

## 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)

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 1)

What is the MOST important consideration from a data security perspective when an organization plans to relocate?

- A. Ensure the fire prevention and detection systems are sufficient to protect personnel
- B. Review the architectural plans to determine how many emergency exits are present
- C. Conduct a gap analysis of a new facilities against existing security requirements
- D. Revise the Disaster Recovery and Business Continuity (DR/BC) plan

**Answer:** C

**NEW QUESTION 5**

- (Exam Topic 2)

In a data classification scheme, the data is owned by the

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

**Answer:** B

**NEW QUESTION 6**

- (Exam Topic 2)

Which of the following BEST describes the responsibilities of a data owner?

- A. Ensuring quality and validation through periodic audits for ongoing data integrity
- B. Maintaining fundamental data availability, including data storage and archiving
- C. Ensuring accessibility to appropriate users, maintaining appropriate levels of data security
- D. Determining the impact the information has on the mission of the organization

**Answer:** C

**NEW QUESTION 7**

- (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 8**

- (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 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)

Which of the following is used by the Point-to-Point Protocol (PPP) to determine packet formats?

- A. Layer 2 Tunneling Protocol (L2TP)
- B. Link Control Protocol (LCP)
- C. Challenge Handshake Authentication Protocol (CHAP)
- D. Packet Transfer Protocol (PTP)

**Answer:** B

**NEW QUESTION 10**

- (Exam Topic 4)

What is the purpose of an Internet Protocol (IP) spoofing attack?

- A. To send excessive amounts of data to a process, making it unpredictable
- B. To intercept network traffic without authorization
- C. To disguise the destination address from a target's IP filtering devices
- D. To convince a system that it is communicating with a known entity

**Answer:** D

**NEW QUESTION 15**

- (Exam Topic 4)

In a Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which layer is responsible for negotiating and establishing a connection with another node?

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

**Answer:** A

**NEW QUESTION 17**

- (Exam Topic 4)

Which of the following is the BEST network defense against unknown types of attacks or stealth attacks in progress?

- A. Intrusion Prevention Systems (IPS)
- B. Intrusion Detection Systems (IDS)
- C. Stateful firewalls
- D. Network Behavior Analysis (NBA) tools

**Answer:** D

**NEW QUESTION 21**

- (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 22**

- (Exam Topic 6)

Which of the following is of GREATEST assistance to auditors when reviewing system configurations?

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

**Answer:** A

**NEW QUESTION 24**

- (Exam Topic 6)

Which of the following is a PRIMARY benefit of using a formalized security testing report format and structure?

- A. Executive audiences will understand the outcomes of testing and most appropriate next steps for corrective actions to be taken
- B. Technical teams will understand the testing objectives, testing strategies applied, and business risk associated with each vulnerability
- C. Management teams will understand the testing objectives and reputational risk to the organization
- D. Technical and management teams will better understand the testing objectives, results of each test phase, and potential impact levels

**Answer:** D

**NEW QUESTION 29**

- (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 30**

- (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)

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 35**

- (Exam Topic 8)

What is the BEST approach to addressing security issues in legacy web applications?

- A. Debug the security issues
- B. Migrate to newer, supported applications where possible
- C. Conduct a security assessment
- D. Protect the legacy application with a web application firewall

**Answer:** D

**NEW QUESTION 38**

- (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 39**

- (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 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 43**

- (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 48**

- (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 49**

- (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 51**

- (Exam Topic 9)

What is the term commonly used to refer to a technique of authenticating one machine to another by forging packets from a trusted source?

- A. Man-in-the-Middle (MITM) attack
- B. Smurfing
- C. Session redirect
- D. Spoofing

**Answer:** D

**NEW QUESTION 54**

- (Exam Topic 9)

During an audit of system management, auditors find that the system administrator has not been trained. What actions need to be taken at once to ensure the integrity of systems?

- A. A review of hiring policies and methods of verification of new employees
- B. A review of all departmental procedures
- C. A review of all training procedures to be undertaken
- D. A review of all systems by an experienced administrator

**Answer:** D

#### **NEW QUESTION 56**

- (Exam Topic 9)

Which security action should be taken FIRST when computer personnel are terminated from their jobs?

- A. Remove their computer access
- B. Require them to turn in their badge
- C. Conduct an exit interview
- D. Reduce their physical access level to the facility

**Answer:** A

#### **NEW QUESTION 58**

- (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 62**

- (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 65**

- (Exam Topic 9)

How can a forensic specialist exclude from examination a large percentage of operating system files residing on a copy of the target system?

- A. Take another backup of the media in question then delete all irrelevant operating system files.
- B. Create a comparison database of cryptographic hashes of the files from a system with the same operating system and patch level.
- C. Generate a message digest (MD) or secure hash on the drive image to detect tampering of the media being examined.
- D. Discard harmless files for the operating system, and known installed programs.

**Answer:** B

#### **NEW QUESTION 69**

- (Exam Topic 9)

As one component of a physical security system, an Electronic Access Control (EAC) token is BEST known for its ability to

- A. overcome the problems of key assignments.
- B. monitor the opening of windows and doors.
- C. trigger alarms when intruders are detected.
- D. lock down a facility during an emergency.

**Answer:** A

#### **NEW QUESTION 74**

- (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 79**

- (Exam Topic 9)

The BEST method of demonstrating a company's security level to potential customers is

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

**Answer:** A

**NEW QUESTION 80**

- (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 81**

- (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 86**

- (Exam Topic 9)

Which of the following is a security feature of Global Systems for Mobile Communications (GSM)?

- A. It uses a Subscriber Identity Module (SIM) for authentication.
- B. It uses encrypting techniques for all communications.
- C. The radio spectrum is divided with multiple frequency carriers.
- D. The signal is difficult to read as it provides end-to-end encryption.

**Answer:** A

**NEW QUESTION 87**

- (Exam Topic 9)

Which of the following statements is TRUE for point-to-point microwave transmissions?

- A. They are not subject to interception due to encryption.
- B. Interception only depends on signal strength.
- C. They are too highly multiplexed for meaningful interception.
- D. They are subject to interception by an antenna within proximity.

**Answer:** D

**NEW QUESTION 91**

- (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 92**

- (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 97**

- (Exam Topic 9)

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

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

**Answer: D**

**NEW QUESTION 101**

- (Exam Topic 9)

Which of the following can BEST prevent security flaws occurring in outsourced software development?

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

**Answer: C**

**NEW QUESTION 103**

- (Exam Topic 9)

What principle requires that changes to the plaintext affect many parts of the ciphertext?

- A. Diffusion
- B. Encapsulation
- C. Obfuscation
- D. Permutation

**Answer: A**

**NEW QUESTION 106**

- (Exam Topic 9)

A security consultant has been asked to research an organization's legal obligations to protect privacy-related information. What kind of reading material is MOST relevant to this project?

- A. The organization's current security policies concerning privacy issues
- B. Privacy-related regulations enforced by governing bodies applicable to the organization
- C. Privacy best practices published by recognized security standards organizations
- D. Organizational procedures designed to protect privacy information

**Answer: B**

**NEW QUESTION 109**

- (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 114**

- (Exam Topic 9)

The birthday attack is MOST effective against which one of the following cipher technologies?

- A. Chaining block encryption
- B. Asymmetric cryptography
- C. Cryptographic hash
- D. Streaming cryptography

**Answer: C**

**NEW QUESTION 116**

- (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 120**

- (Exam Topic 9)

Which type of control recognizes that a transaction amount is excessive in accordance with corporate policy?

- A. Detection
- B. Prevention
- C. Investigation
- D. Correction

**Answer:** A

**NEW QUESTION 122**

- (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 123**

- (Exam Topic 9)

Alternate encoding such as hexadecimal representations is MOST often observed in which of the following forms of attack?

- A. Smurf
- B. Rootkit exploit
- C. Denial of Service (DoS)
- D. Cross site scripting (XSS)

**Answer:** D

**NEW QUESTION 125**

- (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 128**

- (Exam Topic 9)

In a basic SYN flood attack, what is the attacker attempting to achieve?

- A. Exceed the threshold limit of the connection queue for a given service
- B. Set the threshold to zero for a given service
- C. Cause the buffer to overflow, allowing root access
- D. Flush the register stack, allowing hijacking of the root account

**Answer:** A

**NEW QUESTION 132**

- (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 134**

- (Exam Topic 9)

When implementing controls in a heterogeneous end-point network for an organization, it is critical that

- A. hosts are able to establish network communications.
- B. users can make modifications to their security software configurations.
- C. common software security components be implemented across all hosts.

D. firewalls running on each host are fully customizable by the user.

**Answer:** C

**NEW QUESTION 139**

- (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 142**

- (Exam Topic 9)

Which of the following actions should be performed when implementing a change to a database schema in a production system?

- A. Test in development, determine dates, notify users, and implement in production
- B. Apply change to production, run in parallel, finalize change in production, and develop a back-out strategy
- C. Perform user acceptance testing in production, have users sign off, and finalize change
- D. Change in development, perform user acceptance testing, develop a back-out strategy, and implement change

**Answer:** D

**NEW QUESTION 147**

- (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 148**

- (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 153**

- (Exam Topic 9)

Which of the following wraps the decryption key of a full disk encryption implementation and ties the hard disk drive to a particular device?

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

**Answer:** A

**NEW QUESTION 154**

- (Exam Topic 9)

Which of the following Disaster Recovery (DR) sites is the MOST difficult to test?

- A. Hot site
- B. Cold site
- C. Warm site
- D. Mobile site

**Answer:** B

**NEW QUESTION 155**

- (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 157

- (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 158

- (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 159

- (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 organization should ensure that the third party's physical security controls are in place so that they

- A. are more rigorous than the original controls.  
B. are able to limit access to sensitive information.  
C. allow access by the organization staff at any time.  
D. cannot be accessed by subcontractors of the third party.

**Answer:** B

#### NEW QUESTION 164

- (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 168

- (Exam Topic 10)

What physical characteristic does a retinal scan biometric device measure?

- A. The amount of light reflected by the retina  
B. The size, curvature, and shape of the retina  
C. The pattern of blood vessels at the back of the eye  
D. The pattern of light receptors at the back of the eye

**Answer:** C

**NEW QUESTION 173**

- (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 be the PRIMARY security concern as staff is released from the organization?

- A. Inadequate IT support
- B. Loss of data and separation of duties
- C. Undocumented security controls
- D. Additional responsibilities for remaining staff

**Answer: B**

**NEW QUESTION 175**

- (Exam Topic 10)

An online retail company has formulated a record retention schedule for customer transactions. Which of the following is a valid reason a customer transaction is kept beyond the retention schedule?

- A. Pending legal hold
- B. Long term data mining needs
- C. Customer makes request to retain
- D. Useful for future business initiatives

**Answer: A**

**NEW QUESTION 176**

- (Exam Topic 10)

What does secure authentication with logging provide?

- A. Data integrity
- B. Access accountability
- C. Encryption logging format
- D. Segregation of duties

**Answer: B**

**NEW QUESTION 179**

- (Exam Topic 10)

Which of the following is the MOST difficult to enforce when using cloud computing?

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

**Answer: D**

**NEW QUESTION 184**

- (Exam Topic 10)

What is the MOST critical factor to achieve the goals of a security program?

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

**Answer: B**

**NEW QUESTION 186**

- (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 191**

- (Exam Topic 10)

What component of a web application that stores the session state in a cookie can be bypassed by an attacker?

- A. An initialization check
- B. An identification check

- C. An authentication check
- D. An authorization check

**Answer:** C

**NEW QUESTION 194**

- (Exam Topic 10)

Refer to the information below to answer the question.

During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.

If the intrusion causes the system processes to hang, which of the following has been affected?

- A. System integrity
- B. System availability
- C. System confidentiality
- D. System auditability

**Answer:** B

**NEW QUESTION 195**

- (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 200**

- (Exam Topic 10)

Which of the following actions MUST be taken if a vulnerability is discovered during the maintenance stage in a System Development Life Cycle (SDLC)?

- A. Make changes following principle and design guidelines.
- B. Stop the application until the vulnerability is fixed.
- C. Report the vulnerability to product owner.
- D. Monitor the application and review code.

**Answer:** C

**NEW QUESTION 202**

- (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 207**

- (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 208**

- (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 212**

- (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 213**

- (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 214**

- (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 215**

- (Exam Topic 10)

What is the BEST method to detect the most common improper initialization problems in programming languages?

- A. Use and specify a strong character encoding.
- B. Use automated static analysis tools that target this type of weakness.
- C. Perform input validation on any numeric inputs by assuring that they are within the expected range.
- D. Use data flow analysis to minimize the number of false positives.

**Answer:** B

**NEW QUESTION 217**

- (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 221**

- (Exam Topic 10)

Host-Based Intrusion Protection (HIPS) systems are often deployed in monitoring or learning mode during their initial implementation. What is the objective of starting in this mode?

- A. Automatically create exceptions for specific actions or files
- B. Determine which files are unsafe to access and blacklist them
- C. Automatically whitelist actions or files known to the system
- D. Build a baseline of normal or safe system events for review

**Answer:** D

**NEW QUESTION 222**



- (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 227

- (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 228

- (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 232

- (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.

After magnetic drives were degaussed twice according to the product manufacturer's directions, what is the MOST LIKELY security issue with degaussing?

- A. Commercial products often have serious weaknesses of the magnetic force available in the degausser product.
- B. Degausser products may not be properly maintained and operated.
- C. The inability to turn the drive around in the chamber for the second pass due to human error.
- D. Inadequate record keeping when sanitizing media.

**Answer: B**

#### NEW QUESTION 234

- (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 237

- (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 242

- (Exam Topic 10)

What is the PRIMARY reason for ethics awareness and related policy implementation?

- A. It affects the workflow of an organization.

- B. It affects the reputation of an organization.
- C. It affects the retention rate of employees.
- D. It affects the morale of the employees.

**Answer:** B

#### NEW QUESTION 244

- (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 246

- (Exam Topic 10)

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

**Answer:** C

#### NEW QUESTION 247

- (Exam Topic 10)

Refer to the information below to answer the question.

A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.

What additional considerations are there if the third party is located in a different country?

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

**Answer:** C

#### NEW QUESTION 248

- (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 253

- (Exam Topic 10)

Which of the following provides the MOST protection against data theft of sensitive information when a laptop is stolen?

- A. Set up a BIOS and operating system password
- B. Encrypt the virtual drive where confidential files can be stored
- C. Implement a mandatory policy in which sensitive data cannot be stored on laptops, but only on the corporate network
- D. Encrypt the entire disk and delete contents after a set number of failed access attempts

**Answer:** D

#### NEW QUESTION 256

- (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 260**

- (Exam Topic 10)

Refer to the information below to answer the question.

During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.

Aside from the potential records which may have been viewed, which of the following should be the PRIMARY concern regarding the database information?

- A. Unauthorized database changes
- B. Integrity of security logs
- C. Availability of the database
- D. Confidentiality of the incident

**Answer:** A

**NEW QUESTION 262**

- (Exam Topic 11)

What is the process called when impact values are assigned to the security objectives for information types?

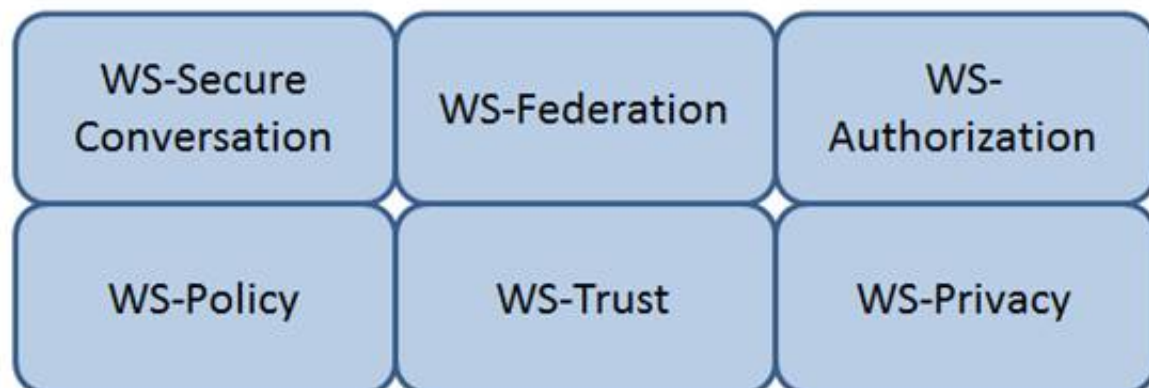
- A. Qualitative analysis
- B. Quantitative analysis
- C. Remediation
- D. System security categorization

**Answer:** D

**NEW QUESTION 267**

- (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 271**

- (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 272**

- (Exam Topic 11)

Which of the following is generally indicative of a replay attack when dealing with biometric authentication?

- A. False Acceptance Rate (FAR) is greater than 1 in 100,000
- B. False Rejection Rate (FRR) is greater than 5 in 100
- C. Inadequately specified templates
- D. Exact match

**Answer:** D

#### NEW QUESTION 275

- (Exam Topic 11)

A security professional has been asked to evaluate the options for the location of a new data center within a multifloor building. Concerns for the data center include emanations and physical access controls.

Which of the following is the BEST location?

- A. On the top floor
- B. In the basement
- C. In the core of the building
- D. In an exterior room with windows

**Answer:** C

#### NEW QUESTION 278

- (Exam Topic 11)

Which of the following is a function of Security Assertion Markup Language (SAML)?

- A. File allocation
- B. Redundancy check
- C. Extended validation
- D. Policy enforcement

**Answer:** D

#### NEW QUESTION 283

- (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 287

- (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 289

- (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 292

- (Exam Topic 11)

How can lessons learned from business continuity training and actual recovery incidents BEST be used?

- A. As a means for improvement
- B. As alternative options for awareness and training
- C. As indicators of a need for policy
- D. As business function gap indicators

Answer: A

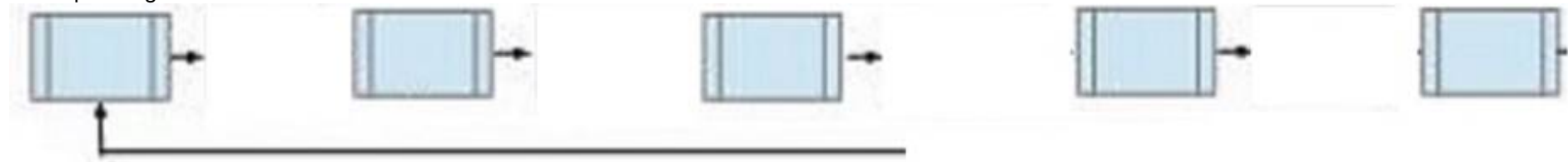
#### NEW QUESTION 297

- (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 300

- (Exam Topic 11)

Regarding asset security and appropriate retention, which of the following INITIAL top three areas are important to focus on?

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

Answer: A

#### NEW QUESTION 302

- (Exam Topic 11)

Which of the following types of security testing is the MOST effective in providing a better indication of the everyday security challenges of an organization when performing a security risk assessment?

- A. External
- B. Overt
- C. Internal
- D. Covert

Answer: D



**NEW QUESTION 306**

- (Exam Topic 11)

Which of the following analyses is performed to protect information assets?

- A. Business impact analysis
- B. Feasibility analysis
- C. Cost benefit analysis
- D. Data analysis

**Answer:** A

**NEW QUESTION 310**

- (Exam Topic 11)

Single Sign-On (SSO) is PRIMARILY designed to address which of the following?

- A. Confidentiality and Integrity
- B. Availability and Accountability
- C. Integrity and Availability
- D. Accountability and Assurance

**Answer:** D

**NEW QUESTION 312**

- (Exam Topic 11)

An organization lacks a data retention policy. Of the following, who is the BEST person to consult for such requirement?

- A. Application Manager
- B. Database Administrator
- C. Privacy Officer
- D. Finance Manager

**Answer:** C

**NEW QUESTION 315**

- (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 317**

- (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 318**

- (Exam Topic 11)

Which of the following explains why record destruction requirements are included in a data retention policy?

- A. To comply with legal and business requirements
- B. To save cost for storage and backup
- C. To meet destruction guidelines
- D. To validate data ownership

**Answer:** A

**NEW QUESTION 319**

- (Exam Topic 11)

Which of the following is the PRIMARY concern when using an Internet browser to access a cloud-based service?

- A. Insecure implementation of Application Programming Interfaces (API)
- B. Improper use and storage of management keys
- C. Misconfiguration of infrastructure allowing for unauthorized access
- D. Vulnerabilities within protocols that can expose confidential data

**Answer:** D



**NEW QUESTION 322**

- (Exam Topic 11)

What type of encryption is used to protect sensitive data in transit over a network?

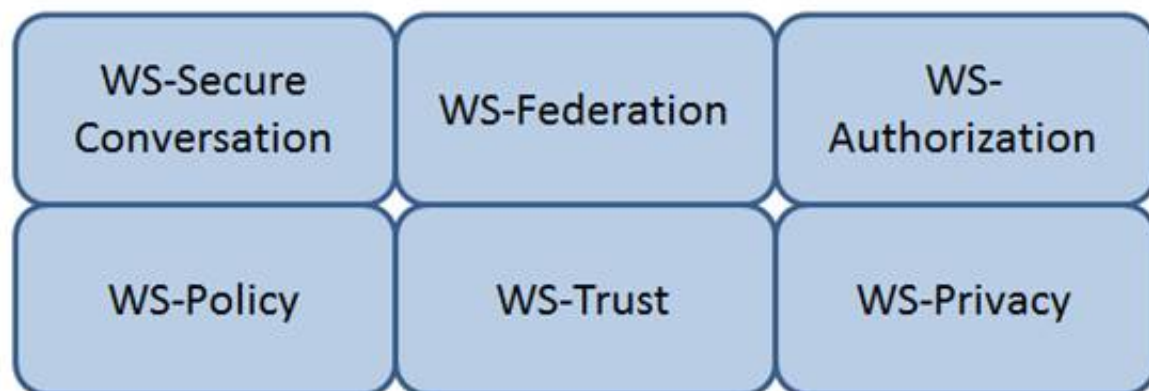
- A. Payload encryption and transport encryption
- B. Authentication Headers (AH)
- C. Keyed-Hashing for Message Authentication
- D. Point-to-Point Encryption (P2PE)

**Answer:** A

**NEW QUESTION 325**

- (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 328**

- (Exam Topic 11)

Which of the following statements is TRUE regarding value boundary 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 threshold of the given functional specifications.
- D. An entire partition can be covered by considering only one representative value from that partition.

**Answer:** C

**NEW QUESTION 331**

- (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 333**

- (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

|   |
|---|
| 1 |
| 2 |
| 3 |
| 4 |

### Method

|  |             |
|--|-------------|
|  | Overwriting |
|  | Degaussing  |
|  | Destruction |
|  | Deleting    |

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

### Sequence

|   |
|---|
| 1 |
| 2 |
| 3 |
| 4 |

### Method

|   |             |
|---|-------------|
| 3 | Overwriting |
| 2 | Degaussing  |
| 1 | Destruction |
| 4 | Deleting    |

#### NEW QUESTION 334

- (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 338

- (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 341

- (Exam Topic 11)

For an organization considering two-factor authentication for secure network access, which of the following is MOST secure?

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

Answer: D

#### NEW QUESTION 345

- (Exam Topic 11)

What is the GREATEST challenge of an agent-based patch management solution?

- A. Time to gather vulnerability information about the computers in the program  
B. Requires that software be installed, running, and managed on all participating computers  
C. The significant amount of network bandwidth while scanning computers  
D. The consistency of distributing patches to each participating computer

Answer: B

#### NEW QUESTION 349

- (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 354**

- (Exam Topic 11)

Which of the following protocols would allow an organization to maintain a centralized list of users that can read a protected webpage?

- A. Lightweight Directory Access Control (LDAP)
- B. Security Assertion Markup Language (SAML)
- C. Hypertext Transfer Protocol (HTTP)
- D. Kerberos

**Answer:** A

**NEW QUESTION 358**

- (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?

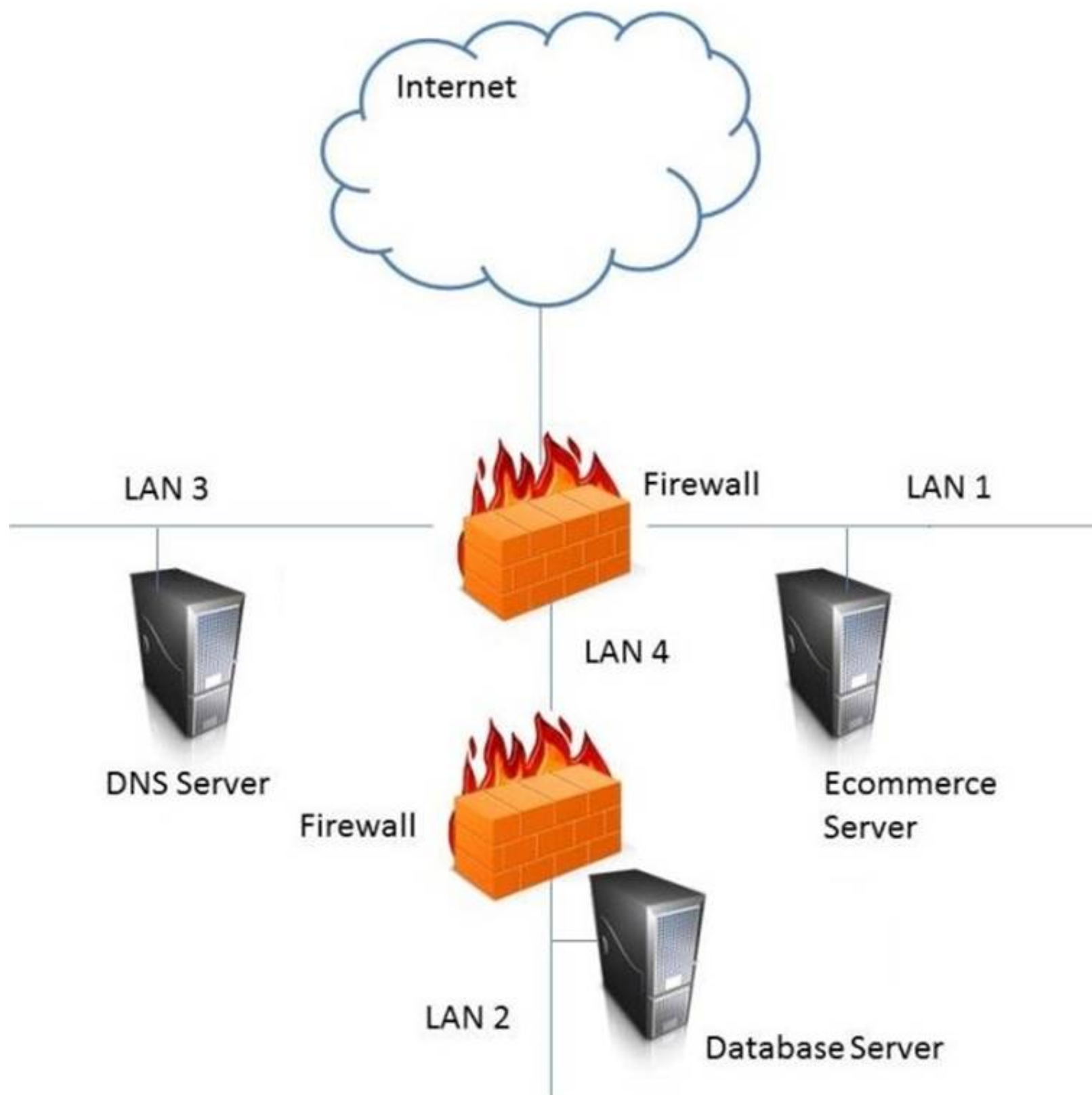
- A. Retention
- B. Reporting
- C. Recovery
- D. Remediation

**Answer:** A

**NEW QUESTION 360**

- (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 365

- (Exam Topic 11)

Which of the following provides the minimum set of privileges required to perform a job function and restricts the user to a domain with the required privileges?

- A. Access based on rules
- B. Access based on user's role
- C. Access determined by the system
- D. Access based on data sensitivity

**Answer:** B

#### NEW QUESTION 370

- (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:

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

#### NEW QUESTION 372

- (Exam Topic 12)

As a best practice, the Security Assessment Report (SAR) should include which of the following sections?

- A. Data classification policy
- B. Software and hardware inventory
- C. Remediation recommendations
- D. Names of participants

Answer: B

#### NEW QUESTION 373

- (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 374

- (Exam Topic 12)

Which of the following is a remote access protocol that uses a static authentication?

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

Answer: C

#### NEW QUESTION 378

- (Exam Topic 12)

Which of the following information MUST be provided for user account provisioning?

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

Answer: B

**NEW QUESTION 383**

- (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 387**

- (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 388**

- (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 389**

- (Exam Topic 12)

Which of the following adds end-to-end security inside a Layer 2 Tunneling Protocol (L2TP) Internet Protocol Security (IPSec) connection?

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

**Answer:** B

**NEW QUESTION 391**

- (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 393**

- (Exam Topic 12)

Which of the following is the MAIN reason for using configuration management?

- A. To provide centralized administration
- B. To reduce the number of changes
- C. To reduce errors during upgrades
- D. To provide consistency in security controls

**Answer:** D

**NEW QUESTION 394**

- (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.



| <u>E-Authentication Token</u>  |  | <u>Description</u>  |
|--------------------------------|--|---|
| 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 397**

- (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 399**

- (Exam Topic 12)

During which of the following processes is least privilege implemented for a user account?

- A. Provision
- B. Approve
- C. Request
- D. Review

**Answer:** A

**NEW QUESTION 404**

- (Exam Topic 12)

Between which pair of Open System Interconnection (OSI) Reference Model layers are routers used as a communications device?

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

**Answer:** B

**NEW QUESTION 409**

- (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 412**

- (Exam Topic 12)

Although code using a specific program language may not be susceptible to a buffer overflow attack,

- A. most calls to plug-in programs are susceptible.
- B. most supporting application code is susceptible.
- C. the graphical images used by the application could be susceptible.
- D. the supporting virtual machine could be susceptible.

**Answer:** C

**NEW QUESTION 417**

- (Exam Topic 12)

What is the BEST way to encrypt web application communications?

- A. Secure Hash Algorithm 1 (SHA-1)
- B. Secure Sockets Layer (SSL)
- C. Cipher Block Chaining Message Authentication Code (CBC-MAC)
- D. Transport Layer Security (TLS)

**Answer:** D

**NEW QUESTION 419**

- (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 420**

- (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 422**

- (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 423**

- (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 424**

- (Exam Topic 12)

Which of the following is BEST suited for exchanging authentication and authorization messages in a multi-party decentralized environment?

- A. Lightweight Directory Access Protocol (LDAP)

- B. Security Assertion Markup Language (SAML)
- C. Internet Mail Access Protocol
- D. Transport Layer Security (TLS)

**Answer:** B

#### NEW QUESTION 426

- (Exam Topic 12)

A security architect plans to reference a Mandatory Access Control (MAC) model for implementation. This indicates that which of the following properties are being prioritized?

- A. Confidentiality
- B. Integrity
- C. Availability
- D. Accessibility

**Answer:** C

#### NEW QUESTION 431

- (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 432

- (Exam Topic 12)

The application of a security patch to a product previously validate at Common Criteria (CC) Evaluation Assurance Level (EAL) 4 would

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

**Answer:** B

#### NEW QUESTION 433

- (Exam Topic 12)

When evaluating third-party applications, which of the following is the GREATEST responsibility of Information Security?

- A. Accept the risk on behalf of the organization.
- B. Report findings to the business to determine security gaps.
- C. Quantify the risk to the business for product selection.
- D. Approve the application that best meets security requirements.

**Answer:** C

#### NEW QUESTION 436

- (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 441

- (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 445

- (Exam Topic 12)

Which of the following is the PRIMARY reason to perform regular vulnerability scanning of an organization network?

- A. Provide vulnerability reports to management.
- B. Validate vulnerability remediation activities.
- C. Prevent attackers from discovering vulnerabilities.
- D. Remediate known vulnerabilities.

**Answer:** B

#### NEW QUESTION 448

- (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 453

- (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 455

- (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 458

- (Exam Topic 13)

Which of the following steps should be performed FIRST when purchasing Commercial Off-The-Shelf (COTS) software?

- A. undergo a security assessment as part of authorization process
- B. establish a risk management strategy
- C. harden the hosting server, and perform hosting and application vulnerability scans
- D. establish policies and procedures on system and services acquisition

**Answer:** D

#### NEW QUESTION 463

- (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 468

- (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 470**

- (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 472**

- (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 475**

- (Exam Topic 13)

Which of the following mechanisms will BEST prevent a Cross-Site Request Forgery (CSRF) attack?

- A. parameterized database queries
- B. whitelist input values
- C. synchronized session tokens
- D. use strong ciphers

**Answer:** C

**NEW QUESTION 478**

- (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 483**

- (Exam Topic 13)

When determining who can accept the risk associated with a vulnerability, which of the following is MOST important?

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

**Answer:** C

**NEW QUESTION 484**

- (Exam Topic 13)

Which of the following is the BEST reason for the use of security metrics?

- A. They ensure that the organization meets its security objectives.
- B. They provide an appropriate framework for Information Technology (IT) governance.
- C. They speed up the process of quantitative risk assessment.
- D. They quantify the effectiveness of security processes.

**Answer:**



B

**NEW QUESTION 486**

- (Exam Topic 13)

A security practitioner is tasked with securing the organization's Wireless Access Points (WAP). Which of these is the MOST effective way of restricting this environment to authorized users?

- A. Enable Wi-Fi Protected Access 2 (WPA2) encryption on the wireless access point
- B. Disable the broadcast of the Service Set Identifier (SSID) name
- C. Change the name of the Service Set Identifier (SSID) to a random value not associated with the organization
- D. Create Access Control Lists (ACL) based on Media Access Control (MAC) addresses

**Answer:** D

**NEW QUESTION 488**

- (Exam Topic 13)

What is the MAIN purpose of a change management policy?

- A. To assure management that changes to the Information Technology (IT) infrastructure are necessary
- B. To identify the changes that may be made to the Information Technology (IT) infrastructure
- C. To verify that changes to the Information Technology (IT) infrastructure are approved
- D. To determine the necessary for implementing modifications to the Information Technology (IT) infrastructure

**Answer:** C

**Explanation:**

Section: Security Operations

**NEW QUESTION 489**

- (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 494**

- (Exam Topic 13)

Mandatory Access Controls (MAC) are based on:

- A. security classification and security clearance
- B. data segmentation and data classification
- C. data labels and user access permissions
- D. user roles and data encryption

**Answer:** A

**NEW QUESTION 495**

- (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 500**

- (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 503**

- (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 507**

- (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 512**

- (Exam Topic 13)

Which of the following is MOST appropriate for protecting confidentiality of data stored on a hard drive?

- A. Triple Data Encryption Standard (3DES)
- B. Advanced Encryption Standard (AES)
- C. Message Digest 5 (MD5)
- D. Secure Hash Algorithm 2(SHA-2)

**Answer:** B

**NEW QUESTION 514**

- (Exam Topic 13)

Which of the following would MINIMIZE the ability of an attacker to exploit a buffer overflow?

- A. Memory review
- B. Code review
- C. Message division
- D. Buffer division

**Answer:** B

**NEW QUESTION 519**

- (Exam Topic 13)

A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report. In which phase of the assessment was this error MOST likely made?

- A. Enumeration
- B. Reporting
- C. Detection
- D. Discovery

**Answer:** A

**Explanation:**

Section: Security Assessment and Testing

**NEW QUESTION 523**

- (Exam Topic 13)

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

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

**Answer:** B

**Explanation:**

Section: Security Assessment and Testing

**NEW QUESTION 528**

- (Exam Topic 13)

Which of the following mandates the amount and complexity of security controls applied to a security risk?

- A. Security vulnerabilities
- B. Risk tolerance
- C. Risk mitigation
- D. Security staff

**Answer:** C

**NEW QUESTION 529**

- (Exam Topic 13)

Who is accountable for the information within an Information System (IS)?

- A. Security manager
- B. System owner
- C. Data owner
- D. Data processor

**Answer:** B

**Explanation:**

Section: Security Operations

**NEW QUESTION 534**

- (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 536**

- (Exam Topic 13)

Digital certificates used in Transport Layer Security (TLS) support which of the following?

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

**Answer:** D

**NEW QUESTION 537**

- (Exam Topic 13)

A chemical plant 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 541**

- (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 543**

- (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 548**

- (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 553**

- (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 557**

- (Exam Topic 13)

As part of an application penetration testing process, session hijacking can BEST be achieved by which of the following?

- A. Known-plaintext attack
- B. Denial of Service (DoS)
- C. Cookie manipulation
- D. Structured Query Language (SQL) injection

**Answer:** D

**Explanation:**

Section: Security Assessment and Testing

**NEW QUESTION 559**

- (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 560**

- (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 562**

- (Exam Topic 13)

Which of the following is BEST achieved through the use of eXtensible Access Markup Language (XACML)?

- A. Minimize malicious attacks from third parties
- B. Manage resource privileges
- C. Share digital identities in hybrid cloud
- D. Defined a standard protocol

**Answer:** D

**NEW QUESTION 567**

- (Exam Topic 13)

The security accreditation task of the System Development Life Cycle (SDLC) process is completed at the end of which phase?

- A. System acquisition and development
- B. System operations and maintenance
- C. System initiation
- D. System implementation

**Answer:** B

**NEW QUESTION 571**

.....

## 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>