

ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)



NEW QUESTION 1

- (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 2

- (Exam Topic 1)

Intellectual property rights are PRIMARY concerned with which of the following?

- A. Owner's ability to realize financial gain
- B. Owner's ability to maintain copyright
- C. Right of the owner to enjoy their creation
- D. Right of the owner to control delivery method

Answer: D

NEW QUESTION 3

- (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 4

- (Exam Topic 2)

Which one of the following affects the classification of data?

- A. Assigned security label
- B. Multilevel Security (MLS) architecture
- C. Minimum query size
- D. Passage of time

Answer: D

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 3)

What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?

- A. Implementation Phase
- B. Initialization Phase
- C. Cancellation Phase
- D. Issued Phase

Answer: D

NEW QUESTION 8

- (Exam Topic 4)

Which of the following operates at the Network Layer of the Open System Interconnection (OSI) model?

- A. Packet filtering
- B. Port services filtering
- C. Content filtering
- D. Application access control

Answer: A

NEW QUESTION 9

- (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 10

- (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 14

- (Exam Topic 6)

In which of the following programs is it MOST important to include the collection of security process data?

- A. Quarterly access reviews
- B. Security continuous monitoring
- C. Business continuity testing
- D. Annual security training

Answer: A

NEW QUESTION 18

- (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 19

- (Exam Topic 7)

A continuous information security monitoring program can BEST reduce risk through which of the following?

- A. Collecting security events and correlating them to identify anomalies

- B. Facilitating system-wide visibility into the activities of critical user accounts
- C. Encompassing people, process, and technology
- D. Logging both scheduled and unscheduled system changes

Answer: B

NEW QUESTION 21

- (Exam Topic 7)

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

Answer: D

NEW QUESTION 25

- (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 29

- (Exam Topic 7)

What should be the FIRST action to protect the chain of evidence when a desktop computer is involved?

- A. Take the computer to a forensic lab
- B. Make a copy of the hard drive
- C. Start documenting
- D. Turn off the computer

Answer: C

NEW QUESTION 34

- (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 37

- (Exam Topic 9)

Internet Protocol (IP) source address spoofing is used to defeat

- A. address-based authentication.
- B. Address Resolution Protocol (ARP).
- C. Reverse Address Resolution Protocol (RARP).
- D. Transmission Control Protocol (TCP) hijacking.

Answer: A

NEW QUESTION 40

- (Exam Topic 9)

Which of the following is the FIRST action that a system administrator should take when it is revealed during a penetration test that everyone in an organization has unauthorized access to a server holding sensitive data?

- A. Immediately document the finding and report to senior management.
- B. Use system privileges to alter the permissions to secure the server
- C. Continue the testing to its completion and then inform IT management
- D. Terminate the penetration test and pass the finding to the server management team

Answer: A

NEW QUESTION 41

- (Exam Topic 9)

Which of the following is a limitation of the Common Vulnerability Scoring System (CVSS) as it relates to conducting code review?

- A. It has normalized severity ratings.
- B. It has many worksheets and practices to implement.
- C. It aims to calculate the risk of published vulnerabilities.
- D. It requires a robust risk management framework to be put in place.

Answer: C

NEW QUESTION 44

- (Exam Topic 9)

To prevent inadvertent disclosure of restricted information, which of the following would be the LEAST effective process for eliminating data prior to the media being discarded?

- A. Multiple-pass overwriting
- B. Degaussing
- C. High-level formatting
- D. Physical destruction

Answer: C

NEW QUESTION 45

- (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 46

- (Exam Topic 9)

An organization allows ping traffic into and out of their network. An attacker has installed a program on the network that uses the payload portion of the ping packet to move data into and out of the network. What type of attack has the organization experienced?

- A. Data leakage
- B. Unfiltered channel
- C. Data emanation
- D. Covert channel

Answer: D

NEW QUESTION 47

- (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 50

- (Exam Topic 9)

The key benefits of a signed and encrypted e-mail include

- A. confidentiality, authentication, and authorization.
- B. confidentiality, non-repudiation, and authentication.
- C. non-repudiation, authorization, and authentication.
- D. non-repudiation, confidentiality, and authorization.

Answer: B

NEW QUESTION 53

- (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 55

- (Exam Topic 9)

Which of the following is considered best practice for preventing e-mail spoofing?

- A. Spam filtering
- B. Cryptographic signature
- C. Uniform Resource Locator (URL) filtering
- D. Reverse Domain Name Service (DNS) lookup

Answer: B

NEW QUESTION 56

- (Exam Topic 9)

An advantage of link encryption in a communications network is that it

- A. makes key management and distribution easier.
- B. protects data from start to finish through the entire network.
- C. improves the efficiency of the transmission.
- D. encrypts all information, including headers and routing information.

Answer: D

NEW QUESTION 59

- (Exam Topic 9)

The process of mutual authentication involves a computer system authenticating a user and authenticating the

- A. user to the audit process.
- B. computer system to the user.
- C. user's access to all authorized objects.
- D. computer system to the audit process.

Answer: B

NEW QUESTION 64

- (Exam Topic 9)

Which of the following is the best practice for testing a Business Continuity Plan (BCP)?

- A. Test before the IT Audit
- B. Test when environment changes
- C. Test after installation of security patches
- D. Test after implementation of system patches

Answer: B

NEW QUESTION 69

- (Exam Topic 9)

The PRIMARY purpose of a security awareness program is to

- A. ensure that everyone understands the organization's policies and procedures.
- B. communicate that access to information will be granted on a need-to-know basis.
- C. warn all users that access to all systems will be monitored on a daily basis.
- D. comply with regulations related to data and information protection.

Answer: A

NEW QUESTION 71

- (Exam Topic 9)

A practice that permits the owner of a data object to grant other users access to that object would usually provide

- A. Mandatory Access Control (MAC).
- B. owner-administered control.
- C. owner-dependent access control.
- D. Discretionary Access Control (DAC).

Answer: D

NEW QUESTION 76

- (Exam Topic 9)

Which one of the following security mechanisms provides the BEST way to restrict the execution of privileged procedures?

- A. Role Based Access Control (RBAC)
- B. Biometric access control
- C. Federated Identity Management (IdM)
- D. Application hardening

Answer:

A

NEW QUESTION 77

- (Exam Topic 9)

An organization is selecting a service provider to assist in the consolidation of multiple computing sites including development, implementation and ongoing support of various computer systems. Which of the following **MUST** be verified by the Information Security Department?

- A. The service provider's policies are consistent with ISO/IEC27001 and there is evidence that the service provider is following those policies.
- B. The service provider will segregate the data within its systems and ensure that each region's policies are met.
- C. The service provider will impose controls and protections that meet or exceed the current systems controls and produce audit logs as verification.
- D. The service provider's policies can meet the requirements imposed by the new environment even if they differ from the organization's current policies.

Answer: D

NEW QUESTION 80

- (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 82

- (Exam Topic 9)

An auditor carrying out a compliance audit requests passwords that are encrypted in the system to verify that the passwords are compliant with policy. Which of the following is the **BEST** response to the auditor?

- A. Provide the encrypted passwords and analysis tools to the auditor for analysis.
- B. Analyze the encrypted passwords for the auditor and show them the results.
- C. Demonstrate that non-compliant passwords cannot be created in the system.
- D. Demonstrate that non-compliant passwords cannot be encrypted in the system.

Answer: C

NEW QUESTION 85

- (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 86

- (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 87

- (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 90

- (Exam Topic 9)

What would be the **PRIMARY** concern when designing and coordinating a security assessment for an Automatic Teller Machine (ATM) system?

- A. Physical access to the electronic hardware
- B. Regularly scheduled maintenance process

- C. Availability of the network connection
- D. Processing delays

Answer: A

NEW QUESTION 92

- (Exam Topic 9)

Which one of the following effectively obscures network addresses from external exposure when implemented on a firewall or router?

- A. Network Address Translation (NAT)
- B. Application Proxy
- C. Routing Information Protocol (RIP) Version 2
- D. Address Masking

Answer: A

NEW QUESTION 97

- (Exam Topic 9)

The Hardware Abstraction Layer (HAL) is implemented in the

- A. system software.
- B. system hardware.
- C. application software.
- D. network hardware.

Answer: A

NEW QUESTION 101

- (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 103

- (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 107

- (Exam Topic 9)

Which one of the following is a fundamental objective in handling an incident?

- A. To restore control of the affected systems
- B. To confiscate the suspect's computers
- C. To prosecute the attacker
- D. To perform full backups of the system

Answer: A

NEW QUESTION 110

- (Exam Topic 9)

When transmitting information over public networks, the decision to encrypt it should be based on

- A. the estimated monetary value of the information.
- B. whether there are transient nodes relaying the transmission.
- C. the level of confidentiality of the information.
- D. the volume of the information.

Answer: C

NEW QUESTION 112

- (Exam Topic 9)

Which of the following would be the FIRST step to take when implementing a patch management program?

- A. Perform automatic deployment of patches.
- B. Monitor for vulnerabilities and threats.
- C. Prioritize vulnerability remediation.
- D. Create a system inventory.

Answer: D

NEW QUESTION 114

- (Exam Topic 9)

While impersonating an Information Security Officer (ISO), an attacker obtains information from company employees about their User IDs and passwords. Which method of information gathering has the attacker used?

- A. Trusted path
- B. Malicious logic
- C. Social engineering
- D. Passive misuse

Answer: C

NEW QUESTION 116

- (Exam Topic 9)

Which of the following defines the key exchange for Internet Protocol Security (IPSec)?

- A. Secure Sockets Layer (SSL) key exchange
- B. Internet Key Exchange (IKE)
- C. Security Key Exchange (SKE)
- D. Internet Control Message Protocol (ICMP)

Answer: B

NEW QUESTION 117

- (Exam Topic 9)

Why MUST a Kerberos server be well protected from unauthorized access?

- A. It contains the keys of all clients.
- B. It always operates at root privilege.
- C. It contains all the tickets for services.
- D. It contains the Internet Protocol (IP) address of all network entities.

Answer: A

NEW QUESTION 119

- (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 120

- (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 125

- (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 128

- (Exam Topic 9)

Passive Infrared Sensors (PIR) used in a non-climate controlled environment should

- A. reduce the detected object temperature in relation to the background temperature.
- B. increase the detected object temperature in relation to the background temperature.
- C. automatically compensate for variance in background temperature.
- D. detect objects of a specific temperature independent of the background temperature.

Answer: C

NEW QUESTION 132

- (Exam Topic 9)

When constructing an Information Protection Policy (IPP), it is important that the stated rules are necessary, adequate, and

- A. flexible.
- B. confidential.
- C. focused.
- D. achievable.

Answer: D

NEW QUESTION 134

- (Exam Topic 9)

Which of the following does Temporal Key Integrity Protocol (TKIP) support?

- A. Multicast and broadcast messages
- B. Coordination of IEEE 802.11 protocols
- C. Wired Equivalent Privacy (WEP) systems
- D. Synchronization of multiple devices

Answer: C

NEW QUESTION 138

- (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 142

- (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 145

- (Exam Topic 9)

Two companies wish to share electronic inventory and purchase orders in a supplier and client relationship. What is the BEST security solution for them?

- A. Write a Service Level Agreement (SLA) for the two companies.
- B. Set up a Virtual Private Network (VPN) between the two companies.
- C. Configure a firewall at the perimeter of each of the two companies.
- D. Establish a File Transfer Protocol (FTP) connection between the two companies.

Answer: B

NEW QUESTION 148

- (Exam Topic 9)

Which Hyper Text Markup Language 5 (HTML5) option presents a security challenge for network data leakage prevention and/or monitoring?

- A. Cross Origin Resource Sharing (CORS)
- B. WebSockets
- C. Document Object Model (DOM) trees
- D. Web Interface Definition Language (IDL)

Answer: B

NEW QUESTION 150

- (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 152

- (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 solutions would have MOST likely detected the use of peer-to-peer programs when the computer was connected to the office network?

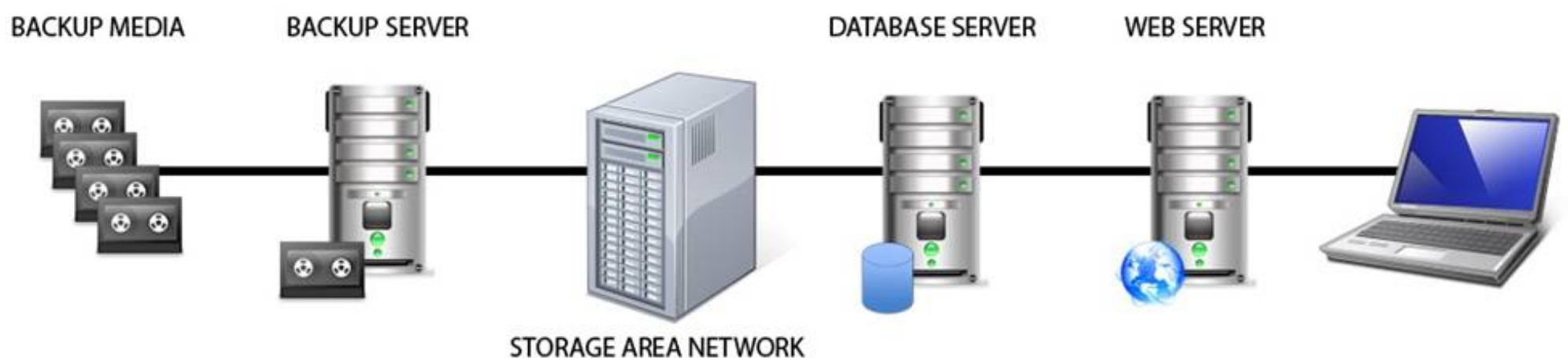
- A. Anti-virus software
- B. Intrusion Prevention System (IPS)
- C. Anti-spyware software
- D. Integrity checking software

Answer: B

NEW QUESTION 155

- (Exam Topic 10)

Identify the component that MOST likely lacks digital accountability related to information access. Click on the correct device in the image below.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Backup Media

Reference: Official (ISC)2 Guide to the CISSP CBK, Third Edition page 1029

NEW QUESTION 156

- (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 159

- (Exam Topic 10)

Which of the following provides effective management assurance for a Wireless Local Area Network (WLAN)?

- A. Maintaining an inventory of authorized Access Points (AP) and connecting devices
- B. Setting the radio frequency to the minimum range required
- C. Establishing a Virtual Private Network (VPN) tunnel between the WLAN client device and a VPN concentrator
- D. Verifying that all default passwords have been changed

Answer: A

NEW QUESTION 161

- (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 163

- (Exam Topic 10)

Which item below is a federated identity standard?

- A. 802.11i
- B. Kerberos
- C. Lightweight Directory Access Protocol (LDAP)
- D. Security Assertion Markup Language (SAML)

Answer: D

NEW QUESTION 168

- (Exam Topic 10)

Which of the following assures that rules are followed in an identity management architecture?

- A. Policy database
- B. Digital signature
- C. Policy decision point
- D. Policy enforcement point

Answer: D

NEW QUESTION 169

- (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 171

- (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 174

- (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.

The third party needs to have

- A. processes that are identical to that of the organization doing the outsourcing.

- B. access to the original personnel that were on staff at the organization.
- C. the ability to maintain all of the applications in languages they are familiar with.
- D. access to the skill sets consistent with the programming languages used by the organization.

Answer: D

NEW QUESTION 179

- (Exam Topic 10)

What is the PRIMARY advantage of using automated application security testing tools?

- A. The application can be protected in the production environment.
- B. Large amounts of code can be tested using fewer resources.
- C. The application will fail less when tested using these tools.
- D. Detailed testing of code functions can be performed.

Answer: B

NEW QUESTION 180

- (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 181

- (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 184

- (Exam Topic 10)

Which of the following is the BEST solution to provide redundancy for telecommunications links?

- A. Provide multiple links from the same telecommunications vendor.
- B. Ensure that the telecommunications links connect to the network in one location.
- C. Ensure that the telecommunications links connect to the network in multiple locations.
- D. Provide multiple links from multiple telecommunications vendors.

Answer: D

NEW QUESTION 185

- (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 186

- (Exam Topic 10)

During the procurement of a new information system, it was determined that some of the security requirements were not addressed in the system specification.

Which of the following is the MOST likely reason for this?

- A. The procurement officer lacks technical knowledge.
- B. The security requirements have changed during the procurement process.

- C. There were no security professionals in the vendor's bidding team.
- D. The description of the security requirements was insufficient.

Answer: D

NEW QUESTION 189

- (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 194

- (Exam Topic 10)

Which of the following MUST system and database administrators be aware of and apply when configuring systems used for storing personal employee data?

- A. Secondary use of the data by business users
- B. The organization's security policies and standards
- C. The business purpose for which the data is to be used
- D. The overall protection of corporate resources and data

Answer: B

NEW QUESTION 196

- (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 201

- (Exam Topic 10)

The use of proximity card to gain access to a building is an example of what type of security control?

- A. Legal
- B. Logical
- C. Physical
- D. Procedural

Answer: C

NEW QUESTION 203

- (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 205

- (Exam Topic 10)

For a service provider, which of the following MOST effectively addresses confidentiality concerns for customers using cloud computing?

- A. Hash functions
- B. Data segregation
- C. File system permissions
- D. Non-repudiation controls

Answer: B

NEW QUESTION 208

- (Exam Topic 10)

From a security perspective, which of the following is a best practice to configure a Domain Name Service (DNS) system?

- A. Configure secondary servers to use the primary server as a zone forwarder.
- B. Block all Transmission Control Protocol (TCP) connections.
- C. Disable all recursive queries on the name servers.
- D. Limit zone transfers to authorized devices.

Answer: D

NEW QUESTION 210

- (Exam Topic 10)

An organization's data policy MUST include a data retention period which is based on

- A. application dismissal.
- B. business procedures.
- C. digital certificates expiration.
- D. regulatory compliance.

Answer: D

NEW QUESTION 213

- (Exam Topic 10)

Without proper signal protection, embedded systems may be prone to which type of attack?

- A. Brute force
- B. Tampering
- C. Information disclosure
- D. Denial of Service (DoS)

Answer: C

NEW QUESTION 216

- (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.

When determining appropriate resource allocation, which of the following is MOST important to monitor?

- A. Number of system compromises
- B. Number of audit findings
- C. Number of staff reductions
- D. Number of additional assets

Answer: B

NEW QUESTION 217

- (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 219

- (Exam Topic 10)

When using third-party software developers, which of the following is the MOST effective method of providing software development Quality Assurance (QA)?

- A. Retain intellectual property rights through contractual wording.
- B. Perform overlapping code reviews by both parties.
- C. Verify that the contractors attend development planning meetings.
- D. Create a separate contractor development environment.

Answer: B

NEW QUESTION 224

- (Exam Topic 10)

Which of the following is the BEST countermeasure to brute force login attacks?

- A. Changing all canonical passwords
- B. Decreasing the number of concurrent user sessions
- C. Restricting initial password delivery only in person
- D. Introducing a delay after failed system access attempts

Answer: D

NEW QUESTION 227

- (Exam Topic 10)

What is the MOST important reason to configure unique user IDs?

- A. Supporting accountability
- B. Reducing authentication errors
- C. Preventing password compromise
- D. Supporting Single Sign On (SSO)

Answer: A

NEW QUESTION 230

- (Exam Topic 10)

Refer to the information below to answer the question.

Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.

Organizational policy requires the deletion of user data from Personal Digital Assistant (PDA) devices before disposal. It may not be possible to delete the user data if the device is malfunctioning. Which destruction method below provides the BEST assurance that the data has been removed?

- A. Knurling
- B. Grinding
- C. Shredding
- D. Degaussing

Answer: C

NEW QUESTION 231

- (Exam Topic 11)

Which of the following statements is TRUE regarding state-based analysis as a functional software testing technique?

- A. It is useful for testing communications protocols and graphical user interfaces.
- B. It is characterized by the stateless behavior of a process implemented in a function.
- C. Test inputs are obtained from the derived boundaries of the given functional specifications.
- D. An entire partition can be covered by considering only one representative value from that partition.

Answer: A

NEW QUESTION 234

- (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 238

- (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 242

- (Exam Topic 11)

Which of the following is a reason to use manual patch installation instead of automated patch management?

- A. The cost required to install patches will be reduced.
- B. The time during which systems will remain vulnerable to an exploit will be decreased.
- C. The likelihood of system or application incompatibilities will be decreased.
- D. The ability to cover large geographic areas is increased.

Answer: C

NEW QUESTION 244

- (Exam Topic 11)

If compromised, which of the following would lead to the exploitation of multiple virtual machines?

- A. Virtual device drivers
- B. Virtual machine monitor
- C. Virtual machine instance
- D. Virtual machine file system

Answer: B

NEW QUESTION 247

- (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 248

- (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 253

- (Exam Topic 11)

Which of the following PRIMARILY contributes to security incidents in web-based applications?

- A. Systems administration and operating systems
- B. System incompatibility and patch management
- C. Third-party applications and change controls
- D. Improper stress testing and application interfaces

Answer: C

NEW QUESTION 254

- (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 255

- (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 259

- (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 260

- (Exam Topic 11)

Which security approach will BEST minimize Personally Identifiable Information (PII) loss from a data breach?

- A. A strong breach notification process
- B. Limited collection of individuals' confidential data
- C. End-to-end data encryption for data in transit
- D. Continuous monitoring of potential vulnerabilities

Answer: B

NEW QUESTION 262

- (Exam Topic 11)

Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

- A. Concept, Development, Production, Utilization, Support, Retirement
- B. Stakeholder Requirements Definition, Architectural Design, Implementation, Verification, Operation
- C. Acquisition, Measurement, Configuration Management, Production, Operation, Support
- D. Concept, Requirements, Design, Implementation, Production, Maintenance, Support, Disposal

Answer: B

NEW QUESTION 267

- (Exam Topic 11)

Which of the following describes the BEST configuration management practice?

- A. After installing a new system, the configuration files are copied to a separate back-up system and hashed to detect tampering.
- B. After installing a new system, the configuration files are copied to an air-gapped system and hashed to detect tampering.
- C. The firewall rules are backed up to an air-gapped system.
- D. A baseline configuration is created and maintained for all relevant systems.

Answer: D

NEW QUESTION 269

- (Exam Topic 11)

Which of the following is the PRIMARY security concern associated with the implementation of smart cards?

- A. The cards have limited memory
- B. Vendor application compatibility
- C. The cards can be misplaced
- D. Mobile code can be embedded in the card

Answer: C

NEW QUESTION 273

- (Exam Topic 11)

A software security engineer is developing a black box-based test plan that will measure the system's reaction to incorrect or illegal inputs or unexpected operational errors and situations. Match the functional testing techniques on the left with the correct input parameters on the right.

Functional Testing
Techniques

State-Based Analysis

Input Parameter
Selection

Select one input that does not belong to any of the identified partitions.

Equivalence Class Analysis

Select inputs that are at the external limits of the domain of valid values.

Decision Table Analysis

Select invalid combinations of input values.

Boundary Value Analysis

Select unexpected inputs corresponding to each known condition.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Functional Testing Techniques		Input Parameter Selection
State-Based Analysis	Equivalence Class Analysis	Select one input that does not belong to any of the identified partitions.
Equivalence Class Analysis	Boundary Value Analysis	Select inputs that are at the external limits of the domain of valid values.
Decision Table Analysis	Decision Table Analysis	Select invalid combinations of input values.
Boundary Value Analysis	State-Based Analysis	Select unexpected inputs corresponding to each known condition.

NEW QUESTION 277

- (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 280

- (Exam Topic 11)
Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).

Secure Architecture		Do you advertise shared security services with guidance for project teams?
Education & Guidance		Are most people tested to ensure a baseline skill- set for secure development practices?
Strategy & Metrics		Does most of the organization know about what's required based on risk ratings?
Vulnerability Management		Are most project teams aware of their security point(s) of contact and response team(s)?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Secure Architecture

Secure Architecture

Do you advertise shared security services with guidance for project teams?

Education & Guidance

Education & Guidance

Are most people tested to ensure a baseline skill- set for secure development practices?

Strategy & Metrics

Strategy & Metrics

Does most of the organization know about what's required based on risk ratings?

Vulnerability Management

Vulnerability Management

Are most project teams aware of their security point(s) of contact and response team(s)?

NEW QUESTION 283

- (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 286

- (Exam Topic 11)

The implementation of which features of an identity management system reduces costs and administration overhead while improving audit and accountability?

- A. Two-factor authentication
- B. Single Sign-On (SSO)
- C. User self-service
- D. A metadirectory

Answer: C

NEW QUESTION 290

- (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 294

- (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 299

- (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 300

- (Exam Topic 11)

Data leakage of sensitive information is MOST often concealed by which of the following?

- A. Secure Sockets Layer (SSL)
- B. Secure Hash Algorithm (SHA)
- C. Wired Equivalent Privacy (WEP)
- D. Secure Post Office Protocol (POP)

Answer: A

NEW QUESTION 301

- (Exam Topic 11)

An organization has decided to contract with a cloud-based service provider to leverage their identity as a service offering. They will use Open Authentication (OAuth) 2.0 to authenticate external users to the organization's services.

As part of the authentication process, which of the following must the end user provide?

- A. An access token
- B. A username and password
- C. A username
- D. A password

Answer: A

NEW QUESTION 302

- (Exam Topic 11)

The PRIMARY outcome of a certification process is that it provides documented

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

Answer: D

NEW QUESTION 307

- (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 308

- (Exam Topic 11)

What type of test assesses a Disaster Recovery (DR) plan using realistic disaster scenarios while maintaining minimal impact to business operations?

- A. Parallel
- B. Walkthrough
- C. Simulation
- D. Tabletop

Answer: C

NEW QUESTION 310

- (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 313

- (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 315

- (Exam Topic 11)

A Simple Power Analysis (SPA) attack against a device directly observes which of the following?

- A. Static discharge
- B. Consumption
- C. Generation
- D. Magnetism

Answer: B

NEW QUESTION 319

- (Exam Topic 11)

Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?

- A. Policy documentation review
- B. Authentication validation
- C. Periodic log reviews
- D. Interface testing

Answer: C

NEW QUESTION 320

- (Exam Topic 11)

In the Open System Interconnection (OSI) model, which layer is responsible for the transmission of binary data over a communications network?

- A. Application Layer
- B. Physical Layer
- C. Data-Link Layer
- D. Network Layer

Answer: B

NEW QUESTION 324

- (Exam Topic 11)

The 802.1x standard provides a framework for what?

- A. Network authentication for only wireless networks
- B. Network authentication for wired and wireless networks
- C. Wireless encryption using the Advanced Encryption Standard (AES)
- D. Wireless network encryption using Secure Sockets Layer (SSL)

Answer: B

NEW QUESTION 327

- (Exam Topic 11)

While investigating a malicious event, only six days of audit logs from the last month were available. What policy should be updated to address this problem?

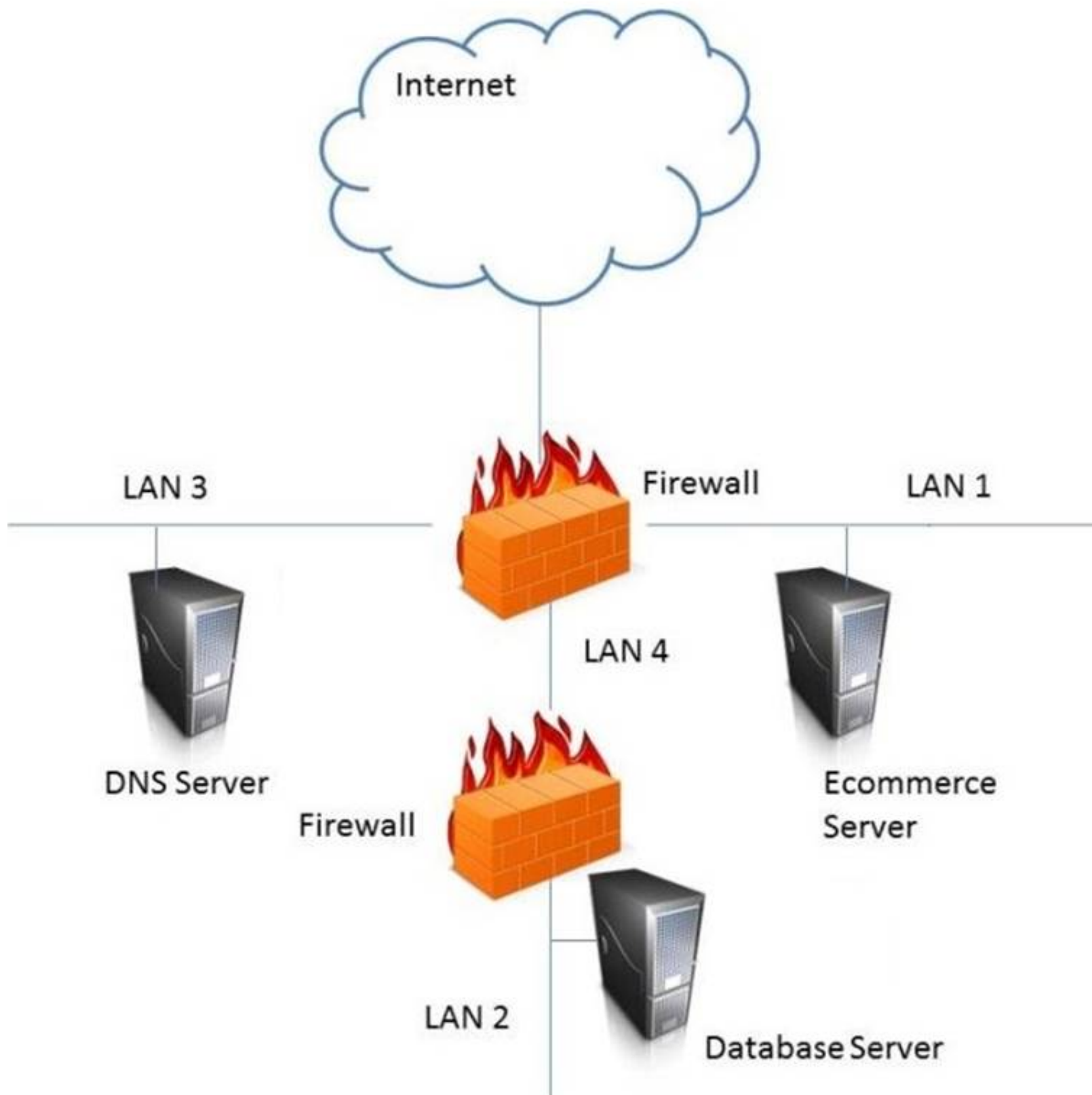
- A. Retention
- B. Reporting
- C. Recovery
- D. Remediation

Answer: A

NEW QUESTION 330

- (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 331

- (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 334

- (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 ping
- B. Lock picking
- C. Lock bumping
- D. Lock bricking

Answer: B

NEW QUESTION 338

- (Exam Topic 11)

The BEST method to mitigate the risk of a dictionary attack on a system is to

- A. use a hardware token.
- B. use complex passphrases.
- C. implement password history.
- D. encrypt the access control list (ACL).

Answer: A

NEW QUESTION 342

- (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 343

- (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 347

- (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 351

- (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 355

- (Exam Topic 12)

Which of the following is the BEST method to reduce the effectiveness of phishing attacks?

- A. User awareness
- B. Two-factor authentication
- C. Anti-phishing software
- D. Periodic vulnerability scan

Answer: A

NEW QUESTION 357

- (Exam Topic 12)

An Intrusion Detection System (IDS) has recently been deployed in a Demilitarized Zone (DMZ). The IDS detects a flood of malformed packets. Which of the following BEST describes what has occurred?

- A. Denial of Service (DoS) attack
- B. Address Resolution Protocol (ARP) spoof
- C. Buffer overflow
- D. Ping flood attack

Answer: A

NEW QUESTION 358

- (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 362

- (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 364

- (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 368

- (Exam Topic 12)

Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

- A. Tactical, strategic, and financial
- B. Management, operational, and technical
- C. Documentation, observation, and manual
- D. Standards, policies, and procedures

Answer: B

NEW QUESTION 373

- (Exam Topic 12)

Match the types of e-authentication tokens to their description.

Drag each e-authentication token on the left to its corresponding description on the right.

E-Authentication Token		Description
Memorized Secret Token		A physical or electronic token that stores a set of secrets between the claimant and the credential service provider
Out-of-Band Token		A physical token that is uniquely addressable and can receive a verifier-selected secret for one-time use
Look-up Secret Token		A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process
Pre-registered Knowledge Token		A secret shared between the subscriber and credential service provider that is typically character strings

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Look-up secret token - A physical or electronic token that stores a set of secrets between the claimant and the credential service provider

Out-of-Band Token - A physical token that is uniquely addressable and can receive a verifier-selected secret for one-time use

Pre-registered Knowledge Token - A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process

Memorized Secret Token - A secret shared between the subscriber and credential service provider that is typically character strings

NEW QUESTION 375

- (Exam Topic 12)

Which of the following restricts the ability of an individual to carry out all the steps of a particular process?

- A. Job rotation
- B. Separation of duties
- C. Least privilege
- D. Mandatory vacations

Answer: B

NEW QUESTION 376

- (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 379

- (Exam Topic 12)

What does the Maximum Tolerable Downtime (MTD) determine?

- A. The estimated period of time a business critical database can remain down before customers are affected.
- B. The fixed length of time a company can endure a disaster without any Disaster Recovery (DR) planning
- C. The estimated period of time a business can remain interrupted beyond which it risks never recovering
- D. The fixed length of time in a DR process before redundant systems are engaged

Answer: C

NEW QUESTION 381

- (Exam Topic 12)

The PRIMARY purpose of accreditation is to:

- A. comply with applicable laws and regulations.
- B. allow senior management to make an informed decision regarding whether to accept the risk of operating the system.
- C. protect an organization's sensitive data.
- D. verify that all security controls have been implemented properly and are operating in the correct manner.

Answer: B

NEW QUESTION 386

- (Exam Topic 12)

Which of the following BEST describes a chosen plaintext attack?

- A. The cryptanalyst can generate ciphertext from arbitrary text.
- B. The cryptanalyst examines the communication being sent back and forth.
- C. The cryptanalyst can choose the key and algorithm to mount the attack.
- D. The cryptanalyst is presented with the ciphertext from which the original message is determined.

Answer: A

NEW QUESTION 391

- (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 396

- (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 398

- (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 400

- (Exam Topic 12)

When writing security assessment procedures, what is the MAIN purpose of the test outputs and reports?

- A. To force the software to fail and document the process
- B. To find areas of compromise in confidentiality and integrity
- C. To allow for objective pass or fail decisions
- D. To identify malware or hidden code within the test results

Answer: C

NEW QUESTION 405

- (Exam Topic 12)

An employee of a retail company has been granted an extended leave of absence by Human Resources (HR). This information has been formally communicated to the access provisioning team. Which of the following is the BEST action to take?

- A. Revoke access temporarily.
- B. Block user access and delete user account after six months.
- C. Block access to the offices immediately.
- D. Monitor account usage temporarily.

Answer: D

NEW QUESTION 407

- (Exam Topic 12)

Which of the following is the PRIMARY benefit of a formalized information classification program?

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

Answer: B

NEW QUESTION 408

- (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 412

- (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 415

- (Exam Topic 12)

An organization's information security strategic plan MUST be reviewed

- A. whenever there are significant changes to a major application.
- B. quarterly, when the organization's strategic plan is updated.
- C. whenever there are major changes to the business.
- D. every three years, when the organization's strategic plan is updated.

Answer: C

NEW QUESTION 418

- (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 420

- (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 421

- (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 426

- (Exam Topic 12)

A user sends an e-mail request asking for read-only access to files that are not considered sensitive. A Discretionary Access Control (DAC) methodology is in place. Which is the MOST suitable approach that the administrator should take?

- A. Administrator should request data owner approval to the user access
- B. Administrator should request manager approval for the user access
- C. Administrator should directly grant the access to the non-sensitive files
- D. Administrator should assess the user access need and either grant or deny the access

Answer: A

NEW QUESTION 427

- (Exam Topic 12)

When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?

- A. Topology diagrams
- B. Mapping tools
- C. Asset register
- D. Ping testing

Answer: D

NEW QUESTION 429

- (Exam Topic 12)

Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?

- A. Notification tool
- B. Message queuing tool
- C. Security token tool
- D. Synchronization tool

Answer: C

NEW QUESTION 432

- (Exam Topic 13)

A security compliance manager of a large enterprise wants to reduce the time it takes to perform network, system, and application security compliance audits while increasing quality and effectiveness of the results. What should be implemented to BEST achieve the desired results?

- A. Configuration Management Database (CMDB)
- B. Source code repository
- C. Configuration Management Plan (CMP)
- D. System performance monitoring application

Answer: C

NEW QUESTION 433

- (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 436

- (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 437

- (Exam Topic 13)

A control to protect from a Denial-of-Service (DoS) attack has been determined to stop 50% of attacks, and additionally reduces the impact of an attack by 50%. What is the residual risk?

- A. 25%
- B. 50%
- C. 75%
- D. 100%

Answer: A

NEW QUESTION 442

- (Exam Topic 13)

Which one of the following is an advantage of an effective release control strategy from a configuration control standpoint?

- A. Ensures that a trace for all deliverables is maintained and auditable
- B. Enforces backward compatibility between releases
- C. Ensures that there is no loss of functionality between releases
- D. Allows for future enhancements to existing features

Answer: C

NEW QUESTION 447

- (Exam Topic 13)

Which of the following is the MOST important security goal when performing application interface testing?

- A. Confirm that all platforms are supported and function properly
- B. Evaluate whether systems or components pass data and control correctly to one another
- C. Verify compatibility of software, hardware, and network connections

D. Examine error conditions related to external interfaces to prevent application details leakage

Answer: B

NEW QUESTION 452

- (Exam Topic 13)

What is the MAIN goal of information security awareness and training?

- A. To inform users of the latest malware threats
- B. To inform users of information assurance responsibilities
- C. To comply with the organization information security policy
- D. To prepare students for certification

Answer: B

NEW QUESTION 456

- (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 461

- (Exam Topic 13)

Due to system constraints, a group of system administrators must share a high-level access set of credentials. Which of the following would be MOST appropriate to implement?

- A. Increased console lockout times for failed logon attempts
- B. Reduce the group in size
- C. A credential check-out process for a per-use basis
- D. Full logging on affected systems

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 465

- (Exam Topic 13)

Who is responsible for the protection of information when it is shared with or provided to other organizations?

- A. Systems owner
- B. Authorizing Official (AO)
- C. Information owner
- D. Security officer

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 466

- (Exam Topic 13)

In an organization where Network Access Control (NAC) has been deployed, a device trying to connect to the network is being placed into an isolated domain. What could be done on this device in order to obtain proper connectivity?

- A. Connect the device to another network jack
- B. Apply remediation's according to security requirements
- C. Apply Operating System (OS) patches
- D. Change the Message Authentication Code (MAC) address of the network interface

Answer: B

NEW QUESTION 467

- (Exam Topic 13)

As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

- A. Use a web scanner to scan for vulnerabilities within the website.
- B. Perform a code review to ensure that the database references are properly addressed.
- C. Establish a secure connection to the web server to validate that only the approved ports are open.

D. Enter only numbers in the web form and verify that the website prompts the user to enter a valid input.

Answer: D

NEW QUESTION 469

- (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 474

- (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 477

- (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 479

- (Exam Topic 13)

An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject's data?

- A. Aggregate it into one database in the US
- B. Process it in the US, but store the information in France
- C. Share it with a third party
- D. Anonymize it and process it in the US

Answer: C

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 480

- (Exam Topic 13)

Which of the following are important criteria when designing procedures and acceptance criteria for acquired software?

- A. Code quality, security, and origin
- B. Architecture, hardware, and firmware
- C. Data quality, provenance, and scaling
- D. Distributed, agile, and bench testing

Answer: A

NEW QUESTION 482

- (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 486

- (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 490

- (Exam Topic 13)

Which of the following is the MOST efficient mechanism to account for all staff during a speedy nonemergency evacuation from a large security facility?

- A. Large mantrap where groups of individuals leaving are identified using facial recognition technology
- B. Radio Frequency Identification (RFID) sensors worn by each employee scanned by sensors at each exitdoor
- C. Emergency exits with push bars with coordinates at each exit checking off the individual against a predefined list
- D. Card-activated turnstile where individuals are validated upon exit

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 494

- (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 498

- (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 500

- (Exam Topic 13)

When developing solutions for mobile devices, in which phase of the Software Development Life Cycle (SDLC) should technical limitations related to devices be specified?

- A. Implementation
- B. Initiation
- C. Review
- D. Development

Answer: A

NEW QUESTION 505

- (Exam Topic 13)

The organization would like to deploy an authorization mechanism for an Information Technology (IT) infrastructure project with high employee turnover. Which access control mechanism would be preferred?

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

Answer: D

NEW QUESTION 507

- (Exam Topic 13)

Which of the following methods of suppressing a fire is environmentally friendly and the MOST appropriate for a data center?

- A. Inert gas fire suppression system
- B. Halon gas fire suppression system
- C. Dry-pipe sprinklers
- D. Wet-pipe sprinklers

Answer: C

NEW QUESTION 508

- (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 513

- (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 518

- (Exam Topic 13)

Match the name of access control model with its associated restriction.

Drag each access control model to its appropriate restriction access on the right.

<u>Access Control Model</u>		<u>Restrictions</u>
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:

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

NEW QUESTION 519

- (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 523

- (Exam Topic 13)

Which type of test would an organization perform in order to locate and target exploitable defects?

- A. Penetration
- B. System
- C. Performance
- D. Vulnerability

Answer: A

NEW QUESTION 527

- (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:

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

NEW QUESTION 528

- (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 530

- (Exam Topic 13)

What is the second step in the identity and access provisioning lifecycle?

- A. Provisioning
- B. Review
- C. Approval
- D. Revocation

Answer: B

NEW QUESTION 531

- (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 536

- (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 538

- (Exam Topic 13)

At a MINIMUM, audits of permissions to individual or group accounts should be scheduled

- A. annually
- B. to correspond with staff promotions
- C. to correspond with terminations
- D. continually

Answer: A

NEW QUESTION 542

- (Exam Topic 13)

Which Identity and Access Management (IAM) process can be used to maintain the principle of least privilege?

- A. identity provisioning
- B. access recovery
- C. multi-factor authentication (MFA)
- D. user access review

Answer: A

NEW QUESTION 545

- (Exam Topic 13)

Which of the following is part of a Trusted Platform Module (TPM)?

- A. A non-volatile tamper-resistant storage for storing both data and signing keys in a secure fashion
- B. A protected Pre-Basic Input/Output System (BIOS) which specifies a method or a metric for “measuring”the state of a computing platform
- C. A secure processor targeted at managing digital keys and accelerating digital signing
- D. A platform-independent software interface for accessing computer functions

Answer: A

NEW QUESTION 550

- (Exam Topic 13)

Which of the following is a responsibility of a data steward?

- A. Ensure alignment of the data governance effort to the organization.
- B. Conduct data governance interviews with the organization.
- C. Document data governance requirements.
- D. Ensure that data decisions and impacts are communicated to the organization.

Answer: A

NEW QUESTION 555

- (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 557

- (Exam Topic 13)

Which of the following is the MOST appropriate action when reusing media that contains sensitive data?

- A. Erase
- B. Sanitize
- C. Encrypt
- D. Degauss

Answer: B

NEW QUESTION 558

- (Exam Topic 13)

A user has infected a computer with malware by connecting a Universal Serial Bus (USB) storage device. Which of the following is MOST effective to mitigate future infections?

- A. Develop a written organizational policy prohibiting unauthorized USB devices
- B. Train users on the dangers of transferring data in USB devices
- C. Implement centralized technical control of USB port connections
- D. Encrypt removable USB devices containing data at rest

Answer: C

NEW QUESTION 559

- (Exam Topic 13)

What is the correct order of steps in an information security assessment?

Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.

<u>Actions</u>		<u>Steps</u>
Define the perimeter.		Step 1
Identify the vulnerability.		Step 2
Assess the risk.		Step 3
Determine the actions.		Step 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<u>Actions</u>		<u>Steps</u>
Define the perimeter.	Identify the vulnerability.	Step 1
Identify the vulnerability.	Define the perimeter.	Step 2
Assess the risk.	Assess the risk.	Step 3
Determine the actions.	Determine the actions.	Step 4

NEW QUESTION 562

- (Exam Topic 13)

During examination of Internet history records, the following string occurs within a Unique Resource Locator (URL):

<http://www.companysite.com/products/products.asp?productid=123>
or 1=1

What type of attack does this indicate?

- A. Directory traversal
- B. Structured Query Language (SQL) injection
- C. Cross-Site Scripting (XSS)
- D. Shellcode injection

Answer: C

NEW QUESTION 565

- (Exam Topic 13)

Who would be the BEST person to approve an organizations information security policy?

- A. Chief Information Officer (CIO)
- B. Chief Information Security Officer (CISO)
- C. Chief internal auditor
- D. Chief Executive Officer (CEO)

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 570

- (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 573

- (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 577

- (Exam Topic 13)

Which of the following provides the MOST comprehensive filtering of Peer-to-Peer (P2P) traffic?

- A. Application proxy
- B. Port filter
- C. Network boundary router
- D. Access layer switch

Answer: A

NEW QUESTION 579

- (Exam Topic 13)

Which of the following techniques is known to be effective in spotting resource exhaustion problems, especially with resources such as processes, memory, and connections?

- A. Automated dynamic analysis
- B. Automated static analysis
- C. Manual code review
- D. Fuzzing

Answer: A

NEW QUESTION 584

- (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 589

- (Exam Topic 13)

Access to which of the following is required to validate web session management?

- A. Log timestamp
- B. Live session traffic
- C. Session state variables
- D. Test scripts

Answer: C

NEW QUESTION 591

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The CISSP Practice Test Here](#)