

## Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

<https://www.2passeasy.com/dumps/CISSP/>



#### NEW QUESTION 1

- (Exam Topic 15)

An organization plans to acquire @ commercial off-the-shelf (COTS) system to replace their aging home-built reporting system. When should the organization's security team FIRST get involved in this acquisition's life cycle?

- A. When the system is being designed, purchased, programmed, developed, or otherwise constructed
- B. When the system is verified and validated
- C. When the system is deployed into production
- D. When the need for a system is expressed and the purpose of the system is documented

**Answer: D**

#### NEW QUESTION 2

- (Exam Topic 15)

An organization is planning a penetration test that simulates the malicious actions of a former network administrator. What kind of penetration test is needed?

- A. Functional test
- B. Unit test
- C. Grey box
- D. White box

**Answer: C**

#### NEW QUESTION 3

- (Exam Topic 15)

Which of the following is the top barrier for companies to adopt cloud technology?

- A. Migration period
- B. Data integrity
- C. Cost
- D. Security

**Answer: D**

#### NEW QUESTION 4

- (Exam Topic 15)

Wi-Fi Protected Access 2 (WPA2) provides users with a higher level of assurance that their data will remain protected by using which protocol?

- A. Secure Shell (SSH)
- B. Internet Protocol Security (IPsec)
- C. Secure Sockets Layer (SSL)
- D. Extensible Authentication Protocol (EAP)

**Answer: A**

#### NEW QUESTION 5

- (Exam Topic 15)

Which of the following is the MOST effective way to ensure the endpoint devices used by remote users are compliant with an organization's approved policies before being allowed on the network?

- A. Group Policy Object (GPO)
- B. Network Access Control (NAC)
- C. Mobile Device Management (MDM)
- D. Privileged Access Management (PAM)

**Answer: B**

#### NEW QUESTION 6

- (Exam Topic 15)

Two computers, each with a single connection on the same physical 10 gigabit Ethernet network segment, need to communicate with each other. The first machine has a single Internet Protocol (IP) Classless Inter-Domain Routing (CIDR) address of 192.168.1.3/30 and the second machine has an IP/CIDR address 192.168.1.6/30. Which of the following is correct?

- A. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network bridge in order to communicate.
- B. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network bridge in order to communicate.
- C. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network router in order to communicate.
- D. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network router in order to communicate.

**Answer: B**

#### NEW QUESTION 7

- (Exam Topic 15)

A database server for a financial application is scheduled for production deployment. Which of the following controls will BEST prevent tampering?

- A. Service accounts removal

- B. Data validation
- C. Logging and monitoring
- D. Data sanitization

**Answer:** B

#### NEW QUESTION 8

- (Exam Topic 15)

Which of the following is the BEST method a security practitioner can use to ensure that systems and sub-systems gracefully handle invalid input?

- A. Unit testing
- B. Integration testing
- C. Negative testing
- D. Acceptance testing

**Answer:** B

#### NEW QUESTION 9

- (Exam Topic 15)

Which of the following access control models is MOST restrictive?

- A. Discretionary Access Control (DAC)
- B. Mandatory Access Control (MAC)
- C. Role Based Access Control (RBAC)
- D. Rule based access control

**Answer:** B

#### NEW QUESTION 10

- (Exam Topic 15)

Which of the following is a PRIMARY security weakness in the design of Domain Name System (DNS)?

- A. A DNS server can be disabled in a denial-of-service (DoS) attack.
- B. A DNS server does not authenticate source of information.
- C. Each DNS server must hold the address of the root servers.
- D. A DNS server database can be injected with falsified checksums.

**Answer:** A

#### NEW QUESTION 10

- (Exam Topic 15)

A breach investigation ..... a website was exploited through an open sourced .....Is The FIRB Stan In the Process that could have prevented this breach?

- A. Application whitelisting
- B. Web application firewall (WAF)
- C. Vulnerability remediation
- D. Software inventory

**Answer:** B

#### NEW QUESTION 14

- (Exam Topic 15)

A cybersecurity engineer has been tasked to research and implement an ultra-secure communications channel to protect the organization's most valuable intellectual property (IP). The primary directive in this initiative is to ensure there is no possible way the communications can be intercepted without detection. Which of the following is the only way to ensure this 'outcome'?

- A. Diffie-Hellman key exchange
- B. Symmetric key cryptography
- C. [Public key infrastructure (PKI)
- D. Quantum Key Distribution

**Answer:** C

#### NEW QUESTION 18

- (Exam Topic 15)

Which of the following is the BEST method a security practitioner can use to ensure that systems and sub-system gracefully handle invalid input?

- A. Negative testing
- B. Integration testing
- C. Unit testing
- D. Acceptance testing

**Answer:** B

#### NEW QUESTION 21

- (Exam Topic 15)

When reviewing vendor certifications for handling and processing of company data, which of the following is the BEST Service Organization Controls (SOC) certification for the vendor to possess?

- A. SOC 1 Type 1
- B. SOC 2 Type 1
- C. SOC 2 Type 2
- D. SOC 3

**Answer: C**

#### NEW QUESTION 22

- (Exam Topic 15)

Which of the following is the BEST method to identify security controls that should be implemented for a web-based application while in development?

- A. Application threat modeling
- B. Secure software development.
- C. Agile software development
- D. Penetration testing

**Answer: A**

#### NEW QUESTION 27

- (Exam Topic 15)

Which of the following is performed to determine a measure of success of a security awareness training program designed to prevent social engineering attacks?

- A. Employee evaluation of the training program
- B. Internal assessment of the training program's effectiveness
- C. Multiple choice tests to participants
- D. Management control of reviews

**Answer: B**

#### NEW QUESTION 28

- (Exam Topic 15)

Which of the following factors should be considered characteristics of Attribute Based Access Control (ABAC) in terms of the attributes used?

- A. Mandatory Access Control (MAC) and Discretionary Access Control (DAC)
- B. Discretionary Access Control (DAC) and Access Control List (ACL)
- C. Role Based Access Control (RBAC) and Mandatory Access Control (MAC)
- D. Role Based Access Control (RBAC) and Access Control List (ACL)

**Answer: D**

#### NEW QUESTION 32

- (Exam Topic 15)

What is the FIRST step for an organization to take before allowing personnel to access social media from a corporate device or user account?

- A. Publish a social media guidelines document.
- B. Publish an acceptable usage policy.
- C. Document a procedure for accessing social media sites.
- D. Deliver security awareness training.

**Answer: A**

#### NEW QUESTION 37

- (Exam Topic 15)

What would be the BEST action to take in a situation where collected evidence was left unattended overnight in an unlocked vehicle?

- A. Report the matter to the local police authorities.
- B. Move evidence to a climate-controlled environment.
- C. Re-inventory the evidence and provide it to the evidence custodian.
- D. Immediately report the matter to the case supervisor.

**Answer: D**

#### NEW QUESTION 39

- (Exam Topic 15)

Which of the following is the MOST effective method of detecting vulnerabilities in web-based applications early in the secure Software Development Life Cycle (SDLC)?

- A. Web application vulnerability scanning
- B. Application fuzzing
- C. Code review
- D. Penetration testing

**Answer: C**

**NEW QUESTION 43**

- (Exam Topic 15)

The Rivest-Shamir-Adleman (RSA) algorithm is BEST suited for which of the following operations?

- A. Bulk data encryption and decryption
- B. One-way secure hashing for user and message authentication
- C. Secure key exchange for symmetric cryptography
- D. Creating digital checksums for message integrity

**Answer: C**

**NEW QUESTION 48**

- (Exam Topic 15)

A software developer installs a game on their organization-provided smartphone. Upon installing the game, the software developer is prompted to allow the game access to call logs, Short Message Service (SMS) messaging, and Global Positioning System (GPS) location data. What has the game MOST likely introduced to the smartphone?

- A. Alerting
- B. Vulnerability
- C. Geo-fencing
- D. Monitoring

**Answer: B**

**NEW QUESTION 51**

- (Exam Topic 15)

Why is authentication by ownership stronger than authentication by knowledge?

- A. It is easier to change.
- B. It can be kept on the user's person.
- C. It is more difficult to duplicate.
- D. It is simpler to control.

**Answer: B**

**NEW QUESTION 54**

- (Exam Topic 15)

What level of Redundant Array of Independent Disks (RAID) is configured PRIMARILY for high-performance data reads and writes?

- A. RAID-0
- B. RAID-1
- C. RAID-5
- D. RAID-6

**Answer: A**

**NEW QUESTION 57**

- (Exam Topic 15)

Which of the following MUST the administrator of a security information and event management (SIEM) system ensure?

- A. All sources are reporting in the exact same Extensible Markup Language (XML) format.
- B. Data sources do not contain information infringing upon privacy regulations.
- C. All sources are synchronized with a common time reference.
- D. Each source uses the same Internet Protocol (IP) address for reporting.

**Answer: C**

**NEW QUESTION 61**

- (Exam Topic 15)

Which audit type is MOST appropriate for evaluating the effectiveness of a security program?

- A. Threat
- B. Assessment
- C. Analysis
- D. Validation

**Answer: B**

**NEW QUESTION 64**

- (Exam Topic 15)

Which of the following types of firewall only examines the "handshaking" between packets before forwarding traffic?

- A. Proxy firewalls
- B. Host-based firewalls
- C. Circuit-level firewalls
- D. Network Address Translation (NAT) firewalls

Answer: C

**NEW QUESTION 68**

- (Exam Topic 15)

What method could be used to prevent passive attacks against secure voice communications between an organization and its vendor?

- A. Encryption in transit
- B. Configure a virtual private network (VPN)
- C. Configure a dedicated connection
- D. Encryption at rest

Answer: A

**NEW QUESTION 71**

- (Exam Topic 15)

Which of the following examples is BEST to minimize the attack surface for a customer's private information?

- A. Obfuscation
- B. Collection limitation
- C. Authentication
- D. Data masking

Answer: A

**NEW QUESTION 76**

- (Exam Topic 15)

What type of investigation applies when malicious behavior is suspected between two organizations?

- A. Regulatory
- B. Criminal
- C. Civil
- D. Operational

Answer: A

**NEW QUESTION 77**

- (Exam Topic 15)

A technician is troubleshooting a client's report about poor wireless performance. Using a client monitor, the technician notes the following information:

SSID	Signal (RSSI)	Channel
Corporate	-50	9
Corporate	-69	10
Corporate	-67	11
Corporate	-63	6

Which of the following is MOST likely the cause of the issue?

- A. Channel overlap
- B. Poor signal
- C. Incorrect power settings
- D. Wrong antenna type

Answer: A

**NEW QUESTION 78**

- (Exam Topic 15)

What is the BEST control to be implemented at a login page in a web application to mitigate the ability to enumerate users?

- A. Implement a generic response for a failed login attempt.
- B. Implement a strong password during account registration.
- C. Implement numbers and special characters in the user name.
- D. Implement two-factor authentication (2FA) to login process.

Answer: A

**NEW QUESTION 81**

- (Exam Topic 15)

An establish information technology (IT) consulting firm is considering acquiring a successful local startup. To gain a comprehensive understanding of the startup's security posture' which type of assessment provides the BEST information?

- A. A security audit
- B. A penetration test
- C. A tabletop exercise
- D. A security threat model

Answer: A

**NEW QUESTION 84**

- (Exam Topic 15)

Which of the following is the GREATEST risk of relying only on Capability Maturity Models (CMM) for software to guide process improvement and assess capabilities of acquired software?

- A. Organizations can only reach a maturity level 3 when using CMMs
- B. CMMs do not explicitly address safety and security
- C. CMMs can only be used for software developed in-house
- D. CMMs are vendor specific and may be biased

Answer: B

**NEW QUESTION 89**

- (Exam Topic 15)

When developing an external facing web-based system, which of the following would be the MAIN focus of the security assessment prior to implementation and production?

- A. Assessing the Uniform Resource Locator (URL)
- B. Ensuring Secure Sockets Layer (SSL) certificates are signed by a certificate authority
- C. Ensuring that input validation is enforced
- D. Ensuring Secure Sockets Layer (SSL) certificates are internally signed

Answer: B

**NEW QUESTION 92**

- (Exam Topic 15)

Which of the following is the MOST common cause of system or security failures?

- A. Lack of system documentation
- B. Lack of physical security controls
- C. Lack of change control
- D. Lack of logging and monitoring

Answer: D

**NEW QUESTION 95**

- (Exam Topic 15)

The Chief Executive Officer (CEO) wants to implement an internal audit of the company's information security posture. The CEO wants to avoid any bias in the audit process; therefore, has assigned the Sales Director to conduct the audit. After significant interaction over a period of weeks the audit concludes that the company's policies and procedures are sufficient, robust and well established. The CEO then moves on to engage an external penetration testing company in order to showcase the organization's robust information security stance. This exercise reveals significant failings in several critical security controls and shows that the incident response processes remain undocumented. What is the MOST likely reason for this disparity in the results of the audit and the external penetration test?

- A. The external penetration testing company used custom zero-day attacks that could not have been predicted.
- B. The information technology (IT) and governance teams have failed to disclose relevant information to the internal audit team leading to an incomplete assessment being formulated.
- C. The scope of the penetration test exercise and the internal audit were significantly different.
- D. The audit team lacked the technical experience and training to make insightful and objective assessments of the data provided to them.

Answer: C

**NEW QUESTION 100**

- (Exam Topic 15)

An organization is setting a security assessment scope with the goal of developing a Security Management Program (SMP). The next step is to select an approach for conducting the risk assessment. Which of the following approaches is MOST effective for the SMP?

- A. Data driven risk assessment with a focus on data
- B. Security controls driven assessment that focuses on controls management
- C. Business processes based risk assessment with a focus on business goals
- D. Asset driven risk assessment with a focus on the assets

Answer: A

**NEW QUESTION 101**

- (Exam Topic 15)

Information Security Continuous Monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Which of the following is the FIRST step in developing an ISCM strategy and implementing an ISCM program?

- A. Define a strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
- B. Conduct a vulnerability assessment to discover current threats against the environment and incorporate them into the program.
- C. Respond to findings with technical management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
- D. Analyze the data collected and report findings, determining the appropriate responses

E. It may be necessary to collect additional information to clarify or supplement existing monitoring data.

**Answer:** A

**NEW QUESTION 103**

- (Exam Topic 15)

Which of the following criteria ensures information is protected relative to its importance to the organization?

- A. The value of the data to the organization's senior management
- B. Legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification
- C. Legal requirements determined by the organization headquarters' location
- D. Organizational stakeholders, with classification approved by the management board

**Answer:** D

**NEW QUESTION 107**

- (Exam Topic 15)

Which of the following are the BEST characteristics of security metrics?

- A. They are generalized and provide a broad overview
- B. They use acronyms and abbreviations to be concise
- C. They use bar charts and Venn diagrams
- D. They are consistently measured and quantitatively expressed

**Answer:** D

**NEW QUESTION 109**

- (Exam Topic 15)

Which Open Systems Interconnection (OSI) layer(s) BEST corresponds to the network access layer in the Transmission Control Protocol/Internet Protocol (TCP/IP) model?

- A. Transport Layer
- B. Data Link and Physical Layers
- C. Application, Presentation, and Session Layers
- D. Session and Network Layers

**Answer:** B

**NEW QUESTION 114**

- (Exam Topic 15)

What security principle addresses the issue of "Security by Obscurity"?

- A. Open design
- B. Segregation of duties (SoD)
- C. Role Based Access Control (RBAC)
- D. Least privilege

**Answer:** D

**NEW QUESTION 119**

- (Exam Topic 15)

A financial organization that works according to agile principles has developed a new application for their external customer base to request a line of credit. A security analyst has been asked to assess the security risk of the minimum viable product (MVP). Which is the MOST important activity the analyst should assess?

- A. The software has the correct functionality.
- B. The software has been code reviewed.
- C. The software had been branded according to corporate standards.
- D. The software has been signed off for release by the product owner.

**Answer:** A

**NEW QUESTION 120**

- (Exam Topic 15)

- A. Obtain information security management approval.
- B. Maintain the integrity of the application.
- C. Obtain feedback before implementation.
- D. Identify vulnerabilities.

**Answer:** D

**NEW QUESTION 123**

- (Exam Topic 15)

Why is it important that senior management clearly communicates the formal Maximum Tolerable Downtime (MTD) decision?

- A. To provide each manager with precise direction on selecting an appropriate recovery alternative
- B. To demonstrate to the regulatory bodies that the company takes business continuity seriously
- C. To demonstrate to the board of directors that senior management is committed to continuity recovery efforts
- D. To provide a formal declaration from senior management as required by internal audit to demonstrate sound business practices

**Answer:** D

#### NEW QUESTION 124

- (Exam Topic 15)

An organization has requested storage area network (SAN) disks for a new project. What Redundant Array of Independent Disks (RAID) level provides the BEST redundancy and fault tolerance?

- A. RAID level 1
- B. RAID level 3
- C. RAID level 4
- D. RAID level 5

**Answer:** D

#### NEW QUESTION 125

- (Exam Topic 15)

Which of the following is the MOST secure password technique?

- A. Passphrase
- B. One-time password
- C. Cognitive password
- D. dphertext

**Answer:** A

#### NEW QUESTION 127

- (Exam Topic 15)

Which of the following is the MAIN difference between a network-based firewall and a host-based firewall?

- A. A network-based firewall is stateful, while a host-based firewall is stateless.
- B. A network-based firewall controls traffic passing through the device, while a host-based firewall controls traffic destined for the device.
- C. A network-based firewall verifies network traffic, while a host-based firewall verifies processes and applications.
- D. A network-based firewall blocks network intrusions, while a host-based firewall blocks malware.

**Answer:** B

#### NEW QUESTION 128

- (Exam Topic 15)

Which of the following terms BEST describes a system which allows a user to log in and access multiple related servers and applications?

- A. Remote Desktop Protocol (RDP)
- B. Federated identity management (FIM)
- C. Single sign-on (SSO)
- D. Multi-factor authentication (MFA)

**Answer:** B

#### NEW QUESTION 132

- (Exam Topic 15)

Which of the following poses the GREATEST privacy risk to personally identifiable information (PII) when disposing of an office printer or copier?

- A. The device could contain a document with PII on the platen glass
- B. Organizational network configuration information could still be present within the device
- C. A hard disk drive (HDD) in the device could contain PII
- D. The device transfer roller could contain imprints of PII

**Answer:** B

#### NEW QUESTION 134

- (Exam Topic 15)

In systems security engineering, what does the security principle of modularity provide?

- A. Documentation of functions
- B. Isolated functions and data
- C. Secure distribution of programs and data
- D. Minimal access to perform a function

**Answer:** A

#### NEW QUESTION 136

- (Exam Topic 15)

When assessing the audit capability of an application, which of the following activities is MOST important?

- A. Determine if audit records contain sufficient information.
- B. Review security plan for actions to be taken in the event of audit failure.
- C. Verify if sufficient storage is allocated for audit records.
- D. Identify procedures to investigate suspicious activity.

**Answer: C**

#### NEW QUESTION 140

- (Exam Topic 15)

An organization has discovered that organizational data is posted by employees to data storage accessible to the general public. What is the PRIMARY step an organization must take to ensure data is properly protected from public release?

- A. Implement a data classification policy.
- B. Implement a data encryption policy.
- C. Implement a user training policy.
- D. Implement a user reporting policy.

**Answer: C**

#### NEW QUESTION 142

- (Exam Topic 15)

While classifying credit card data related to Payment Card Industry Data Security Standards (PCI-DSS), which of the following is a PRIMARY security requirement?

- A. Processor agreements with card holders
- B. Three-year retention of data
- C. Encryption of data
- D. Specific card disposal methodology

**Answer: C**

#### NEW QUESTION 143

- (Exam Topic 15)

What is the FINAL step in the waterfall method for contingency planning?

- A. Maintenance
- B. Testing
- C. Implementation
- D. Training

**Answer: A**

#### NEW QUESTION 144

- (Exam Topic 15)

Which of the following is the reason that transposition ciphers are easily recognizable?

- A. Key
- B. Block
- C. Stream
- D. Character

**Answer: B**

#### NEW QUESTION 147

- (Exam Topic 15)

A security architect is developing an information system for a client. One of the requirements is to deliver a platform that mitigates against common vulnerabilities and attacks, What is the MOST efficient option used to prevent buffer overflow attacks?

- A. Process isolation
- B. Address Space Layout Randomization (ASLR)
- C. Processor states
- D. Access control mechanisms

**Answer: B**

#### NEW QUESTION 151

- (Exam Topic 15)

Which of the following addresses requirements of security assessments during software acquisition?

- A. Software configuration management (SCM)
- B. Data loss prevention (DLP) policy
- C. Continuous monitoring
- D. Software assurance policy

Answer: A

#### NEW QUESTION 155

- (Exam Topic 15)

Which of the following measures serves as the BEST means for protecting data on computers, smartphones, and external storage devices when traveling to high-risk countries?

- A. Review applicable destination country laws, forensically clean devices prior to travel, and only download sensitive data over a virtual private network (VPN) upon arriving at the destination.
- B. Keep laptops, external storage devices, and smartphones in the hotel room when not in use.
- C. Leverage a Secure Socket Layer (SSL) connection over a virtual private network (VPN) to download sensitive data upon arriving at the destination.
- D. Use multi-factor authentication (MFA) to gain access to data stored on laptops or external storage devices and biometric fingerprint access control isms to unlock smartphones.

Answer: D

#### NEW QUESTION 159

- (Exam Topic 15)

Data remanence is the biggest threat in which of the following scenarios?

- A. A physical disk drive has been overwritten and reused within a datacenter.
- B. A physical disk drive has been degaussed, verified, and released to a third party for dest.....
- C. A flash drive has been overwritten, verified, and reused within a datacenter.
- D. A flash drive has been overwritten and released to a third party for destruction.

Answer: D

#### NEW QUESTION 161

- (Exam Topic 15)

The acquisition of personal data being obtained by a lawful and fair means is an example of what principle?

- A. Data Quality Principle
- B. Openness Principle
- C. Purpose Specification Principle
- D. Collection Limitation Principle

Answer: D

#### NEW QUESTION 162

- (Exam Topic 15)

At the destination host, which of the following OSI model layers will discard a segment with a bad checksum in the UDP header?

- A. Network
- B. Data link
- C. Transport
- D. Session

Answer: C

#### NEW QUESTION 167

- (Exam Topic 15)

When conducting a third-party risk assessment of a new supplier, which of the following reports should be reviewed to confirm the operating effectiveness of the security, availability, confidentiality, and privacy trust principles?

- A. Service Organization Control (SOC) 1, Type 2
- B. Service Organization Control (SOC) 2, Type 2
- C. International Organization for Standardization (ISO) 27001
- D. International Organization for Standardization (ISO) 27002

Answer: B

#### NEW QUESTION 169

- (Exam Topic 15)

Where can the Open Web Application Security Project (OWASP) list of associated vulnerabilities be found?

- A. OWASP Top 10 Project
- B. OWASP Software Assurance Maturity Model (SAMM) Project
- C. OWASP Guide Project
- D. OWASP Mobile Project

Answer: A

#### NEW QUESTION 173

- (Exam Topic 15)

Which of the following frameworks provides vulnerability metrics and characteristics to support the National Vulnerability Database (NVD)?

- A. Center for Internet Security (CIS)
- B. Common Vulnerabilities and Exposures (CVE)
- C. Open Web Application Security Project (OWASP)
- D. Common Vulnerability Scoring System (CVSS)

**Answer: D**

#### NEW QUESTION 178

- (Exam Topic 15)

An organization's internal audit team performed a security audit on the company's system and reported that the manufacturing application is rarely updated along with other issues categorized as minor. Six months later, an external audit team reviewed the same system with the same scope, but identified severe weaknesses in the manufacturing application's security controls. What is MOST likely to be the root cause of the internal audit team's failure in detecting these security issues?

- A. Inadequate test coverage analysis
- B. Inadequate security patch testing
- C. Inadequate log reviews
- D. Inadequate change control procedures

**Answer: A**

#### NEW QUESTION 182

- (Exam Topic 15)

Which of the following types of hosts should be operating in the demilitarized zone (DMZ)?

- A. Hosts intended to provide limited access to public resources
- B. Database servers that can provide useful information to the public
- C. Hosts that store unimportant data such as demographical information
- D. File servers containing organizational data

**Answer: A**

#### NEW QUESTION 185

- (Exam Topic 15)

When resolving ethical conflicts, the information security professional MUST consider many factors. In what order should these considerations be prioritized?

- A. Public safety, duties to individuals, duties to the profession, and duties to principals
- B. Public safety, duties to principals, duties to individuals, and duties to the profession
- C. Public safety, duties to the profession, duties to principals, and duties to individuals
- D. Public safety, duties to principals, duties to the profession, and duties to individuals

**Answer: C**

#### NEW QUESTION 189

- (Exam Topic 15)

What Hypertext Transfer Protocol (HTTP) response header can be used to disable the execution of inline JavaScript and the execution of eval()-type functions?

- A. Strict-Transport-Security
- B. X-XSS-Protection
- C. X-Frame-Options
- D. Content-Security-Policy

**Answer: D**

#### NEW QUESTION 191

- (Exam Topic 15)

Which of the following is a key responsibility for a data steward assigned to manage an enterprise data lake?

- A. Ensure proper business definition, value, and usage of data collected and stored within the enterprise data lake.
- B. Ensure proper and identifiable data owners for each data element stored within an enterprise data lake.
- C. Ensure adequate security controls applied to the enterprise data lake.
- D. Ensure that any data passing within remit is being used in accordance with the rules and regulations of the business.

**Answer: A**

#### NEW QUESTION 193

- (Exam Topic 15)

Which of the following is a unique feature of attribute-based access control (ABAC)?

- A. A user is granted access to a system based on group affinity.
- B. A user is granted access to a system with biometric authentication.
- C. A user is granted access to a system at a particular time of day.
- D. A user is granted access to a system based on username and password.

**Answer: C**

**NEW QUESTION 198**

- (Exam Topic 15)

Which change management role is responsible for the overall success of the project and supporting the change throughout the organization?

- A. Change driver
- B. Change implementer
- C. Program sponsor
- D. Project manager

**Answer: D**

**NEW QUESTION 200**

- (Exam Topic 15)

What is the MOST important factor in establishing an effective Information Security Awareness Program?

- A. Obtain management buy-in.
- B. Conduct an annual security awareness event.
- C. Mandate security training.
- D. Hang information security posters on the walls,

**Answer: C**

**NEW QUESTION 204**

- (Exam Topic 15)

Which of the following is TRUE for an organization that is using a third-party federated identity service?

- A. The organization enforces the rules to other organization's user provisioning
- B. The organization establishes a trust relationship with the other organizations
- C. The organization defines internal standard for overall user identification
- D. The organization specifies alone how to authenticate other organization's users

**Answer: C**

**NEW QUESTION 209**

- (Exam Topic 15)

A new site's gateway isn't able to form a tunnel to the existing site-to-site Internet Protocol Security (IPsec) virtual private network (VPN) device at headquarters. Devices at the new site have no problem accessing resources on the Internet. When testing connectivity between the remote site's gateway, it was observed that the external Internet Protocol (IP) address of the gateway was set to 192.168.1.1. and was configured to send outbound traffic to the Internet Service Provider (ISP) gateway at 192.168.1.2. Which of the following would be the BEST way to resolve the issue and get the remote site connected?

- A. Enable IPsec tunnel mode on the VPN devices at the new site and the corporate headquarters.
- B. Enable Layer 2 Tunneling Protocol (L2TP) on the VPN devices at the new site and the corporate headquarters.
- C. Enable Point-to-Point Tunneling Protocol (PPTP) on the VPN devices at the new site and the corporate headquarters.
- D. Enable Network Address Translation (NAT) - Traversal on the VPN devices at the new site and the corporate headquarters.

**Answer: A**

**NEW QUESTION 212**

- (Exam Topic 15)

Which of the following is the MOST appropriate technique for destroying magnetic platter style hard disk drives (HDD) containing data with a "HIGH" security categorization?

- A. Drill through the device and platters.
- B. Mechanically shred the entire HDD.
- C. Remove the control electronics.
- D. HP iProcess the HDD through a degaussing device.

**Answer: D**

**NEW QUESTION 214**

- (Exam Topic 15)

At what stage of the Software Development Life Cycle (SDLC) does software vulnerability remediation MOST likely cost the least to implement?

- A. Development
- B. Testing
- C. Deployme
- D. Design

**Answer: D**

**NEW QUESTION 215**

- (Exam Topic 15)

Which of the following would be the BEST guideline to follow when attempting to avoid the exposure of sensitive data?

- A. Store sensitive data only when necessary.
- B. Educate end-users on methods of attacks on sensitive data.
- C. Establish report parameters for sensitive data.

D. Monitor mail servers for sensitive data being exfiltrated.

**Answer:** A

**NEW QUESTION 216**

- (Exam Topic 15)

When determining data and information asset handling, regardless of the specific toolset being used, which of the following is one of the common components of big data?

- A. Consolidated data collection
- B. Distributed storage locations
- C. Distributed data collection
- D. Centralized processing location

**Answer:** C

**NEW QUESTION 217**

- (Exam Topic 15)

What does the result of Cost-Benefit Analysis (CBA) on new security initiatives provide?

- A. Quantifiable justification
- B. Baseline improvement
- C. Risk evaluation
- D. Formalized acceptance

**Answer:** A

**NEW QUESTION 220**

- (Exam Topic 15)

A recent security audit is reporting several unsuccessful login attempts being repeated at specific times during the day on an Internet facing authentication server. No alerts have been generated by the security information and event management (SIEM) system. What PRIMARY action should be taken to improve SIEM performance?

- A. Implement role-based system monitoring
- B. Audit firewall logs to identify the source of login attempts
- C. Enhance logging detail
- D. Confirm alarm thresholds

**Answer:** B

**NEW QUESTION 225**

- (Exam Topic 15)

Which is the PRIMARY mechanism for providing the workforce with the information needed to protect an agency's vital information resources?

- A. Incorporating security awareness and training as part of the overall information security program
- B. An information technology (IT) security policy to preserve the confidentiality, integrity, and availability of systems
- C. Implementation of access provisioning process for coordinating the creation of user accounts
- D. Execution of periodic security and privacy assessments to the organization

**Answer:** A

**NEW QUESTION 228**

- (Exam Topic 15)

Which of the following statements is TRUE about Secure Shell (SSH)?

- A. SSH does not protect against man-in-the-middle (MITM) attacks.
- B. SSH supports port forwarding, which can be used to protect less secured protocols.
- C. SSH can be used with almost any application because it is concerned with maintaining a circuit.
- D. SSH is easy to deploy because it requires a Web browser only.

**Answer:** B

**NEW QUESTION 229**

- (Exam Topic 15)

A Chief Information Officer (CIO) has delegated responsibility of their system security to the head of the information technology (IT) department. While corporate policy dictates that only the CIO can make decisions on the level of data protection required, technical implementation decisions are done by the head of the IT department. Which of the following BEST describes the security role filled by the head of the IT department?

- A. System analyst
- B. System security officer
- C. System processor
- D. System custodian

**Answer:** D

**NEW QUESTION 234**

- (Exam Topic 15)

Which of the following is included in the Global System for Mobile Communications (GSM) security framework?

- A. Public-Key Infrastructure (PKI)
- B. Symmetric key cryptography
- C. Digital signatures
- D. Biometric authentication

**Answer: C**

#### NEW QUESTION 238

- (Exam Topic 15)

Which of the following encryption technologies has the ability to function as a stream cipher?

- A. Cipher Feedback (CFB)
- B. Feistel cipher
- C. Cipher Block Chaining (CBC) with error propagation
- D. Electronic Code Book (ECB)

**Answer: A**

#### NEW QUESTION 242

- (Exam Topic 15)

Which technique helps system designers consider potential security concerns of their systems and applications?

- A. Penetration testing
- B. Threat modeling
- C. Manual inspections and reviews
- D. Source code review

**Answer: B**

#### NEW QUESTION 245

- (Exam Topic 15)

Of the following, which BEST provides non-repudiation with regards to access to a server room?

- A. Fob and Personal Identification Number (PIN)
- B. Locked and secured cages
- C. Biometric readers
- D. Proximity readers

**Answer: C**

#### NEW QUESTION 248

- (Exam Topic 15)

An attacker has intruded into the source code management system and is able to download but not modify the code. Which of the following aspects of the code theft has the HIGHEST security impact?

- A. The attacker could publicly share confidential comments found in the stolen code.
- B. Competitors might be able to steal the organization's ideas by looking at the stolen code.
- C. A competitor could run their own copy of the organization's website using the stolen code.
- D. Administrative credentials or keys hard-coded within the stolen code could be used to access sensitive data.

**Answer: A**

#### NEW QUESTION 250

- (Exam Topic 15)

Which organizational department is ultimately responsible for information governance related to e-mail and other e-records?

- A. Audit
- B. Compliance
- C. Legal
- D. Security

**Answer: C**

#### NEW QUESTION 251

- (Exam Topic 15)

Which of the following BEST describes the purpose of Border Gateway Protocol (BGP)?

- A. Maintain a list of network paths between internet routers.
- B. Provide Routing Information Protocol (RIP) version 2 advertisements to neighboring layer 3 devices.
- C. Provide firewall services to cloud-enabled applications.
- D. Maintain a list of efficient network paths between autonomous systems.

**Answer: B**

**NEW QUESTION 254**

- (Exam Topic 15)

When assessing web vulnerabilities, how can navigating the dark web add value to a penetration test?

- A. The actual origin and tools used for the test can be hidden.
- B. Information may be found on related breaches and hacking.
- C. Vulnerabilities can be tested without impact on the tested environment.
- D. Information may be found on hidden vendor patches.

**Answer: D**

**NEW QUESTION 255**

- (Exam Topic 15)

Which of the following BEST ensures the integrity of transactions to intended recipients?

- A. Public key infrastructure (PKI)
- B. Blockchain technology
- C. Pre-shared key (PSK)
- D. Web of trust

**Answer: A**

**NEW QUESTION 260**

- (Exam Topic 15)

What are the first two components of logical access control?

- A. Confidentiality and authentication
- B. Authentication and identification
- C. Identification and confidentiality
- D. Authentication and availability

**Answer: B**

**NEW QUESTION 265**

- (Exam Topic 15)

Before allowing a web application into the production environment, the security practitioner performs multiple types of tests to confirm that the web application performs as expected. To test the username field, the security practitioner creates a test that enters more characters into the field than is allowed. Which of the following BEST describes the type of test performed?

- A. Misuse case testing
- B. Penetration testing
- C. Web session testing
- D. Interface testing

**Answer: A**

**NEW QUESTION 269**

- (Exam Topic 15)

Write Once, Read Many (WORM) data storage devices are designed to BEST support which of the following core security concepts?

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

**Answer: A**

**NEW QUESTION 274**

- (Exam Topic 15)

When telephones in a city are connected by a single exchange, the caller can only connect with the switchboard operator. The operator then manually connects the call.

This is an example of which type of network topology?

- A. Star
- B. Tree
- C. Point-to-Point Protocol (PPP)
- D. Bus

**Answer: A**

**NEW QUESTION 279**

- (Exam Topic 15)

The MAIN purpose of placing a tamper seal on a computer system's case is to:

- A. raise security awareness.
- B. detect efforts to open the case.
- C. expedite physical auditing.

D. make it difficult to steal internal components.

**Answer:** A

**NEW QUESTION 282**

- (Exam Topic 15)

Why would a system be structured to isolate different classes of information from one another and segregate them by user jurisdiction?

- A. The organization can avoid e-discovery processes in the event of litigation.
- B. The organization's infrastructure is clearly arranged and scope of responsibility is simplified.
- C. The organization can vary its system policies to comply with conflicting national laws.
- D. The organization is required to provide different services to various third-party organizations.

**Answer:** C

**NEW QUESTION 286**

- (Exam Topic 15)

International bodies established a regulatory scheme that defines how weapons are exchanged between the signatories. It also addresses cyber weapons, including malicious software, Command and Control (C2) software, and internet surveillance software. This is a description of which of the following?

- A. General Data Protection Regulation (GDPR)
- B. Palermo convention
- C. Wassenaar arrangement
- D. International Traffic in Arms Regulations (ITAR)

**Answer:** C

**NEW QUESTION 290**

- (Exam Topic 15)

A recent information security risk assessment identified weak system access controls on mobile devices as a high me In order to address this risk and ensure only authorized staff access company information, which of the following should the organization implement?

- A. Intrusion prevention system (IPS)
- B. Multi-factor authentication (MFA)
- C. Data loss protection (DLP)
- D. Data at rest encryption

**Answer:** B

**NEW QUESTION 291**

- (Exam Topic 15)

A company wants to store data related to users on an offsite server. What method can be deployed to protect the privacy of the user's information while maintaining the field-level configuration of the database?

- A. Encryption
- B. Encoding
- C. Tokenization
- D. Hashing

**Answer:** A

**NEW QUESTION 292**

- (Exam Topic 15)

An employee's home address should be categorized according to which of the following references?

- A. The consent form terms and conditions signed by employees
- B. The organization's data classification model
- C. Existing employee data classifications
- D. An organization security plan for human resources

**Answer:** B

**NEW QUESTION 294**

- (Exam Topic 15)

How should the retention period for an organization's social media content be defined?

- A. By the retention policies of each social media service
- B. By the records retention policy of the organization
- C. By the Chief Information Officer (CIO)
- D. By the amount of available storage space

**Answer:** B

**NEW QUESTION 299**

- (Exam Topic 15)

In software development, developers should use which type of queries to prevent a Structured Query Language (SQL) injection?

- A. Parameterised
- B. Dynamic
- C. Static
- D. Controlled

**Answer:** A

#### NEW QUESTION 303

- (Exam Topic 15)

An organization wants a service provider to authenticate users via the users' organization domain credentials. Which markup language should the organization's security personnel use to support the integration?

- A. Security Assertion Markup Language (SAML)
- B. YAML Ain't Markup Language (YAML)
- C. Hypertext Markup Language (HTML)
- D. Extensible Markup Language (XML)

**Answer:** A

#### NEW QUESTION 305

- (Exam Topic 15)

In what phase of the System Development Life Cycle (SDLC) should security training for the development team begin?

- A. Development/Acquisition
- B. Initiation
- C. Implementation/ Assessment
- D. Disposal

**Answer:** A

#### NEW QUESTION 306

- (Exam Topic 15)

When conducting a remote access session using Internet Protocol Security (IPSec), which Open Systems Interconnection (OSI) model layer does this connection use?

- A. Transport
- B. Network
- C. Data link
- D. Presentation

**Answer:** B

#### NEW QUESTION 309

- (Exam Topic 15)

Which of the following is the BEST method to gather evidence from a computer's hard drive?

- A. Disk duplication
- B. Disk replacement
- C. Forensic signature
- D. Forensic imaging

**Answer:** D

#### NEW QUESTION 310

- (Exam Topic 15)

Which of the following is a security weakness in the evaluation of common criteria (CC) products?

- A. The manufacturer can state what configuration of the product is to be evaluated.
- B. The product can be evaluated by labs in other countries.
- C. The Target of Evaluation's (TOE) testing environment is identical to the operating environment
- D. The evaluations are expensive and time-consuming to perform.

**Answer:** A

#### NEW QUESTION 313

- (Exam Topic 15)

A security engineer is required to integrate security into a software project that is implemented by small groups test quickly, continuously, and independently develop, test, and deploy code to the cloud. The engineer will MOST likely integrate with which software development process?

- A. Service-oriented architecture (SOA)
- B. Spiral Methodology
- C. Structured Waterfall Programming Development
- D. Devops Integrated Product Team (IPT)

**Answer:** C

#### NEW QUESTION 314

- (Exam Topic 15)

Which of the following protects personally identifiable information (PII) used by financial services organizations?

- A. National Institute of Standards and Technology (NIST) SP 800-53
- B. Gramm-Leach-Bliley Act (GLBA)
- C. Payment Card Industry Data Security Standard (PCI-DSS)
- D. Health Insurance Portability and Accountability Act (HIPAA)

**Answer: B**

#### NEW QUESTION 318

- (Exam Topic 15)

What is the overall goal of software security testing?

- A. Identifying the key security features of the software
- B. Ensuring all software functions perform as specified
- C. Reducing vulnerabilities within a software system
- D. Making software development more agile

**Answer: B**

#### NEW QUESTION 321

- (Exam Topic 15)

A security professional can BEST mitigate the risk of using a Commercial Off-The-Shelf (COTS) solution by deploying the application with which of the following controls in ?

- A. Whitelisting application
- B. Network segmentation
- C. Hardened configuration
- D. Blacklisting application

**Answer: A**

#### NEW QUESTION 325

- (Exam Topic 15)

A security professional needs to find a secure and efficient method of encrypting data on an endpoint. Which solution includes a root key?

- A. Bitlocker
- B. Trusted Platform Module (TPM)
- C. Virtual storage array network (VSAN)
- D. Hardware security module (HSM)

**Answer: D**

#### NEW QUESTION 328

- (Exam Topic 15)

When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner's first consideration?

- A. Resiliency of the system
- B. Detection of sophisticated attackers
- C. Risk assessment of the system
- D. Topology of the network used for the system

**Answer: A**

#### NEW QUESTION 333

- (Exam Topic 15)

Which of the following is used to ensure that data mining activities Will NOT reveal sensitive data?

- A. Implement two-factor authentication on the underlying infrastructure.
- B. Encrypt data at the field level and tightly control encryption keys.
- C. Preprocess the databases to see if inn ..... can be disclosed from the learned patterns.
- D. Implement the principle of least privilege on data elements so a reduced number of users can access the database.

**Answer: D**

#### NEW QUESTION 337

- (Exam Topic 15)

How is Remote Authentication Dial-In User Service (RADIUS) authentication accomplished?

- A. It uses clear text and firewall rules.
- B. It relies on Virtual Private Networks (VPN).
- C. It uses clear text and shared secret keys.
- D. It relies on asymmetric encryption keys.

Answer: C

**NEW QUESTION 338**

- (Exam Topic 15)

Which of the following roles is responsible for ensuring that important datasets are developed, maintained, and are accessible within their defined specifications?

- A. Data Reviewer
- B. Data User
- C. Data Custodian
- D. Data Owner

Answer: D

**NEW QUESTION 342**

- (Exam Topic 15)

Which of the following is the MOST effective corrective control to minimize the effects of a physical intrusion?

- A. Automatic videotaping of a possible intrusion
- B. Rapid response by guards or police to apprehend a possible intruder
- C. Activating bright lighting to frighten away a possible intruder
- D. Sounding a loud alarm to frighten away a possible intruder

Answer: C

**NEW QUESTION 344**

- (Exam Topic 15)

Which of the following BEST describes centralized identity management?

- A. Service providers rely on a trusted third party (TTP) to provide requestors with both credentials and identifiers.
- B. Service providers agree to integrate identity system recognition across organizational boundaries.
- C. Service providers identify an entity by behavior analysis versus an identification factor.
- D. Service providers perform as both the credential and identity provider (IdP).

Answer: B

**NEW QUESTION 346**

- (Exam Topic 15)

How is it possible to extract private keys securely stored on a cryptographic smartcard?

- A. Bluebugging
- B. Focused ion-beam
- C. Bluejacking
- D. Power analysis

Answer: D

**NEW QUESTION 348**

- (Exam Topic 15)

In order to provide dual assurance in a digital signature system, the design MUST include which of the following?

- A. The public key must be unique for the signed document.
- B. signature process must generate adequate authentication credentials.
- C. The hash of the signed document must be present.
- D. The encrypted private key must be provided in the signing certificate.

Answer: B

**NEW QUESTION 353**

- (Exam Topic 15)

Which of the following is a covert channel type?

- A. Storage
- B. Pipe
- C. Memory
- D. Monitoring

Answer: A

**NEW QUESTION 354**

- (Exam Topic 15)

Which of the following activities should a forensic examiner perform FIRST when determining the priority of digital evidence collection at a crime scene?

- A. Gather physical evidence,
- B. Establish order of volatility.
- C. Assign responsibilities to personnel on the scene.

D. Establish a list of files to examine.

**Answer: C**

**NEW QUESTION 358**

- (Exam Topic 15)

When are security requirements the LEAST expensive to implement?

- A. When identified by external consultants
- B. During the application rollout phase
- C. During each phase of the project cycle
- D. When built into application design

**Answer: D**

**NEW QUESTION 361**

- (Exam Topic 15)

The Chief Information Officer (CIO) has decided that as part of business modernization efforts the organization will move towards a cloud architecture. All business-critical data will be migrated to either internal or external cloud services within the next two years. The CIO has a PRIMARY obligation to work with personnel in which role in order to ensure proper protection of data during and after the cloud migration?

- A. Information owner
- B. General Counsel
- C. Chief Information Security Officer (CISO)
- D. Chief Security Officer (CSO)

**Answer: A**

**NEW QUESTION 363**

- (Exam Topic 15)

Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

- A. Trusted Computing Base (TCB)
- B. Time separation
- C. Security kernel
- D. Reference monitor

**Answer: C**

**NEW QUESTION 367**

- (Exam Topic 15)

Which is MOST important when negotiating an Internet service provider (ISP) service-level agreement (SLA) by an organization that solely provides Voice over Internet Protocol (VoIP) services?

- A. Mean time to repair (MTTR)
- B. Quality of Service (QoS) between applications
- C. Availability of network services
- D. Financial penalties in case of disruption

**Answer: B**

**NEW QUESTION 369**

- (Exam Topic 15)

A criminal organization is planning an attack on a government network. Which of the following scenarios presents the HIGHEST risk to the organization?

- A. Network is flooded with communication traffic by the attacker.
- B. Organization loses control of their network devices.
- C. Network management communications is disrupted.
- D. Attacker accesses sensitive information regarding the network topology.

**Answer: B**

**NEW QUESTION 370**

- (Exam Topic 15)

In Federated Identity Management (FIM), which of the following represents the concept of federation?

- A. Collection of information logically grouped into a single entity
- B. Collection, maintenance, and deactivation of user objects and attributes in one or more systems, directories or applications
- C. Collection of information for common identities in a system
- D. Collection of domains that have established trust among themselves

**Answer: D**

**NEW QUESTION 371**

- (Exam Topic 15)

Who should perform the design review to uncover security design flaws as part of the Software Development Life Cycle (SDLC)?

- A. The business owner
- B. security subject matter expert (SME)
- C. The application owner
- D. A developer subject matter expert (SME)

**Answer: B**

#### NEW QUESTION 373

- (Exam Topic 15)

Which of the following features is MOST effective in mitigating against theft of data on a corporate mobile device which has been stolen?

- A. Mobile Device Management (MDM) with device wipe
- B. Whole device encryption with key escrow
- C. Virtual private network (VPN) with traffic encryption
- D. Mobile device tracking with geolocation

**Answer: A**

#### NEW QUESTION 378

- (Exam Topic 15)

A retail company is looking to start a development project that will utilize open source components in its code for the first time. The development team has already acquired several 'open source components and utilized them in proof of concept (POC) code. The team recognizes that the legal and operational risks are outweighed by the benefits of open-source software use. What MUST the organization do next?

- A. Mandate that all open-source components be approved by the Information Security Manager (ISM).
- B. Scan all open-source components for security vulnerabilities.
- C. Establish an open-source compliance policy.
- D. Require commercial support for all open-source components.

**Answer: C**

#### NEW QUESTION 383

- (Exam Topic 15)

Which of the following statements is MOST accurate regarding information assets?

- A. International Organization for Standardization (ISO) 27001 compliance specifies which information assets must be included in asset inventory.
- B. S3 Information assets include any information that is valuable to the organization,
- C. Building an information assets register is a resource-intensive job.
- D. Information assets inventory is not required for risk assessment.

**Answer: B**

#### NEW QUESTION 388

- (Exam Topic 15)

An internal audit for an organization recently identified malicious actions by a user account. Upon further investigation, it was determined the offending user account was used by multiple people at multiple locations simultaneously for various services and applications. What is the BEST method to prevent this problem in the future?

- A. Ensure the security information and event management (SIEM) is set to alert.
- B. Inform users only one user should be using the account at a time.
- C. Ensure each user has their own unique account,
- D. Allow several users to share a generic account.

**Answer: A**

#### NEW QUESTION 393

- (Exam Topic 15)

Which of the following are all elements of a disaster recovery plan (DRP)?

- A. Document the actual location of the ORP, developing an incident notification procedure, evaluating costs of critical components
- B. Document the actual location of the ORP, developing an incident notification procedure, establishing recovery locations
- C. Maintain proper documentation of all server logs, developing an incident notification procedure, establishing recovery locations
- D. Document the actual location of the ORP, recording minutes at all ORP planning sessions, establishing recovery locations

**Answer: C**

#### NEW QUESTION 394

- (Exam Topic 15)

What are the PRIMARY responsibilities of security operations for handling and reporting violations and incidents?

- A. Monitoring and identifying system failures, documenting incidents for future analysis, and scheduling patches for systems
- B. Scheduling patches for systems, notifying the help desk, and alerting key personnel
- C. Monitoring and identifying system failures, alerting key personnel, and containing events
- D. Documenting incidents for future analysis, notifying end users, and containing events

Answer: D

**NEW QUESTION 396**

- (Exam Topic 15)

A large organization's human resources and security teams are planning on implementing technology to eliminate manual user access reviews and improve compliance. Which of the following options is MOST likely to resolve the issues associated with user access?

- A. Implement a role-based access control (RBAC) system.
- B. Implement identity and access management (IAM) platform.
- C. Implement a Privileged Access Management (PAM) system.
- D. Implement a single sign-on (SSO) platform.

Answer: B

**NEW QUESTION 399**

- (Exam Topic 15)

A security professional has been requested by the Board of Directors and Chief Information Security Officer (CISO) to perform an internal and external penetration test. What is the BEST course of action?

- A. Review data localization requirements and regulations.
- B. Review corporate security policies and procedures,
- C. With notice to the Configuring a Wireless Access Point (WAP) with the same Service Set Identifier external test.
- D. With notice to the organization, perform an external penetration test first, then an internal test.

Answer: D

**NEW QUESTION 404**

- (Exam Topic 15)

Building blocks for software-defined networks (SDN) require which of the following?

- A. The SDN is mostly composed of virtual machines (VM).
- B. The SDN is composed entirely of client-server pairs.
- C. Virtual memory is used in preference to random-access memory (RAM).
- D. Random-access memory (RAM) is used in preference to virtual memory.

Answer: C

**NEW QUESTION 405**

- (Exam Topic 14)

Which one of the following documentation should be included in a Disaster Recovery (DR) package?

- A. Source code, compiled code, firmware updates, operational log book and manuals.
- B. Data encrypted in original format, auditable transaction data, and recovery instructions for future extraction on demand.
- C. Hardware configuration instructions, hardware configuration software, an operating system image, a data restoration option, media retrieval instructions,.....
- D. System configuration including hardware, software, hardware, interfaces, software Application Programming Interface (API) configuration, data structure, ....

Answer: C

**NEW QUESTION 406**

- (Exam Topic 14)

An organization wants to enable users to authenticate across multiple security domains. To accomplish this they have decided to use Federated Identity Management (FIM). Which of the following is used behind the scenes in a FIM deployment?

- A. Standard Generalized Markup Language (SGML)
- B. Extensible Markup Language (XML)
- C. Security Assertion Markup Language (SAML)
- D. Transaction Authority Markup Language (XAML)

Answer: C

**NEW QUESTION 409**

- (Exam Topic 14)

Which of the following is the PRIMARY risk associated with Extensible Markup Language (XML) applications?

- A. Users can manipulate the code.
- B. The stack data structure cannot be replicated.
- C. The stack data structure is repetitive.
- D. Potential sensitive data leakage.

Answer: A

**NEW QUESTION 414**

- (Exam Topic 14)

Physical assets defined in an organization's Business Impact Analysis (BIA) could include which of the following?

- A. Personal belongings of organizational staff members
- B. Supplies kept off-site at a remote facility
- C. Cloud-based applications
- D. Disaster Recovery (DR) line-item revenues

**Answer: B**

**NEW QUESTION 419**

- (Exam Topic 14)

How long should the records on a project be retained?

- A. For the duration of the project, or at the discretion of the record owner
- B. Until they are no longer useful or required by policy
- C. Until five years after the project ends, then move to archives
- D. For the duration of the organization fiscal year

**Answer: B**

**NEW QUESTION 420**

- (Exam Topic 14)

Vulnerability scanners may allow for the administrator to assign which of the following in order to assist in prioritizing remediation activities?

- A. Definitions for each exposure type
- B. Vulnerability attack vectors
- C. Asset values for networks
- D. Exploit code metrics

**Answer: C**

**NEW QUESTION 425**

- (Exam Topic 14)

- A. Verify the camera's log for recent logins outside of the Internet Technology (IT) department.
- B. Verify the security and encryption protocol the camera uses.
- C. Verify the security camera requires authentication to log into the management console.
- D. Verify the most recent firmware version is installed on the camera.

**Answer: D**

**NEW QUESTION 430**

- (Exam Topic 14)

Additional padding may be added to the Encapsulating Security Protocol (ESP) trailer to provide which of the following?

- A. Access control
- B. Partial traffic flow confidentiality
- C. Protection against replay attack
- D. Data origin authentication

**Answer: C**

**NEW QUESTION 432**

- (Exam Topic 14)

Compared with hardware cryptography, software cryptography is generally

- A. less expensive and slower.
- B. more expensive and faster.
- C. more expensive and slower.
- D. less expensive and faster.

**Answer: A**

**Explanation:**

Reference:

<https://www.ontrack.com/uk/blog/making-data-simple/hardware-encryption-vs-software-encryption-the-simple>

**NEW QUESTION 434**

- (Exam Topic 14)

Which of the following is the PRIMARY mechanism used to limit the range of objects available to a given subject within different execution domains?

- A. Process isolation
- B. Data hiding and abstraction
- C. Use of discrete layering and Application Programming Interfaces (API)
- D. Virtual Private Network (VPN)

**Answer: C**

**Explanation:**

Reference: <https://books.google.com.pk/books?id=LnjxBwAAQBAJ&pg=PT504&lpg=PT504&dq=CISSP+mechanism+us>

**NEW QUESTION 436**

- (Exam Topic 14)

Which is the MOST critical aspect of computer-generated evidence?

- A. Objectivity
- B. Integrity
- C. Timeliness
- D. Relevancy

**Answer: B**

**NEW QUESTION 440**

- (Exam Topic 14)

A user downloads a file from the Internet, then applies the Secure Hash Algorithm 3 (SHA-3c)?

- A. It verifies the integrity of the file.
- B. It checks the file for malware.
- C. It ensures the entire file downloaded.
- D. It encrypts the entire file.

**Answer: A**

**Explanation:**

Reference: <https://blog.logsign.com/how-to-check-the-integrity-of-a-file/>

**NEW QUESTION 442**

- (Exam Topic 14)

Which of the following is the PRIMARY consideration when determining the frequency an automated control should be assessed or monitored?

- A. The complexity of the automated control
- B. The level of automation of the control
- C. The range of values of the automated control
- D. The volatility of the automated control

**Answer: B**

**NEW QUESTION 445**

- (Exam Topic 14)

During a Disaster Recovery (DR) assessment, additional coverage for assurance is required. What should an assessor do?

- A. Increase the number and type of relevant staff to interview.
- B. Conduct a comprehensive examination of the Disaster Recovery Plan (DRP).
- C. Increase the level of detail of the interview questions.
- D. Conduct a detailed review of the organization's DR policy.

**Answer: A**

**NEW QUESTION 450**

- (Exam Topic 14)

When conducting a security assessment of access controls, Which activity is part of the data analysis phase?

- A. Collect logs and reports.
- B. Present solutions to address audit exceptions.
- C. Categorize and Identify evidence gathered during the audit
- D. Conduct statistical sampling of data transactions.

**Answer: C**

**NEW QUESTION 451**

- (Exam Topic 14)

Which of the following is the final phase of the identity and access provisioning lifecycle?

- A. Recertification
- B. Revocation
- C. Removal
- D. Validation

**Answer: B**

**Explanation:**

Reference: <https://books.google.com.pk/books?id=W2TvAgAAQBAJ&pg=PA256&lpg=PA256&dq=process+in+the+acce>

**NEW QUESTION 455**

- (Exam Topic 14)

From an asset security perspective, what is the BEST countermeasure to prevent data theft due to data remanence when a sensitive data storage media is no longer needed?

- A. Return the media to the system owner.
- B. Delete the sensitive data from the media.
- C. Physically destroy the retired media.
- D. Encrypt data before it is stored on the media.

**Answer: C**

**NEW QUESTION 458**

- (Exam Topic 14)

An organization that has achieved a Capability Maturity model Integration (CMMI) level of 4 has done which of the following?

- A. Addressed continuous innovative process improvement
- B. Addressed the causes of common process variance
- C. Achieved optimized process performance
- D. Achieved predictable process performance

**Answer: C**

**NEW QUESTION 460**

- (Exam Topic 14)

Which of the following open source software issues pose the MOST risk to an application?

- A. The software is beyond end of life and the vendor is out of business.
- B. The software is not used or popular in the development community.
- C. The software has multiple Common Vulnerabilities and Exposures (CVE) and only some are remediated.
- D. The software has multiple Common Vulnerabilities and Exposures (CVE) but the CVEs are classified as low risks.

**Answer: D**

**NEW QUESTION 464**

- (Exam Topic 14)

Which of the following BEST provides for non-repudiation of user account actions?

- A. Centralized authentication system
- B. File auditing system
- C. Managed Intrusion Detection System (IDS)
- D. Centralized logging system

**Answer: D**

**NEW QUESTION 468**

- (Exam Topic 14)

What is the PRIMARY benefit of analyzing the partition layout of a hard disk volume when performing forensic analysis?

- A. Sectors which are not assigned to a perform may contain data that was purposely hidden.
- B. Volume address information for the hard disk may have been modified.
- C. partition tables which are not completely utilized may contain data that was purposely hidden
- D. Physical address information for the hard disk may have been modified.

**Answer: A**

**NEW QUESTION 473**

- (Exam Topic 14)

Which of the following BEST describes how access to a system is granted to federated user accounts?

- A. With the federation assurance level
- B. Based on defined criteria by the Relying Party (RP)
- C. Based on defined criteria by the Identity Provider (IdP)
- D. With the identity assurance level

**Answer: C**

**Explanation:**

Reference: <https://resources.infosecinstitute.com/cissp-domain-5-refresh-identity-and-access-management/>

**NEW QUESTION 476**

- (Exam Topic 14)

Which of the following would an internal technical security audit BEST validate?

- A. Whether managerial controls are in place
- B. Support for security programs by executive management

- C. Appropriate third-party system hardening
- D. Implementation of changes to a system

Answer: D

**NEW QUESTION 477**

- (Exam Topic 14)

Which of the following needs to be included in order for High Availability (HA) to continue operations during planned system outages?

- A. Redundant hardware, disk spanning, and patching
- B. Load balancing, power reserves, and disk spanning
- C. Backups, clustering, and power reserves
- D. Clustering, load balancing, and fault-tolerant options

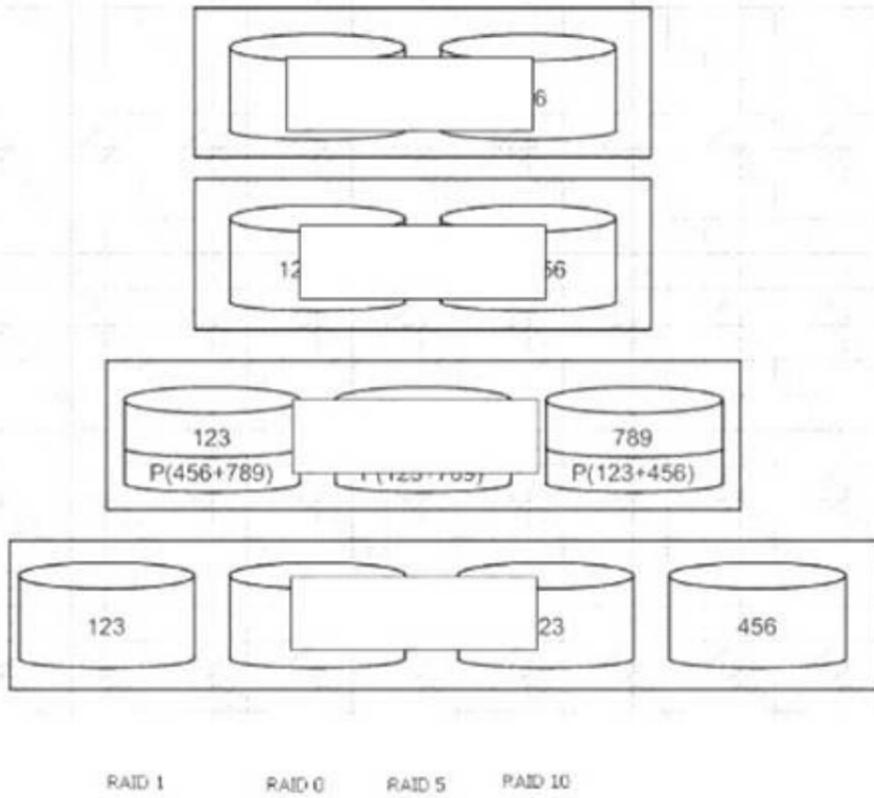
Answer: D

**NEW QUESTION 482**

- (Exam Topic 14)

Given a file containing ordered number, i.e. "123456789," match each of the following redundant Array of independent Disks (RAID) levels to the corresponding visual representation. Note: P() = parity.

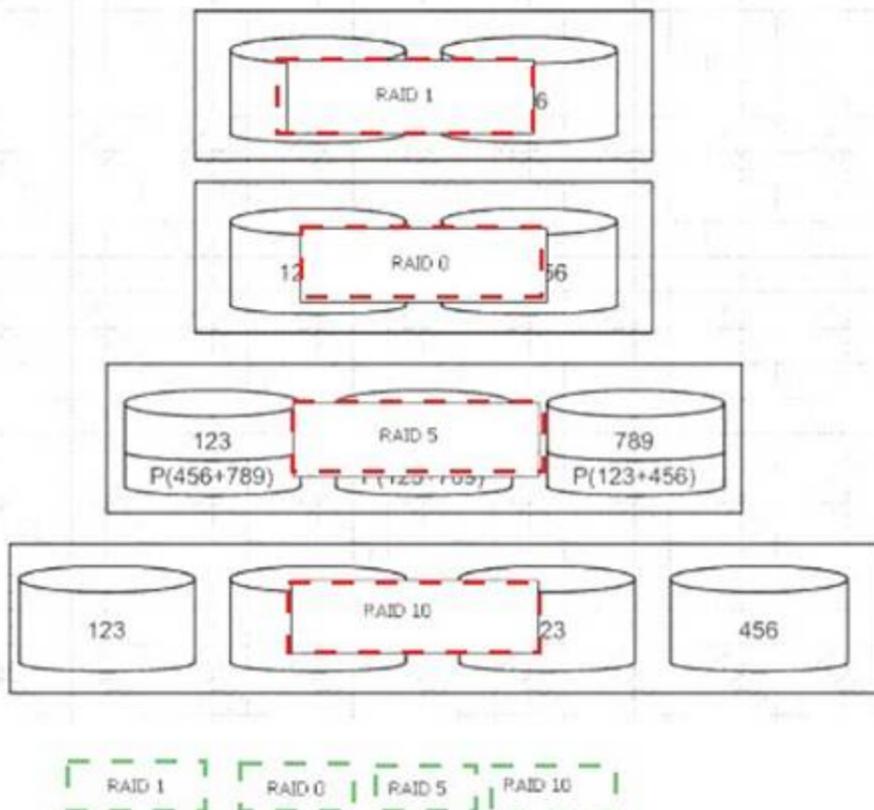
Drag each level to the appropriate place on the diagram.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



**NEW QUESTION 483**

- (Exam Topic 14)

Which of the following is the PRIMARY reason a sniffer operating on a network is collecting packets only from its own host?

- A. An Intrusion Detection System (IDS) has dropped the packets.
- B. The network is connected using switches.
- C. The network is connected using hubs.
- D. The network's firewall does not allow sniffing.

**Answer: A**

**NEW QUESTION 487**

- (Exam Topic 14)

What is the FIRST step required in establishing a records retention program?

- A. Identify and inventory all records.
- B. Identify and inventory all records storage locations
- C. Classify records based on sensitivity.
- D. Draft a records retention policy.

**Answer: D**

**NEW QUESTION 492**

- (Exam Topic 14)

Which type of fire alarm system sensor is intended to detect fire at its earliest stage?

- A. Ionization
- B. Infrared
- C. Thermal
- D. Photoelectric

**Answer: A**

**NEW QUESTION 495**

- (Exam Topic 14)

Which of the following security testing strategies is BEST suited for companies with low to moderate security maturity?

- A. Load Testing
- B. White-box testing
- C. Black -box testing
- D. Performance testing

**Answer: B**

**NEW QUESTION 498**

- (Exam Topic 14)

According to the Capability Maturity Model Integration (CMMI), which of the following levels is identified by a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines?

- A. Level 0: Incomplete
- B. Level 1: Performed
- C. Level 2: Managed
- D. Level 3: Defined

**Answer: D**

**NEW QUESTION 503**

- (Exam Topic 14)

Which of the following is the MOST important reason for timely installation of software patches?

- A. Attackers may be conducting network analysis.
- B. Patches are only available for a specific time.
- C. Attackers reverse engineer the exploit from the patch.
- D. Patches may not be compatible with proprietary software

**Answer: C**

**NEW QUESTION 506**

- (Exam Topic 14)

Utilizing a public wireless Local Area network (WLAN) to connect to a private network should be done only in which of the following situations?

- A. Extensible Authentication Protocol (EAP) is utilized to authenticate the user.
- B. The client machine has a personal firewall and utilizes a Virtual Private Network (VPN) to connect to the network.
- C. The client machine has antivirus software and has been seamed to determine if unauthorized ports are open.
- D. The wireless Access Point (AP) is placed in the internal private network.

Answer: A

**NEW QUESTION 508**

- (Exam Topic 14)

As users switch roles within an organization, their accounts are given additional permissions to perform the duties of their new position. After a recent audit, it was discovered that many of these accounts maintained their old permissions as well. The obsolete permissions identified by the audit have been remediated and accounts have only the appropriate permissions to complete their jobs.

Which of the following is the BEST way to prevent access privilege creep?

- A. Implementing Identity and Access Management (IAM) solution
- B. Time-based review and certification
- C. Internet audit
- D. Trigger-based review and certification

Answer: A

**NEW QUESTION 510**

- (Exam Topic 14)

What is the BEST way to correlate large volumes of disparate data sources in a Security Operations Center (SOC) environment?

- A. Implement Intrusion Detection System (IDS).
- B. Implement a Security Information and Event Management (SIEM) system.
- C. Hire a team of analysts to consolidate data and generate reports.
- D. Outsource the management of the SOC.

Answer: B

**NEW QUESTION 514**

- (Exam Topic 14)

Which of the following practices provides the development of security and identification of threats in designing software?

- A. Stakeholder review
- B. Requirements review
- C. Penetration testing
- D. Threat modeling

Answer: D

**NEW QUESTION 518**

- (Exam Topic 14)

Asymmetric algorithms are used for which of the following when using Secure Sockets Layer/Transport Layer Security (SSL/TLS) for implementing network security?

- A. Peer authentication
- B. Payload data encryption
- C. Session encryption
- D. Hashing digest

Answer: C

**NEW QUESTION 521**

- (Exam Topic 14)

Which of the following is a peer entity authentication method for Point-to-Point Protocol (PPP)?

- A. Challenge Handshake Authentication Protocol (CHAP)
- B. Message Authentication Code (MAC)
- C. Transport Layer Security (TLS) handshake protocol
- D. Challenge-response authentication mechanism

Answer: A

**NEW QUESTION 526**

- (Exam Topic 14)

Which of the following media is least problematic with data remanence?

- A. Magnetic disk
- B. Electrically Erasable Programming read-only Memory (EEPROM)
- C. Dynamic Random Access Memory (DRAM)
- D. Flash memory

Answer: C

**NEW QUESTION 528**

- (Exam Topic 14)

Which of the following will help identify the source internet protocol (IP) address of malware being executed on a computer?

- A. List of open network connections
- B. Display Transmission Control Protocol/Internet Protocol (TCP/IP) network configuration information.
- C. List of running processes
- D. Display the Address Resolution Protocol (ARP) table.

**Answer:** A

#### NEW QUESTION 530

- (Exam Topic 14)

Which of the following provides the GREATEST level of data security for a Virtual Private Network (VPN) connection?

- A. Internet Protocol Payload Compression (IPComp)
- B. Internet Protocol Security (IPSec)
- C. Extensible Authentication Protocol (EAP)
- D. Remote Authentication Dial-In User Service (RADIUS)

**Answer:** B

#### NEW QUESTION 534

- (Exam Topic 14)

Which of the following is the MOST important action regarding authentication?

- A. Granting access rights
- B. Enrolling in the system
- C. Establishing audit controls
- D. Obtaining executive authorization

**Answer:** B

#### NEW QUESTION 539

- (Exam Topic 14)

When can a security program be considered effective?

- A. Audits are rec/party performed and reviewed.
- B. Vulnerabilities are proactively identified.
- C. Risk is lowered to an acceptable level.
- D. Badges are regulatory performed and validated

**Answer:** C

#### NEW QUESTION 541

- (Exam Topic 14)

Directive controls are a form of change management policy and procedures. Which of the following subsections are recommended as part of the change management process?

- A. Build and test
- B. Implement security controls
- C. Categorize Information System (IS)
- D. Select security controls

**Answer:** A

#### Explanation:

Reference: <https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA570&lpg=PA570&dq=CISSP+Directive+cont>

#### NEW QUESTION 544

- (Exam Topic 14)

Which of the following is the PRIMARY security consideration for how an organization should handle Information Technology (IT) assets?

- A. The monetary value of the asset
- B. The controls implemented on the asset
- C. The physical form factor of the asset
- D. The classification of the data on the asset

**Answer:** D

#### NEW QUESTION 545

- (Exam Topic 14)

A security professional recommends that a company integrate threat modeling into its Agile development processes. Which of the following BEST describes the benefits of this approach?

- A. Reduce application development costs.
- B. Potential threats are addressed later in the Software Development Life Cycle (SDLC).
- C. Improve user acceptance of implemented security controls.
- D. Potential threats are addressed earlier in the Software Development Life Cycle (SDLC).

**Answer:**

D

**NEW QUESTION 548**

- (Exam Topic 14)

Which would result in the GREATEST impact following a breach to a cloud environment?

- A. The hypervisor host is poorly secured
- B. The same Logical Unit Number (LUN) is used for all VMs
- C. Insufficient network segregation
- D. Insufficient hardening of Virtual Machines (VM)

**Answer: C**

**NEW QUESTION 552**

- (Exam Topic 14)

Which of the following is the BEST way to protect against structured Query language (SQL) injection?

- A. Enforce boundary checking.
- B. Restrict use of SELECT command.
- C. Restrict Hyper Text Markup Language (HTML) source code access.
- D. Use stored procedures.

**Answer: D**

**NEW QUESTION 557**

- (Exam Topic 14)

When would an organization review a Business Continuity Management (BCM) system?

- A. When major changes occur on systems
- B. When personnel changes occur
- C. Before and after Disaster Recovery (DR) tests
- D. At planned intervals

**Answer: D**

**NEW QUESTION 561**

- (Exam Topic 14)

Which of the following is applicable to a publicly held company concerned about information handling and storage requirements specific to the financial reporting?

- A. Privacy Act of 1974
- B. Clinger-Cohan Act of 1996
- C. Sarbanes-Oxley (SOX) Act of 2002
- D. International Organization for Standardization (ISO) 27001

**Answer: C**

**NEW QUESTION 565**

- (Exam Topic 14)

Why is planning the MOST critical phase of a Role Based Access Control (RBAC) implementation?

- A. The criteria for measuring risk is defined.
- B. User populations to be assigned to each role is determined.
- C. Role mining to define common access patterns is performed.
- D. The foundational criteria are defined.

**Answer: B**

**NEW QUESTION 568**

- (Exam Topic 14)

Which of the following techniques is MOST useful when dealing with Advanced persistent Threat (APT) intrusions on live virtualized environments?

- A. Antivirus operations
- B. Reverse engineering
- C. Memory forensics
- D. Logfile analysis

**Answer: B**

**NEW QUESTION 571**

- (Exam Topic 14)

Which of the following will help prevent improper session handling?

- A. Ensure that all UIWebView calls do not execute without proper input validation.
- B. Ensure that tokens are sufficiently long, complex, and pseudo-random.
- C. Ensure JavaScript and plugin support is disabled.
- D. Ensure that certificates are valid and fail closed.

**Answer: B**

**NEW QUESTION 574**

- (Exam Topic 14)

A project requires the use of an authentication mechanism where playback must be protected and plaintext secret must be used. Which of the following should be used?

- A. Password Authentication Protocol (PAP)
- B. Extensible Authentication Protocol (EAP)
- C. Secure Hash Algorithm (SHA)
- D. Challenge Handshake Authentication Protocol (CHAP)

**Answer: A**

**NEW QUESTION 577**

- (Exam Topic 14)

Individual access to a network is BEST determined based on

- A. risk matrix.
- B. value of the data.
- C. business need.
- D. data classification.

**Answer: C**

**NEW QUESTION 578**

- (Exam Topic 14)

What is maintained by using write blocking devices when forensic evidence is examined?

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

**Answer: B**

**NEW QUESTION 580**

- (Exam Topic 14)

An Internet software application requires authentication before a user is permitted to utilize the resource. Which testing scenario BEST validates the functionality of the application?

- A. Reasonable data testing
- B. Input validation testing
- C. Web session testing
- D. Allowed data bounds and limits testing

**Answer: B**

**NEW QUESTION 585**

- (Exam Topic 14)

Which attack defines a piece of code that is inserted into software to trigger a malicious function?

- A. Phishing
- B. Salami
- C. Back door
- D. Logic bomb

**Answer: D**

**NEW QUESTION 589**

- (Exam Topic 14)

Which of the following was developed to support multiple protocols as well as provide login, password, and error correction capabilities?

- A. Challenge Handshake Authentication Protocol (CHAP)
- B. Point-to-Point Protocol (PPP)
- C. Password Authentication Protocol (PAP)
- D. Post Office Protocol (POP)

**Answer: A**

**NEW QUESTION 594**

- (Exam Topic 14)

Which inherent password weakness does a One Time Password (OTP) generator overcome?

- A. Static passwords must be changed frequently.

- B. Static passwords are too predictable.
- C. Static passwords are difficult to generate.
- D. Static passwords are easily disclosed.

**Answer:** D

**NEW QUESTION 598**

- (Exam Topic 14)

What is the PRIMARY objective for conducting an internal security audit?

- A. Verify that all systems and Standard Operating Procedures (SOP) are properly documented.
- B. Verify that all personnel supporting a system are knowledgeable of their responsibilities.
- C. Verify that security controls are established following best practices.
- D. Verify that applicable security controls are implemented and effective.

**Answer:** D

**NEW QUESTION 603**

- (Exam Topic 14)

In the common criteria (CC) for information technology (IT) security evaluation, increasing Evaluation Assurance Levels (EAL) results in which of the following?

- A. Increased functionality
- B. Increased interoperability
- C. Increase in resource requirement
- D. Increase in evaluated systems

**Answer:** B

**NEW QUESTION 608**

- (Exam Topic 14)

Which of the following is a common measure within a Local Area Network (LAN) to provide an additional level of security through segmentation?

- A. Building Virtual Local Area Networks (VLAN)
- B. Building Demilitarized Zones (DMZ)
- C. Implementing a virus scanner
- D. Implementing an Intrusion Detection System (IDS)

**Answer:** A

**NEW QUESTION 613**

- (Exam Topic 14)

A security professional should consider the protection of which of the following elements FIRST when developing a defense-in-depth strategy for a mobile workforce?

- A. Network perimeters
- B. Demilitarized Zones (DMZ)
- C. Databases and back-end servers
- D. End-user devices

**Answer:** D

**NEW QUESTION 617**

- (Exam Topic 14)

Which of the following is critical if an employee is dismissed due to violation of an organization's acceptable use policy (Aup) ?

- A. Appropriate documentation
- B. privilege suspension
- C. proxy records
- D. Internet access logs

**Answer:** A

**NEW QUESTION 621**

- (Exam Topic 14)

What determines the level of security of a combination lock?

- A. Complexity of combination required to open the lock
- B. Amount of time it takes to brute force the combination
- C. The number of barrels associated with the internal mechanism
- D. The hardness score of the metal lock material

**Answer:** A

**Explanation:**

Reference:

<https://books.google.com.pk/books?id=RbihG-YALUKC&pg=PA976&lpg=PA976&dq=CISSP+determines+the>

**NEW QUESTION 623**

- (Exam Topic 14)

Once the types of information have been identified, who should an information security practitioner work with to ensure that the information is properly categorized?

- A. Information Owner (IO)
- B. System Administrator
- C. Business Continuity (BC) Manager
- D. Chief Information Officer (CIO)

**Answer: A**

**NEW QUESTION 626**

- (Exam Topic 14)

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

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

**Answer: B**

**NEW QUESTION 631**

- (Exam Topic 13)

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

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

**Answer: A**

**NEW QUESTION 632**

- (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 633**

- (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 635**

- (Exam Topic 13)

From a security perspective, which of the following assumptions MUST be made about input to an application?

- A. It is tested
- B. It is logged
- C. It is verified
- D. It is untrusted

**Answer: D**

**NEW QUESTION 637**

- (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 640**

- (Exam Topic 13)

What is the MAIN reason for testing a Disaster Recovery Plan (DRP)?

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

**Answer:** B

**NEW QUESTION 641**

- (Exam Topic 13)

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

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

**Answer:** B

**Explanation:**

Section: Security Operations

**NEW QUESTION 643**

- (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 647**

- (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 652**

- (Exam Topic 13)

Which security access policy contains fixed security attributes that are used by the system to determine a user's access to a file or object?

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

**Answer:** A

**NEW QUESTION 655**

- (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 659**

- (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 662**

- (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 663**

- (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 668**

- (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 669**

- (Exam Topic 13)

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

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

**Answer: A**

**NEW QUESTION 671**

- (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 674**

- (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 678**

- (Exam Topic 13)

Which of the following is the BEST metric to obtain when gaining support for an Identify and Access Management (IAM) solution?

- A. Application connection successes resulting in data leakage
- B. Administrative costs for restoring systems after connection failure
- C. Employee system timeouts from implementing wrong limits
- D. Help desk costs required to support password reset requests

**Answer:** D

**NEW QUESTION 681**

- (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:** A

**NEW QUESTION 684**

- (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:** B

**Explanation:**

Section: Security Assessment and Testing

**NEW QUESTION 688**

- (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 692**

- (Exam Topic 13)

Which of the following is the MOST important part of an awareness and training plan to prepare employees for emergency situations?

- A. Having emergency contacts established for the general employee population to get information
- B. Conducting business continuity and disaster recovery training for those who have a direct role in the recovery
- C. Designing business continuity and disaster recovery training programs for different audiences
- D. Publishing a corporate business continuity and disaster recovery plan on the corporate website

**Answer:** C

**NEW QUESTION 693**

- (Exam Topic 13)

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

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

**Answer:** A

**NEW QUESTION 695**

- (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 697**

- (Exam Topic 13)

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

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

**Answer: C**

**NEW QUESTION 702**

- (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 706**

- (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 708**

- (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 709**

- (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 714**

- (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:**

C

**NEW QUESTION 718**

- (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 723**

- (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 725**

- (Exam Topic 13)

Which of the following is the GREATEST benefit of implementing a Role Based Access Control (RBAC) system?

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

**Answer: D**

**NEW QUESTION 729**

- (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 733**

- (Exam Topic 12)

What does the Maximum Tolerable Downtime (MTD) determine?

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

**Answer: C**

**NEW QUESTION 735**

- (Exam Topic 12)

Which of the following BEST describes a chosen plaintext attack?

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

**Answer: A**

**NEW QUESTION 738**

- (Exam Topic 12)

Backup information that is critical to the organization is identified through a

- A. Vulnerability Assessment (VA).
- B. Business Continuity Plan (BCP).
- C. Business Impact Analysis (BIA).
- D. data recovery analysis.

**Answer:** D

#### NEW QUESTION 742

- (Exam Topic 12)

The PRIMARY purpose of accreditation is to:

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

**Answer:** B

#### NEW QUESTION 747

- (Exam Topic 12)

What type of wireless network attack BEST describes an Electromagnetic Pulse (EMP) attack?

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

**Answer:** B

#### NEW QUESTION 748

- (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 752

- (Exam Topic 12)

From a cryptographic perspective, the service of non-repudiation includes which of the following features?

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

**Answer:** C

#### NEW QUESTION 756

- (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 761

- (Exam Topic 12)

What is a characteristic of Secure Socket Layer (SSL) and Transport Layer Security (TLS)?

- A. SSL and TLS provide a generic channel security mechanism on top of Transmission Control Protocol (TCP).
- B. SSL and TLS provide nonrepudiation by default.
- C. SSL and TLS do not provide security for most routed protocols.
- D. SSL and TLS provide header encapsulation over HyperText Transfer Protocol (HTTP).

**Answer:** A

#### NEW QUESTION 763

- (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 766**

- (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: B**

**NEW QUESTION 769**

- (Exam Topic 12)

Knowing the language in which an encrypted message was originally produced might help a cryptanalyst to perform a

- A. clear-text attack.
- B. known cipher attack.
- C. frequency analysis.
- D. stochastic assessment.

**Answer: C**

**NEW QUESTION 774**

- (Exam Topic 12)

An application developer is deciding on the amount of idle session time that the application allows before a timeout. The BEST reason for determining the session timeout requirement is

- A. organization policy.
- B. industry best practices.
- C. industry laws and regulations.
- D. management feedback.

**Answer: A**

**NEW QUESTION 777**

- (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 779**

- (Exam Topic 12)

How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

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

**Answer: C**

**NEW QUESTION 783**

- (Exam Topic 12)

A vulnerability in which of the following components would be MOST difficult to detect?

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

**Answer: C**

**NEW QUESTION 786**

- (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 790**

- (Exam Topic 12)

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

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

**Answer: A**

**NEW QUESTION 793**

- (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 795**

- (Exam Topic 12)

Which of the following is the MOST important consideration when developing a Disaster Recovery Plan (DRP)?

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

**Answer: C**

**NEW QUESTION 797**

- (Exam Topic 12)

When building a data classification scheme, which of the following is the PRIMARY concern?

- A. Purpose
- B. Cost effectiveness
- C. Availability
- D. Authenticity

**Answer: D**

**NEW QUESTION 800**

- (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 805**

- (Exam Topic 12)

Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

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

**Answer:**

C

**NEW QUESTION 807**

- (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 809**

- (Exam Topic 12)

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

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

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Mandatory Access Control – End user cannot set controls

Discretionary Access Control (DAC) – Subject has total control over objects

Role Based Access Control (RBAC) – Dynamically assigns roles permissions to particular duties based on job function

Rule Based access control – Dynamically assigns roles to subjects based on criteria assigned by a custodian.

**NEW QUESTION 813**

- (Exam Topic 12)

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

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

**Answer: C**

**NEW QUESTION 816**

- (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 821**

- (Exam Topic 11)

What is one way to mitigate the risk of security flaws in custom software?

- A. Include security language in the Earned Value Management (EVM) contract
- B. Include security assurance clauses in the Service Level Agreement (SLA)
- C. Purchase only Commercial Off-The-Shelf (COTS) products
- D. Purchase only software with no open source Application Programming Interfaces (APIs)

**Answer: B**

**NEW QUESTION 822**

- (Exam Topic 11)

Which of the following BEST avoids data remanence disclosure for cloud hosted resources?

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

**Answer: A**

**NEW QUESTION 825**

- (Exam Topic 11)

Which of the following has the GREATEST impact on an organization's security posture?

- A. International and country-specific compliance requirements
- B. Security violations by employees and contractors
- C. Resource constraints due to increasing costs of supporting security
- D. Audit findings related to employee access and permissions process

**Answer: A**

**NEW QUESTION 830**

- (Exam Topic 11)

What is the PRIMARY goal for using Domain Name System Security Extensions (DNSSEC) to sign records?

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

**Answer: A**

**NEW QUESTION 832**

- (Exam Topic 11)

Which of the following could elicit a Denial of Service (DoS) attack against a credential management system?

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

**Answer: B**

**NEW QUESTION 835**

- (Exam Topic 11)

Which of the following describes the BEST configuration management practice?

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

**Answer: D**

**NEW QUESTION 839**

- (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 841**

- (Exam Topic 11)

Which of the following entities is ultimately accountable for data remanence vulnerabilities with data replicated by a cloud service provider?

- A. Data owner
- B. Data steward
- C. Data custodian
- D. Data processor

Answer: A

**NEW QUESTION 842**

- (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 847**

- (Exam Topic 11)

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

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

Answer: C

**NEW QUESTION 848**

- (Exam Topic 11)

Application of which of the following Institute of Electrical and Electronics Engineers (IEEE) standards will prevent an unauthorized wireless device from being attached to a network?

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

Answer: D

**NEW QUESTION 851**

- (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 853**

- (Exam Topic 11)

Secure Sockets Layer (SSL) encryption protects

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

Answer: C

**NEW QUESTION 856**

- (Exam Topic 11)

The PRIMARY security concern for handheld devices is the

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

Answer: C

**NEW QUESTION 858**

- (Exam Topic 11)

Which of the following is the BEST example of weak management commitment to the protection of security assets and resources?

- A. poor governance over security processes and procedures

- B. immature security controls and procedures
- C. variances against regulatory requirements
- D. unanticipated increases in security incidents and threats

**Answer:** A

**NEW QUESTION 861**

- (Exam Topic 11)

Which of the following is the PRIMARY benefit of implementing data-in-use controls?

- A. If the data is lost, it must be decrypted to be opened.
- B. If the data is lost, it will not be accessible to unauthorized users.
- C. When the data is being viewed, it can only be printed by authorized users.
- D. When the data is being viewed, it must be accessed using secure protocols.

**Answer:** C

**NEW QUESTION 862**

- (Exam Topic 11)

What does an organization FIRST review to assure compliance with privacy requirements?

- A. Best practices
- B. Business objectives
- C. Legal and regulatory mandates
- D. Employee's compliance to policies and standards

**Answer:** C

**NEW QUESTION 865**

- (Exam Topic 11)

An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?

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

**Answer:** A

**NEW QUESTION 869**

- (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 871**

.....

## 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