# Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

**https://www.2passeasy.com/dumps/CISSP/**

**NEW QUESTION 1**
- (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 2**
- (Exam Topic 3)
Who in the organization is accountable for classification of data information assets?

A. Data owner
B. Data architect
C. Chief Information Security Officer (CISO)
D. Chief Information Officer (CIO)

**Answer:** A


**NEW QUESTION 3**
- (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 4**
- (Exam Topic 4)
Which of the following factors contributes to the weakness of Wired Equivalent Privacy (WEP) protocol?

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

**Answer:** A


**NEW QUESTION 5**
- (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 6**
- (Exam Topic 7)
What is the MOST important step during forensic analysis when trying to learn the purpose of an unknown application?

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

**Answer:** D


**NEW QUESTION 7**
- (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 8**
- (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 9**
- (Exam Topic 9)
Which of the following is a method used to prevent Structured Query Language (SQL) injection attacks?

A. Data compression
B. Data classification
C. Data warehousing
D. Data validation

**Answer:** D

**NEW QUESTION 10**
- (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 10**
- (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 13**
- (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 16**
- (Exam Topic 9)
What technique BEST describes antivirus software that detects viruses by watching anomalous behavior?

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

**Answer:** D

**NEW QUESTION 18**
- (Exam Topic 9)

Checking routing information on e-mail to determine it is in a valid format and contains valid information is an example of which of the following anti-spam approaches?

A. Simple Mail Transfer Protocol (SMTP) blacklist
B. Reverse Domain Name System (DNS) lookup
C. Hashing algorithm
D. Header analysis

**Answer:** D


**NEW QUESTION 20**
- (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 22**
- (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 27**
- (Exam Topic 9)
Which of the following is an attacker MOST likely to target to gain privileged access to a system?

A. Programs that write to system resources
B. Programs that write to user directories
C. Log files containing sensitive information
D. Log files containing system calls

**Answer:** A


**NEW QUESTION 32**
- (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 35**
- (Exam Topic 9)
A security professional has just completed their organization's Business Impact Analysis (BIA). Following Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) best practices, what would be the professional's NEXT step?

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

**Answer:** A


**NEW QUESTION 36**
- (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 37**
- (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 39**
- (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 systemscontrols 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 43**
- (Exam Topic 9)
The use of strong authentication, the encryption of Personally Identifiable Information (PII) on database servers, application security reviews, and the encryption of data transmitted across networks provide

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

**Answer:** B


**NEW QUESTION 44**
- (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 46**
- (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 47**
- (Exam Topic 9)
In a data classification scheme, the data is owned by the

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

**Answer:** B


**NEW QUESTION 49**
- (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 52**
- (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 57**
- (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 59**
- (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 62**
- (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 67**
- (Exam Topic 9)
By allowing storage communications to run on top of Transmission Control Protocol/Internet Protocol (TCP/IP) with a Storage Area Network (SAN), the

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

**Answer:** B


**NEW QUESTION 70**
- (Exam Topic 9)
The goal of software assurance in application development is to

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

**Answer:** C


**NEW QUESTION 73**
- (Exam Topic 9)
Why must all users be positively identified prior to using multi-user computers?

A. To provide access to system privileges
B. To provide access to the operating system

C. To ensure that unauthorized persons cannot access the computers
D. To ensure that management knows what users are currently logged on

**Answer:** C

---

**NEW QUESTION 76**
- (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 80**
- (Exam Topic 10)
Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?

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

**Answer:** A

---

**NEW QUESTION 82**
- (Exam Topic 10)
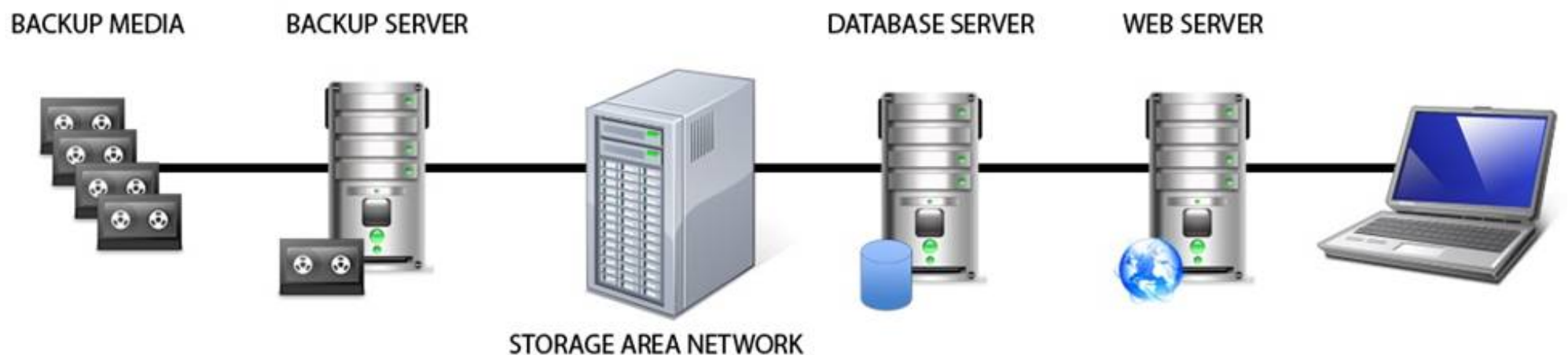What do Capability Maturity Models (CMM) serve as a benchmark for in an organization?

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

**Answer:** D

---

**NEW QUESTION 83**
- (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 86**
- (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 it is discovered that large quantities of information have been copied by the unauthorized individual, what attribute of the data has been compromised?

A. Availability
B. Integrity
C. Accountability

D. Confidentiality

**Answer:** D


**NEW QUESTION 87**
- (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 88**
- (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 90**
- (Exam Topic 10)
What is the MOST effective method for gaining unauthorized access to a file protected with a long complex password?

A. Brute force attack
B. Frequency analysis
C. Social engineering
D. Dictionary attack

**Answer:** C


**NEW QUESTION 92**
- (Exam Topic 10)
Multi-Factor Authentication (MFA) is necessary in many systems given common types of password attacks. Which of the following is a correct list of password attacks?

A. Masquerading, salami, malware, polymorphism
B. Brute force, dictionary, phishing, keylogger
C. Zeus, netbus, rabbit, turtle
D. Token, biometrics, IDS, DLP

**Answer:** B


**NEW QUESTION 93**
- (Exam Topic 10)
Which of the following are required components for implementing software configuration management systems?

A. Audit control and signoff
B. User training and acceptance
C. Rollback and recovery processes
D. Regression testing and evaluation

**Answer:** C


**NEW QUESTION 96**
- (Exam Topic 10)
Which of the following BEST mitigates a replay attack against a system using identity federation and Security Assertion Markup Language (SAML) implementation?

A. Two-factor authentication
B. Digital certificates and hardware tokens
C. Timed sessions and Secure Socket Layer (SSL)
D. Passwords with alpha-numeric and special characters

**Answer:** C


**NEW QUESTION 101**
- (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 102**
- (Exam Topic 10)
Which of the following is a detective access control mechanism?

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

**Answer:** A


**NEW QUESTION 105**
- (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 109**
- (Exam Topic 10)
When is security personnel involvement in the Systems Development Life Cycle (SDLC) process MOST beneficial?

A. Testing phase
B. Development phase
C. Requirements definition phase
D. Operations and maintenance phase

**Answer:** C


**NEW QUESTION 110**
- (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** | | | **Table B** | |
|---|---|---|---|---|---|
| User | Clearance Level | | Files | Security Class | |
| A | Restricted | | 1 | Restricted | |
| B | Confidential | | 2 | Confidential | |
| C | Secret | | 3 | Secret | |
| D | Top Secret | | 4 | Top Secret | |

In a Bell-LaPadula system, which user cannot write to File 3?

A. User A
B. User B
C. User C
D. User D

**Answer:** D


**NEW QUESTION 113**
- (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.
Which of the following is considered the MOST important priority for the information security officer?

A. Formal acceptance of the security strategy
B. Disciplinary actions taken against unethical behavior
C. Development of an awareness program for new employees

D. Audit of all organization system configurations for faults

**Answer:** A

**NEW QUESTION 115**
- (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 120**
- (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 124**
- (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 127**
- (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 | | | Table B | |
| --- | --- | --- | --- | --- |
| **User** | **Clearance Level** | | **Files** | **Security Class** |
| A | Restricted | | 1 | Restricted |
| B | Confidential | | 2 | Confidential |
| C | Secret | | 3 | Secret |
| D | Top Secret | | 4 | Top Secret |

In a Bell-LaPadula system, which user has the MOST restrictions when writing data to any of the four files?

A. User A
B. User B
C. User C
D. User D

**Answer:** D

**NEW QUESTION 129**
- (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 132**
- (Exam Topic 10)
An organization decides to implement a partial Public Key Infrastructure (PKI) with only the servers having digital certificates. What is the security benefit of this implementation?

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

**Answer:** D


**NEW QUESTION 135**
- (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 140**
- (Exam Topic 10)
Which of the following is critical for establishing an initial baseline for software components in the operation and maintenance of applications?

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

**Answer:** B


**NEW QUESTION 142**
- (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 144**
- (Exam Topic 11)
A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

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

**Answer:** A


**NEW QUESTION 148**
- (Exam Topic 11)
What is the MOST effective method of testing custom application code?

A. Negative testing
B. White box testing
C. Penetration testing
D. Black box testing

**Answer:** B


**NEW QUESTION 149**
- (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 150**
- (Exam Topic 11)
Which of the following BEST describes a Protection Profile (PP)?

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

**Answer:** A

**NEW QUESTION 151**
- (Exam Topic 11)
Changes to a Trusted Computing Base (TCB) system that could impact the security posture of that system and trigger a recertification activity are documented in the

A. security impact analysis.
B. structured code review.
C. routine self assessment.
D. cost benefit analysis.

**Answer:** A

**NEW QUESTION 154**
- (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 157**
- (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 159**
- (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 161**
- (Exam Topic 11)
Which of the following is the BEST method to assess the effectiveness of an organization's vulnerability management program?

A. Review automated patch deployment reports
B. Periodic third party vulnerability assessment
C. Automated vulnerability scanning
D. Perform vulnerability scan by security team

**Answer:** B

**NEW QUESTION 165**
- (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 168**
- (Exam Topic 11)
Which of the following is the MOST likely cause of a non-malicious data breach when the source of the data breach was an un-marked file cabinet containing sensitive documents?

A. Ineffective data classification
B. Lack of data access controls
C. Ineffective identity management controls
D. Lack of Data Loss Prevention (DLP) tools

**Answer:** A


**NEW QUESTION 173**
- (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 175**
- (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 178**
- (Exam Topic 11)
Which of the following standards/guidelines requires an Information Security Management System (ISMS) to be defined?

A. International Organization for Standardization (ISO) 27000 family
B. Information Technology Infrastructure Library (ITIL)
C. Payment Card Industry Data Security Standard (PCIDSS)
D. ISO/IEC 20000

**Answer:** A


**NEW QUESTION 181**
- (Exam Topic 11)
During a fingerprint verification process, which of the following is used to verify identity and authentication?

A. A pressure value is compared with a stored template
B. Sets of digits are matched with stored values
C. A hash table is matched to a database of stored value
D. A template of minutiae is compared with a stored template

**Answer:** D


**NEW QUESTION 182**
- (Exam Topic 11)
How does Encapsulating Security Payload (ESP) in transport mode affect the Internet Protocol (IP)?

A. Encrypts and optionally authenticates the IP header, but not the IP payload
B. Encrypts and optionally authenticates the IP payload, but not the IP header
C. Authenticates the IP payload and selected portions of the IP header
D. Encrypts and optionally authenticates the complete IP packet

**Answer:** B


**NEW QUESTION 187**
- (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 192**
- (Exam Topic 11)
Which of the following BEST describes a rogue Access Point (AP)?

A. An AP that is not protected by a firewall
B. An AP not configured to use Wired Equivalent Privacy (WEP) with Triple Data Encryption Algorithm (3DES)
C. An AP connected to the wired infrastructure but not under the management of authorized network administrators
D. An AP infected by any kind of Trojan or Malware

**Answer:** C

**NEW QUESTION 195**
- (Exam Topic 11)
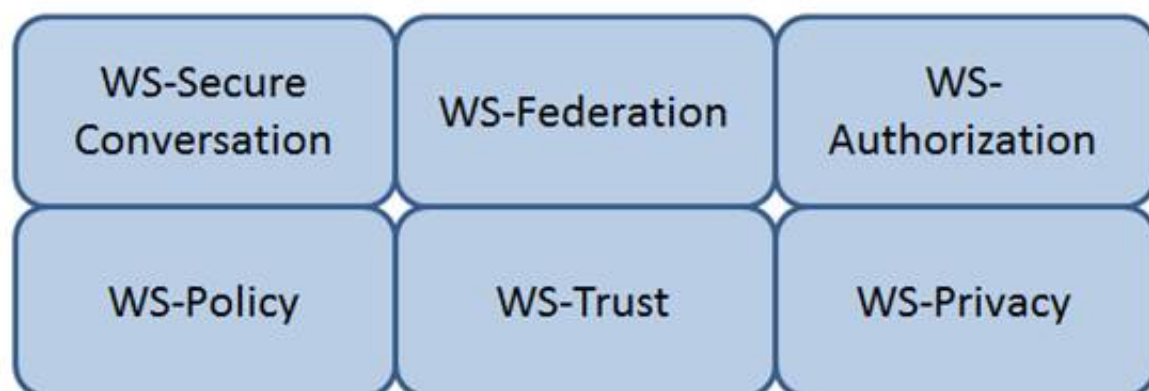Retaining system logs for six months or longer can be valuable for what activities?

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 197**
- (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 199**
- (Exam Topic 11)
Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).

| | |
|---|---|
| Secure Architecture | [ ] |
| Education & Guidance | [ ] |
| Strategy & Metrics | [ ] |
| Vulnerability Management | [ ] |

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

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

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

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 204**
- (Exam Topic 11)
Which methodology is recommended for penetration testing to be effective in the development phase of the life-cycle process?

A. White-box testing
B. Software fuzz testing
C. Black-box testing
D. Visual testing

**Answer:** A

**NEW QUESTION 209**
- (Exam Topic 11)
The PRIMARY characteristic of a Distributed Denial of Service (DDoS) attack is that it

A. exploits weak authentication to penetrate networks.
B. can be detected with signature analysis.
C. looks like normal network activity.
D. is commonly confused with viruses or worms.

**Answer:** C

**NEW QUESTION 213**
- (Exam Topic 11)
Which of the following controls is the FIRST step in protecting privacy in an information system?

A. Data Redaction
B. Data Minimization
C. Data Encryption
D. Data Storage

**Answer:** B

**NEW QUESTION 214**
- (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 216**
- (Exam Topic 11)
Which one of the following is a common risk with network configuration management?

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

**Answer:** D


**NEW QUESTION 221**
- (Exam Topic 11)
The goal of a Business Continuity Plan (BCP) training and awareness program is to

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

**Answer:** A


**NEW QUESTION 224**
- (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 226**
- (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 229**
- (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 233**
- (Exam Topic 11)
While inventorying storage equipment, it is found that there are unlabeled, disconnected, and powered off devices. Which of the following is the correct procedure for handling such equipment?

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

**Answer:** C


**NEW QUESTION 235**
- (Exam Topic 11)

Which of the following is the MOST important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?

A. Application interface entry and endpoints
B. The likelihood and impact of a vulnerability
C. Countermeasures and mitigations for vulnerabilities
D. A data flow diagram for the application and attack surface analysis

**Answer:** D


**NEW QUESTION 238**
- (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 240**
- (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?
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?

A. Document the system as high risk
B. Perform a vulnerability assessment
C. Perform a quantitative threat assessment
D. Notate the information and move on

**Answer:** B


**NEW QUESTION 243**
- (Exam Topic 11)
In order for a security policy to be effective within an organization, it MUST include

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

**Answer:** D


**NEW QUESTION 246**
- (Exam Topic 11)
By carefully aligning the pins in the lock, which of the following defines the opening of a mechanical lock without the proper key?

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

**Answer:** B


**NEW QUESTION 251**
- (Exam Topic 11)
The MAIN reason an organization conducts a security authorization process is to

A. force the organization to make conscious risk decisions.
B. assure the effectiveness of security controls.
C. assure the correct security organization exists.
D. force the organization to enlist management support.

**Answer:** A


**NEW QUESTION 253**
- (Exam Topic 11)
A global organization wants to implement hardware tokens as part of a multifactor authentication solution for remote access. The PRIMARY advantage of this implementation is

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

**Answer:** C


**NEW QUESTION 254**
- (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 258**
- (Exam Topic 12)
A proxy firewall operates at what layer of the Open System Interconnection (OSI) model?

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

**Answer:** D


**NEW QUESTION 259**
- (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 263**
- (Exam Topic 12)
A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

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

**Answer:** A

**NEW QUESTION 267**
- (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 268**
- (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 273**
- (Exam Topic 12)
Which of the following is an advantage of on-premise Credential Management Systems?

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

**Answer:** B


**NEW QUESTION 275**
- (Exam Topic 12)
Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

A. dig
B. ipconfig
C. ifconfig
D. nbstat

**Answer:** A


**NEW QUESTION 280**
- (Exam Topic 12)
A company was ranked as high in the following National Institute of Standards and Technology (NIST) functions: Protect, Detect, Respond and Recover. However, a low maturity grade was attributed to the Identify function. In which of the following the controls categories does this company need to improve when analyzing its processes individually?

A. Asset Management, Business Environment, Governance and Risk Assessment
B. Access Control, Awareness and Training, Data Security and Maintenance
C. Anomalies and Events, Security Continuous Monitoring and Detection Processes
D. Recovery Planning, Improvements and Communications

**Answer:** A


**NEW QUESTION 282**
- (Exam Topic 12)
At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

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

**Answer:** C


**NEW QUESTION 286**
- (Exam Topic 12)
Which of the following approaches is the MOST effective way to dispose of data on multiple hard drives?

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

**Answer:** D

**NEW QUESTION 291**
- (Exam Topic 12)
In order to assure authenticity, which of the following are required?

A. Confidentiality and authentication
B. Confidentiality and integrity
C. Authentication and non-repudiation
D. Integrity and non-repudiation

**Answer:** D

**NEW QUESTION 296**
- (Exam Topic 12)
In configuration management, what baseline configuration information MUST be maintained for each computer system?

A. Operating system and version, patch level, applications running, and versions.
B. List of system changes, test reports, and change approvals
C. Last vulnerability assessment report and initial risk assessment report
D. Date of last update, test report, and accreditation certificate

**Answer:** A

**NEW QUESTION 300**
- (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 305**
- (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 309**
- (Exam Topic 12)
For network based evidence, which of the following contains traffic details of all network sessions in order to detect anomalies?

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

**Answer:** D

**NEW QUESTION 311**
- (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 315**
- (Exam Topic 12)
What is the MOST important element when considering the effectiveness of a training program for Business Continuity (BC) and Disaster Recovery (DR)?

A. Management support
B. Consideration of organizational need

C. Technology used for delivery
D. Target audience

**Answer:** B


**NEW QUESTION 317**
- (Exam Topic 13)
Which one of the following data integrity models assumes a lattice of integrity levels?

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

**Answer:** B


**NEW QUESTION 322**
- (Exam Topic 13)
Which of the following is the MOST effective practice in managing user accounts when an employee is terminated?

A. Implement processes for automated removal of access for terminated employees.
B. Delete employee network and system IDs upon termination.
C. Manually remove terminated employee user-access to all systems and applications.
D. Disable terminated employee network ID to remove all access.

**Answer:** B


**NEW QUESTION 326**
- (Exam Topic 13)
A control to protect from a Denial-of-Service (DoS) attach 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 329**
- (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 331**
- (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 335**
- (Exam Topic 13)
Which of the following MUST be in place to recognize a system attack?

A. Stateful firewall
B. Distributed antivirus
C. Log analysis
D. Passive honeypot

**Answer:** A

**NEW QUESTION 336**
- (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 338**
- (Exam Topic 13)
What is the PRIMARY role of a scrum master in agile development?

A. To choose the primary development language
B. To choose the integrated development environment
C. To match the software requirements to the delivery plan
D. To project manage the software delivery

**Answer:** D

**NEW QUESTION 341**
- (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 342**
- (Exam Topic 13)
Drag the following Security Engineering terms on the left to the BEST definition on the right.



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Risk - A measure of the extent to which an entity is threatened by a potential circumstance of event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.
Protection Needs Assessment - The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to

characterize the adverse impact or consequences should be asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Threat assessment - The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Security Risk Treatment - The method used to identify feasible security risk mitigation options and plans.

**NEW QUESTION 346**
- (Exam Topic 13)
It is MOST important to perform which of the following to minimize potential impact when implementing a new vulnerability scanning tool in a production environment?

A. Negotiate schedule with the Information Technology (IT) operation's team
B. Log vulnerability summary reports to a secured server
C. Enable scanning during off-peak hours
D. Establish access for Information Technology (IT) management

**Answer:** A

**Explanation:**
Section: Security Operations

**NEW QUESTION 347**
- (Exam Topic 13)
Which factors MUST be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?

A. System owner roles and responsibilities, data handling standards, storage and secure development lifecycle requirements
B. Data stewardship roles, data handling and storage standards, data lifecycle requirements
C. Compliance office roles and responsibilities, classified material handling standards, storage system lifecycle requirements
D. System authorization roles and responsibilities, cloud computing standards, lifecycle requirements

**Answer:** A

**NEW QUESTION 348**
- (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 353**
- (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 357**
- (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 360**
- (Exam Topic 13)
What is the MOST significant benefit of an application upgrade that replaces randomly generated session keys with certificate based encryption for communications with backend servers?

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

**Answer:** A

**NEW QUESTION 364**
- (Exam Topic 13)
What does electronic vaulting accomplish?

A. It protects critical files.
B. It ensures the fault tolerance of Redundant Array of Independent Disks (RAID) systems
C. It stripes all database records
D. It automates the Disaster Recovery Process (DRP)

**Answer:** A

**Explanation:**
Section: Security Operations

**NEW QUESTION 369**
- (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:



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**



**NEW QUESTION 373**
- (Exam Topic 13)
Which of the following would an attacker BEST be able to accomplish through the use of Remote Access
Tools (RAT)?

A. Reduce the probability of identification
B. Detect further compromise of the target
C. Destabilize the operation of the host
D. Maintain and expand control

**Answer:** D

**NEW QUESTION 377**
- (Exam Topic 13)
What is the PRIMARY goal of fault tolerance?

A. Elimination of single point of failure

B. Isolation using a sandbox
C. Single point of repair
D. Containment to prevent propagation

**Answer:** A


## NEW QUESTION 380
- (Exam Topic 13)
Within the company, desktop clients receive Internet Protocol (IP) address over Dynamic Host Configuration Protocol (DHCP).
Which of the following represents a valid measure to help protect the network against unauthorized access?

A. Implement path management
B. Implement port based security through 802.1x
C. Implement DHCP to assign IP address to server systems
D. Implement change management

**Answer:** B


## NEW QUESTION 381
- (Exam Topic 13)
Which of the following is MOST appropriate for protecting confidentially 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 385
- (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 387
- (Exam Topic 13)
Which of the following entails identification of data and links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

A. Security governance
B. Risk management
C. Security portfolio management
D. Risk assessment

**Answer:** B


## NEW QUESTION 392
- (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 395
- (Exam Topic 13)
When developing a business case for updating a security program, the security program owner MUST do
which of the following?

A. Identify relevant metrics
B. Prepare performance test reports
C. Obtain resources for the security program
D. Interview executive management

**Answer:** A


## NEW QUESTION 397

- (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 400
- (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 404
- (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 409
- (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 410
- (Exam Topic 13)
An organization has discovered that users are visiting unauthorized websites using anonymous proxies. Which of the following is the BEST way to prevent future occurrences?

A. Remove the anonymity from the proxy
B. Analyze Internet Protocol (IP) traffic for proxy requests
C. Disable the proxy server on the firewall
D. Block the Internet Protocol (IP) address of known anonymous proxies

**Answer:** C

## NEW QUESTION 412
- (Exam Topic 13)
Which of the BEST internationally recognized standard for evaluating security products and systems?

A. Payment Card Industry Data Security Standards (PCI-DSS)
B. Common Criteria (CC)
C. Health Insurance Portability and Accountability Act (HIPAA)
D. Sarbanes-Oxley (SOX)

**Answer:** B

## NEW QUESTION 417
- (Exam Topic 13)
In a High Availability (HA) environment, what is the PRIMARY goal of working with a virtual router address as the gateway to a network?

A. The second of two routers can periodically check in to make sure that the first router is operational.
B. The second of two routers can better absorb a Denial of Service (DoS) attack knowing the first router is present.
C. The first of two routers fails and is reinstalled, while the second handles the traffic flawlessly.
D. The first of two routers can better handle specific traffic, while the second handles the rest of the traffic seamlessly.

**Answer:** C


**NEW QUESTION 420**
- (Exam Topic 13)
Attack trees are MOST useful for which of the following?

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

**Answer:** A


**NEW QUESTION 422**
- (Exam Topic 13)
Which of the following management process allows ONLY those services required for users to accomplish
their tasks, change default user passwords, and set servers to retrieve antivirus updates?

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

**Answer:** A


**NEW QUESTION 424**
- (Exam Topic 13)
Which one of the following considerations has the LEAST impact when considering transmission security?

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

**Answer:** C


**NEW QUESTION 426**
- (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 429**
- (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 430**
......

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CISSP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CISSP Product From:

## https://www.2passeasy.com/dumps/CISSP/

# Money Back Guarantee

## 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