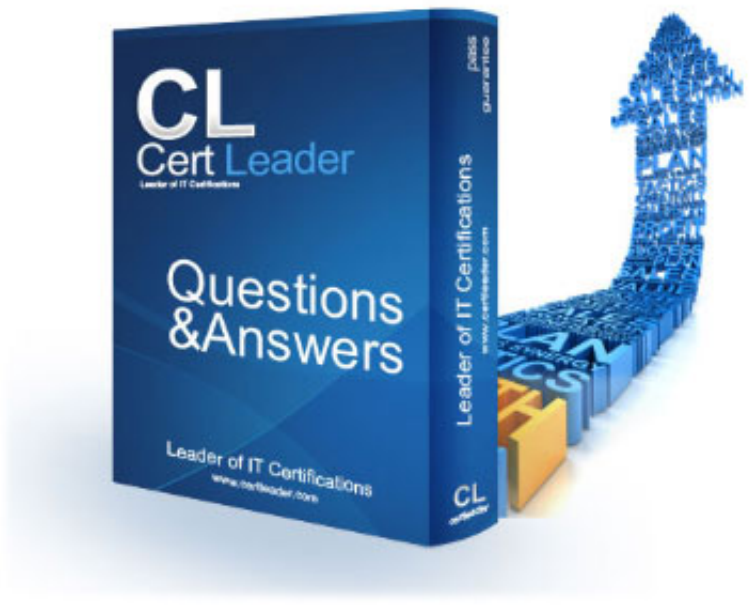
CISSP Dumps

Certified Information Systems Security Professional (CISSP)

https://www.certleader.com/CISSP-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined?

A. Only when assets are clearly defined
B. Only when standards are defined
C. Only when controls are put in place
D. Only procedures are defined

Answer: A

NEW QUESTION 2
- (Exam Topic 1)
Which of the following actions will reduce risk to a laptop before traveling to a high risk area?

A. Examine the device for physical tampering
B. Implement more stringent baseline configurations
C. Purge or re-image the hard disk drive
D. Change access codes

Answer: D

NEW QUESTION 3
- (Exam Topic 2)
When implementing a data classification program, why is it important to avoid too much granularity?

A. The process will require too many resources
B. It will be difficult to apply to both hardware and software
C. It will be difficult to assign ownership to the data
D. The process will be perceived as having value

Answer: A

NEW QUESTION 4
- (Exam Topic 3)
Which of the following mobile code security models relies only on trust?

A. Code signing
B. Class authentication
C. Sandboxing
D. Type safety

Answer: A

NEW QUESTION 5
- (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 6
- (Exam Topic 4)
Which of the following factors contributes to the weakness of Wired Equivalent Privacy (WEP) protocol?

A. WEP uses a small range Initialization Vector (IV)
B. WEP uses Message Digest 5 (MD5)
C. WEP uses Diffie-Hellman
D. WEP does not use any Initialization Vector (IV)

Answer: A

NEW QUESTION 7
- (Exam Topic 5)
Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee's salary?

A. Limit access to predefined queries
B. Segregate the database into a small number of partitions each with a separate security level

C. Implement Role Based Access Control (RBAC)
D. Reduce the number of people who have access to the system for statistical purposes

Answer: C

NEW QUESTION 8
- (Exam Topic 5)
What is the BEST approach for controlling access to highly sensitive information when employees have the same level of security clearance?

A. Audit logs
B. Role-Based Access Control (RBAC)
C. Two-factor authentication
D. Application of least privilege

Answer: B

NEW QUESTION 9
- (Exam Topic 7)
What would be the MOST cost effective solution for a Disaster Recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours?

A. Warm site
B. Hot site
C. Mirror site
D. Cold site

Answer: A

NEW QUESTION 10
- (Exam Topic 7)
What is the MOST important step during forensic analysis when trying to learn the purpose of an unknown application?

A. Disable all unnecessary services
B. Ensure chain of custody
C. Prepare another backup of the system
D. Isolate the system from the network

Answer: D

NEW QUESTION 10
- (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 12
- (Exam Topic 8)
When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?

A. After the system preliminary design has been developed and the data security categorization has been performed
B. After the vulnerability analysis has been performed and before the system detailed design begins
C. After the system preliminary design has been developed and before the data security categorization begins
D. After the business functional analysis and the data security categorization have been performed

Answer: C

NEW QUESTION 16
- (Exam Topic 8)
Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

A. Lack of software documentation
B. License agreements requiring release of modified code
C. Expiration of the license agreement
D. Costs associated with support of the software

Answer: D

NEW QUESTION 17
- (Exam Topic 9)
Logical access control programs are MOST effective when they are

A. approved by external auditors.
B. combined with security token technology.
C. maintained by computer security officers.
D. made part of the operating system.

Answer: D

NEW QUESTION 20
- (Exam Topic 9)
Which one of the following is a threat related to the use of web-based client side input validation?

A. Users would be able to alter the input after validation has occurred
B. The web server would not be able to validate the input after transmission
C. The client system could receive invalid input from the web server
D. The web server would not be able to receive invalid input from the client

Answer: A

NEW QUESTION 24
- (Exam Topic 9)
Which of the following is a physical security control that protects Automated Teller Machines (ATM) from skimming?

A. Anti-tampering
B. Secure card reader
C. Radio Frequency (RF) scanner
D. Intrusion Prevention System (IPS)

Answer: A

NEW QUESTION 26
- (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 28
- (Exam Topic 9)
Which layer of the Open Systems Interconnections (OSI) model implementation adds information concerning the logical connection between the sender and receiver?

A. Physical
B. Session
C. Transport
D. Data-Link

Answer: C

NEW QUESTION 31
- (Exam Topic 9)
The type of authorized interactions a subject can have with an object is

A. control.
B. permission.
C. procedure.
D. protocol.

Answer: B

NEW QUESTION 35
- (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 40

- (Exam Topic 9)
Which one of the following considerations has the LEAST impact when considering transmission security?

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

Answer: C

NEW QUESTION 44
- (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 45
- (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 46
- (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 51
- (Exam Topic 9)
In a financial institution, who has the responsibility for assigning the classification to a piece of information?

A. Chief Financial Officer (CFO)
B. Chief Information Security Officer (CISO)
C. Originator or nominated owner of the information
D. Department head responsible for ensuring the protection of the information

Answer: C

NEW QUESTION 56
- (Exam Topic 9)
What security management control is MOST often broken by collusion?

A. Job rotation
B. Separation of duties
C. Least privilege model
D. Increased monitoring

Answer: B

NEW QUESTION 58
- (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 61
- (Exam Topic 9)
Which of the following is an essential element of a privileged identity lifecycle management?

A. Regularly perform account re-validation and approval
B. Account provisioning based on multi-factor authentication
C. Frequently review performed activities and request justification
D. Account information to be provided by supervisor or line manager

Answer: A

NEW QUESTION 62
- (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 66
- (Exam Topic 9)
Which of the following is the BEST way to verify the integrity of a software patch?

A. Cryptographic checksums
B. Version numbering
C. Automatic updates
D. Vendor assurance

Answer: A

NEW QUESTION 71
- (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 76
- (Exam Topic 9)
Which one of the following describes granularity?

A. Maximum number of entries available in an Access Control List (ACL)
B. Fineness to which a trusted system can authenticate users
C. Number of violations divided by the number of total accesses
D. Fineness to which an access control system can be adjusted

Answer: D

NEW QUESTION 81
- (Exam Topic 9)
A disadvantage of an application filtering firewall is that it can lead to

A. a crash of the network as a result of user activities.
B. performance degradation due to the rules applied.
C. loss of packets on the network due to insufficient bandwidth.
D. Internet Protocol (IP) spoofing by hackers.

Answer: B

NEW QUESTION 82
- (Exam Topic 9)
Which of the following is the FIRST step of a penetration test plan?

A. Analyzing a network diagram of the target network
B. Notifying the company's customers
C. Obtaining the approval of the company's management
D. Scheduling the penetration test during a period of least impact

Answer: C

NEW QUESTION 84
- (Exam Topic 9)
What is an effective practice when returning electronic storage media to third parties for repair?

A. Ensuring the media is not labeled in any way that indicates the organization's name.
B. Disassembling the media and removing parts that may contain sensitive datA.
C. Physically breaking parts of the media that may contain sensitive datA.
D. Establishing a contract with the third party regarding the secure handling of the mediA.

Answer: D

NEW QUESTION 88
- (Exam Topic 9)
Which of the following is a network intrusion detection technique?

A. Statistical anomaly
B. Perimeter intrusion
C. Port scanning
D. Network spoofing

Answer: A

NEW QUESTION 89
- (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 92
- (Exam Topic 9)
Following the completion of a network security assessment, which of the following can BEST be demonstrated?

A. The effectiveness of controls can be accurately measured
B. A penetration test of the network will fail
C. The network is compliant to industry standards
D. All unpatched vulnerabilities have been identified

Answer: A

NEW QUESTION 97
- (Exam Topic 9)
When designing a networked Information System (IS) where there will be several different types of individual access, what is the FIRST step that should be taken to ensure all access control requirements are addressed?

A. Create a user profile.
B. Create a user access matrix.
C. Develop an Access Control List (ACL).
D. Develop a Role Based Access Control (RBAC) list.

Answer: B

NEW QUESTION 98
- (Exam Topic 9)
Which of the following is a potential risk when a program runs in privileged mode?

A. It may serve to create unnecessary code complexity
B. It may not enforce job separation duties
C. It may create unnecessary application hardening
D. It may allow malicious code to be inserted

Answer: D

NEW QUESTION 103
- (Exam Topic 9)
What is the MOST effective countermeasure to a malicious code attack against a mobile system?

A. Sandbox
B. Change control
C. Memory management
D. Public-Key Infrastructure (PKI)

Answer: A

NEW QUESTION 105
- (Exam Topic 9)
A system has been scanned for vulnerabilities and has been found to contain a number of communication ports that have been opened without authority. To which of the following might this system have been subjected?

A. Trojan horse
B. Denial of Service (DoS)
C. Spoofing
D. Man-in-the-Middle (MITM)

Answer: A

NEW QUESTION 110
- (Exam Topic 9)
By allowing storage communications to run on top of Transmission Control Protocol/Internet Protocol (TCP/IP) with a Storage Area Network (SAN), the

A. confidentiality of the traffic is protected.
B. opportunity to sniff network traffic exists.
C. opportunity for device identity spoofing is eliminated.
D. storage devices are protected against availability attacks.

Answer: B

NEW QUESTION 114
- (Exam Topic 9)
Which of the following BEST represents the principle of open design?

A. Disassembly, analysis, or reverse engineering will reveal the security functionality of the computer system.
B. Algorithms must be protected to ensure the security and interoperability of the designed system.
C. A knowledgeable user should have limited privileges on the system to prevent their ability to compromise security capabilities.
D. The security of a mechanism should not depend on the secrecy of its design or implementation.

Answer: D

NEW QUESTION 116
- (Exam Topic 9)
Which of the following statements is TRUE of black box testing?

A. Only the functional specifications are known to the test planner.
B. Only the source code and the design documents are known to the test planner.
C. Only the source code and functional specifications are known to the test planner.
D. Only the design documents and the functional specifications are known to the test planner.

Answer: A

NEW QUESTION 120
- (Exam Topic 10)
Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?

A. Requirements Analysis
B. Development and Deployment
C. Production Operations
D. Utilization Support

Answer: A

NEW QUESTION 123
- (Exam Topic 10)
When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?

A. Perform a service provider PCI-DSS assessment on a yearly basis.
B. Validate the service provider's PCI-DSS compliance status on a regular basis.
C. Validate that the service providers security policies are in alignment with those of the organization.
D. Ensure that the service provider updates and tests its Disaster Recovery Plan (DRP) on a yearly basis.

Answer: B

NEW QUESTION 125
- (Exam Topic 10)
Refer to the information below to answer the question.
In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

Which of the following is true according to the star property (*property)?

A. User D can write to File 1
B. User B can write to File 1
C. User A can write to File 1
D. User C can write to File 1

Answer: C

NEW QUESTION 126
- (Exam Topic 10)
During an investigation of database theft from an organization's web site, it was determined that the Structured Query Language (SQL) injection technique was used despite input validation with client-side scripting. Which of the following provides the GREATEST protection against the same attack occurring again?

A. Encrypt communications between the servers
B. Encrypt the web server traffic
C. Implement server-side filtering
D. Filter outgoing traffic at the perimeter firewall

Answer: C

NEW QUESTION 130
- (Exam Topic 10)
If an attacker in a SYN flood attack uses someone else's valid host address as the source address, the system under attack will send a large number of Synchronize/Acknowledge (SYN/ACK) packets to the

A. default gateway.
B. attacker's address.
C. local interface being attacked.
D. specified source address.

Answer: D

NEW QUESTION 134
- (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 MUST the plan include in order to reduce client-side exploitation?

A. Approved web browsers
B. Network firewall procedures
C. Proxy configuration
D. Employee education

Answer: D

NEW QUESTION 137
- (Exam Topic 10)
Which of the following is required to determine classification and ownership?

A. System and data resources are properly identified
B. Access violations are logged and audited
C. Data file references are identified and linked
D. System security controls are fully integrated

Answer: A

NEW QUESTION 138
- (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.
What MUST the access control logs contain in addition to the identifier?

A. Time of the access
B. Security classification
C. Denied access attempts

D. Associated clearance

Answer: A

NEW QUESTION 141
- (Exam Topic 10)
What is a common challenge when implementing Security Assertion Markup Language (SAML) for identity integration between on-premise environment and an external identity provider service?

A. Some users are not provisioned into the service.
B. SAML tokens are provided by the on-premise identity provider.
C. Single users cannot be revoked from the service.
D. SAML tokens contain user information.

Answer: A

NEW QUESTION 143
- (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 documents explains the proper use of the organization's assets?

A. Human resources policy
B. Acceptable use policy
C. Code of ethics
D. Access control policy

Answer: B

NEW QUESTION 146
- (Exam Topic 10)
Which of the following is the MOST effective attack against cryptographic hardware modules?

A. Plaintext
B. Brute force
C. Power analysis
D. Man-in-the-middle (MITM)

Answer: C

NEW QUESTION 147
- (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 150
- (Exam Topic 10)
With data labeling, which of the following MUST be the key decision maker?

A. Information security
B. Departmental management
C. Data custodian
D. Data owner

Answer: D

NEW QUESTION 151
- (Exam Topic 10)
Which of the following is the MOST crucial for a successful audit plan?

A. Defining the scope of the audit to be performed
B. Identifying the security controls to be implemented
C. Working with the system owner on new controls
D. Acquiring evidence of systems that are not compliant

Answer: A

NEW QUESTION 156
- (Exam Topic 10)
Which of the following BEST describes Recovery Time Objective (RTO)?

A. Time of data validation after disaster
B. Time of data restoration from backup after disaster
C. Time of application resumption after disaster
D. Time of application verification after disaster

Answer: C

NEW QUESTION 157
- (Exam Topic 10)
A system is developed so that its business users can perform business functions but not user administration functions. Application administrators can perform administration functions but not user business functions. These capabilities are BEST described as

A. least privilege.
B. rule based access controls.
C. Mandatory Access Control (MAC).
D. separation of duties.

Answer: D

NEW QUESTION 158
- (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.
Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?

A. Severity of risk
B. Complexity of strategy
C. Frequency of incidents
D. Ongoing awareness

Answer: A

NEW QUESTION 163
- (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 168
- (Exam Topic 10)
Which of the following is the MAIN goal of a data retention policy?

A. Ensure that data is destroyed properly.
B. Ensure that data recovery can be done on the datA.
C. Ensure the integrity and availability of data for a predetermined amount of time.
D. Ensure the integrity and confidentiality of data for a predetermined amount of time.

Answer: C

NEW QUESTION 171
- (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 175
- (Exam Topic 10)
A risk assessment report recommends upgrading all perimeter firewalls to mitigate a particular finding. Which of the following BEST supports this recommendation?

A. The inherent risk is greater than the residual risk.
B. The Annualized Loss Expectancy (ALE) approaches zero.
C. The expected loss from the risk exceeds mitigation costs.
D. The infrastructure budget can easily cover the upgrade costs.

Answer: C

NEW QUESTION 180
- (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.

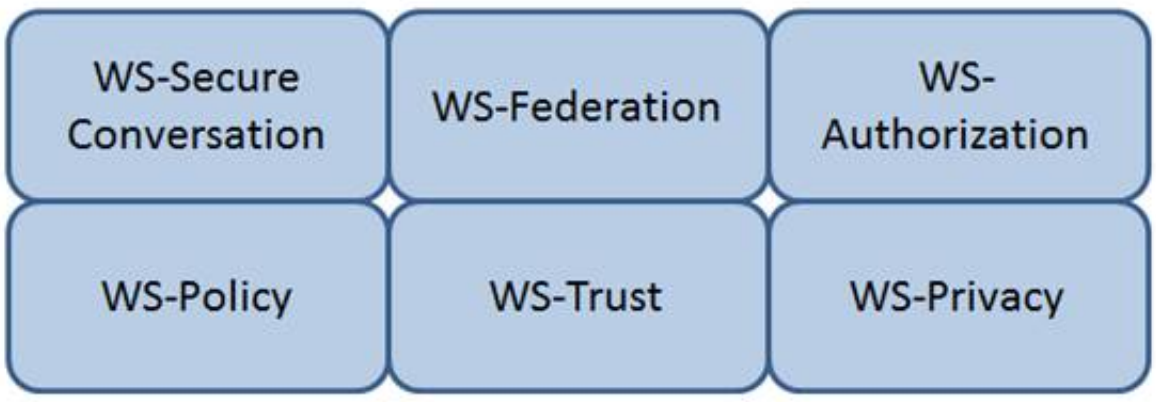
Answer: A

NEW QUESTION 183
- (Exam Topic 11)
What is the process called when impact values are assigned to the security objectives for information types?

A. Qualitative analysis
B. Quantitative analysis
C. Remediation
D. System security categorization

Answer: D

NEW QUESTION 185
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
WS-Authorization
Reference: Java Web Services: Up and Running" By Martin Kalin page 228

NEW QUESTION 186
- (Exam Topic 11)
Which of the following BEST describes the purpose of performing security certification?

A. To identify system threats, vulnerabilities, and acceptable level of risk
B. To formalize the confirmation of compliance to security policies and standards
C. To formalize the confirmation of completed risk mitigation and risk analysis
D. To verify that system architecture and interconnections with other systems are effectively implemented

Answer: B

NEW QUESTION 188
- (Exam Topic 11)
Which of the following prevents improper aggregation of privileges in Role Based Access Control (RBAC)?

A. Hierarchical inheritance
B. Dynamic separation of duties
C. The Clark-Wilson security model
D. The Bell-LaPadula security model

Answer: B

NEW QUESTION 189
- (Exam Topic 11)
The application of which of the following standards would BEST reduce the potential for data breaches?

A. ISO 9000
B. ISO 20121
C. ISO 26000
D. ISO 27001

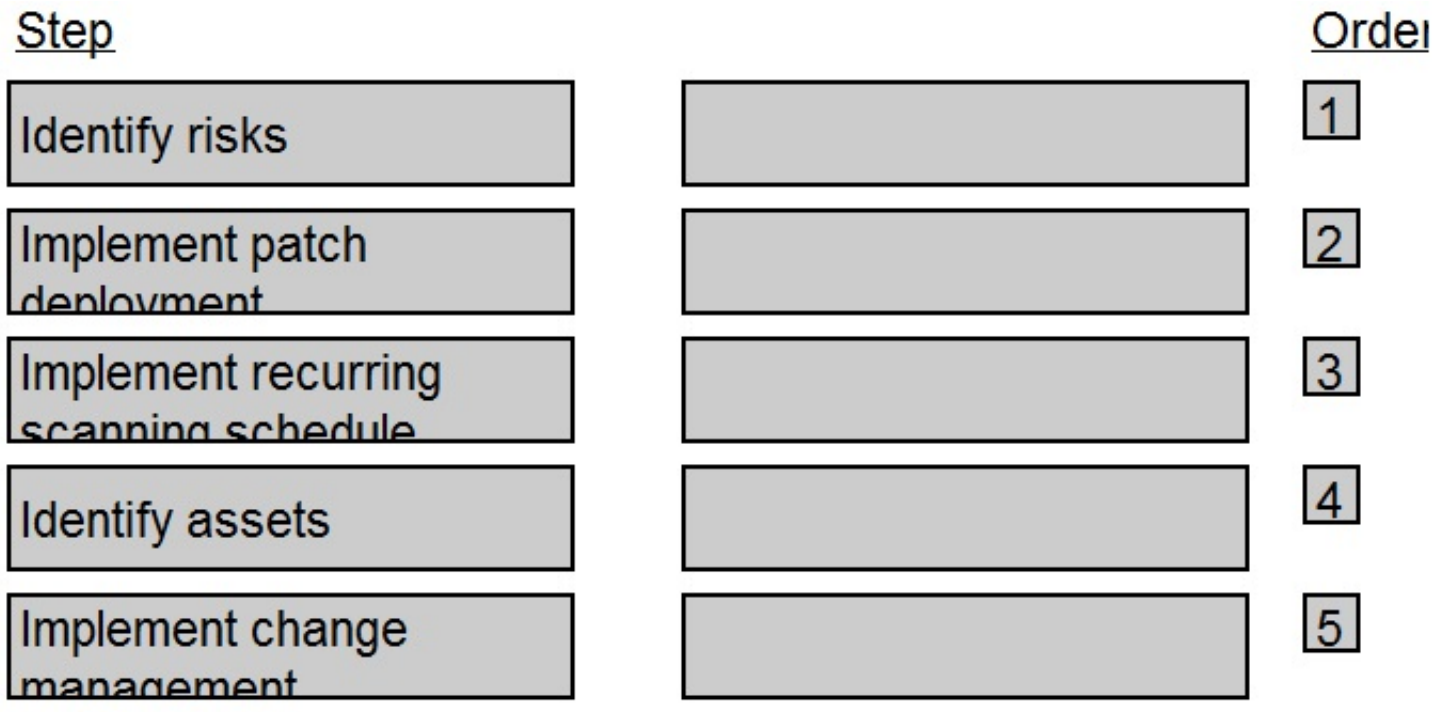
Answer: D

NEW QUESTION 194
- (Exam Topic 11)
Which of the following BEST describes a Protection Profile (PP)?

A. A document that expresses an implementation independent set of security requirements for an IT product that meets specific consumer needs.
B. A document that is used to develop an IT security product from its security requirements definition.
C. A document that expresses an implementation dependent set of security requirements which contains only the security functional requirements.
D. A document that represents evaluated products where there is a one-to-one correspondence between a PP and a Security Target (ST).

Answer: A

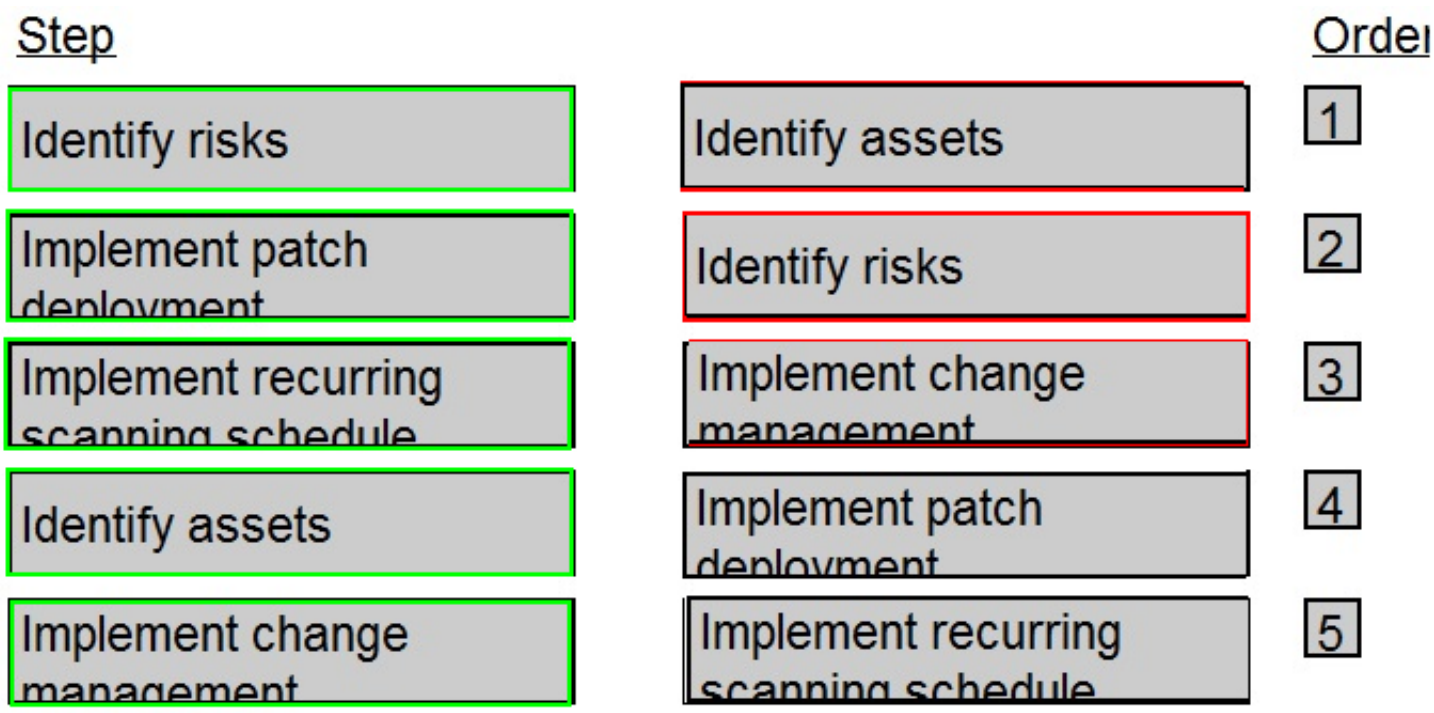
NEW QUESTION 197
- (Exam Topic 11)
Order the below steps to create an effective vulnerability management process.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 201
- (Exam Topic 11)
Which of the following is the MOST important element of change management documentation?

A. List of components involved
B. Number of changes being made
C. Business case justification
D. A stakeholder communication

Answer: C

NEW QUESTION 203
- (Exam Topic 11)
What should happen when an emergency change to a system must be performed?

A. The change must be given priority at the next meeting of the change control board.
B. Testing and approvals must be performed quickly.
C. The change must be performed immediately and then submitted to the change board.
D. The change is performed and a notation is made in the system log.

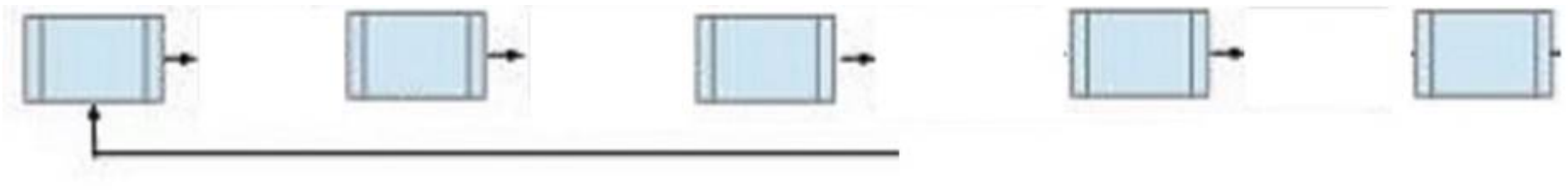
Answer: B

NEW QUESTION 206
- (Exam Topic 11)
After a thorough analysis, it was discovered that a perpetrator compromised a network by gaining access to the network through a Secure Socket Layer (SSL) Virtual Private Network (VPN) gateway. The perpetrator guessed a username and brute forced the password to gain access. Which of the following BEST mitigates this issue?

A. Implement strong passwords authentication for VPN
B. Integrate the VPN with centralized credential stores
C. Implement an Internet Protocol Security (IPSec) client
D. Use two-factor authentication mechanisms

Answer: D

NEW QUESTION 211
- (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.



Risk Assessment

Business Impact Analysis

Mitigation Strategy Development

BC\DR Plan Development

Training, Testing & Auditing

Plan Maintenance

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Risk Assessment

Business Impact Analysis

Mitigation Strategy Development

BC\DR Plan Development

Training, Testing & Auditing

Plan Maintenance

NEW QUESTION 212
- (Exam Topic 11)
What is an important characteristic of Role Based Access Control (RBAC)?

A. Supports Mandatory Access Control (MAC)
B. Simplifies the management of access rights
C. Relies on rotation of duties
D. Requires two factor authentication

Answer: B

NEW QUESTION 214
- (Exam Topic 11)
Which of the following is the BIGGEST weakness when using native Lightweight Directory Access Protocol (LDAP) for authentication?

A. Authorizations are not included in the server response
B. Unsalted hashes are passed over the network
C. The authentication session can be replayed
D. Passwords are passed in cleartext

Answer: D

NEW QUESTION 215
- (Exam Topic 11)
Discretionary Access Control (DAC) restricts access according to

A. data classification labeling.
B. page views within an application.
C. authorizations granted to the user.
D. management accreditation.

Answer: C

NEW QUESTION 219
- (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 222
- (Exam Topic 11)
An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?

A. Limits and scope of the testing.
B. Physical location of server room and wiring closet.
C. Logical location of filters and concentrators.
D. Employee directory and organizational chart.

Answer: A

NEW QUESTION 227
- (Exam Topic 11)
When planning a penetration test, the tester will be MOST interested in which information?

A. Places to install back doors
B. The main network access points
C. Job application handouts and tours
D. Exploits that can attack weaknesses

Answer: B

NEW QUESTION 228
- (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 231
- (Exam Topic 11)
Which of the following is an essential step before performing Structured Query Language (SQL) penetration tests on a production system?

A. Verify countermeasures have been deactivated.
B. Ensure firewall logging has been activated.
C. Validate target systems have been backed up.
D. Confirm warm site is ready to accept connections.

Answer: C

NEW QUESTION 234
- (Exam Topic 11)
What type of encryption is used to protect sensitive data in transit over a network?

A. Payload encryption and transport encryption
B. Authentication Headers (AH)
C. Keyed-Hashing for Message Authentication
D. Point-to-Point Encryption (P2PE)

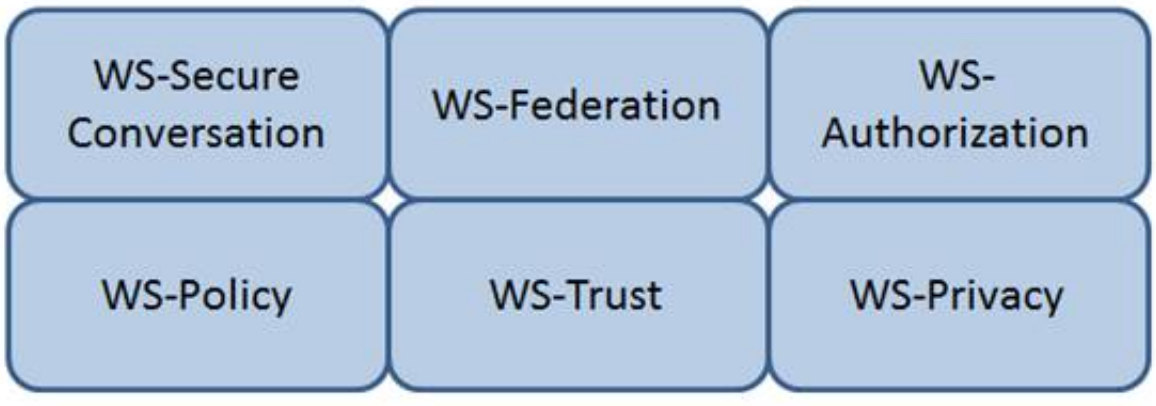
Answer: A

NEW QUESTION 238
- (Exam Topic 11)
An organization has developed a major application that has undergone accreditation testing. After receiving the results of the evaluation, what is the final step before the application can be accredited?

A. Acceptance of risk by the authorizing official
B. Remediation of vulnerabilities
C. Adoption of standardized policies and procedures
D. Approval of the System Security Plan (SSP)

Answer: A

NEW QUESTION 240
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
WS-Federation
Reference: Java Web Services: Up and Running" By Martin Kalin page 228

NEW QUESTION 241
- (Exam Topic 11)
Secure Sockets Layer (SSL) encryption protects

A. data at rest.
B. the source IP address.
C. data transmitted.
D. data availability.

Answer: C

NEW QUESTION 245
- (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 249
- (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

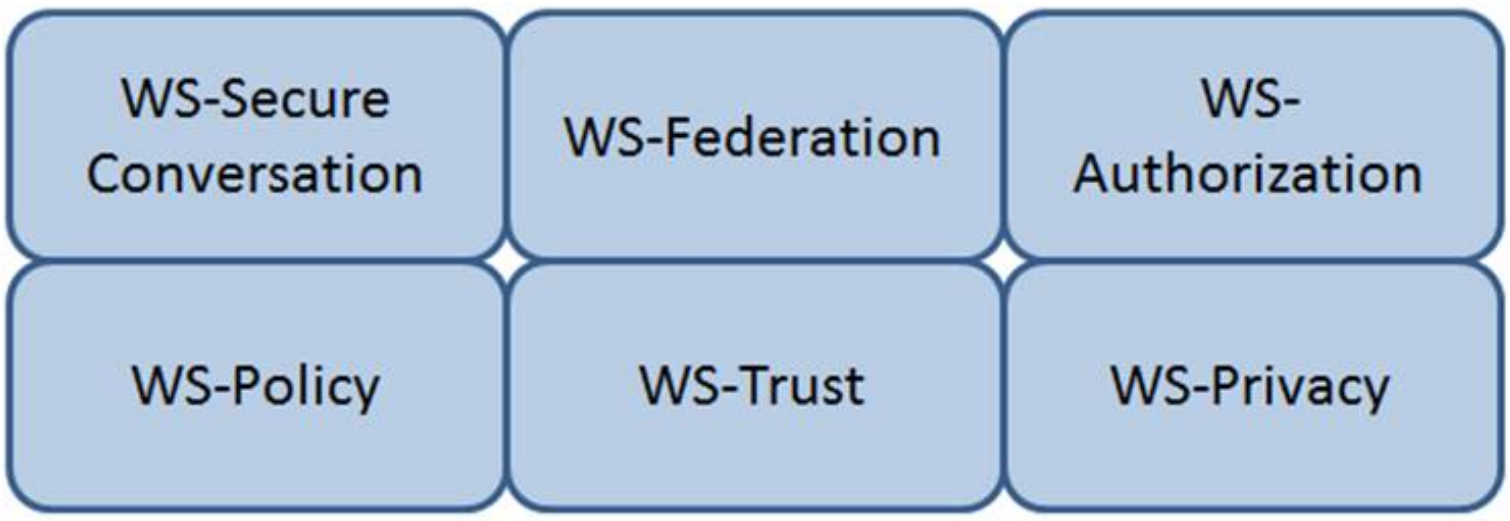
Answer: B

NEW QUESTION 251
- (Exam Topic 11)
The PRIMARY security concern for handheld devices is the

A. strength of the encryption algorithm.
B. spread of malware during synchronization.
C. ability to bypass the authentication mechanism.
D. strength of the Personal Identification Number (PIN).

Answer: C

NEW QUESTION 254
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated? Click on the correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
WS-Trust
The protocol used for issuing security tokens is based on WS-Trust. WS-Trust is a Web service specification that builds on WS-Security. It describes a protocol used for issuance, exchange, and validation of security tokens. WS-Trust provides a solution for interoperability by defining a protocol for issuing and exchanging security tokens, based on token format, namespace, or trust boundaries.
Reference: https://msdn.microsoft.com/en-us/library/ff650503.aspx

NEW QUESTION 257
- (Exam Topic 11)
Software Code signing is used as a method of verifying what security concept?

A. Integrity
B. Confidentiality
C. Availability
D. Access Control

Answer: A

NEW QUESTION 260
- (Exam Topic 11)
The goal of a Business Continuity Plan (BCP) training and awareness program is to

A. enhance the skills required to create, maintain, and execute the plan.
B. provide for a high level of recovery in case of disaster.
C. describe the recovery organization to new employees.
D. provide each recovery team with checklists and procedures.

Answer: A

NEW QUESTION 263

- (Exam Topic 11)
Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic mediA.

Sequence		Method
1		Overwriting
2		Degaussing
3		Destruction
4		Deleting

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Sequence		Method
1	3	Overwriting
2	2	Degaussing
3	1	Destruction
4	4	Deleting

NEW QUESTION 265
- (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 270
- (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)
Which of the following secures web transactions at the Transport Layer?

A. Secure HyperText Transfer Protocol (S-HTTP)
B. Secure Sockets Layer (SSL)
C. Socket Security (SOCKS)
D. Secure Shell (SSH)

Answer: B

NEW QUESTION 277
- (Exam Topic 11)
Which of the following is the PRIMARY issue when collecting detailed log information?

A. Logs may be unavailable when required
B. Timely review of the data is potentially difficult
C. Most systems and applications do not support logging
D. Logs do not provide sufficient details of system and individual activities

Answer: B

NEW QUESTION 281
- (Exam Topic 11)
An organization is found lacking the ability to properly establish performance indicators for its Web hosting solution during an audit. What would be the MOST probable cause?

A. Improper deployment of the Service-Oriented Architecture (SOA)
B. Absence of a Business Intelligence (BI) solution
C. Inadequate cost modeling
D. Insufficient Service Level Agreement (SLA)

Answer: D

NEW QUESTION 286
- (Exam Topic 11)
By carefully aligning the pins in the lock, which of the following defines the opening of a mechanical lock without the proper key?

A. Lock pinging
B. Lock picking
C. Lock bumping
D. Lock bricking

Answer: B

NEW QUESTION 288
- (Exam Topic 11)
Which of the following could elicit a Denial of Service (DoS) attack against a credential management system?

A. Delayed revocation or destruction of credentials
B. Modification of Certificate Revocation List
C. Unauthorized renewal or re-issuance
D. Token use after decommissioning

Answer: B

NEW QUESTION 290
- (Exam Topic 11)
A global organization wants to implement hardware tokens as part of a multifactor authentication solution for remote access. The PRIMARY advantage of this implementation is

A. the scalability of token enrollment.
B. increased accountability of end users.
C. it protects against unauthorized access.
D. it simplifies user access administration.

Answer: C

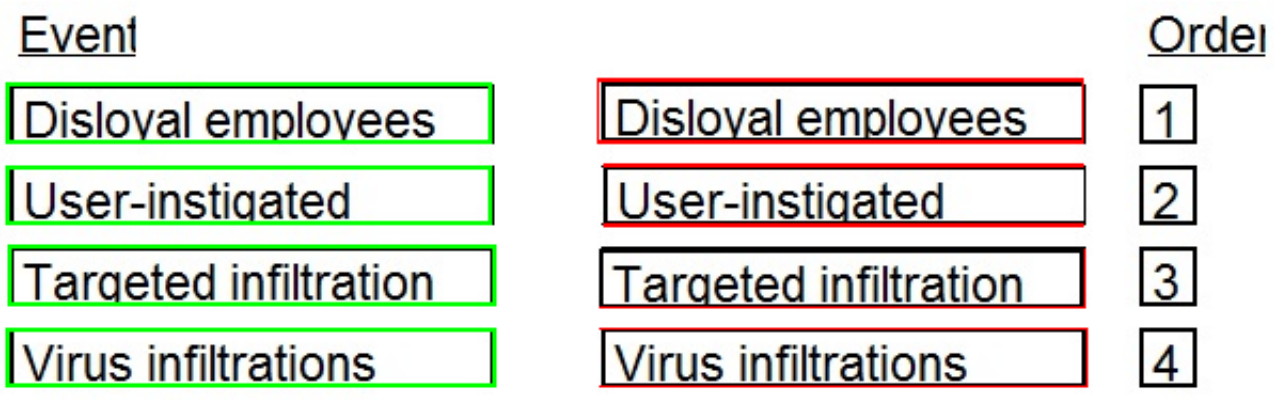
NEW QUESTION 295
- (Exam Topic 11)
In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?

Event	Order
Disloyal employees	1
User-instigated	2
Targeted infiltration	3
Virus infiltrations	4

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 298
- (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 302
- (Exam Topic 12)
The restoration priorities of a Disaster Recovery Plan (DRP) are based on which of the following documents?

A. Service Level Agreement (SLA)
B. Business Continuity Plan (BCP)
C. Business Impact Analysis (BIA)
D. Crisis management plan

Answer: B

NEW QUESTION 305
- (Exam Topic 12)
Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

A. Addresses and protocols of network-based logs are analyzed.
B. Host-based system logging has files stored in multiple locations.
C. Properly handled network-based logs may be more reliable and valid.
D. Network-based systems cannot capture users logging into the console.

Answer: A

NEW QUESTION 309
- (Exam Topic 12)
How should an organization determine the priority of its remediation efforts after a vulnerability assessment has been conducted?

A. Use an impact-based approach.
B. Use a risk-based approach.
C. Use a criticality-based approach.
D. Use a threat-based approach.

Answer: B

NEW QUESTION 312
- (Exam Topic 12)
What type of wireless network attack BEST describes an Electromagnetic Pulse (EMP) attack?

A. Radio Frequency (RF) attack
B. Denial of Service (DoS) attack
C. Data modification attack
D. Application-layer attack

Answer: B

NEW QUESTION 315
- (Exam Topic 12)
Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item?

A. Property book
B. Chain of custody form
C. Search warrant return

D. Evidence tag

Answer: D

NEW QUESTION 317
- (Exam Topic 12)
Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

A. Reversal
B. Gray box
C. Blind
D. White box

Answer: B

NEW QUESTION 321
- (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 326
- (Exam Topic 12)
What operations role is responsible for protecting the enterprise from corrupt or contaminated media?

A. Information security practitioner
B. Information librarian
C. Computer operator
D. Network administrator

Answer: B

NEW QUESTION 327
- (Exam Topic 12)
Which of the following BEST describes Recovery Time Objective (RTO)?

A. Time of application resumption after disaster
B. Time of application verification after disaster.
C. Time of data validation after disaster.
D. Time of data restoration from backup after disaster.

Answer: A

NEW QUESTION 331
- (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 333
- (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 336
- (Exam Topic 12)
Which of the following BEST represents the concept of least privilege?

A. Access to an object is denied unless access is specifically allowed.
B. Access to an object is only available to the owner.
C. Access to an object is allowed unless it is protected by the information security policy.
D. Access to an object is only allowed to authenticated users via an Access Control List (ACL).

Answer: A

NEW QUESTION 340
- (Exam Topic 12)
Which of the following is needed to securely distribute symmetric cryptographic keys?

A. Officially approved Public-Key Infrastructure (PKI) Class 3 or Class 4 certificates
B. Officially approved and compliant key management technology and processes
C. An organizationally approved communication protection policy and key management plan
D. Hardware tokens that protect the user's private key.

Answer: C

NEW QUESTION 342
- (Exam Topic 12)
Which of the following approaches is the MOST effective way to dispose of data on multiple hard drives?

A. Delete every file on each drive.
B. Destroy the partition table for each drive using the command line.
C. Degauss each drive individually.
D. Perform multiple passes on each drive using approved formatting methods.

Answer: D

NEW QUESTION 346
- (Exam Topic 12)
Which one of the following activities would present a significant security risk to organizations when employing a Virtual Private Network (VPN) solution?

A. VPN bandwidth
B. Simultaneous connection to other networks
C. Users with Internet Protocol (IP) addressing conflicts
D. Remote users with administrative rights

Answer: B

NEW QUESTION 351
- (Exam Topic 12)
Which of the following is the PRIMARY reason for employing physical security personnel at entry points in facilities where card access is in operation?

A. To verify that only employees have access to the facility.
B. To identify present hazards requiring remediation.
C. To monitor staff movement throughout the facility.
D. To provide a safe environment for employees.

Answer: D

NEW QUESTION 355
- (Exam Topic 12)
Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

A. Length of Initialization Vector (IV)
B. Protection against message replay
C. Detection of message tampering
D. Built-in provision to rotate keys

Answer: A

NEW QUESTION 358
- (Exam Topic 12)
An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a PRIMARY security concern?

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

Answer: C

NEW QUESTION 360
- (Exam Topic 12)

Which of the following are effective countermeasures against passive network-layer attacks?

A. Federated security and authenticated access controls
B. Trusted software development and run time integrity controls
C. Encryption and security enabled applications
D. Enclave boundary protection and computing environment defense

Answer: C

NEW QUESTION 361
- (Exam Topic 12)
From a cryptographic perspective, the service of non-repudiation includes which of the following features?

A. Validity of digital certificates
B. Validity of the authorization rules
C. Proof of authenticity of the message
D. Proof of integrity of the message

Answer: C

NEW QUESTION 364
- (Exam Topic 12)
For network based evidence, which of the following contains traffic details of all network sessions in order to detect anomalies?

A. Alert data
B. User data
C. Content data
D. Statistical data

Answer: D

NEW QUESTION 365
- (Exam Topic 12)
Reciprocal backup site agreements are considered to be

A. a better alternative than the use of warm sites.
B. difficult to test for complex systems.
C. easy to implement for similar types of organizations.
D. easy to test and implement for complex systems.

Answer: B

NEW QUESTION 368
- (Exam Topic 12)
What balance MUST be considered when web application developers determine how informative application error messages should be constructed?

A. Risk versus benefit
B. Availability versus auditability
C. Confidentiality versus integrity
D. Performance versus user satisfaction

Answer: A

NEW QUESTION 369
- (Exam Topic 12)
Which of the following countermeasures is the MOST effective in defending against a social engineering attack?

A. Mandating security policy acceptance
B. Changing individual behavior
C. Evaluating security awareness training
D. Filtering malicious e-mail content

Answer: C

NEW QUESTION 370
- (Exam Topic 13)
Which one of the following data integrity models assumes a lattice of integrity levels?

A. Take-Grant
B. Biba
C. Harrison-Ruzzo
D. Bell-LaPadula

Answer: B

NEW QUESTION 375

- (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 379
- (Exam Topic 13)
Which of the following is the MOST effective method to mitigate Cross-Site Scripting (XSS) attacks?

A. Use Software as a Service (SaaS)
B. Whitelist input validation
C. Require client certificates
D. Validate data output

Answer: B

NEW QUESTION 383
- (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 386
- (Exam Topic 13)
What protocol is often used between gateway hosts on the Internet?

A. Exterior Gateway Protocol (EGP)
B. Border Gateway Protocol (BGP)
C. Open Shortest Path First (OSPF)
D. Internet Control Message Protocol (ICMP)

Answer: B

NEW QUESTION 391
- (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 396
- (Exam Topic 13)
An organization plan on purchasing a custom software product developed by a small vendor to support its
business model. Which unique consideration should be made part of the contractual agreement potential long-term risks associated with creating this dependency?

A. A source code escrow clause
B. Right to request an independent review of the software source code
C. Due diligence form requesting statements of compliance with security requirements
D. Access to the technical documentation

Answer: B

NEW QUESTION 399
- (Exam Topic 13)
Which of the following is the MOST common method of memory protection?

A. Compartmentalization
B. Segmentation
C. Error correction
D. Virtual Local Area Network (VLAN) tagging

Answer: B

NEW QUESTION 402
- (Exam Topic 13)
Which security access policy contains fixed security attributes that are used by the system to determine a user's access to a file or object?

A. Mandatory Access Control (MAC)
B. Access Control List (ACL)
C. Discretionary Access Control (DAC)
D. Authorized user control

Answer: A

NEW QUESTION 404
- (Exam Topic 13)
Which of the following could be considered the MOST significant security challenge when adopting DevOps practices compared to a more traditional control framework?

A. Achieving Service Level Agreements (SLA) on how quickly patches will be released when a security flaw is found.
B. Maintaining segregation of duties.
C. Standardized configurations for logging, alerting, and security metrics.
D. Availability of security teams at the end of design process to perform last-minute manual audits and reviews.

Answer: B

NEW QUESTION 405
- (Exam Topic 13)
Which of the following combinations would MOST negatively affect availability?

A. Denial of Service (DoS) attacks and outdated hardware
B. Unauthorized transactions and outdated hardware
C. Fire and accidental changes to data
D. Unauthorized transactions and denial of service attacks

Answer: A

NEW QUESTION 407
- (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 412
- (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 416
- (Exam Topic 13)
What can happen when an Intrusion Detection System (IDS) is installed inside a firewall-protected internal network?

A. The IDS can detect failed administrator logon attempts from servers.
B. The IDS can increase the number of packets to analyze.
C. The firewall can increase the number of packets to analyze.
D. The firewall can detect failed administrator login attempts from servers

Answer: A

NEW QUESTION 417

- (Exam Topic 13)
What are the steps of a risk assessment?

A. identification, analysis, evaluation
B. analysis, evaluation, mitigation
C. classification, identification, risk management
D. identification, evaluation, mitigation

Answer: A

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 421
- (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 423
- (Exam Topic 13)
What is the MOST significant benefit of an application upgrade that replaces randomly generated session keys with certificate based encryption for communications with backend servers?

A. Non-repudiation
B. Efficiency
C. Confidentially
D. Privacy

Answer: A

NEW QUESTION 426
- (Exam Topic 13)
Proven application security principles include which of the following?

A. Minimizing attack surface area
B. Hardening the network perimeter
C. Accepting infrastructure security controls
D. Developing independent modules

Answer: A

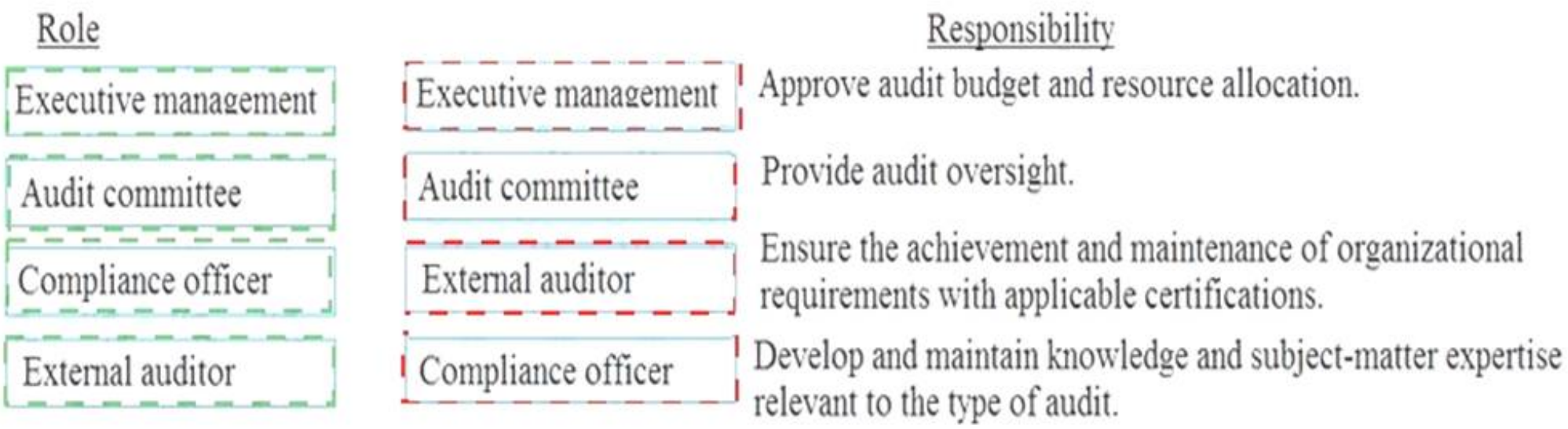
NEW QUESTION 427
- (Exam Topic 13)
Match the functional roles in an external audit to their responsibilities. Drag each role on the left to its corresponding responsibility on the right. Select and Place:

Role		Responsibility
Executive management		Approve audit budget and resource allocation.
Audit committee		Provide audit oversight.
Compliance officer		Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor		Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 430
- (Exam Topic 13)
The core component of Role Based Access Control (RBAC) must be constructed of defined data elements. Which elements are required?

A. Users, permissions, operations, and protected objects
B. Roles, accounts, permissions, and protected objects
C. Users, roles, operations, and protected objects
D. Roles, operations, accounts, and protected objects

Answer: C

NEW QUESTION 432
- (Exam Topic 13)
What is the expected outcome of security awareness in support of a security awareness program?

A. Awareness activities should be used to focus on security concerns and respond to those concerns accordingly
B. Awareness is not an activity or part of the training but rather a state of persistence to support the program
C. Awareness is trainin
D. The purpose of awareness presentations is to broaden attention of security.
E. Awareness is not trainin
F. The purpose of awareness presentation is simply to focus attention on security.

Answer: C

NEW QUESTION 433
- (Exam Topic 13)
An Information Technology (IT) professional attends a cybersecurity seminar on current incident response methodologies.
What code of ethics canon is being observed?

A. Provide diligent and competent service to principals
B. Protect society, the commonwealth, and the infrastructure
C. Advance and protect the profession
D. Act honorable, honesty, justly, responsibly, and legally

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 436
- (Exam Topic 13)
Which of the following MUST be scalable to address security concerns raised by the integration of third-party identity services?

A. Mandatory Access Controls (MAC)
B. Enterprise security architecture
C. Enterprise security procedures
D. Role Based Access Controls (RBAC)

Answer: D

NEW QUESTION 439
- (Exam Topic 13)
When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

A. Log all activities associated with sensitive systems
B. Provide links to security policies
C. Confirm that confidentially agreements are signed
D. Employ strong access controls

Answer: D

NEW QUESTION 443
- (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 444
- (Exam Topic 13)
A security professional determines that a number of outsourcing contracts inherited from a previous merger do not adhere to the current security requirements.
Which of the following BEST minimizes the risk of this
happening again?

A. Define additional security controls directly after the merger
B. Include a procurement officer in the merger team
C. Verify all contracts before a merger occurs
D. Assign a compliancy officer to review the merger conditions

Answer: D

NEW QUESTION 447
- (Exam Topic 13)
What does a Synchronous (SYN) flood attack do?

A. Forces Transmission Control Protocol /Internet Protocol (TCP/IP) connections into a reset state
B. Establishes many new Transmission Control Protocol / Internet Protocol (TCP/IP) connections
C. Empties the queue of pending Transmission Control Protocol /Internet Protocol (TCP/IP) requests
D. Exceeds the limits for new Transmission Control Protocol /Internet Protocol (TCP/IP) connections

Answer: B

NEW QUESTION 448
- (Exam Topic 13)
Who has the PRIMARY responsibility to ensure that security objectives are aligned with organization goals?

A. Senior management
B. Information security department
C. Audit committee
D. All users

Answer: C

NEW QUESTION 449
- (Exam Topic 13)
Which of the following is the GREATEST benefit of implementing a Role Based Access Control (RBAC)
system?

A. Integration using Lightweight Directory Access Protocol (LDAP)
B. Form-based user registration process
C. Integration with the organizations Human Resources (HR) system
D. A considerably simpler provisioning process

Answer: D

NEW QUESTION 453
- (Exam Topic 13)
A Security Operations Center (SOC) receives an incident response notification on a server with an active
intruder who has planted a backdoor. Initial notifications are sent and communications are established. What MUST be considered or evaluated before performing the next step?

A. Notifying law enforcement is crucial before hashing the contents of the server hard drive
B. Identifying who executed the incident is more important than how the incident happened
C. Removing the server from the network may prevent catching the intruder
D. Copying the contents of the hard drive to another storage device may damage the evidence

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 455
- (Exam Topic 13)
Which of the following management process allows ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

A. Configuration
B. Identity
C. Compliance
D. Patch

Answer: A

NEW QUESTION 459
- (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 460
- (Exam Topic 13)
A post-implementation review has identified that the Voice Over Internet Protocol (VoIP) system was designed to have gratuitous Address Resolution Protocol (ARP) disabled.
Why did the network architect likely design the VoIP system with gratuitous ARP disabled?

A. Gratuitous ARP requires the use of Virtual Local Area Network (VLAN) 1.
B. Gratuitous ARP requires the use of insecure layer 3 protocols.
C. Gratuitous ARP requires the likelihood of a successful brute-force attack on the phone.
D. Gratuitous ARP requires the risk of a Man-in-the-Middle (MITM) attack.

Answer: D

NEW QUESTION 463
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISSP Exam with Our Prep Materials Via below:

https://www.certleader.com/CISSP-dumps.html