# ISC2

## Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

**NEW QUESTION 1**
- (Exam Topic 15)
In addition to life, protection of which of the following elements is MOST important when planning a data center site?

A. Data and hardware
B. Property and operations
C. Profits and assets
D. Resources and reputation

**Answer:** D

**NEW QUESTION 2**
- (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 3**
- (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 4**
- (Exam Topic 15)
Which of the following virtual network configuration options is BEST to protect virtual machines (VM)?

A. Traffic filtering
B. Data encryption
C. Data segmentation
D. Traffic throttling

**Answer:** D

**NEW QUESTION 5**
- (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 6**
- (Exam Topic 15)
A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes. What is the
BEST design approach to securing this environment?

A. Place firewalls around critical devices, isolating them from the rest of the environment.
B. Layer multiple detective and preventative technologies at the environment perimeter.
C. Use reverse proxies to create a secondary "shadow" environment for critical systems.
D. Align risk across all interconnected elements to ensure critical threats are detected and handled.

**Answer:** B

**NEW QUESTION 7**
- (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 8**
- (Exam Topic 15)
A new employee formally reported suspicious behavior to the organization security team. The report claims that someone not affiliated with the organization was inquiring about the member's work location, length of employment, and building access controls. The employee's reporting is MOST likely the result of which of the following?

A. Risk avoidance
B. Security engineering
C. security awareness
D. Phishing

**Answer:** C

**NEW QUESTION 9**
- (Exam Topic 15)
Which of the following ensures old log data is not overwritten?

A. Increase log file size
B. Implement Syslog
C. Log preservation
D. Log retention

**Answer:** D

**NEW QUESTION 10**
- (Exam Topic 15)
When reviewing the security logs, the password shown for an administrative login event was ' OR ' '1'='1' --. This is an example of which of the following kinds of attack?

A. Brute Force Attack
B. Structured Query Language (SQL) Injection
C. Cross-Site Scripting (XSS)
D. Rainbow Table Attack

**Answer:** B

**NEW QUESTION 10**
- (Exam Topic 15)
What is the PRIMARY consideration when testing industrial control systems (ICS) for security weaknesses?

A. ICS often do not have availability requirements.
B. ICS are often isolated and difficult to access.
C. ICS often run on UNIX operating systems.
D. ICS are often sensitive to unexpected traffic.

**Answer:** B

**NEW QUESTION 15**
- (Exam Topic 15)
What is the MAIN purpose of conducting a business impact analysis (BIA)?

A. To determine the critical resources required to recover from an incident within a specified time period
B. To determine the effect of mission-critical information system failures on core business processes
C. To determine the cost for restoration of damaged information system
D. To determine the controls required to return to business critical operations

**Answer:** B

**NEW QUESTION 18**
- (Exam Topic 15)
Information security practitioners are in the midst of implementing a new firewall. Which of the following failure methods would BEST prioritize security in the event of failure?

A. Fail-Closed
B. Fail-Open
C. Fail-Safe
D. Failover

**Answer:** A

**NEW QUESTION 21**
- (Exam Topic 15)
Which of the following is the BEST way to protect against Structured Query language (SQL) injection?

A. Enforce boundary checking.
B. Ratfrict um of SELECT command.
C. Restrict HyperText Markup Language (HTML) source code
D. Use stored procedures.

**Answer:** D

**NEW QUESTION 24**
- (Exam Topic 15)
Which access control method is based on users issuing access requests on system resources, features assigned to those resources, the operational or situational context, and a set of policies specified in terms of those features and context?

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

**Answer:** B

**NEW QUESTION 27**
- (Exam Topic 15)
Which of the following uses the destination IP address to forward packets?

A. A bridge
B. A Layer 2 switch
C. A router
D. A repeater

**Answer:** C

**NEW QUESTION 28**
- (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 33**
- (Exam Topic 15)
Why is data classification control important to an organization?

A. To ensure its integrity, confidentiality and availability
B. To enable data discovery
C. To control data retention in alignment with organizational policies and regulation
D. To ensure security controls align with organizational risk appetite

**Answer:** A

**NEW QUESTION 38**
- (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 41**
- (Exam Topic 15)
A user is allowed to access the file labeled “Financial Forecast,” but only between 9:00 a.m. and 5:00 p.m., Monday through Friday. Which type of access mechanism should be used to accomplish this?

A. Minimum access control
B. Rule-based access control
C. Limited role-based access control (RBAC)

D. Access control list (ACL)

**Answer:** B

**NEW QUESTION 42**
- (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 45**
- (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 48**
- (Exam Topic 15)
Which of the following is an indicator that a company's new user security awareness training module has been effective?

A. There are more secure connections to the internal database servers.
B. More incidents of phishing attempts are being reported.
C. There are more secure connections to internal e-mail servers.
D. Fewer incidents of phishing attempts are being reported.

**Answer:** B

**NEW QUESTION 51**
- (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 54**
- (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 56**
- (Exam Topic 15)
Which of the following actions should be taken by a security professional when a mission critical computer network attack is suspected?

A. Isolate the network, log an independent report, fix the problem, and redeploy the computer.
B. Isolate the network, install patches, and report the occurrence.
C. Prioritize, report, and investigate the occurrence.
D. Turn the rooter off, perform forensic analysis, apply the appropriate fin, and log incidents.

**Answer:** C

**NEW QUESTION 58**
- (Exam Topic 15)

A. Require the cloud 1AM provider to use declarative security instead of programmatic authentication checks.
B. Integrate a Web-Application Firewall (WAF) In reverie-proxy mode in front of the service provider.
C. Apply Transport layer Security (TLS) to the cloud-based authentication checks.
D. Install an on-premise Authentication Gateway Service (AGS) In front of the service provider.

**Answer:** D

**NEW QUESTION 59**
- (Exam Topic 15)
The disaster recovery (DR) process should always include

A. plan maintenance.
B. periodic vendor review.
C. financial data analysis.
D. periodic inventory review.

**Answer:** A

**NEW QUESTION 63**
- (Exam Topic 15)
In supervisory control and data acquisition (SCADA) systems, which of the following controls can be used to reduce device exposure to malware?

A. Disable all command line interfaces.
B. Disallow untested code in the execution space of the SCADA device.
C. Prohibit the use of unsecure scripting languages.
D. Disable Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port 138 and 139 on the SCADA device.

**Answer:** B

**NEW QUESTION 67**
- (Exam Topic 15)
Which of the following services can be deployed via a cloud service or on-premises to integrate with Identity as a Service (IDaaS) as the authoritative source of user identities?

A. Directory
B. User database
C. Multi-factor authentication (MFA)
D. Single sign-on (SSO)

**Answer:** A

**NEW QUESTION 72**
- (Exam Topic 15)
A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

A. Omni
B. Directional
C. Yagi
D. Parabolic

**Answer:** A

**NEW QUESTION 77**
- (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 80**
- (Exam Topic 15)
Which of the following are mandatory canons for the (ISC)* Code of Ethics?

A. Develop comprehensive security strategies for the organization.
B. Perform is, honestly, fairly, responsibly, and lawfully for the organization.

C. Create secure data protection policies to principals.
D. Provide diligent and competent service to principals.

**Answer:** D

**NEW QUESTION 82**
- (Exam Topic 15)
Which of the following is MOST important to follow when developing information security controls for an organization?

A. Exercise due diligence with regard to all risk management information to tailor appropriate controls.
B. Perform a risk assessment and choose a standard that addresses existing gaps.
C. Use industry standard best practices for security controls in the organization.
D. Review all local and international standards and choose the most stringent based on location.

**Answer:** C

**NEW QUESTION 85**
- (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 88**
- (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 90**
- (Exam Topic 15)
In the last 15 years a company has experienced three electrical failures. The cost associated with each failure is listed below.
Which of the following would be a reasonable annual loss expectation?

| | |
|---|---|
| Availability | 60,000 |
| Integrity | 10,000 |
| Confidentiality | 0 |
| Total Impact | 70,000 |

A. 140,000
B. 3,500
C. 350,000
D. 14,000

**Answer:** B

**NEW QUESTION 94**
- (Exam Topic 15)
A security professional was tasked with rebuilding a company's wireless infrastructure. Which of the following are the MOST important factors to consider while making a decision on which wireless spectrum to deploy?

A. Hybrid frequency band, service set identifier (SSID), and interpolation
B. Performance, geographic location, and radio signal interference
C. Facility size, intermodulation, and direct satellite service
D. Existing client devices, manufacturer reputation, and electrical interference

**Answer:** D

**NEW QUESTION 98**
- (Exam Topic 15)
What is the MOST important criterion that needs to be adhered to during the data collection process of an active investigation?

A. Capturing an image of the system
B. Maintaining the chain of custody
C. Complying with the organization's security policy
D. Outlining all actions taken during the investigation

**Answer:** A

**NEW QUESTION 102**
- (Exam Topic 15)
Which of the following is the MOST effective countermeasure against data remanence?

A. Destruction
B. Clearing
C. Purging
D. Encryption

**Answer:** A

**NEW QUESTION 104**
- (Exam Topic 15)
What is the BEST way to restrict access to a file system on computing systems?

A. Allow a user group to restrict access.
B. Use a third-party tool to restrict access.
C. Use least privilege at each level to restrict access.
D. Restrict access to all users.

**Answer:** C

**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 110**
- (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 112**
- (Exam Topic 15)
Which of the following would qualify as an exception to the "right to be forgotten" of the General Data Protection Regulation's (GDPR)?

A. For the establishment, exercise, or defense of legal claims
B. The personal data has been lawfully processed and collected
C. The personal data remains necessary to the purpose for which it was collected
D. For the reasons of private interest

**Answer:** C

**NEW QUESTION 115**
- (Exam Topic 15)
A security professional should ensure that clients support which secondary algorithm for digital signatures when a Secure Multipurpose Internet Mail Extension (S/MIME) is used?

A. Triple Data Encryption Standard (3DES)
B. Advanced Encryption Standard (AES)
C. Digital Signature Algorithm (DSA)
D. Rivest-Shamir-Adieman (RSA)

**Answer:** C

**NEW QUESTION 117**
- (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 118**
- (Exam Topic 15)
The existence of physical barriers, card and personal identification number (PIN) access systems, cameras, alarms, and security guards BEST describes this security approach?

A. Security information and event management (SIEM)
B. Security perimeter
C. Defense-in-depth
D. Access control

**Answer:** B

**NEW QUESTION 123**
- (Exam Topic 15)
In software development, which of the following entities normally signs the code to protect the code integrity?

A. The organization developing the code
B. The quality control group
C. The data owner
D. The developer

**Answer:** B

**NEW QUESTION 127**
- (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 128**
- (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 133**
- (Exam Topic 15)
Using Address Space Layout Randomization (ASLR) reduces the potential for which of the following attacks?

A. SQL injection (SQLi)
B. Man-in-the-middle (MITM)
C. Cross-Site Scripting (XSS)
D. Heap overflow

**Answer:** D

**NEW QUESTION 134**
- (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 139**
- (Exam Topic 15)
When designing a new Voice over Internet Protocol (VoIP) network, an organization's top concern is preventing unauthorized users accessing the VoIP network. Which of the following will BEST help secure the VoIP network?

A. Transport Layer Security (TLS)
B. 802.1x
C. 802.119
D. Web application firewall (WAF)

**Answer:** A

**NEW QUESTION 140**
- (Exam Topic 15)
An organization is trying to secure instant messaging (IM) communications through its network perimeter. Which of the following is the MOST significant challenge?

A. IM clients can interoperate between multiple vendors.
B. IM clients can run without administrator privileges.
C. IM clients can utilize random port numbers.
D. IM clients can run as executable that do not require installation.

**Answer:** B

**NEW QUESTION 143**
- (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 147**
- (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 151**
- (Exam Topic 15)
What is the MOST important goal of conducting security assessments?

A. To prepare the organization for an external audit, particularly by a regulatory entity
B. To discover unmitigated security vulnerabilities, and propose paths for mitigating them
C. To align the security program with organizational risk appetite
D. To demonstrate proper function of security controls and processes to senior management

**Answer:** B

**NEW QUESTION 154**
- (Exam Topic 15)
A small office is running WiFi 4 APs, and neighboring offices do not want to increase the throughput to associated devices. Which of the following is the MOST cost-efficient way for the office to increase network performance?

A. Add another AP.
B. Disable the 2.4GHz radios
C. Enable channel bonding.
D. Upgrade to WiFi 5.

**Answer:** C

**NEW QUESTION 159**
- (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 163**
- (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 166**
- (Exam Topic 15)
Which of the following is MOST appropriate to collect evidence of a zero-day attack?

A. Firewall
B. Honeypot
C. Antispam
D. Antivirus

**Answer:** A

**NEW QUESTION 171**
- (Exam Topic 15)
What is the benefit of using Network Admission Control (NAC)?

A. Operating system (OS) versions can be validated prior to allowing network access.
B. NAC supports validation of the endpoint's security posture prior to allowing the session to go into an authorized state.
C. NAC can require the use of certificates, passwords, or a combination of both before allowing network admission.
D. NAC only supports Windows operating systems (OS).

**Answer:** C

**NEW QUESTION 175**
- (Exam Topic 15)
Which of the following is the PRIMARY issue when analyzing detailed log information?

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

**Answer:** D

**NEW QUESTION 180**
- (Exam Topic 15)
Which of the following outsourcing agreement provisions has the HIGHEST priority from a security operations perspective?

A. Conditions to prevent the use of subcontractors
B. Terms for contract renegotiation in case of disaster
C. Escalation process for problem resolution during incidents
D. Root cause analysis for application performance issue

**Answer:** D

**NEW QUESTION 184**
- (Exam Topic 15)
Which of the following will an organization's network vulnerability testing process BEST enhance?

A. Firewall log review processes
B. Asset management procedures
C. Server hardening processes
D. Code review procedures

**Answer:**

C

**NEW QUESTION 185**
- (Exam Topic 15)
Which of the following is the BEST way to protect privileged accounts?

A. Quarterly user access rights audits
B. Role-based access control (RBAC)
C. Written supervisory approval
D. Multi-factor authentication (MFA)

**Answer:** D

**NEW QUESTION 188**
- (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 193**
- (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 195**
- (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 198**
- (Exam Topic 15)
An organization is planning to have an it audit of its as a Service (SaaS) application to demonstrate to external parties that the security controls around availability are designed. The audit report must also cover a certain period of time to show the operational effectiveness of the controls. Which Service Organization Control (SOC) report would BEST fit their needs?

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

**Answer:** D

**NEW QUESTION 200**
- (Exam Topic 15)
Which of the following is required to verify the authenticity of a digitally signed document?

A. Digital hash of the signed document
B. Sender's private key
C. Recipient's public key
D. Agreed upon shared secret

**Answer:** A

**NEW QUESTION 205**
- (Exam Topic 15)
An organization has determined that its previous waterfall approach to software development is not keeping pace with business demands. To adapt to the rapid

changes required for product delivery, the organization has decided to move towards an Agile software development and release cycle. In order to ensure the success of the Agile methodology, who is MOST critical in creating acceptance tests or acceptance criteria for each release?

A. Project managers
B. Software developers
C. Independent testers
D. Business customers

**Answer:** D

**NEW QUESTION 207**
- (Exam Topic 15)
What documentation is produced FIRST when performing an effective physical loss control process?

A. Deterrent controls list
B. Security standards list
C. inventory list
D. Asset valuation list

**Answer:** C

**NEW QUESTION 211**
- (Exam Topic 15)
Which of the following would be the BEST mitigation practice for man-in-the-middle (MITM) Voice over Internet Protocol (VoIP) attacks?

A. Use Media Gateway Control Protocol (MGCP)
B. Use Transport Layer Security (TLS) protocol
C. Use File Transfer Protocol (FTP)
D. Use Secure Shell (SSH) protocol

**Answer:** B

**NEW QUESTION 214**
- (Exam Topic 15)
Within a large organization, what business unit is BEST positioned to initiate provisioning and deprovisioning of user accounts?

A. Training department
B. Internal audit
C. Human resources
D. Information technology (IT)

**Answer:** C

**NEW QUESTION 215**
- (Exam Topic 15)
Which of the following is considered the FIRST step when designing an internal security control assessment?

A. Create a plan based on recent vulnerability scans of the systems in question.
B. Create a plan based on comprehensive knowledge of known breaches.
C. Create a plan based on a recognized framework of known controls.
D. Create a plan based on reconnaissance of the organization's infrastructure.

**Answer:** D

**NEW QUESTION 220**
- (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 222**
- (Exam Topic 15)
Which of the following BEST describes the purpose of the reference monitor when defining access control to enforce the security model?

A. Quality design principles to ensure quality by design
B. Policies to validate organization rules
C. Cyber hygiene to ensure organizations can keep systems healthy
D. Strong operational security to keep unit members safe

**Answer:** B

**NEW QUESTION 227**
- (Exam Topic 15)
A company is enrolled in a hard drive reuse program where decommissioned equipment is sold back to the vendor when it is no longer needed. The vendor pays more money for functioning drives than equipment that is no longer operational. Which method of data sanitization would provide the most secure means of preventing unauthorized data loss, while also receiving the most money from the vendor?

A. Pinning
B. Single-pass wipe
C. Degaussing
D. Multi-pass wipes

**Answer:** C

**NEW QUESTION 231**
- (Exam Topic 15)
Which of the following explains why classifying data is an important step in performing a Risk assessment?

A. To provide a framework for developing good security metrics
B. To justify the selection of costly security controls
C. To classify the security controls sensitivity that helps scope the risk assessment
D. To help determine the appropriate level of data security controls

**Answer:** D

**NEW QUESTION 235**
- (Exam Topic 15)
According to the (ISC)? ethics canon “act honorably, honestly, justly, responsibly, and legally," which order should be used when resolving conflicts?

A. Public safety and duties to principals, individuals, and the profession
B. Individuals, the profession, and public safety and duties to principals
C. Individuals, public safety and duties to principals, and the profession
D. The profession, public safety and duties to principals, and individuals

**Answer:** A

**NEW QUESTION 236**
- (Exam Topic 15)
A software architect has been asked to build a platform to distribute music to thousands of users on a global scale. The architect has been reading about content delivery networks (CDN). Which of the following is a principal task to undertake?

A. Establish a service-oriented architecture (SOA).
B. Establish a media caching methodology.
C. Establish relationships with hundreds of Internet service providers (ISP).
D. Establish a low-latency wide area network (WAN).

**Answer:** B

**NEW QUESTION 240**
- (Exam Topic 15)
A hospital enforces the Code of Fair Information Practices. What practice applies to a patient requesting their medical records from a web portal?

A. Use limitation
B. Individual participation
C. Purpose specification
D. Collection limitation

**Answer:** D

**NEW QUESTION 241**
- (Exam Topic 15)
Upon commencement of an audit within an organization, which of the following actions is MOST important for the auditor(s) to take?

A. Understand circumstances which may delay the overall audit timelines.
B. Review all prior audit results to remove all areas of potential concern from the audit scope.
C. Meet with stakeholders to review methodology, people to be interviewed, and audit scope.
D. Meet with stakeholders to understand which types of audits have been completed.

**Answer:** C

**NEW QUESTION 243**
- (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 247**
- (Exam Topic 15)
The security team has been tasked with performing an interface test against a frontend external facing application and needs to verify that all input fields protect against
invalid input. Which of the following BEST assists this process?

A. Application fuzzing
B. Instruction set simulation
C. Regression testing
D. Sanity testing

**Answer:** A

**NEW QUESTION 250**
- (Exam Topic 15)
Which section of the assessment report addresses separate vulnerabilities, weaknesses, and gaps?

A. Key findings section
B. Executive summary with full details
C. Risk review section
D. Findings definition section

**Answer:** A

**NEW QUESTION 252**
- (Exam Topic 15)
What is the FIRST step in risk management?

A. Establish the expectations of stakeholder involvement.
B. Identify the factors that have potential to impact business.
C. Establish the scope and actions required.
D. Identify existing controls in the environment.

**Answer:** C

**NEW QUESTION 257**
- (Exam Topic 15)
A subscription service which provides power, climate control, raised flooring, and telephone wiring but NOT the computer and peripheral equipment is BEST described as a:

A. warm site.
B. reciprocal site.
C. sicold site.
D. hot site.

**Answer:** C

**NEW QUESTION 261**
- (Exam Topic 15)
Which of the following is a correct feature of a virtual local area network (VLAN)?

A. A VLAN segregates network traffic therefore information security is enhanced significantly.
B. Layer 3 routing is required to allow traffic from one VLAN to another.
C. VLAN has certain security features such as where the devices are physically connected.
D. There is no broadcast allowed within a single VLAN due to network segregation.

**Answer:** A

**NEW QUESTION 266**
- (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 269**
- (Exam Topic 15)
Which of the following factors is á PRIMARY reason to drive changes in an Information Security Continuous Monitoring (ISCM) strategy?

A. Testing and Evaluation (TE) personnel changes
B. Changes to core missions or business processes
C. Increased Cross-Site Request Forgery (CSRF) attacks
D. Changes in Service Organization Control (SOC) 2 reporting requirements

**Answer:** B

**NEW QUESTION 270**
- (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 272**
- (Exam Topic 15)
An organization is implementing security review as part of system development. Which of the following is the BEST technique to follow?

A. Engage a third-party auditing firm.
B. Review security architecture.
C. Perform incremental assessments.
D. Conduct penetration testing.

**Answer:** C

**NEW QUESTION 276**
- (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 at4 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 277**
- (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 exfilltrated.

**Answer:** A

**NEW QUESTION 281**
- (Exam Topic 15)
An organization wants to share data securely with their partners via the Internet. Which standard port is typically used to meet this requirement?

A. Setup a server on User Datagram Protocol (UDP) port 69
B. Setup a server on Transmission Control Protocol (TCP) port 21
C. Setup a server on Transmission Control Protocol (TCP) port 22
D. Setup a server on Transmission Control Protocol (TCP) port 80

**Answer:** C

**NEW QUESTION 284**
- (Exam Topic 15)
The security operations center (SOC) has received credible intelligence that a threat actor is planning to attack with multiple variants of a destructive virus. After obtaining a sample set of this virus’ variants and reverse engineering them to understand how they work, a commonality was found. All variants are coded to write to a specific memory location. It is determined this virus is of no threat to the organization because they had the focresight to enable what feature on all endpoints?

A. Process isolation
B. Trusted Platform Module (TPM)
C. Address Space Layout Randomization (ASLR)
D. Virtualization

**Answer:** C

**NEW QUESTION 289**
- (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 292**
- (Exam Topic 15)
A malicious user gains access to unprotected directories on a web server. Which of the following is MOST likely the cause for this information disclosure?

A. Security misconfiguration
B. Cross-site request forgery (CSRF)
C. Structured Query Language injection (SQLi)
D. Broken authentication management

**Answer:** A

**NEW QUESTION 296**
- (Exam Topic 15)
When auditing the Software Development Life Cycle (SDLC) which of the following is one of the high-level audit phases?

A. Requirements
B. Risk assessment
C. Due diligence
D. Planning

**Answer:** B

**NEW QUESTION 298**
- (Exam Topic 15)
A company is attempting to enhance the security of its user authentication processes. After evaluating several options, the company has decided to utilize Identity as a Service (IDaaS).
Which of the following factors leads the company to choose an IDaaS as their solution?

A. In-house development provides more control.
B. In-house team lacks resources to support an on-premise solution.
C. Third-party solutions are inherently more secure.
D. Third-party solutions are known for transferring the risk to the vendor.

**Answer:** B

**NEW QUESTION 303**
- (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 307**
- (Exam Topic 15)
Which evidence collecting technique would be utilized when it is believed an attacker is employing a rootkit and a quick analysis is needed?

A. Memory collection
B. Forensic disk imaging
C. Malware analysis
D. Live response

**Answer:** A

**NEW QUESTION 309**
- (Exam Topic 15)
Which of the following is a limitation of the Bell-LaPadula model?

A. Segregation of duties (SoD) is difficult to implement as the "no read-up" rule limits the ability of an object to access information with a higher classification.
B. Mandatory access control (MAC) is enforced at all levels making discretionary access control (DAC) impossible to implement.
C. It contains no provision or policy for changing data access control and works well only with access systems that are static in nature.
D. It prioritizes integrity over confidentiality which can lead to inadvertent information disclosure.

**Answer:** A

**NEW QUESTION 310**
- (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 312**
- (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 315**
- (Exam Topic 15)
Which of the following is the BEST option to reduce the network attack surface of a system?

A. Ensuring that there are no group accounts on the system
B. Removing unnecessary system user accounts
C. Disabling unnecessary ports and services
D. Uninstalling default software on the system

**Answer:** C

**NEW QUESTION 320**
- (Exam Topic 15)
a large organization uses biometrics to allow access to its facilities. It adjusts the biometric value for incorrectly granting or denying access so that the two numbers are the same.
What is this value called?

A. False Rejection Rate (FRR)
B. Accuracy acceptance threshold
C. Equal error rate
D. False Acceptance Rate (FAR)

**Answer:** C

**NEW QUESTION 322**
- (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 326**
- (Exam Topic 15)
An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch. Which of the following command-line tools should the technician use to determine where the incident is occurring?

A. nslookup
B. show config
C. netstat
D. show interface
E. show counters

**Answer:** D

**NEW QUESTION 331**

- (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 334**
- (Exam Topic 15)
An organization purchased a commercial off-the-shelf (COTS) software several years ago. The information technology (IT) Director has decided to migrate the application into the cloud, but is concerned about the application security of the software in the organization's dedicated environment with a cloud service provider. What is the BEST way to prevent and correct the software's security weal

A. Implement a dedicated COTS sandbox environment
B. Follow the software end-of-life schedule
C. Transfer the risk to the cloud service provider
D. Examine the software updating and patching process

**Answer:** A

**NEW QUESTION 339**
- (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 341**
- (Exam Topic 15)
Which of the following protocols will allow the encrypted transfer of content on the Internet?

A. Server Message Block (SMB)
B. Secure copy
C. Hypertext Transfer Protocol (HTTP)
D. Remote copy

**Answer:** B

**NEW QUESTION 344**
- (Exam Topic 15)
Which of the following is considered the PRIMARY security issue associated with encrypted e-mail messages?

A. Key distribution
B. Storing attachments in centralized repositories
C. Scanning for viruses and other malware
D. Greater costs associated for backups and restores

**Answer:** C

**NEW QUESTION 349**
- (Exam Topic 15)
Which of the following vulnerabilities can be BEST detected using automated analysis?

A. Valid cross-site request forgery (CSRF) vulnerabilities
B. Multi-step process attack vulnerabilities
C. Business logic flaw vulnerabilities
D. Typical source code vulnerabilities

**Answer:** D

**NEW QUESTION 353**
- (Exam Topic 15)
What term is commonly used to describe hardware and software assets that are stored in a configuration management database (CMDB)?

A. Configuration element
B. Asset register
C. Ledger item
D. Configuration item

**Answer:** D

**NEW QUESTION 354**
- (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 356**
- (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 357**
- (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 359**
- (Exam Topic 15)
A manager identified two conflicting sensitive user functions that were assigned to a single user account that had the potential to result in financial and regulatory risk to the company. The manager MOST likely discovered this during which of the following?

A. Security control assessment.
B. Separation of duties analysis
C. Network Access Control (NAC) review
D. Federated identity management (FIM) evaluation

**Answer:** B

**NEW QUESTION 361**
- (Exam Topic 15)
Which is the BEST control to meet the Statement on Standards for Attestation Engagements 18 (SSAE-18) confidentiality category?

A. Data processing
B. Storage encryption
C. File hashing
D. Data retention policy

**Answer:** C

**NEW QUESTION 362**
- (Exam Topic 15)
Assuming an individual has taken all of the steps to keep their internet connection private, which of the following is the BEST to browse the web privately?

A. Prevent information about browsing activities from being stored in the cloud.
B. Store browsing activities in the cloud.
C. Prevent information about browsing activities farm being stored on the personal device.
D. Store information about browsing activities on the personal device.

**Answer:** A

**NEW QUESTION 363**
- (Exam Topic 15)
Which of the following is the FIRST requirement a data owner should consider before implementing a data retention policy?

A. Training
B. Legal
C. Business
D. Storage

**Answer:** B

**NEW QUESTION 366**
- (Exam Topic 15)
A Certified Information Systems Security Professional (CISSP) with identity and access management (IAM) responsibilities is asked by the Chief Information Security Officer (CISO) to4 perform a vulnerability assessment on a web application to pass a Payment Card Industry (PCI) audit. The CISSP has never performed this before. According to the (ISC)? Code of Professional Ethics, which of the following should the CISSP do?

A. Review the CISSP guidelines for performing a vulnerability assessment before proceeding to complete it
B. Review the PCI requirements before performing the vulnerability assessment
C. Inform the CISO that they are unable to perform the task because they should render only those services for which they are fully competent and qualified
D. Since they are CISSP certified, they have enough knowledge to assist with the request, but will need assistance in order to complete it in a timely manner

**Answer:** C

**NEW QUESTION 369**
- (Exam Topic 15)
The security team is notified that a device on the network is infected with malware. Which of the following is MOST effective in enabling the device to be quickly located and remediated?

A. Data loss protection (DLP)
B. Intrusion detection
C. Vulnerability scanner
D. Information Technology Asset Management (ITAM)

**Answer:** D

**NEW QUESTION 371**
- (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 372**
- (Exam Topic 15)
Why are packet filtering routers used in low-risk environments?

A. They are high-resolution source discrimination and identification tools.
B. They are fast and flexible, and protect against Internet Protocol (IP) spoofing.
C. They are fast, flexible, and transparent.
D. They enforce strong user authentication and audit tog generation.

**Answer:** B

**NEW QUESTION 377**
- (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 379**
- (Exam Topic 15)
Which of the following describes the BEST method of maintaining the inventory of software and hardware within the organization?

A. Maintaining the inventory through a combination of desktop configuration, administration management, and procurement management tools
B. Maintaining the inventory through a combination of asset owner interviews, open-source system management, and open-source management tools
C. Maintaining the inventory through a combination of on-premise storage configuration, cloud management, and partner management tools
D. Maintaining the inventory through a combination of system configuration, network management, and license management tools

**Answer:** C

**NEW QUESTION 384**
- (Exam Topic 15)
What is the FIRST step prior to executing a test of an organisation’s disaster recovery (DR) or business continuity plan (BCP)?

A. identify key stakeholders,
B. Develop recommendations for disaster scenarios.
C. Identify potential failure points.
D. Develop clear evaluation criteria.

**Answer:** D

**NEW QUESTION 389**
- (Exam Topic 15)
The Chief Information Security Officer (CISO) of an organization has requested that a Service Organization Control (SOC) report be created to outline the security and availability of a
particular system over a 12-month period. Which type of SOC report should be utilized?

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

**Answer:** C

**NEW QUESTION 390**
- (Exam Topic 15)
Which algorithm gets its security from the difficulty of calculating discrete logarithms in a finite field and is used to distribute keys, but cannot be used to encrypt or decrypt messages?

A. Diffie-Hellman
B. Digital Signature Algorithm (DSA)
C. Rivest-Shamir-Adleman (RSA)
D. Kerberos

**Answer:** C

**NEW QUESTION 395**
- (Exam Topic 15)
employee training, risk management, and data handling procedures and policies could be characterized as which type of security measure?

A. Non-essential
B. Management
C. Preventative
D. Administrative

**Answer:** D

**NEW QUESTION 397**
- (Exam Topic 15)
What is the BEST design for securing physical perimeter protection?

A. Crime Prevention through Environmental Design (CPTED)
B. Barriers, fences, gates, and walls
C. Business continuity planning (BCP)
D. Closed-circuit television (CCTV)

**Answer:** B

**NEW QUESTION 399**
- (Exam Topic 15)
What is a security concern when considering implementing software-defined networking (SDN)?

A. It increases the attack footprint.
B. It uses open source protocols.
C. It has a decentralized architecture.
D. It is cloud based.

**Answer:** C

**NEW QUESTION 403**
- (Exam Topic 15)
An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex. Which of the following is the MOST likely cause of this issue?

A. The link is improperly terminated
B. One of the devices is misconfigured
C. The cable length is excessive.
D. One of the devices has a hardware issue.

**Answer:** A

**NEW QUESTION 406**
- (Exam Topic 15)
Which of the following VPN configurations should be used to separate Internet and corporate traffic?

A. Split-tunnel
B. Remote desktop gateway
C. Site-to-site
D. Out-of-band management

**Answer:** A

**NEW QUESTION 407**
- (Exam Topic 15)
Which of the following techniques evaluates the secure Bet principles of network or software architectures?

A. Threat modeling
B. Risk modeling
C. Waterfall method
D. Fuzzing

**Answer:** A

**NEW QUESTION 408**
- (Exam Topic 15)
Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

A. Centralized network provisioning
B. Centralized network administrator control
C. Reduced network latency when scaled
D. Reduced hardware footprint and cost

**Answer:** B

**NEW QUESTION 412**
- (Exam Topic 15)
Which media sanitization methods should be used for data with a high security categorization?

A. Clear or destroy
B. Clear or purge
C. Destroy or delete
D. Purge or destroy

**Answer:** D

**NEW QUESTION 415**
- (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 418**
- (Exam Topic 15)
Which of the following protection is provided when using a Virtual Private Network (VPN) with Authentication Header (AH)?

A. Payload encryption
B. Sender confidentiality
C. Sender non-repudiation
D. Multi-factor authentication (MFA)

**Answer:** C

**NEW QUESTION 420**
- (Exam Topic 15)
An organization outgrew its internal data center and is evaluating third-party hosting facilities. In this evaluation, which of the following is a PRIMARY factor for selection?

A. Facility provides an acceptable level of risk
B. Facility provides disaster recovery (DR) services
C. Facility provides the most cost-effective solution
D. Facility has physical access protection measures

**Answer:**

C

**NEW QUESTION 424**
- (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 428**
- (Exam Topic 15)
What is the HIGHEST priority in agile development?

A. Selecting appropriate coding language
B. Managing costs of product delivery
C. Early and continuous delivery of software
D. Maximizing the amount of code delivered

**Answer:** C

**NEW QUESTION 429**
- (Exam Topic 15)
Which of the following contributes MOST to the effectiveness of a security officer?

A. Understanding the regulatory environment
B. Developing precise and practical security plans
C. Integrating security into the business strategies
D. Analyzing the strengths and weakness of the organization

**Answer:** A

**NEW QUESTION 434**
- (Exam Topic 15)
During testing, where are the requirements to inform parent organizations, law enforcement, and a computer incident response team documented?

A. Unit test results
B. Security assessment plan
C. System integration plan
D. Security Assessment Report (SAR)

**Answer:** D

**NEW QUESTION 437**
- (Exam Topic 15)
Which of the following is a covert channel type?

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

**Answer:** A

**NEW QUESTION 440**
- (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 441**
- (Exam Topic 15)
A hospital’s building controls system monitors and operates the environmental equipment to maintain a safe and comfortable environment. Which of the following could be
used to minimize the risk of utility supply interruption?

A. Digital devices that can turn equipment off and continuously cycle rapidly in order to increase supplies and conceal activity on the hospital network
B. Standardized building controls system software with high connectivity to hospital networks

C. Lock out maintenance personnel from the building controls system access that can impact critical utility supplies
D. Digital protection and control devices capable of minimizing the adverse impact to critical utility

**Answer:** D

**NEW QUESTION 442**
- (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 447**
- (Exam Topic 15)
What is the MOST appropriate hierarchy of documents when implementing a security program?

A. Organization principle, policy, standard, guideline
B. Policy, organization principle, standard, guideline
C. Standard, policy, organization principle, guideline
D. Organization principle, guideline, policy, standard

**Answer:** C

**NEW QUESTION 452**
- (Exam Topic 15)
Which of the following is a risk matrix?

A. A database of risks associated with a specific information system.
B. A table of risk management factors for management to consider.
C. A two-dimensional picture of risk for organizations, products, projects, or other items of interest.
D. A tool for determining risk management decisions for an activity or system.

**Answer:** C

**NEW QUESTION 453**
- (Exam Topic 15)
What is the FIRST step in reducing the exposure of a network to Internet Control Message Protocol (ICMP) based attacks?

A. Implement egress filtering at the organization's network boundary.
B. Implement network access control lists (ACL).
C. Implement a web application firewall (WAF).
D. Implement an intrusion prevention system (IPS).

**Answer:** B

**NEW QUESTION 458**
- (Exam Topic 15)
When MUST an organization's information security strategic plan be reviewed?

A. Quarterly, when the organization's strategic plan is updated
B. Whenever there are significant changes to a major application
C. Every three years, when the organization's strategic plan is updated
D. Whenever there are major changes to the business

**Answer:** D

**NEW QUESTION 460**
- (Exam Topic 15)
To comply with industry requirements, a security assessment on the cloud server should identify which protocols and weaknesses are being exposed to attackers on the Internet.
Which of the following tools is the MOST appropriate to complete the assessment?

A. Use tcpdump and parse the output file in a protocol analyzer.
B. Use an IP scanner and target the cloud WAN network addressing
C. Run netstat in each cloud server and retrieve the running processes.
D. Use nmap and set the servers' public IPs as the target

**Answer:** D

**NEW QUESTION 464**
- (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. Time separation
B. Trusted Computing Base (TCB)
C. Reference monitor
D. Security kernel

**Answer:** D

**NEW QUESTION 468**
- (Exam Topic 15)
How should the retention period for an organization's social media content be defined?

A. Wireless Access Points (AP)
B. Token-based authentication
C. Host-based firewalls
D. Trusted platforms

**Answer:** C

**NEW QUESTION 472**
- (Exam Topic 15)
What is the BEST approach to anonymizing personally identifiable information (PII) in a test environment?

A. Randomizing data
B. Swapping data
C. Encrypting data
D. Encoding data

**Answer:** C

**NEW QUESTION 476**
- (Exam Topic 15)
What are the three key benefits that application developers should derive from the northbound application programming interface (API) of software defined networking (SDN)?

A. Familiar syntax, abstraction of network topology, and definition of network protocols
B. Network syntax, abstraction of network flow, and abstraction of network protocols
C. Network syntax, abstraction of network commands, and abstraction of network protocols
D. Familiar syntax, abstraction of network topology, and abstraction of network protocols

**Answer:** C

**NEW QUESTION 477**
- (Exam Topic 15)
A healthcare insurance organization chose a vendor to develop a software application. Upon review of the draft contract, the information security professional notices that software security is not addressed. What is the BEST approach to address the issue?

A. Update the service level agreement (SLA) to provide the organization the right to audit the vendor.
B. Update the service level agreement (SLA) to require the vendor to provide security capabilities.
C. Update the contract so that the vendor is obligated to provide security capabilities.
D. Update the contract to require the vendor to perform security code reviews.

**Answer:** C

**NEW QUESTION 482**
- (Exam Topic 15)
In an IDEAL encryption system, who has sole access to the decryption key?

A. System owner
B. Data owner
C. Data custodian
D. System administrator

**Answer:** B

**NEW QUESTION 483**
- (Exam Topic 15)
Which security audit standard provides the BEST way for an organization to understand a vendor's Information Systems (IS) in relation to confidentiality, integrity, and availability?

A. Statement on Auditing Standards (SAS) 70
B. Service Organization Control (SOC) 2
C. Service Organization Control (SOC) 1
D. Statement on Standards for Attestation Engagements (SSAE) 18

**Answer:** B

**NEW QUESTION 486**
- (Exam Topic 15)
Which of the following is the BEST method to validate secure coding techniques against injection and overflow attacks?

A. Scheduled team review of coding style and techniques for vulnerability patterns
B. Using automated programs to test for the latest known vulnerability patterns
C. The regular use of production code routines from similar applications already in use
D. Ensure code editing tools are updated against known vulnerability patterns

**Answer:** B

**NEW QUESTION 487**
- (Exam Topic 15)
Which of the following is the MAIN benefit of off-site storage?

A. Cost effectiveness
B. Backup simplicity
C. Fast recovery
D. Data availability

**Answer:** A

**NEW QUESTION 491**
- (Exam Topic 14)
Which of the following is the BEST technique to facilitate secure software development?

A. Adhere to secure coding practices for the software application under development.
B. Conduct penetrating testing for the software application under development.
C. Develop a threat modeling review for the software application under development.
D. Perform a code review process for the software application under development.

**Answer:** A

**NEW QUESTION 494**
- (Exam Topic 14)
Which of the following entails identification of data end links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

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

**Answer:** A

**NEW QUESTION 496**
- (Exam Topic 14)
What is a warn site when conducting Business continuity planning (BCP)

A. A location, other than the normal facility, used to process data on a daily basis
B. An area partially equipped with equipment and resources to recover business functions
C. A place void of any resources or equipment except air conditioning and raised flooring
D. An alternate facility that allows for Immediate cutover to enable continuation of business functions

**Answer:** B

**NEW QUESTION 501**
- (Exam Topic 14)
Activity to baseline, tailor, and scope security controls tikes place dring which National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) step?

A. Authorize IS.
B. Assess security controls.
C. Categorize Information system (IS).
D. Select security controls.

**Answer:** D

**NEW QUESTION 505**
- (Exam Topic 14)
What protocol is often used between gateway hosts on the Internet' To control the scope of a Business Continuity Management (BCM) system, a security practitioner should identify which of the following?

A. Size, nature, and complexity of the organization
B. Business needs of the security organization
C. All possible risks

D. Adaptation model for future recovery planning

**Answer:** B

**NEW QUESTION 507**
- (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 512**
- (Exam Topic 14)
An organization has implemented a new backup process which protects confidential data by encrypting the information stored on backup tapes. Which of the following is a MAJOR data confidentiality concern after the implementation of this new backup process?

A. Tape backup rotation
B. Pre-existing backup tapes
C. Tape backup compression
D. Backup tape storage location

**Answer:** D

**NEW QUESTION 514**
- (Exam Topic 14)
For the purpose of classification, which of the following is used to divide trust domain and trust boundaries?

A. Network architecture
B. Integrity
C. Identity Management (IdM)
D. Confidentiality management

**Answer:** A

**NEW QUESTION 519**
- (Exam Topic 14)
What access control scheme uses fine-grained rules to specify the conditions under which access to each data item or applications is granted?

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

**Answer:** D

**Explanation:**
Reference: https://en.wikipedia.org/wiki/Attribute-based_access_control

**NEW QUESTION 520**
- (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 521**
- (Exam Topic 14)
Which of the following encryption types is used in Hash Message Authentication Code (HMAC) for key distribution?

A. Symmetric
B. Asymmetric
C. Ephemeral
D. Permanent

**Answer:** A

**Explanation:**
Reference: https://www.brainscape.com/flashcards/cryptography-message-integrity-6886698/packs/10957693

**NEW QUESTION 525**
- (Exam Topic 14)
A corporate security policy specifies that all devices on the network must have updated operating system patches and anti-malware software. Which technology should be used to enforce this policy?

A. Network Address Translation (NAT)
B. Stateful Inspection
C. Packet filtering
D. Network Access Control (NAC)

**Answer:** D

**NEW QUESTION 529**
- (Exam Topic 14)
Which of the following is the GREATEST security risk associated with the user of identity as a service (IDaaS) when an organization its own software?

A. Incompatibility with Federated Identity Management (FIM)
B. Increased likelihood of confidentiality breach
C. Denial of access due to reduced availability
D. Security Assertion Markup Language (SAM) integration

**Answer:** B

**NEW QUESTION 532**
- (Exam Topic 14)
Which of the following is mobile device remote fingerprinting?

A. Installing an application to retrieve common characteristics of the device
B. Storing information about a remote device in a cookie file
C. Identifying a device based on common characteristics shared by all devices of a certain type
D. Retrieving the serial number of the mobile device

**Answer:** C

**NEW QUESTION 537**
- (Exam Topic 14)
An organization has a short-term agreement with a public Cloud Service Provider (CSP). Which of the following BEST protects sensitive data once the agreement expires and the assets are reused?

A. Recommended that the business data owners use continuous monitoring and analysis of applications to prevent data loss.
B. Recommend that the business data owners use internal encryption keys for data-at-rest and data-in-transit to the storage environment.
C. Use a contractual agreement to ensure the CSP wipes the data from the storage environment.
D. Use a National Institute of Standards and Technology (NIST) recommendation for wiping data on the storage environment.

**Answer:** C

**NEW QUESTION 538**
- (Exam Topic 14)
What is the PRIMARY purpose for an organization to conduct a security audit?

A. To ensure the organization is adhering to a well-defined standard
B. To ensure the organization is applying security controls to mitigate identified risks
C. To ensure the organization is configuring information systems efficiently
D. To ensure the organization is documenting findings

**Answer:** A

**NEW QUESTION 543**
- (Exam Topic 14)
Which of the following will have the MOST influence on the definition and creation of data classification and data ownership policies?

A. Data access control policies
B. Threat modeling
C. Common Criteria (CC)
D. Business Impact Analysis (BIA)

**Answer:** A

**NEW QUESTION 547**
- (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 551**
- (Exam Topic 14)
Which of the following is the BEST definition of Cross-Site Request Forgery (CSRF)?

A. An attack which forces an end user to execute unwanted actions on a web application in which they are currently authenticated
B. An attack that injects a script into a web page to execute a privileged command
C. An attack that makes an illegal request across security zones and thereby forges itself into the security database of the system
D. An attack that forges a false Structure Query Language (SQL) command across systems

**Answer:** A

**Explanation:**
Reference: https://portswigger.net/web-security/csrf

**NEW QUESTION 554**
- (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 559**
- (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 563**
- (Exam Topic 14)
What is the BEST approach for maintaining ethics when a security professional is unfamiliar with the culture of a country and is asked to perform a questionable task?

A. Exercise due diligence when deciding to circumvent host government requests.
B. Become familiar with the means in which the code of ethics is applied and considered.
C. Complete the assignment based on the customer's wishes.
D. Execute according to the professional's comfort level with the code of ethics.

**Answer:** B

**NEW QUESTION 564**
- (Exam Topic 14)
Which layer of the Open system Interconnect (OSI) model is responsible for secure data transfer between applications, flow control, and error detection and correction?

A. Layer 2
B. Layer 4
C. Layer 5
D. Layer 6

**Answer:** B

**NEW QUESTION 567**
- (Exam Topic 14)
Who determines the required level of independence for security control Assessors (SCA)?

A. Business owner
B. Authorizing Official (AO)
C. Chief Information Security Officer (CISC)
D. System owner

**Answer:** B

**NEW QUESTION 572**
- (Exam Topic 14)
Which of the following is considered the last line defense in regard to a Governance, Risk managements, and compliance (GRC) program?

A. Internal audit
B. Internal controls
C. Board review
D. Risk management

**Answer:** B

**NEW QUESTION 576**
- (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 577**
- (Exam Topic 14)
Which layer handle packet fragmentation and reassembly in the Open system interconnection (OSI) Reference model?

A. Session
B. Transport
C. Data Link
D. Network

**Answer:** B

**NEW QUESTION 580**
- (Exam Topic 14)
An organization is outsourcing its payroll system and is requesting to conduct a full audit on the third-party information technology (IT) systems. During the due diligence process, the third party provides previous audit report on its IT system.
Which of the following MUST be considered by the organization in order for the audit reports to be acceptable?

A. The audit assessment has been conducted by an independent assessor.
B. The audit reports have been signed by the third-party senior management.
C. The audit reports have been issued in the last six months.
D. The audit assessment has been conducted by an international audit firm.

**Answer:** A

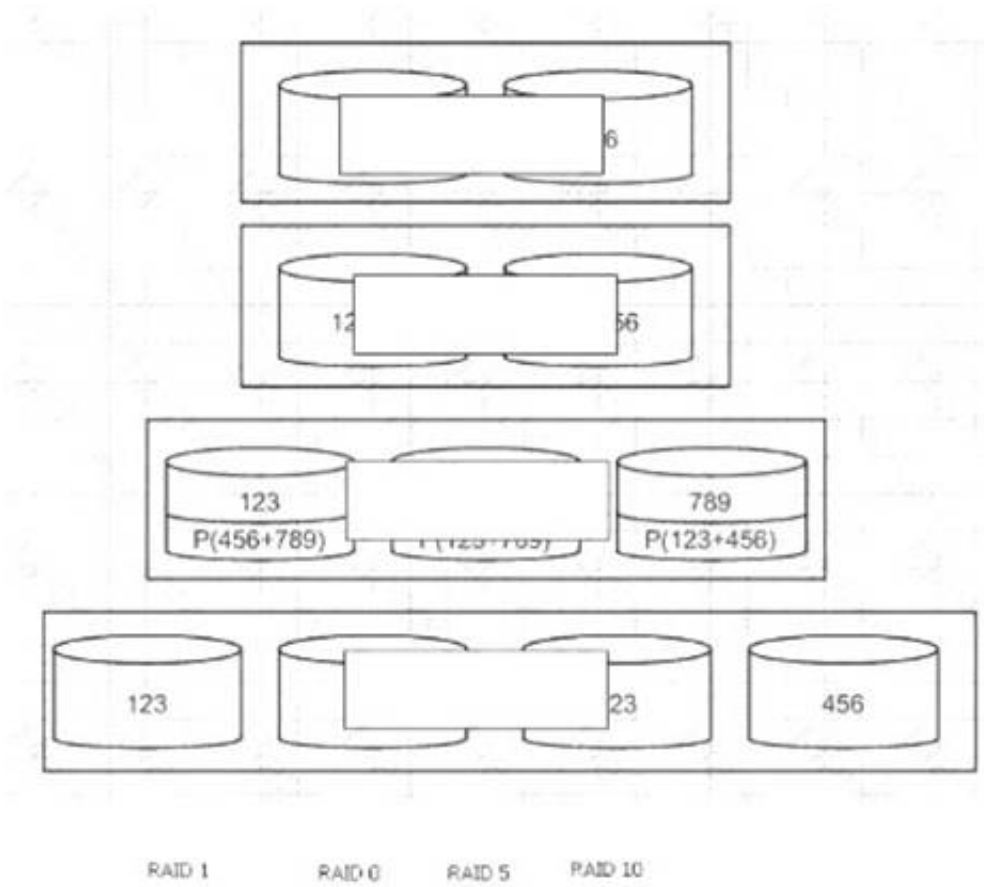
**NEW QUESTION 585**
- (Exam Topic 14)
Which of the following is a process in the access provisioning lifecycle that will MOST likely identify access aggregation issues?

A. Test
B. Assessment
C. Review
D. Peer review

**Answer:** C

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

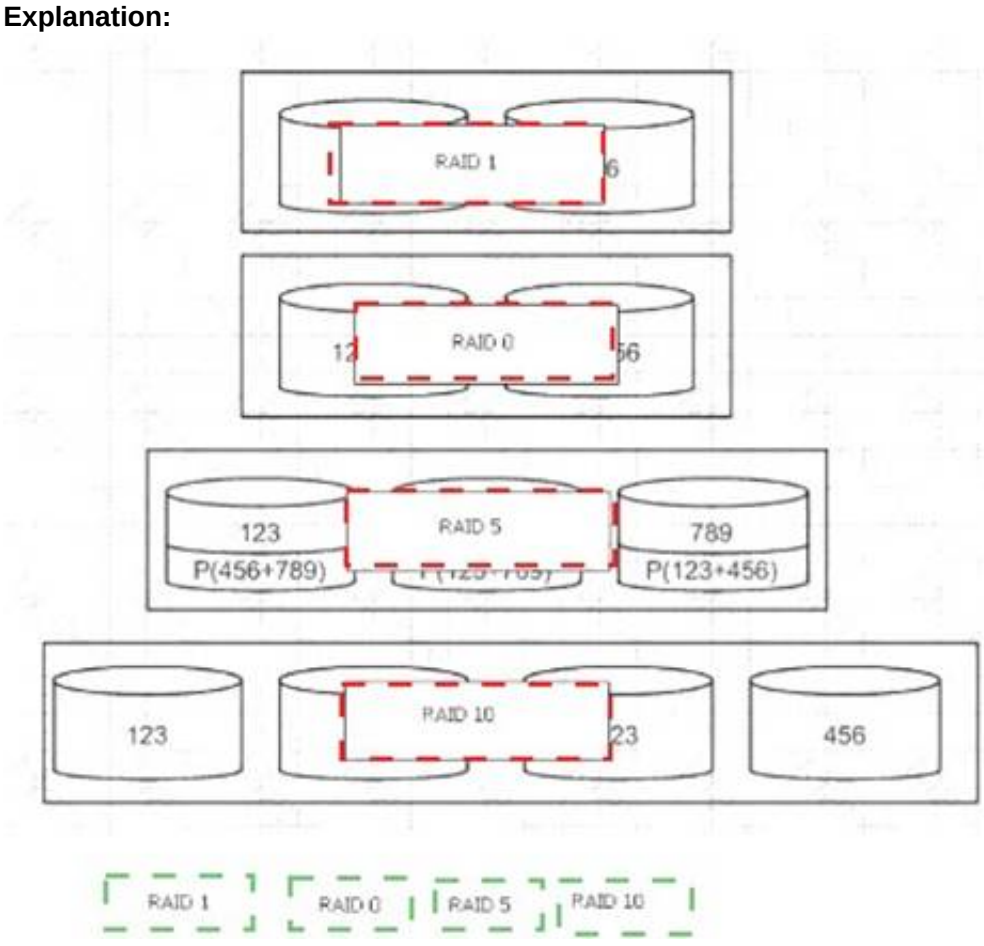
**NEW QUESTION 586**
- (Exam Topic 14)
Given a file containing ordered number, i.e. “123456789,” match each of the following redundant Array of independent Disks (RAID) levels to the corresponding visual representation visual representation. Note: P() = parity.
Drag each level to the appropriate place on the diagram.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 591**
- (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 592**
- (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 594**
- (Exam Topic 14)
A vehicle of a private courier company that transports backup data for offsite storage was robbed while in transport backup data for offsite was robbed while in transit. The incident management team is now responsible to estimate the robbery, which of the following would help the incident management team to MOST effectively analyze the business impact of the robbery?

A. Log of backup administrative actions
B. Log of the transported media and its classification marking
C. Log of the transported media and Its detailed contents
D. Log of backed up data and their respective data custodians

**Answer:** B

**NEW QUESTION 598**
- (Exam Topic 14)
Which of the following models uses unique groups contained in unique conflict classes?

A. Chinese Wall
B. Bell-LaPadula
C. Clark-Wilson
D. Biba

**Answer:** C

**NEW QUESTION 603**
- (Exam Topic 14)
An organization implements a Remote Access Server (RAS). Once users correct to the server, digital certificates are used to authenticate their identity. What type of Extensible Authentication Protocol (EAP) would the organization use dring this authentication?

A. Transport layer security (TLS)
B. Message Digest 5 (MD5)
C. Lightweight Extensible Authentication Protocol (EAP)
D. Subscriber Identity Module (SIM)

**Answer:** A

**NEW QUESTION 604**
- (Exam Topic 14)
Which of the following initiates the systems recovery phase of a disaster recovery plan?

A. Issuing a formal disaster declaration
B. Activating the organization's hot site
C. Evacuating the disaster site
D. Assessing the extent of damage following the disaster

**Answer:** A

**NEW QUESTION 609**
- (Exam Topic 14)
Which of the following is the BEST identity-as-a-service (IDaaS) solution for validating users?

A. Lightweight Directory Access Protocol (LDAP)
B. Security Assertion Markup Language (SAM.)
C. Single Sign-on (SSO)
D. Open Authentication (OAuth)

**Answer:** A

**NEW QUESTION 611**
- (Exam Topic 14)
Which of the following is MOST critical in a contract in a contract for data disposal on a hard drive with a third party?

A. Authorized destruction times
B. Allowed unallocated disk space
C. Amount of overwrites required
D. Frequency of recovered media

**Answer:** C

**NEW QUESTION 613**
- (Exam Topic 14)
Which of the following management processes allots ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

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

**Answer:** B

**NEW QUESTION 616**
- (Exam Topic 14)
Digital certificates used transport Layer security (TLS) support which of the following?

A. Server identify and data confidentially
B. Information input validation
C. Multi-Factor Authentication (MFA)
D. Non-reputation controls and data encryption

**Answer:** A

**NEW QUESTION 617**
- (Exam Topic 14)
Which of the following features is MOST effective in mitigating against theft of data on a corporate mobile device Which has stolen?

A. Whole device encryption with key escrow
B. Mobile Device Management (MDMJ with device wipe
C. Mobile device tracking with geolocation
D. Virtual Private Network (VPN) with traffic encryption

**Answer:** B

**NEW QUESTION 620**
- (Exam Topic 14)
Which is the second phase of public key Infrastructure (pk1) key/certificate life-cycle management?

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

**Answer:** C

**NEW QUESTION 624**
- (Exam Topic 14)
Which of the following phases involves researching a target's configuration from
public sources when performing a penetration test?

A. Information gathering
B. Social engineering
C. Target selection
D. Traffic enumeration

**Answer:** A

**NEW QUESTION 629**
- (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 632**
- (Exam Topic 14)
During a recent assessment an organization has discovered that the wireless signal can be detected outside the campus area. What logical control should be implemented in order to BFST protect One confidentiality of information traveling One wireless transmission media?

A. Configure a firewall to logically separate the data at the boundary.
B. Configure the Access Points (AP) to use Wi-Fi Protected Access 2 (WPA2) encryption.
C. Disable the Service Set Identifier (SSID) broadcast on the Access Points (AP).
D. Perform regular technical assessments on the Wireless Local Area Network (WLAN).

**Answer:** B

**NEW QUESTION 633**

- (Exam Topic 14)
After a breach incident, investigators narrowed the attack to a specific network administrator's credentials. However, there was no evidence to determine how the hackers obtained the credentials. Much of the following actions could have BEST avoided the above breach per the investigation described above?

A. A periodic review of network access loos
B. A periodic review of active users en the network
C. A periodic review of all privileged accounts actions
D. A periodic review of password strength of all users across the organization

**Answer:** C

**NEW QUESTION 637**
- (Exam Topic 14)
What is the FIRST step required in establishing a records retention program?

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

**Answer:** D

**NEW QUESTION 641**
- (Exam Topic 14)
Which of the following steps should be conducted during the FIRST phase of software assurance in a generic acquisition process?

A. Establishing and consenting to the contract work schedule
B. Issuing a Request for proposal (RFP) with a work statement
C. Developing software requirements to be included in work statement
D. Reviewing and accepting software deliverables

**Answer:** C

**NEW QUESTION 642**
- (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 645**
- (Exam Topic 14)
An employee receives a promotion that entities them to access higher-level functions on the company’s accounting system, as well as keeping their access to the previous system that is no longer needed or applicable. What is the name of the process that tries to remove this excess privilege?

A. Access provisioning
B. Segregation of Duties (SoD)
C. Access certification
D. Access aggregation

**Answer:** B

**NEW QUESTION 649**
- (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 651**
- (Exam Topic 14)
The adoption of an enterprise-wide business continuity program requires Which of the following?

A. Good communication throughout the organization
B. Formation of Disaster Recovery (DP) project team
C. A completed Business Impact Analysis (BIA)
D. Well-documented information asset classification

**Answer:** D

**NEW QUESTION 656**
- (Exam Topic 14)
Which of the following trust services principles refers to the accessibility of information used by the systems, products, or services offered to a third-party provider's customers?

A. Security
B. Privacy
C. Access
D. Availability

**Answer:** C

**Explanation:**
Reference: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/tr

**NEW QUESTION 660**
- (Exam Topic 14)
Which of the following is used to support the of defense in depth during development phase of a software product?

A. Security auditing
B. Polyinstantiation
C. Maintenance
D. Known vulnerability list

**Answer:** B

**NEW QUESTION 661**
- (Exam Topic 14)
Which of the following MUST an organization do to effectively communicate is security strategy to all affected parties?

A. Involve representatives from each key organizational area.
B. Provide regular updates to the board of directors.
C. Notify staff of changes to the strategy.
D. Remove potential communication barriers.

**Answer:** C

**NEW QUESTION 664**
- (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 667**
- (Exam Topic 14)
Which of the following is MOST important when determining appropriate countermeasures for an identified risk?

A. Interaction with existing controls
B. Cost
C. Organizational risk tolerance
D. Patch availability

**Answer:** C

**NEW QUESTION 671**
- (Exam Topic 14)
Which of the following will help prevent improper session handling?

A. Ensure that all UlWebView 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 675**
- (Exam Topic 14)
How does identity as a service (IDaaS) provide an easy mechanism for integrating identity service into individual applications with minimal development effort?

A. By allowing the identification logic and storage of an identity's attributes to be maintained externally
B. By integrating internal provisioning procedures with external authentication processes
C. By allowing for internal provisioning of user accounts
D. By keeping all user information in easily accessible cloud repositories

**Answer:** D

**NEW QUESTION 679**
- (Exam Topic 14)
A security consultant has been hired by a company to establish its vulnerability management program. The consultant is now in the deployment phase. Which of the following tasks is part of this process?

A. Select and procure supporting technologies.
B. Determine a budget and cost analysis for the program.
C. Measure effectiveness of the program's stated goals.
D. Educate and train key stakeholders.

**Answer:** C

**NEW QUESTION 684**
- (Exam Topic 14)
Which of the following should be included in a hardware retention policy? Which of the following should be included in a hardware retention policy?

A. The use of encryption technology to encrypt sensitive data prior to retention
B. Retention of data for only one week and outsourcing the retention to a third-party vendor
C. Retention of all sensitive data on media and hardware
D. A plan to retain data required only for business purposes and a retention schedule

**Answer:** A

**NEW QUESTION 687**
- (Exam Topic 14)
Which of the following needs to be taken into account when assessing vulnerability?

A. Risk identification and validation
B. Threat mapping
C. Risk acceptance criteria
D. Safeguard selection

**Answer:** A

**Explanation:**
Reference: https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA478&lpg=PA478&dq=CISSP+taken+into+acc

**NEW QUESTION 691**
- (Exam Topic 14)
Which of the following is the key requirement for test results when implementing forensic procedures?

A. The test results must be cost-effective.
B. The test result must be authorized.
C. The test results must be quantifiable.
D. The test results must be reproducible.

**Answer:** B

**NEW QUESTION 696**
- (Exam Topic 14)
Which of the following is an advantage of' Secure Shell (SSH)?

A. It operates at the network layer.
B. It encrypts transmitted User ID and passwords.
C. It uses challenge-response to authenticate each party.
D. It uses the International Data Encryption Algorithm (IDEA) for data privacy.

**Answer:** C

**NEW QUESTION 699**
- (Exam Topic 14)
Which programming methodology allows a programmer to use pre-determined blocks of code end consequently reducing development time and programming costs?

A. Application security
B. Object oriented
C. Blocked algorithm
D. Assembly language

**Answer:**

B

**NEW QUESTION 702**
- (Exam Topic 14)
Which of the following techniques BEST prevents buffer overflows?

A. Boundary and perimeter offset
B. Character set encoding
C. Code auditing
D. Variant type and bit length

**Answer:** B

**Explanation:**
Some products installed on systems can also watch for input values that might result in buffer overflows, but the best countermeasure is proper programming. This means use bounds checking. If an input value is only sup-posed to be nine characters, then the application should only accept nine characters and no more. Some languages are more susceptible to buffer overflows than others, so programmers should understand these issues, use the right languages for the right purposes, and carry out code review to identify buffer overflow vulnerabilities.

**NEW QUESTION 703**
- (Exam Topic 14)
Which of the following provides the BEST method to verify that security baseline configurations are maintained?

A. Perform regular system security testing.
B. Design security early in the development cycle.
C. Analyze logs to determine user activities.
D. Perform quarterly risk assessments.

**Answer:** A

**NEW QUESTION 704**
- (Exam Topic 14)

A. The signer verifies that the software being loaded is the software originated by the signer.
B. The vendor certifies the software being loaded is free of malicious code and that it was originated by the signer.
C. The signer verifies that the software being loaded is free of malicious code.
D. Both vendor and the signer certify the software being loaded is free of malicious code and it was originated by the signer.

**Answer:** A

**NEW QUESTION 709**
- (Exam Topic 14)
Which of the following findings would MOST likely indicate a high risk in a vulnerability assessment report?

A. Transmission control protocol (TCP) port 443 open
B. Non-standard system naming convention used
C. Unlicensed software installed
D. End of life system detected

**Answer:** A

**NEW QUESTION 712**
- (Exam Topic 14)
A client has reviewed a vulnerability assessment report and has stated it is inaccurate. The client states that the vulnerabilities listed are not valid because the host's Operating system (OS) was not properly detected.
Where in the vulnerability assessment process did the error MOST likely occur?

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

**Answer:** A

**NEW QUESTION 715**
- (Exam Topic 14)
Rank the Hypertext Transfer protocol (HTTP) authentication types shows below in order of relative strength. Drag the authentication type on the correct positions on the right according to strength from weakest to
strongest.


A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**


**NEW QUESTION 720**
- (Exam Topic 14)
Which of the following would present the higher annualized loss expectancy (ALE)?

| Event | Loss Expectancy | Annualized Rate of Occurrence | Insurance Coverage |
|---|---|---|---|
| Fire | $1,000,000 | 0.1 | 80% |
| Flood | $250,000 | 0.2 | 50% |
| Windstorm | $50,000 | 0.5 | 80% |
| Earthquake | $800,000 | 0.02 | None |

A. Fire
B. Earthquake
C. Windstorm
D. Flood

**Answer:** A

**NEW QUESTION 721**
- (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 723**
- (Exam Topic 14)
Which of the following attacks is dependent upon the compromise of a secondary target in order to reach the primary target?

A. Watering hole
B. Brute force
C. Spear phishing
D. Address Resolution Protocol (ARP) poisoning

**Answer:** D

**NEW QUESTION 724**
- (Exam Topic 14)
An organization implements a remote access server (RAS), Once users connect to the server, digital certificates are used to authenticate their identity. What type of extensible Authentication protocol (EAP) would the organization use during this authentication?

A. Message Digest 5 (MD5)
B. Subscriber Identity Module (SIM)

C. Lightweight Extensible Authentication Protocol (EAP)
D. Transport layer security (TLS)

**Answer:** D

**NEW QUESTION 726**
- (Exam Topic 14)
Which of the following is critical if an empolyee 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 728**
- (Exam Topic 14)
Which of the following is critical if an employee is dismissed due to violation of an organization's Acceptable Use Policy (ALP)?

A. Privilege suspension
B. Internet access logs
C. Proxy records
D. Appropriate documentation

**Answer:** B

**NEW QUESTION 732**
- (Exam Topic 14)
Which of the following attributes could be used to describe a protection mechanism of an open design methodology?

A. lt must be tamperproof to protect it from malicious attacks.
B. It can facilitate independent confirmation of the design security.
C. It can facilitate blackbox penetration testing.
D. It exposes the design to vulnerabilities and malicious attacks.

**Answer:** A

**NEW QUESTION 733**
- (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 735**
- (Exam Topic 14)
As a security manger which of the following is the MOST effective practice for providing value to an organization?

A. Assess business risk and apply security resources accordingly
B. Coordinate security implementations with internal audit
C. Achieve compliance regardless of related technical issues
D. Identify confidential information and protect it

**Answer:** D

**NEW QUESTION 736**
- (Exam Topic 14)
Which of the following processes has the PRIMARY purpose of identifying outdated software versions, missing patches, and lapsed system updates?

A. Penetration testing
B. Vulnerability management
C. Software Development Life Cycle (SDLC)
D. Life cycle management

**Answer:** B

**Explanation:**
Reference:
https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-operations/vulnerab

**NEW QUESTION 740**
- (Exam Topic 14)
Which of the following is the weakest form of protection for an application that handles Personally Identifiable Information (PII)?

A. Transport Layer Security (TLS)
B. Ron Rivest Cipher 4 (RC4) encryption
C. Security Assertion Markup Language (SAML)
D. Multifactor authentication

**Answer:** B

**NEW QUESTION 741**
- (Exam Topic 14)
What does the term “100-year floodplain” mean to emergency preparedness officials?

A. The area is expected to be safe from flooding for at least 100 years.
B. The odds of a flood at this level are 1 in 100 in any given year.
C. The odds are that the next significant flood will hit within the next 100 years.
D. The last flood of any kind to hit the area was more than 100 years ago.

**Answer:** B

**NEW QUESTION 746**
- (Exam Topic 13)
Which one of the following is an advantage of an effective release control strategy form 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 749**
- (Exam Topic 14)
Individuals have been identified and determined as having a need-to-know for the information. Which of the following access control methods MUST include a consistent set of rules for controlling and limiting access?

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

**Answer:** D

**NEW QUESTION 752**
- (Exam Topic 13)
Who is responsible for the protection of information when it is shared with or provided to other organizations?

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

**Answer:** C

**Explanation:**
Section: Security Operations

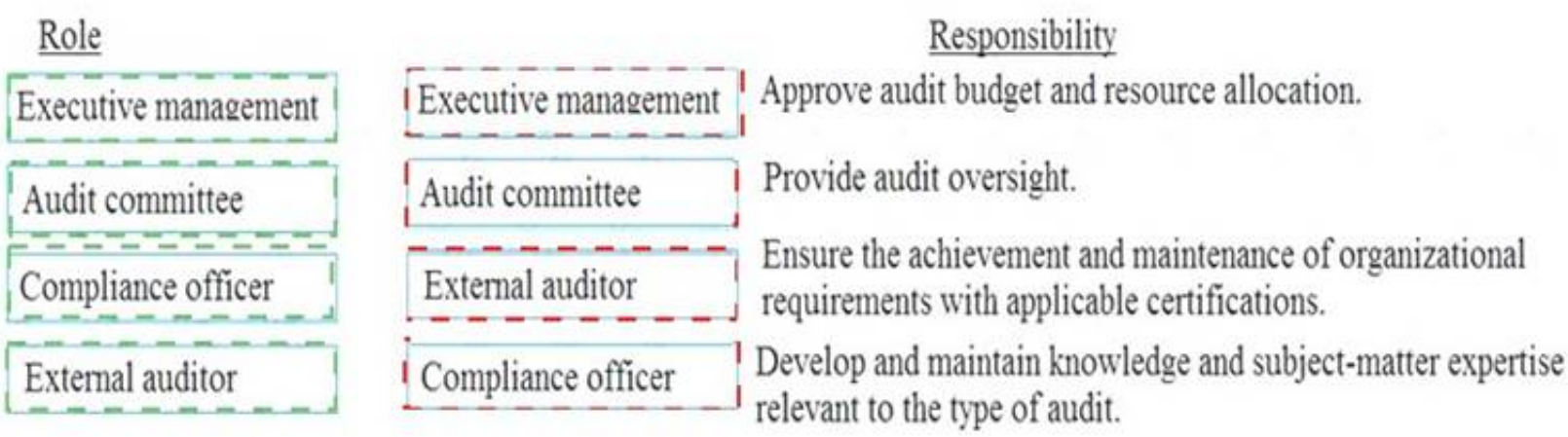
**NEW QUESTION 756**
- (Exam Topic 13)
Match the functional roles in an external audit to their responsibilities. Drag each role on the left to its corresponding responsibility on the right. Select and Place:

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

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 757**
- (Exam Topic 13)
What is the MAIN purpose of a change management policy?

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

**Answer:** C

**Explanation:**
Section: Security Operations

**NEW QUESTION 758**
- (Exam Topic 13)
A minimal implementation of endpoint security includes which of the following?

A. Trusted platforms
B. Host-based firewalls
C. Token-based authentication
D. Wireless Access Points (AP)

**Answer:** B

**NEW QUESTION 763**
- (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 765**
- (Exam Topic 13)
Which of the following would MINIMIZE the ability of an attacker to exploit a buffer overflow?

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

**Answer:** B

**NEW QUESTION 768**
- (Exam Topic 13)
A Denial of Service (DoS) attack on a syslog server exploits weakness in which of the following protocols?

A. Point-to-Point Protocol (PPP) and Internet Control Message Protocol (ICMP)
B. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
C. Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)
D. Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

**Answer:** B

**NEW QUESTION 772**
- (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 775**
- (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 778**
- (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 782**
- (Exam Topic 13)
During examination of Internet history records, the following string occurs within a Unique Resource Locator (URL):
http://www.companysite.com/products/products.asp?productid=123 or 1=1
What type of attack does this indicate?

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

**Answer:** C

**NEW QUESTION 786**
- (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 787**
- (Exam Topic 13)
Which of the following is a direct monetary cost of a security incident?

A. Morale
B. Reputation
C. Equipment
D. Information

**Answer:** C

**NEW QUESTION 792**
- (Exam Topic 13)
When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

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

**Answer:** D

**NEW QUESTION 795**
- (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 796**
- (Exam Topic 13)
What are the steps of a risk assessment?

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

**Answer:** A

**Explanation:**
Section: Security Assessment and Testing

**NEW QUESTION 797**
- (Exam Topic 13)
Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) only provides which of the following?

A. Mutual authentication
B. Server authentication
C. User authentication
D. Streaming ciphertext data

**Answer:** C

**NEW QUESTION 798**
- (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 799**
- (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 802**
- (Exam Topic 13)
What is the MAIN goal of information security awareness and training?

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

**Answer:** B

**NEW QUESTION 803**
- (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 808**
- (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 812**
- (Exam Topic 13)
Which of the following is the MOST challenging issue in apprehending cyber criminals?

A. They often use sophisticated method to commit a crime.
B. It is often hard to collect and maintain integrity of digital evidence.
C. The crime is often committed from a different jurisdiction.
D. There is often no physical evidence involved.

**Answer:** C

**NEW QUESTION 816**
- (Exam Topic 13)
Which of the following is a characteristic of an internal audit?

A. An internal audit is typically shorter in duration than an external audit.
B. The internal audit schedule is published to the organization well in advance.
C. The internal auditor reports to the Information Technology (IT) department
D. Management is responsible for reading and acting upon the internal audit results

**Answer:** D

**NEW QUESTION 817**
- (Exam Topic 13)
As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

A. Use a web scanner to scan for vulnerabilities within the website.
B. Perform a code review to ensure that the database references are properly addressed.
C. Establish a secure connection to the web server to validate that only the approved ports are open.
D. Enter only numbers in the web form and verify that the website prompts the user to enter a valid input.

**Answer:** D

**NEW QUESTION 819**
- (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 820**
- (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 825**
- (Exam Topic 13)
Which Identity and Access Management (IAM) process can be used to maintain the principle of least privilege?

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

**Answer:** A

**NEW QUESTION 828**
- (Exam Topic 13)
What Is the FIRST step in establishing an information security program?

A. Establish an information security policy.
B. Identify factors affecting information security.
C. Establish baseline security controls.
D. Identify critical security infrastructure.

**Answer:** A

**NEW QUESTION 831**
- (Exam Topic 13)
An organization recently conducted a review of the security of its network applications. One of the vulnerabilities found was that the session key used in encrypting sensitive information to a third party server
had been hard-coded in the client and server applications. Which of the following would be MOST effective in mitigating this vulnerability?

A. Diffle-Hellman (DH) algorithm
B. Elliptic Curve Cryptography (ECC) algorithm
C. Digital Signature algorithm (DSA)
D. Rivest-Shamir-Adleman (RSA) algorithm

**Answer:** D

**NEW QUESTION 836**
- (Exam Topic 13)
The security accreditation task of the System Development Life Cycle (SDLC) process is completed at the end of which phase?

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

**Answer:** B

**NEW QUESTION 837**
- (Exam Topic 13)
An organization has discovered that users are visiting unauthorized websites using anonymous proxies. Which of the following is the BEST way to prevent future occurrences?

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

**Answer:** D

**NEW QUESTION 841**
- (Exam Topic 13)
A Security Operations Center (SOC) receives an incident response notification on a server with an active intruder who has planted a backdoor. Initial notifications are sent and communications are established. What MUST be considered or evaluated before performing the next step?

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

**Answer:** D

**Explanation:**
Section: Security Operations

**NEW QUESTION 845**

.....

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons and Answers in PDF Format

## CISSP Practice Exam Features:

* CISSP Questions and Answers Updated Frequently

* CISSP Practice Questions Verified by Expert Senior Certified Staff

* CISSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year