based Intrusion Detection Systems (HIDS)
C. Require strong authentication for administrators

D. Implement logical network segmentation at the switches

Answer: D

NEW QUESTION 8
- (Exam Topic 4)
In a Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which layer is responsible for negotiating and establishing a connection with another node?

A. Transport layer
B. Application layer
C. Network layer
D. Session layer

Answer: A

NEW QUESTION 9
- (Exam Topic 4)
At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

A. Link layer
B. Physical layer
C. Session layer
D. Application layer

Answer: D

NEW QUESTION 10
- (Exam Topic 6)
A Virtual Machine (VM) environment has five guest Operating Systems (OS) and provides strong isolation. What MUST an administrator review to audit a user's access to data files?

A. Host VM monitor audit logs
B. Guest OS access controls
C. Host VM access controls
D. Guest OS audit logs

Answer: A

NEW QUESTION 10
- (Exam Topic 6)
Which of the following is of GREATEST assistance to auditors when reviewing system configurations?

A. Change management processes
B. User administration procedures
C. Operating System (OS) baselines
D. System backup documentation

Answer: A

NEW QUESTION 14
- (Exam Topic 7)
A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?

A. Guaranteed recovery of all business functions
B. Minimization of the need decision making during a crisis
C. Insurance against litigation following a disaster
D. Protection from loss of organization resources

Answer: D

NEW QUESTION 15
- (Exam Topic 7)
Which of the following is a PRIMARY advantage of using a third-party identity service?

A. Consolidation of multiple providers
B. Directory synchronization
C. Web based logon
D. Automated account management

Answer: D

NEW QUESTION 19
- (Exam Topic 7)
What is the PRIMARY reason for implementing change management?

A. Certify and approve releases to the environment
B. Provide version rollbacks for system changes
C. Ensure that all applications are approved
D. Ensure accountability for changes to the environment

Answer: D

NEW QUESTION 21
- (Exam Topic 8)
Which of the following is the BEST method to prevent malware from being introduced into a production environment?

A. Purchase software from a limited list of retailers
B. Verify the hash key or certificate key of all updates
C. Do not permit programs, patches, or updates from the Internet
D. Test all new software in a segregated environment

Answer: D

NEW QUESTION 23
- (Exam Topic 9)
A vulnerability test on an Information System (IS) is conducted to

A. exploit security weaknesses in the IS.
B. measure system performance on systems with weak security controls.
C. evaluate the effectiveness of security controls.
D. prepare for Disaster Recovery (DR) planning.

Answer: C

NEW QUESTION 24
- (Exam Topic 9)
Contingency plan exercises are intended to do which of the following?

A. Train personnel in roles and responsibilities
B. Validate service level agreements
C. Train maintenance personnel
D. Validate operation metrics

Answer: A

NEW QUESTION 29
- (Exam Topic 9)
In the area of disaster planning and recovery, what strategy entails the presentation of information about the plan?

A. Communication
B. Planning
C. Recovery
D. Escalation

Answer: A

NEW QUESTION 33
- (Exam Topic 9)
What technique BEST describes antivirus software that detects viruses by watching anomalous behavior?

A. Signature
B. Inference
C. Induction
D. Heuristic

Answer: D

NEW QUESTION 36
- (Exam Topic 9)
An internal Service Level Agreement (SLA) covering security is signed by senior managers and is in place. When should compliance to the SLA be reviewed to ensure that a good security posture is being delivered?

A. As part of the SLA renewal process
B. Prior to a planned security audit
C. Immediately after a security breach
D. At regularly scheduled meetings

Answer: D

NEW QUESTION 41

- (Exam Topic 9)
The overall goal of a penetration test is to determine a system's

A. ability to withstand an attack.
B. capacity management.
C. error recovery capabilities.
D. reliability under stress.

Answer: A

NEW QUESTION 46
- (Exam Topic 9)
The Structured Query Language (SQL) implements Discretionary Access Controls (DAC) using

A. INSERT and DELETE.
B. GRANT and REVOKE.
C. PUBLIC and PRIVATE.
D. ROLLBACK and TERMINATE.

Answer: B

NEW QUESTION 47
- (Exam Topic 9)
Including a Trusted Platform Module (TPM) in the design of a computer system is an example of a technique to what?

A. Interface with the Public Key Infrastructure (PKI)
B. Improve the quality of security software
C. Prevent Denial of Service (DoS) attacks
D. Establish a secure initial state

Answer: D

NEW QUESTION 52
- (Exam Topic 9)
Multi-threaded applications are more at risk than single-threaded applications to

A. race conditions.
B. virus infection.
C. packet sniffing.
D. database injection.

Answer: A

NEW QUESTION 53
- (Exam Topic 9)
Which of the following is an authentication protocol in which a new random number is generated uniquely for each login session?

A. Challenge Handshake Authentication Protocol (CHAP)
B. Point-to-Point Protocol (PPP)
C. Extensible Authentication Protocol (EAP)
D. Password Authentication Protocol (PAP)

Answer: A

NEW QUESTION 56
- (Exam Topic 9)
A security professional has just completed their organization's Business Impact Analysis (BIA). Following Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) best practices, what would be the professional's NEXT step?

A. Identify and select recovery strategies.
B. Present the findings to management for funding.
C. Select members for the organization's recovery teams.
D. Prepare a plan to test the organization's ability to recover its operations.

Answer: A

NEW QUESTION 60
- (Exam Topic 9)
The BEST method of demonstrating a company's security level to potential customers is

A. a report from an external auditor.
B. responding to a customer's security questionnaire.
C. a formal report from an internal auditor.
D. a site visit by a customer's security team.

Answer: A

NEW QUESTION 63
- (Exam Topic 9)
Which of the following does the Encapsulating Security Payload (ESP) provide?

A. Authorization and integrity
B. Availability and integrity
C. Integrity and confidentiality
D. Authorization and confidentiality

Answer: C

NEW QUESTION 68
- (Exam Topic 9)
Which of the following assessment metrics is BEST used to understand a system's vulnerability to potential exploits?

A. Determining the probability that the system functions safely during any time period
B. Quantifying the system's available services
C. Identifying the number of security flaws within the system
D. Measuring the system's integrity in the presence of failure

Answer: C

NEW QUESTION 73
- (Exam Topic 9)
The use of strong authentication, the encryption of Personally Identifiable Information (PII) on database servers, application security reviews, and the encryption of data transmitted across networks provide

A. data integrity.
B. defense in depth.
C. data availability.
D. non-repudiation.

Answer: B

NEW QUESTION 77
- (Exam Topic 9)
The FIRST step in building a firewall is to

A. assign the roles and responsibilities of the firewall administrators.
B. define the intended audience who will read the firewall policy.
C. identify mechanisms to encourage compliance with the policy.
D. perform a risk analysis to identify issues to be addressed.

Answer: D

NEW QUESTION 81
- (Exam Topic 9)
Which of the following is TRUE about Disaster Recovery Plan (DRP) testing?

A. Operational networks are usually shut down during testing.
B. Testing should continue even if components of the test fail.
C. The company is fully prepared for a disaster if all tests pass.
D. Testing should not be done until the entire disaster plan can be tested.

Answer: B

NEW QUESTION 82
- (Exam Topic 9)
Which of the following is the MOST important consideration when storing and processing Personally Identifiable Information (PII)?

A. Encrypt and hash all PII to avoid disclosure and tampering.
B. Store PII for no more than one year.
C. Avoid storing PII in a Cloud Service Provider.
D. Adherence to collection limitation laws and regulations.

Answer: D

NEW QUESTION 84
- (Exam Topic 9)
The BEST way to check for good security programming practices, as well as auditing for possible backdoors, is to conduct

A. log auditing.
B. code reviews.
C. impact assessments.
D. static analysis.

Answer:

B

NEW QUESTION 89
- (Exam Topic 9)
An external attacker has compromised an organization's network security perimeter and installed a sniffer onto an inside computer. Which of the following is the MOST effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information?

A. Implement packet filtering on the network firewalls
B. Require strong authentication for administrators
C. Install Host Based Intrusion Detection Systems (HIDS)
D. Implement logical network segmentation at the switches

Answer: D

NEW QUESTION 90
- (Exam Topic 9)
Which of the following can BEST prevent security flaws occurring in outsourced software development?

A. Contractual requirements for code quality
B. Licensing, code ownership and intellectual property rights
C. Certification of the quality and accuracy of the work done
D. Delivery dates, change management control and budgetary control

Answer: C

NEW QUESTION 92
- (Exam Topic 9)
Which of the following is an appropriate source for test data?

A. Production data that is secured and maintained only in the production environment.
B. Test data that has no similarities to production datA.
C. Test data that is mirrored and kept up-to-date with production datA.
D. Production data that has been sanitized before loading into a test environment.

Answer: D

NEW QUESTION 94
- (Exam Topic 9)
Who must approve modifications to an organization's production infrastructure configuration?

A. Technical management
B. Change control board
C. System operations
D. System users

Answer: B

NEW QUESTION 95
- (Exam Topic 9)
Which of the following is an effective method for avoiding magnetic media data remanence?

A. Degaussing
B. Encryption
C. Data Loss Prevention (DLP)
D. Authentication

Answer: A

NEW QUESTION 97
- (Exam Topic 9)
What is the MOST important purpose of testing the Disaster Recovery Plan (DRP)?

A. Evaluating the efficiency of the plan
B. Identifying the benchmark required for restoration
C. Validating the effectiveness of the plan
D. Determining the Recovery Time Objective (RTO)

Answer: C

NEW QUESTION 99
- (Exam Topic 9)
The goal of software assurance in application development is to

A. enable the development of High Availability (HA) systems.
B. facilitate the creation of Trusted Computing Base (TCB) systems.
C. prevent the creation of vulnerable applications.

D. encourage the development of open source applications.

Answer: C

NEW QUESTION 102
- (Exam Topic 9)
Which of the following wraps the decryption key of a full disk encryption implementation and ties the hard disk drive to a particular device?

A. Trusted Platform Module (TPM)
B. Preboot eXecution Environment (PXE)
C. Key Distribution Center (KDC)
D. Simple Key-Management for Internet Protocol (SKIP)

Answer: A

NEW QUESTION 103
- (Exam Topic 10)
What do Capability Maturity Models (CMM) serve as a benchmark for in an organization?

A. Experience in the industry
B. Definition of security profiles
C. Human resource planning efforts
D. Procedures in systems development

Answer: D

NEW QUESTION 107
- (Exam Topic 10)
Which of the following violates identity and access management best practices?

A. User accounts
B. System accounts
C. Generic accounts
D. Privileged accounts

Answer: C

NEW QUESTION 109
- (Exam Topic 10)
Which of the following describes the concept of a Single Sign-On (SSO) system?

A. Users are authenticated to one system at a time.
B. Users are identified to multiple systems with several credentials.
C. Users are authenticated to multiple systems with one login.
D. Only one user is using the system at a time.

Answer: C

NEW QUESTION 110
- (Exam Topic 10)
According to best practice, which of the following groups is the MOST effective in performing an information security compliance audit?

A. In-house security administrators
B. In-house Network Team
C. Disaster Recovery (DR) Team
D. External consultants

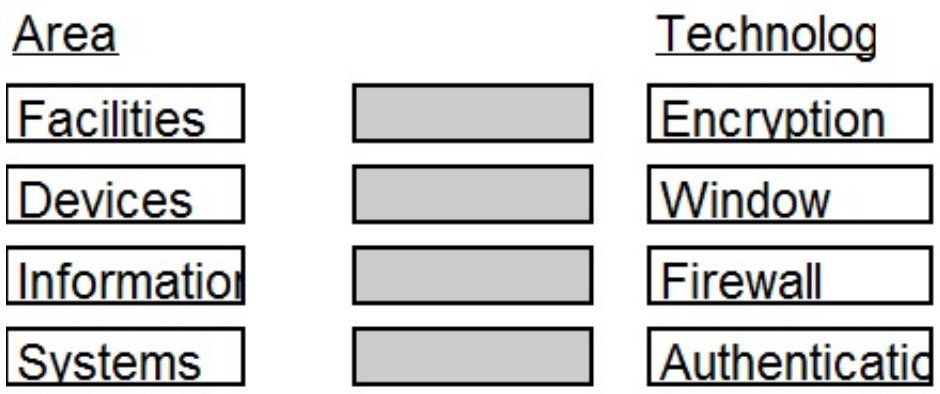
Answer: D

NEW QUESTION 114
- (Exam Topic 10)
Which of the following is the MOST difficult to enforce when using cloud computing?

A. Data access
B. Data backup
C. Data recovery
D. Data disposal

Answer: D

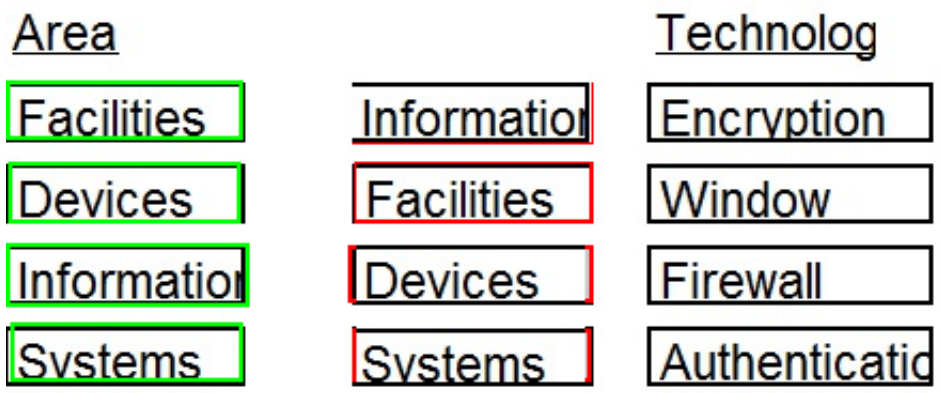
NEW QUESTION 119
- (Exam Topic 10)
Given the various means to protect physical and logical assets, match the access management area to the technology.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 124
- (Exam Topic 10)
What is the MOST critical factor to achieve the goals of a security program?

A. Capabilities of security resources
B. Executive management support
C. Effectiveness of security management
D. Budget approved for security resources

Answer: B

NEW QUESTION 129
- (Exam Topic 10)
A business has implemented Payment Card Industry Data Security Standard (PCI-DSS) compliant handheld credit card processing on their Wireless Local Area Network (WLAN) topology. The network team partitioned the WLAN to create a private segment for credit card processing using a firewall to control device access and route traffic to the card processor on the Internet. What components are in the scope of PCI-DSS?

A. The entire enterprise network infrastructure.
B. The handheld devices, wireless access points and border gateway.
C. The end devices, wireless access points, WLAN, switches, management console, and firewall.
D. The end devices, wireless access points, WLAN, switches, management console, and Internet

Answer: C

NEW QUESTION 133
- (Exam Topic 10)
Which of the following is a MAJOR consideration in implementing a Voice over IP (VoIP) network?

A. Use of a unified messaging.
B. Use of separation for the voice network.
C. Use of Network Access Control (NAC) on switches.
D. Use of Request for Comments (RFC) 1918 addressing.

Answer: B

NEW QUESTION 134
- (Exam Topic 10)
Which of the following is a detective access control mechanism?

A. Log review
B. Least privilege
C. Password complexity
D. Non-disclosure agreement

Answer: A

NEW QUESTION 137
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
Which of the following will indicate where the IT budget is BEST allocated during this time?

A. Policies
B. Frameworks
C. Metrics
D. Guidelines

Answer: C

NEW QUESTION 141
- (Exam Topic 10)
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
In the plan, what is the BEST approach to mitigate future internal client-based attacks?

A. Block all client side web exploits at the perimeter.
B. Remove all non-essential client-side web services from the network.
C. Screen for harmful exploits of client-side services before implementation.
D. Harden the client image before deployment.

Answer: D

NEW QUESTION 143
- (Exam Topic 10)
When implementing a secure wireless network, which of the following supports authentication and authorization for individual client endpoints?

A. Temporal Key Integrity Protocol (TKIP)
B. Wi-Fi Protected Access (WPA) Pre-Shared Key (PSK)
C. Wi-Fi Protected Access 2 (WPA2) Enterprise
D. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

Answer: C

NEW QUESTION 146
- (Exam Topic 10)
Which of the following is a BEST practice when traveling internationally with laptops containing Personally Identifiable Information (PII)?

A. Use a thumb drive to transfer information from a foreign computer.
B. Do not take unnecessary information, including sensitive information.
C. Connect the laptop only to well-known networks like the hotel or public Internet cafes.
D. Request international points of contact help scan the laptop on arrival to ensure it is protected.

Answer: B

NEW QUESTION 148
- (Exam Topic 10)
Which of the following problems is not addressed by using OAuth (Open Standard to Authorization) 2.0 to integrate a third-party identity provider for a service?

A. Resource Servers are required to use passwords to authenticate end users.
B. Revocation of access of some users of the third party instead of all the users from the third party.
C. Compromise of the third party means compromise of all the users in the service.
D. Guest users need to authenticate with the third party identity provider.

Answer: C

NEW QUESTION 150
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
Following best practice, where should the permitted access for each department and job classification combination be specified?

A. Security procedures
B. Security standards
C. Human resource policy
D. Human resource standards

Answer: B

NEW QUESTION 151
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
Which of the following BEST describes the access control methodology used?

A. Least privilege
B. Lattice Based Access Control (LBAC)
C. Role Based Access Control (RBAC)
D. Lightweight Directory Access Control (LDAP)

Answer: C

NEW QUESTION 155
- (Exam Topic 10)
Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following methods is the MOST effective way of removing the Peer-to-Peer (P2P) program from the computer?

A. Run software uninstall
B. Re-image the computer
C. Find and remove all installation files
D. Delete all cookies stored in the web browser cache

Answer: B

NEW QUESTION 159
- (Exam Topic 10)
A Business Continuity Plan (BCP) is based on

A. the policy and procedures manual.
B. an existing BCP from a similar organization.
C. a review of the business processes and procedures.
D. a standard checklist of required items and objectives.

Answer: C

NEW QUESTION 161
- (Exam Topic 10)
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
What is the BEST reason for the organization to pursue a plan to mitigate client-based attacks?

A. Client privilege administration is inherently weaker than server privilege administration.
B. Client hardening and management is easier on clients than on servers.
C. Client-based attacks are more common and easier to exploit than server and network based attacks.
D. Client-based attacks have higher financial impact.

Answer: C

NEW QUESTION 165
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
In addition to authentication at the start of the user session, best practice would require re-authentication

A. periodically during a session.
B. for each business process.
C. at system sign-off.
D. after a period of inactivity.

Answer: D

NEW QUESTION 170
- (Exam Topic 10)
A large university needs to enable student access to university resources from their homes. Which of the following provides the BEST option for low maintenance and ease of deployment?

A. Provide students with Internet Protocol Security (IPSec) Virtual Private Network (VPN) client software.
B. Use Secure Sockets Layer (SSL) VPN technology.
C. Use Secure Shell (SSH) with public/private keys.

D. Require students to purchase home router capable of VPN.

Answer: B

NEW QUESTION 172
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
The security program can be considered effective when

A. vulnerabilities are proactively identified.
B. audits are regularly performed and reviewed.
C. backups are regularly performed and validated.
D. risk is lowered to an acceptable level.

Answer: D

NEW QUESTION 177
- (Exam Topic 10)
An organization decides to implement a partial Public Key Infrastructure (PKI) with only the servers having digital certificates. What is the security benefit of this implementation?

A. Clients can authenticate themselves to the servers.
B. Mutual authentication is available between the clients and servers.
C. Servers are able to issue digital certificates to the client.
D. Servers can authenticate themselves to the client.

Answer: D

NEW QUESTION 182
- (Exam Topic 10)
Which of the following is the PRIMARY benefit of a formalized information classification program?

A. It drives audit processes.
B. It supports risk assessment.
C. It reduces asset vulnerabilities.
D. It minimizes system logging requirements.

Answer: B

NEW QUESTION 185
- (Exam Topic 10)
A thorough review of an organization's audit logs finds that a disgruntled network administrator has intercepted emails meant for the Chief Executive Officer (CEO) and changed them before forwarding them to their intended recipient. What type of attack has MOST likely occurred?

A. Spoofing
B. Eavesdropping
C. Man-in-the-middle
D. Denial of service

Answer: C

NEW QUESTION 190
- (Exam Topic 10)
During an audit, the auditor finds evidence of potentially illegal activity. Which of the following is the MOST appropriate action to take?

A. Immediately call the police
B. Work with the client to resolve the issue internally
C. Advise the person performing the illegal activity to cease and desist
D. Work with the client to report the activity to the appropriate authority

Answer: D

NEW QUESTION 195
- (Exam Topic 10)
Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
What additional considerations are there if the third party is located in a different country?

A. The organizational structure of the third party and how it may impact timelines within the organization
B. The ability of the third party to respond to the organization in a timely manner and with accurate information
C. The effects of transborder data flows and customer expectations regarding the storage or processing of their data
D. The quantity of data that must be provided to the third party and how it is to be used

Answer: C

NEW QUESTION 198
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
The effectiveness of the security program can PRIMARILY be measured through

A. audit findings.
B. risk elimination.
C. audit requirements.
D. customer satisfaction.

Answer: A

NEW QUESTION 203
- (Exam Topic 10)
Which of the following is critical for establishing an initial baseline for software components in the operation and maintenance of applications?

A. Application monitoring procedures
B. Configuration control procedures
C. Security audit procedures
D. Software patching procedures

Answer: B

NEW QUESTION 208
- (Exam Topic 11)
A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

A. Public Key Infrastructure (PKI) and digital signatures
B. Trusted server certificates and passphrases
C. User ID and password
D. Asymmetric encryption and User ID

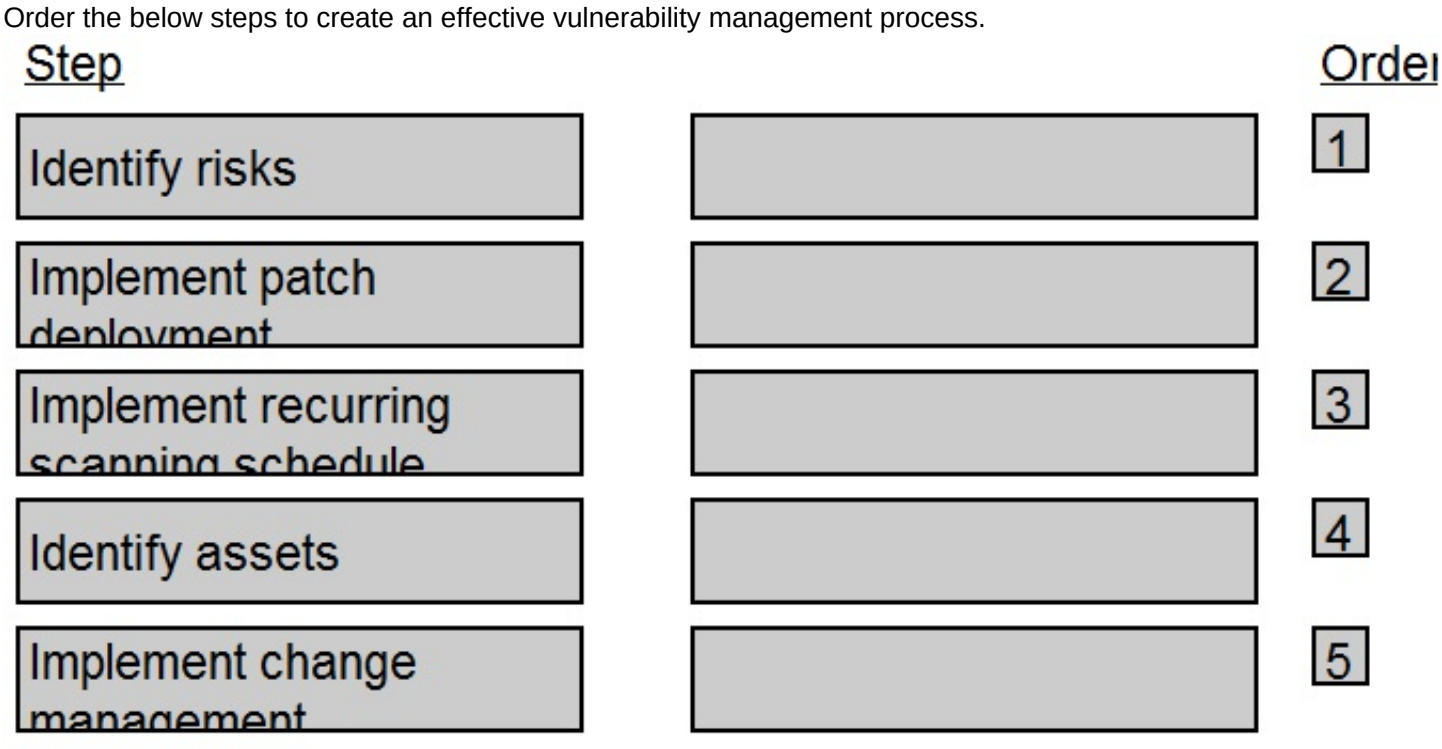
Answer: A

NEW QUESTION 211
- (Exam Topic 11)
Data remanence refers to which of the following?

A. The remaining photons left in a fiber optic cable after a secure transmission.
B. The retention period required by law or regulation.
C. The magnetic flux created when removing the network connection from a server or personal computer.
D. The residual information left on magnetic storage media after a deletion or erasure.

Answer: D

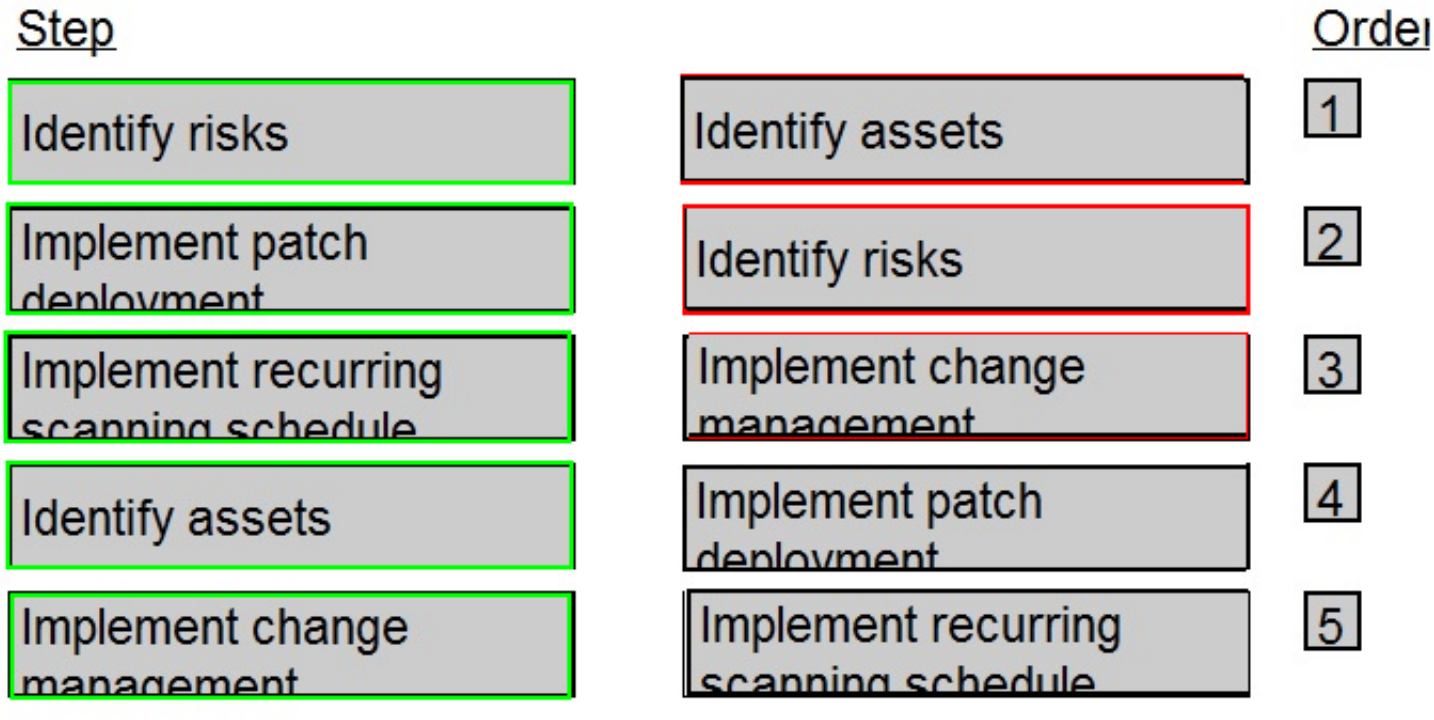
NEW QUESTION 213
- (Exam Topic 11)
Order the below steps to create an effective vulnerability management process.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

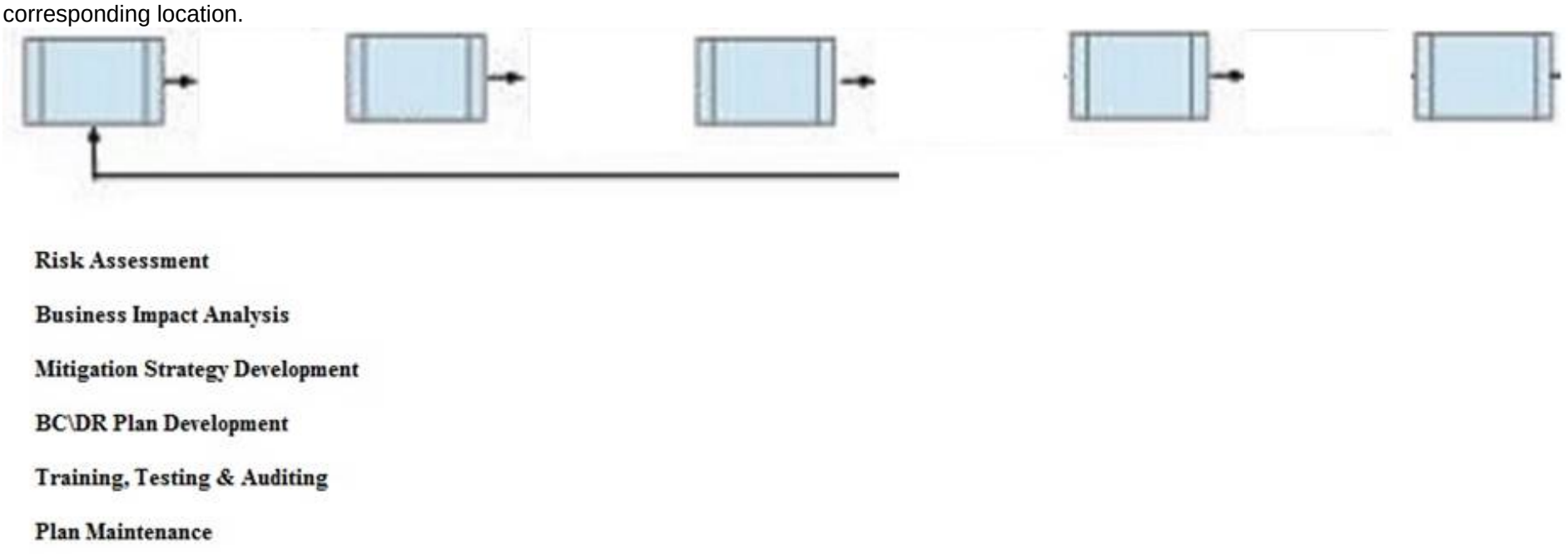


NEW QUESTION 216
- (Exam Topic 11)
A mobile device application that restricts the storage of user information to just that which is needed to accomplish lawful business goals adheres to what privacy principle?

A. Onward transfer
B. Collection Limitation
C. Collector Accountability
D. Individual Participation

Answer: B

NEW QUESTION 220
- (Exam Topic 11)
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.
What is the best approach for the CISO?
Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 221
- (Exam Topic 11)
Regarding asset security and appropriate retention, which of the following INITIAL top three areas are important to focus on?

A. Security control baselines, access controls, employee awareness and training
B. Human resources, asset management, production management
C. Supply chain lead time, inventory control, encryption
D. Polygraphs, crime statistics, forensics

Answer: A

NEW QUESTION 224
- (Exam Topic 11)
Which of the following is most helpful in applying the principle of LEAST privilege?

A. Establishing a sandboxing environment
B. Setting up a Virtual Private Network (VPN) tunnel
C. Monitoring and reviewing privileged sessions
D. Introducing a job rotation program

Answer: A

NEW QUESTION 228
- (Exam Topic 11)
What is the MOST efficient way to secure a production program and its data?

A. Disable default accounts and implement access control lists (ACL)
B. Harden the application and encrypt the data
C. Disable unused services and implement tunneling
D. Harden the servers and backup the data

Answer: B

NEW QUESTION 232
- (Exam Topic 11)
The World Trade Organization's (WTO) agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires authors of computer software to be given the

A. right to refuse or permit commercial rentals.
B. right to disguise the software's geographic origin.
C. ability to tailor security parameters based on location.
D. ability to confirm license authenticity of their works.

Answer: A

NEW QUESTION 236
- (Exam Topic 11)
Retaining system logs for six months or longer can be valuable for what activities?

A. Disaster recovery and business continuity
B. Forensics and incident response
C. Identity and authorization management
D. Physical and logical access control

Answer: B

NEW QUESTION 239
- (Exam Topic 11)
Application of which of the following Institute of Electrical and Electronics Engineers (IEEE) standards will prevent an unauthorized wireless device from being attached to a network?

A. IEEE 802.1F
B. IEEE 802.1H
C. IEEE 802.1Q
D. IEEE 802.1X

Answer: D

NEW QUESTION 242
- (Exam Topic 11)
Which of the following is an advantage of on-premise Credential Management Systems?

A. Improved credential interoperability
B. Control over system configuration
C. Lower infrastructure capital costs
D. Reduced administrative overhead

Answer: B

NEW QUESTION 247
- (Exam Topic 11)
Which one of the following is a common risk with network configuration management?

A. Patches on the network are difficult to keep current.
B. It is the responsibility of the systems administrator.
C. User ID and passwords are never set to expire.
D. Network diagrams are not up to date.

Answer: D

NEW QUESTION 251
- (Exam Topic 11)
Which of the following methods can be used to achieve confidentiality and integrity for data in transit?

A. Multiprotocol Label Switching (MPLS)
B. Internet Protocol Security (IPSec)
C. Federated identity management
D. Multi-factor authentication

Answer: B

NEW QUESTION 252
- (Exam Topic 11)
Which of the following questions can be answered using user and group entitlement reporting?

A. When a particular file was last accessed by a user
B. Change control activities for a particular group of users
C. The number of failed login attempts for a particular user
D. Where does a particular user have access within the network

Answer: D

NEW QUESTION 255
- (Exam Topic 11)
For an organization considering two-factor authentication for secure network access, which of the following is MOST secure?

A. Challenge response and private key
B. Digital certificates and Single Sign-On (SSO)
C. Tokens and passphrase
D. Smart card and biometrics

Answer: D

NEW QUESTION 260
- (Exam Topic 11)
Which of the following BEST avoids data remanence disclosure for cloud hosted resources?

A. Strong encryption and deletion of the keys after data is deleted.
B. Strong encryption and deletion of the virtual host after data is deleted.
C. Software based encryption with two factor authentication.
D. Hardware based encryption on dedicated physical servers.

Answer:

A

NEW QUESTION 265
- (Exam Topic 11)
Who is ultimately responsible to ensure that information assets are categorized and adequate measures are taken to protect them?

A. Data Custodian
B. Executive Management
C. Chief Information Security Officer
D. Data/Information/Business Owners

Answer: B

NEW QUESTION 267
- (Exam Topic 11)
Which of the following is a recommended alternative to an integrated email encryption system?

A. Sign emails containing sensitive data
B. Send sensitive data in separate emails
C. Encrypt sensitive data separately in attachments
D. Store sensitive information to be sent in encrypted drives

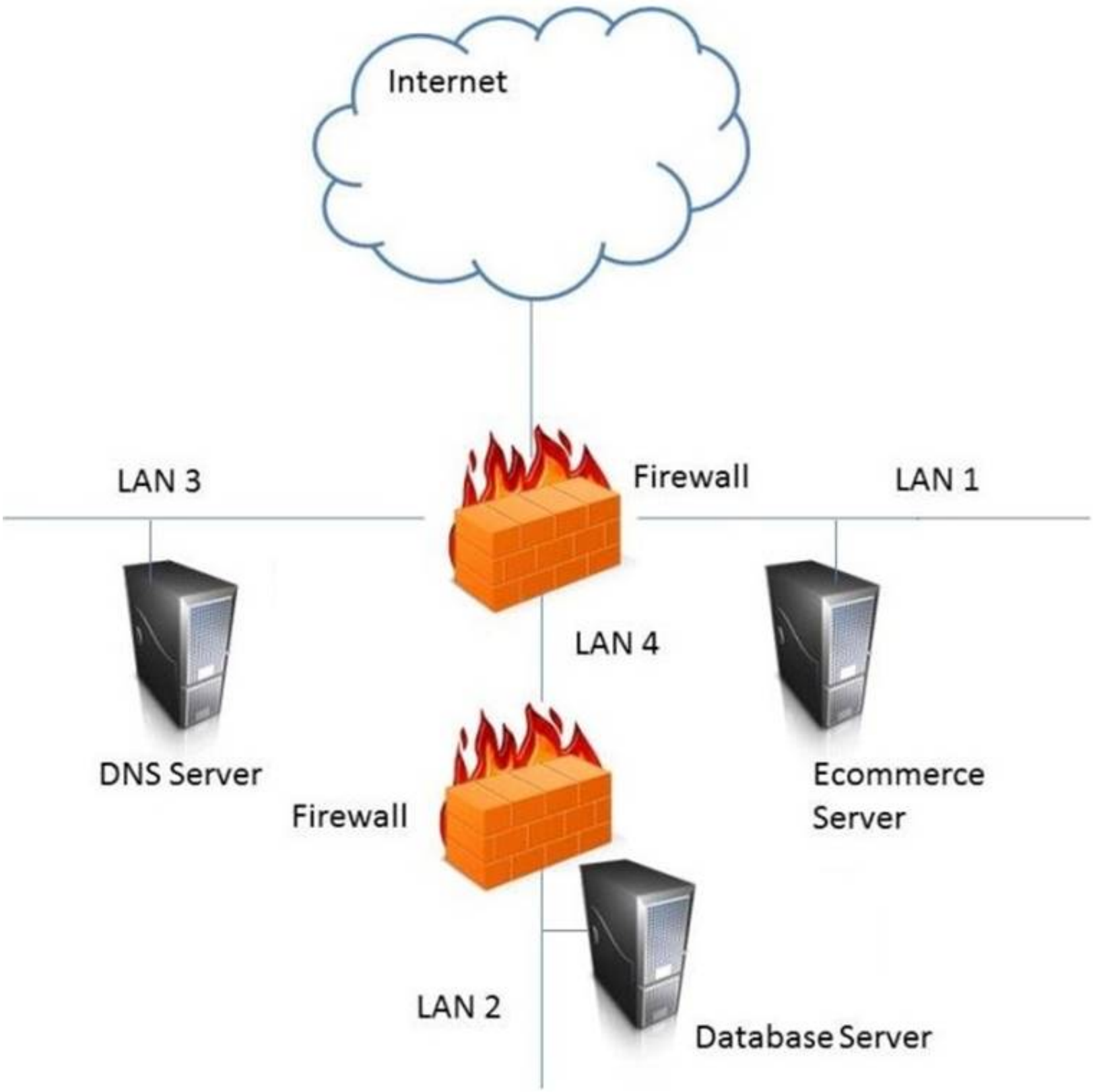
Answer: C

NEW QUESTION 272
- (Exam Topic 11)
While inventorying storage equipment, it is found that there are unlabeled, disconnected, and powered off devices. Which of the following is the correct procedure for handling such equipment?

A. They should be recycled to save energy.
B. They should be recycled according to NIST SP 800-88.
C. They should be inspected and sanitized following the organizational policy.
D. They should be inspected and categorized properly to sell them for reuse.

Answer: C

NEW QUESTION 276
- (Exam Topic 11)
In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?



A. Mastered
B. Not Mastered

Answer: A

Explanation:
LAN 4

NEW QUESTION 277
- (Exam Topic 11)
In order for a security policy to be effective within an organization, it MUST include

A. strong statements that clearly define the problem.
B. a list of all standards that apply to the policy.
C. owner information and date of last revision.
D. disciplinary measures for non compliance.

Answer: D

NEW QUESTION 281
- (Exam Topic 12)
A proxy firewall operates at what layer of the Open System Interconnection (OSI) model?

A. Transport
B. Data link
C. Network
D. Application

Answer: D

NEW QUESTION 286
- (Exam Topic 12)
What is the difference between media marking and media labeling?

A. Media marking refers to the use of human-readable security attributes, while media labeling refers to the use of security attributes in internal data structures.
B. Media labeling refers to the use of human-readable security attributes, while media marking refers to the use of security attributes in internal data structures.
C. Media labeling refers to security attributes required by public policy/law, while media marking refers to security required by internal organizational policy.
D. Media marking refers to security attributes required by public policy/law, while media labeling refers to security attributes required by internal organizational policy.

Answer: D

NEW QUESTION 288
- (Exam Topic 12)
Which of the following is a remote access protocol that uses a static authentication?

A. Point-to-Point Tunneling Protocol (PPTP)
B. Routing Information Protocol (RIP)
C. Password Authentication Protocol (PAP)
D. Challenge Handshake Authentication Protocol (CHAP)

Answer: C

NEW QUESTION 293
- (Exam Topic 12)
Match the name of access control model with its associated restriction.
Drag each access control model to its appropriate restriction access on the right.

Access Control Model		Restrictions
Mandatory Access Control		End user cannot set controls
Discretionary Access Control (DAC)		Subject has total control over objects
Role Based Access Control (RBAC)		Dynamically assigns permissions to particular duties based on job function
Rule based access control		Dynamically assigns roles to subjects based on criteria assigned by a custodian

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Mandatory Access Control – End user cannot set controls
Discretionary Access Control (DAC) – Subject has total control over objects
Role Based Access Control (RBAC) – Dynamically assigns roles permissions to particular duties based on job function
Rule Based access control – Dynamically assigns roles to subjects based on criteria assigned by a custodian.

NEW QUESTION 297
- (Exam Topic 12)
A vulnerability in which of the following components would be MOST difficult to detect?

A. Kernel
B. Shared libraries
C. Hardware
D. System application

Answer: A

NEW QUESTION 300
- (Exam Topic 12)
Which of the following information MUST be provided for user account provisioning?

A. Full name
B. Unique identifier
C. Security question
D. Date of birth

Answer: B

NEW QUESTION 304
- (Exam Topic 12)
A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

A. Enterprise asset management framework
B. Asset baseline using commercial off the shelf software
C. Asset ownership database using domain login records
D. A script to report active user logins on assets

Answer: A

NEW QUESTION 305
- (Exam Topic 12)
Which Radio Frequency Interference (RFI) phenomenon associated with bundled cable runs can create information leakage?

A. Transference
B. Covert channel
C. Bleeding
D. Cross-talk

Answer: D

NEW QUESTION 306
- (Exam Topic 12)
Which of the following adds end-to-end security inside a Layer 2 Tunneling Protocol (L2TP) Internet Protocol Security (IPSec) connection?

A. Temporal Key Integrity Protocol (TKIP)
B. Secure Hash Algorithm (SHA)
C. Secure Shell (SSH)
D. Transport Layer Security (TLS)

Answer: B

NEW QUESTION 310
- (Exam Topic 12)
The PRIMARY outcome of a certification process is that it provides documented

A. interconnected systems and their implemented security controls.
B. standards for security assessment, testing, and process evaluation.
C. system weakness for remediation.
D. security analyses needed to make a risk-based decision.

Answer: D

NEW QUESTION 313
- (Exam Topic 12)
Which of the following is an advantage of on-premise Credential Management Systems?

A. Lower infrastructure capital costs
B. Control over system configuration
C. Reduced administrative overhead
D. Improved credential interoperability

Answer: B

NEW QUESTION 315
- (Exam Topic 12)
Which of the following media sanitization techniques is MOST likely to be effective for an organization using public cloud services?

A. Low-level formatting
B. Secure-grade overwrite erasure
C. Cryptographic erasure
D. Drive degaussing

Answer: B

NEW QUESTION 317
- (Exam Topic 12)
Match the access control type to the example of the control type. Drag each access control type net to its corresponding example.

Access Control Type		Example
Administrative		Labeling of sensitive data
Technical		Biometrics for authentication
Logical		Constrained user interface
Physical		Radio Frequency Identification (RFID) badge

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Administrative – labeling of sensitive data Technical – Constrained user interface Logical – Biometrics for authentication
Physical – Radio Frequency Identification 9RFID) badge

NEW QUESTION 321
- (Exam Topic 12)
Determining outage costs caused by a disaster can BEST be measured by the

A. cost of redundant systems and backups.
B. cost to recover from an outage.
C. overall long-term impact of the outage.
D. revenue lost during the outage.

Answer: C

NEW QUESTION 324
- (Exam Topic 12)
How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

A. Examines log messages or other indications on the system.
B. Monitors alarms sent to the system administrator
C. Matches traffic patterns to virus signature files
D. Examines the Access Control List (ACL)

Answer: C

NEW QUESTION 329
- (Exam Topic 12)
Which of the following is BEST suited for exchanging authentication and authorization messages in a multi-party decentralized environment?

A. Lightweight Directory Access Protocol (LDAP)
B. Security Assertion Markup Language (SAML)
C. Internet Mail Access Protocol
D. Transport Layer Security (TLS)

Answer: B

NEW QUESTION 334
- (Exam Topic 12)
Which of the following is the MOST important consideration when developing a Disaster Recovery Plan (DRP)?

A. The dynamic reconfiguration of systems
B. The cost of downtime
C. A recovery strategy for all business processes
D. A containment strategy

Answer: C

NEW QUESTION 335
- (Exam Topic 12)

In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of

A. systems integration.
B. risk management.
C. quality assurance.
D. change management.

Answer: D

NEW QUESTION 338
- (Exam Topic 12)
The application of a security patch to a product previously validate at Common Criteria (CC) Evaluation Assurance Level (EAL) 4 would

A. require an update of the Protection Profile (PP).
B. require recertification.
C. retain its current EAL rating.
D. reduce the product to EAL 3.

Answer: B

NEW QUESTION 339
- (Exam Topic 13)
Which of the following is the BEST reason for writing an information security policy?

A. To support information security governance
B. To reduce the number of audit findings
C. To deter attackers
D. To implement effective information security controls

Answer: A

NEW QUESTION 342
- (Exam Topic 13)
A security analyst for a large financial institution is reviewing network traffic related to an incident. The analyst determines the traffic is irrelevant to the investigation but in the process of the review, the analyst also finds that an applications data, which included full credit card cardholder data, is transferred in clear text between the server and user's desktop. The analyst knows this violates the Payment Card Industry Data Security Standard (PCI-DSS). Which of the following is the analyst's next step?

A. Send the log file co-workers for peer review
B. Include the full network traffic logs in the incident report
C. Follow organizational processes to alert the proper teams to address the issue.
D. Ignore data as it is outside the scope of the investigation and the analyst's role.

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 344
- (Exam Topic 13)
An organization's security policy delegates to the data owner the ability to assign which user roles have access to a particular resource. What type of authorization mechanism is being used?

A. Discretionary Access Control (DAC)
B. Role Based Access Control (RBAC)
C. Media Access Control (MAC)
D. Mandatory Access Control (MAC)

Answer: A

NEW QUESTION 347
- (Exam Topic 13)
What is the MAIN reason for testing a Disaster Recovery Plan (DRP)?

A. To ensure Information Technology (IT) staff knows and performs roles assigned to each of them
B. To validate backup sites' effectiveness
C. To find out what does not work and fix it
D. To create a high level DRP awareness among Information Technology (IT) staff

Answer: B

NEW QUESTION 350
- (Exam Topic 13)
A company seizes a mobile device suspected of being used in committing fraud. What would be the BEST method used by a forensic examiner to isolate the powered-on device from the network and preserve the evidence?

A. Put the device in airplane mode

B. Suspend the account with the telecommunication provider
C. Remove the SIM card
D. Turn the device off

Answer: A

NEW QUESTION 354
- (Exam Topic 13)
Which of the following is a direct monetary cost of a security incident?

A. Morale
B. Reputation
C. Equipment
D. Information

Answer: C

NEW QUESTION 357
- (Exam Topic 13)
Drag the following Security Engineering terms on the left to the BEST definition on the right.

Security Engineering Term		Definition
Risk		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment		The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment		The method used to identify feasible security risk mitigation options and plans.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Risk - A measure of the extent to which an entity is threatened by a potential circumstance of event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.
Protection Needs Assessment - The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should be asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Threat assessment - The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Security Risk Treatment - The method used to identify feasible security risk mitigation options and plans.

NEW QUESTION 362
- (Exam Topic 13)
A Denial of Service (DoS) attack on a syslog server exploits weakness in which of the following protocols?

A. Point-to-Point Protocol (PPP) and Internet Control Message Protocol (ICMP)
B. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
C. Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)
D. Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

Answer: B

NEW QUESTION 366
- (Exam Topic 13)

Which security modes is MOST commonly used in a commercial environment because it protects the integrity of financial and accounting data?

A. Biba
B. Graham-Denning
C. Clark-Wilson
D. Beil-LaPadula

Answer: C

NEW QUESTION 371
- (Exam Topic 13)
What is the process of removing sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique?

A. Purging
B. Encryption
C. Destruction
D. Clearing

Answer: A

NEW QUESTION 372
- (Exam Topic 13)
Which of the following is a benefit in implementing an enterprise Identity and Access Management (IAM) solution?

A. Password requirements are simplified.
B. Risk associated with orphan accounts is reduced.
C. Segregation of duties is automatically enforced.
D. Data confidentiality is increased.

Answer: A

NEW QUESTION 375
- (Exam Topic 13)
When determining who can accept the risk associated with a vulnerability, which of the following is MOST important?

A. Countermeasure effectiveness
B. Type of potential loss
C. Incident likelihood
D. Information ownership

Answer: C

NEW QUESTION 378
- (Exam Topic 13)
An organization has outsourced its financial transaction processing to a Cloud Service Provider (CSP) who will provide them with Software as a Service (SaaS). If there was a data breach who is responsible for monetary losses?

A. The Data Protection Authority (DPA)
B. The Cloud Service Provider (CSP)
C. The application developers
D. The data owner

Answer: B

NEW QUESTION 379
- (Exam Topic 13)
Which of the following is a common characteristic of privacy?

A. Provision for maintaining an audit trail of access to the private data
B. Notice to the subject of the existence of a database containing relevant credit card data
C. Process for the subject to inspect and correct personal data on-site
D. Database requirements for integration of privacy data

Answer: A

NEW QUESTION 381
- (Exam Topic 13)
Which of the following is a responsibility of the information owner?

A. Ensure that users and personnel complete the required security training to access the Information System (IS)
B. Defining proper access to the Information System (IS), including privileges or access rights
C. Managing identification, implementation, and assessment of common security controls
D. Ensuring the Information System (IS) is operated according to agreed upon security requirements

Answer: C

NEW QUESTION 383
- (Exam Topic 13)
Which of the following is considered a secure coding practice?

A. Use concurrent access for shared variables and resources
B. Use checksums to verify the integrity of libraries
C. Use new code for common tasks
D. Use dynamic execution functions to pass user supplied data

Answer: B

NEW QUESTION 384
- (Exam Topic 13)
Assessing a third party's risk by counting bugs in the code may not be the best measure of an attack surface within the supply chain.
Which of the following is LEAST associated with the attack surface?

A. Input protocols
B. Target processes
C. Error messages
D. Access rights

Answer: C

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 388
- (Exam Topic 13)
Which of the following is the MOST challenging issue in apprehending cyber criminals?

A. They often use sophisticated method to commit a crime.
B. It is often hard to collect and maintain integrity of digital evidence.
C. The crime is often committed from a different jurisdiction.
D. There is often no physical evidence involved.

Answer: C

NEW QUESTION 393
- (Exam Topic 13)
What MUST each information owner do when a system contains data from multiple information owners?

A. Provide input to the Information System (IS) owner regarding the security requirements of the data
B. Review the Security Assessment report (SAR) for the Information System (IS) and authorize the IS to operate.
C. Develop and maintain the System Security Plan (SSP) for the Information System (IS) containing the data
D. Move the data to an Information System (IS) that does not contain data owned by other information owners

Answer: C

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 394
- (Exam Topic 13)
After following the processes defined within the change management plan, a super user has upgraded a device within an Information system.
What step would be taken to ensure that the upgrade did NOT affect the network security posture?

A. Conduct an Assessment and Authorization (A&A)
B. Conduct a security impact analysis
C. Review the results of the most recent vulnerability scan
D. Conduct a gap analysis with the baseline configuration

Answer: B

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 395
- (Exam Topic 13)
Digital certificates used in Transport Layer Security (TLS) support which of the following?

A. Information input validation
B. Non-repudiation controls and data encryption
C. Multi-Factor Authentication (MFA)
D. Server identity and data confidentially

Answer: D

NEW QUESTION 396
- (Exam Topic 13)
A chemical plan wants to upgrade the Industrial Control System (ICS) to transmit data using Ethernet instead of RS422. The project manager wants to simplify administration and maintenance by utilizing the office network infrastructure and staff to implement this upgrade.
Which of the following is the GREATEST impact on security for the network?

A. The network administrators have no knowledge of ICS
B. The ICS is now accessible from the office network
C. The ICS does not support the office password policy
D. RS422 is more reliable than Ethernet

Answer: B

NEW QUESTION 397
- (Exam Topic 13)
Attack trees are MOST useful for which of the following?

A. Determining system security scopes
B. Generating attack libraries
C. Enumerating threats
D. Evaluating Denial of Service (DoS) attacks

Answer: A

NEW QUESTION 401
- (Exam Topic 13)
Which of the following would BEST support effective testing of patch compatibility when patches are applied to an organization's systems?

A. Standardized configurations for devices
B. Standardized patch testing equipment
C. Automated system patching
D. Management support for patching

Answer: A

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 405
- (Exam Topic 13)
In Disaster Recovery (DR) and Business Continuity (DC) training, which BEST describes a functional drill?

A. a functional evacuation of personnel
B. a specific test by response teams of individual emergency response functions
C. an activation of the backup site
D. a full-scale simulation of an emergency and the subsequent response functions.

Answer: D

NEW QUESTION 410
- (Exam Topic 13)
The MAIN use of Layer 2 Tunneling Protocol (L2TP) is to tunnel data

A. through a firewall at the Session layer
B. through a firewall at the Transport layer
C. in the Point-to-Point Protocol (PPP)
D. in the Payload Compression Protocol (PCP)

Answer: C

NEW QUESTION 411
- (Exam Topic 13)
Which one of the following considerations has the LEAST impact when considering transmission security?

A. Network availability
B. Node locations
C. Network bandwidth
D. Data integrity

Answer: C

NEW QUESTION 415
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CISSP Practice Exam Features:

* CISSP Questions and Answers Updated Frequently

* CISSP Practice Questions Verified by Expert Senior Certified Staff

* CISSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year