ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

NEW QUESTION 1
- (Exam Topic 15)
What is the FIRST step when developing an Information Security Continuous Monitoring (ISCM) program?

A. Establish an ISCM technical architecture.
B. Collect the security-related information required for metrics, assessments, and reporting.
C. Establish an ISCM program determining metrics, status monitoring frequencies, and control assessment frequencies.
D. Define an ISCM strategy based on risk tolerance.

Answer: D

NEW QUESTION 2
- (Exam Topic 15)
Which of the following is an important requirement when designing a secure remote access system?

A. Configure a Demilitarized Zone (DMZ) to ensure that user and service traffic is separated.
B. Provide privileged access rights to computer files and systems.
C. Ensure that logging and audit controls are included.
D. Reduce administrative overhead through password self service.

Answer: C

NEW QUESTION 3
- (Exam Topic 15)
An organization is planning a penetration test that simulates the malicious actions of a former network administrator. What kind of penetration test is needed?

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

Answer: C

NEW QUESTION 4
- (Exam Topic 15)
In the common criteria, which of the following is a formal document that expresses an implementation-independent set of security requirements?

A. Organizational Security Policy
B. Security Target (ST)
C. Protection Profile (PP)
D. Target of Evaluation (TOE)

Answer: C

NEW QUESTION 5
- (Exam Topic 15)
In which process MUST security be considered during the acquisition of new software?

A. Contract negotiation
B. Request for proposal (RFP)
C. Implementation
D. Vendor selection

Answer: B

NEW QUESTION 6
- (Exam Topic 15)
Which of the following is the top barrier for companies to adopt cloud technology?

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

Answer: D

NEW QUESTION 7
- (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 8
- (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 9
- (Exam Topic 15)
Wireless users are reporting intermittent Internet connectivity. Connectivity is restored when the users disconnect and reconnect, utilizing the web authentication process each time.
The network administrator can see the devices connected to the APs at all times. Which of the following steps will MOST likely determine the cause of the issue?

A. Verify the session time-out configuration on the captive portal settings
B. Check for encryption protocol mismatch on the client's wireless settings.
C. Confirm that a valid passphrase is being used during the web authentication.
D. Investigate for a client's disassociation caused by an evil twin AP

Answer: A

NEW QUESTION 10
- (Exam Topic 15)
While reviewing the financial reporting risks of a third-party application, which of the following Service Organization Control (SOC) reports will be the MOST useful?

A. ISIsOC 1
B. SOC 2
C. SOC 3
D. SOC for cybersecurity

Answer: A

NEW QUESTION 10
- (Exam Topic 15)
Which of the following provides the MOST secure method for Network Access Control (NAC)?

A. Media Access Control (MAC) filtering
B. 802.IX authentication
C. Application layer filtering
D. Network Address Translation (NAT)

Answer: B

NEW QUESTION 14
- (Exam Topic 15)
During a penetration test, what are the three PRIMARY objectives of the planning phase?

A. Determine testing goals, identify rules of engagement, and conduct an initial discovery scan.
B. Finalize management approval, determine testing goals, and gather port and service information.
C. Identify rules of engagement, finalize management approval, and determine testing goals.
D. Identify rules of engagement, document management approval, and collect system and application information.

Answer: D

NEW QUESTION 19
- (Exam Topic 15)
Which of the following is the BEST method a security practitioner can use to ensure that systems and sub-system gracefully handle invalid input?

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

Answer: B

NEW QUESTION 20
- (Exam Topic 15)
An organization wants to define its physical perimeter. What primary device should be used to accomplish this objective if the organization's perimeter MUST cost-efficiently deter casual trespassers?

A. Fences eight or more feet high with three strands of barbed wire
B. Fences three to four feet high with a turnstile
C. Fences accompanied by patrolling security guards
D. Fences six to seven feet high with a painted gate

Answer: A

NEW QUESTION 23
- (Exam Topic 15)
Which of the following is a common term for log reviews, synthetic transactions, and code reviews?

A. Security control testing
B. Application development
C. Spiral development functional testing
D. DevOps Integrated Product Team (IPT) development

Answer: B

NEW QUESTION 25
- (Exam Topic 15)
When reviewing vendor certifications for handling and processing of company data, which of the following is the BEST Service Organization Controls (SOC) certification for the vendor to possess?

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

Answer: C

NEW QUESTION 29
- (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 32
- (Exam Topic 15)
Which of the following is the BEST way to protect an organization's data assets?

A. Monitor and enforce adherence to security policies.
B. Encrypt data in transit and at rest using up-to-date cryptographic algorithms.
C. Create the Demilitarized Zone (DMZ) with proxies, firewalls and hardened bastion hosts.
D. Require Multi-Factor Authentication (MFA) and Separation of Duties (SoD).

Answer: B

NEW QUESTION 34
- (Exam Topic 15)
Which of the following is the strongest physical access control?

A. Biometrics and badge reader
B. Biometrics, a password, and personal identification number (PIN)
C. Individual password for each user
D. Biometrics, a password, and badge reader

Answer: D

NEW QUESTION 39
- (Exam Topic 15)
A company is moving from the V model to Agile development. How can the information security department BEST ensure that secure design principles are implemented in the new methodology?

A. All developers receive a mandatory targeted information security training.
B. The non-financial information security requirements remain mandatory for the new model.
C. The information security department performs an information security assessment after each sprint.
D. Information security requirements are captured in mandatory user stories.

Answer: D

NEW QUESTION 44
- (Exam Topic 15)
In order to support the least privilege security principle when a resource is transferring within the organization from a production support system administration role to a developer role, what changes should be made to the resource's access to the production operating system (OS) directory structure?

A. From Read Only privileges to No Access Privileges
B. From Author privileges to Administrator privileges
C. From Administrator privileges to No Access privileges
D. From No Access Privileges to Author privileges

Answer: C

NEW QUESTION 45
- (Exam Topic 15)
Which of the following factors should be considered characteristics of Attribute Based Access Control (ABAC) in terms of the attributes used?

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

Answer: D

NEW QUESTION 46
- (Exam Topic 15)
An attacker is able to remain indefinitely logged into a exploiting to remain on the web service?

A. Alert management
B. Password management
C. Session management
D. Identity management (IM)

Answer: C

NEW QUESTION 48
- (Exam Topic 15)
Recently, an unknown event has disrupted a single Layer-2 network that spans between two geographically diverse data centers. The network engineers have asked for assistance in identifying the root cause of the event. Which of the following is the MOST likely cause?

A. Misconfigured routing protocol
B. Smurf attack
C. Broadcast domain too large
D. Address spoofing

Answer: D

NEW QUESTION 50
- (Exam Topic 15)
A security practitioner has been asked to model best practices for disaster recovery (DR) and business continuity. The practitioner has decided that a formal committee is needed to establish a business continuity policy. Which of the following BEST describes this stage of business continuity development?

A. Project Initiation and Management
B. Risk Evaluation and Control
C. Developing and Implementing business continuity plans (BCP)
D. Business impact analysis (BIA)

Answer: D

NEW QUESTION 51
- (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 56
- (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 58
- (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 63
- (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 65
- (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 68
- (Exam Topic 15)
Which of the following is the BEST way to mitigate circumvention of access controls?

A. Multi-layer access controls working in isolation
B. Multi-vendor approach to technology implementation
C. Multi-layer firewall architecture with Internet Protocol (IP) filtering enabled
D. Multi-layer access controls with diversification of technologies

Answer: D

NEW QUESTION 71
- (Exam Topic 15)
Which of the following examples is BEST to minimize the attack surface for a customer's private information?

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

Answer: A

NEW QUESTION 75
- (Exam Topic 15)
Which element of software supply chain management has the GREATEST security risk to organizations?

A. New software development skills are hard to acquire.
B. Unsupported libraries are often used.
C. Applications with multiple contributors are difficult to evaluate.
D. Vulnerabilities are difficult to detect.

Answer: B

NEW QUESTION 79
- (Exam Topic 15)
Physical Access Control Systems (PACS) allow authorized security personnel to manage and monitor access control for subjects through which function?

A. Remote access administration
B. Personal Identity Verification (PIV)
C. Access Control List (ACL)
D. Privileged Identity Management (PIM)

Answer: B

NEW QUESTION 84
- (Exam Topic 15)
What is the BEST control to be implemented at a login page in a web application to mitigate the ability to enumerate users?

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

Answer: A

NEW QUESTION 86
- (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 90
- (Exam Topic 15)
What is the MOST effective response to a hacker who has already gained access to a network and will attempt to pivot to other resources?

A. Reset all passwords.
B. Shut down the network.
C. Warn users of a breach.
D. Segment the network.

Answer: D

NEW QUESTION 95
- (Exam Topic 15)
Which of the following phases in the software acquisition process does developing evaluation criteria take place?

A. Follow-On
B. Planning
C. Contracting
D. Monitoring and Acceptance

Answer: D

NEW QUESTION 96
- (Exam Topic 15)
A financial services organization has employed a security consultant to review processes used by employees across various teams. The consultant interviewed a member of the application development practice and found gaps in their threat model. Which of the following correctly represents a trigger for when a threat model should be revised?

A. A new data repository is added.
B. is After operating system (OS) patches are applied
C. After a modification to the firewall rule policy
D. A new developer is hired into the team.

Answer: D

NEW QUESTION 98
- (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 101

- (Exam Topic 15)
What is the FIRST step that should be considered in a Data Loss Prevention (DLP) program?

A. Configuration management (CM)
B. Information Rights Management (IRM)
C. Policy creation
D. Data classification

Answer: D

NEW QUESTION 105
- (Exam Topic 15)
When configuring Extensible Authentication Protocol (EAP) in a Voice over Internet Protocol (VoIP) network, which of the following authentication types is the MOST secure?

A. EAP-Transport Layer Security (TLS)
B. EAP-Flexible Authentication via Secure Tunneling
C. EAP-Tunneled Transport Layer Security (TLS)
D. EAP-Protected Extensible Authentication Protocol (PEAP)

Answer: C

NEW QUESTION 106
- (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 107
- (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 109
- (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 110
- (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 115
- (Exam Topic 15)
Which of the following determines how traffic should flow based on the status of the infrastructure layer?

A. Traffic plane
B. Application plane
C. Data plane
D. Control plane

Answer: A

NEW QUESTION 116
- (Exam Topic 15)
Which of the following is an open standard for exchanging authentication and authorization data between parties?

A. Wired markup language
B. Hypertext Markup Language (HTML)
C. Extensible Markup Language (XML)
D. Security Assertion Markup Language (SAML)

Answer: D

NEW QUESTION 118
- (Exam Topic 15)
A software development company has a short timeline in which to deliver a software product. The software development team decides to use open-source software libraries to reduce the development time. What concept should software developers consider when using open-source software libraries?

A. Open source libraries contain known vulnerabilities, and adversaries regularly exploit those vulnerabilities in the wild.
B. Open source libraries can be used by everyone, and there is a common understanding that the vulnerabilities in these libraries will not be exploited.
C. Open source libraries are constantly updated, making it unlikely that a vulnerability exists for an adversary to exploit.
D. Open source libraries contain unknown vulnerabilities, so they should not be used.

Answer: A

NEW QUESTION 121
- (Exam Topic 15)
Which of the following criteria ensures information is protected relative to its importance to the organization?

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

Answer: D

NEW QUESTION 125
- (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 127
- (Exam Topic 15)
Which of the following is a common risk with fiber optical communications, and what is the associated mitigation measure?

A. Data emanation, deploying Category (CAT) 6 and higher cable wherever feasible
B. Light leakage, deploying shielded cable wherever feasible
C. Cable damage, deploying ring architecture wherever feasible
D. Electronic eavesdropping, deploying end-to-end encryption wherever feasible

Answer: B

NEW QUESTION 131
- (Exam Topic 15)
Why is it important that senior management clearly communicates the formal Maximum Tolerable Downtime (MTD) decision?

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

Answer: D

NEW QUESTION 133
- (Exam Topic 15)
An organization has requested storage area network (SAN) disks for a new project. What Redundant Array of Independent Disks (RAID) level provides the BEST redundancy and fault tolerance?

A. RAID level 1

B. RAID level 3
C. RAID level 4
D. RAID level 5

Answer: D

NEW QUESTION 136
- (Exam Topic 15)
An information technology (IT) employee who travels frequently to various ies remotely to an organization' the following solutions BEST serves as a secure control mechanism to meet the organization's requirements? to troubleshoot p Which of the following solutions BEST serves as a secure control mechanisn to meet the organization's requirements?

A. Update the firewall rules to include the static Internet Protocol (IP) addresses of the locations where the employee connects from.
B. Install a third-party screen sharing solution that provides remote connection from a public website.
C. Implement a Dynamic Domain Name Services (DDNS) account to initiate a virtual private network (VPN) using the DDNS record.
D. Install a bastion host in the demilitarized zone (DMZ) and allow multi-factor authentication (MFA) access.

Answer: D

NEW QUESTION 137
- (Exam Topic 15)
Which of the following departments initiates the request, approval, and provisioning business process?

A. Operations
B. Human resources (HR)
C. Information technology (IT)
D. Security

Answer: A

NEW QUESTION 138
- (Exam Topic 15)
Which one of the following BEST protects vendor accounts that are used for emergency maintenance?

A. Encryption of routing tables
B. Vendor access should be disabled until needed
C. Role-based access control (RBAC)
D. Frequent monitoring of vendor access

Answer: B

NEW QUESTION 139
- (Exam Topic 15)
Which type of disaster recovery plan (DRP) testing carries the MOST operational risk?

A. Cutover
B. Walkthrough
C. Tabletop
D. Parallel

Answer: C

NEW QUESTION 143
- (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 145
- (Exam Topic 15)
Dumpster diving is a technique used in which stage of penetration testing methodology?

A. Attack
B. Discovery
C. Reporting
D. Planning

Answer: B

NEW QUESTION 146

- (Exam Topic 15)
What is the benefit of an operating system (OS) feature that is designed to prevent an application from executing code from a non-executable memory region?

A. Identifies which security patches still need to be installed on the system
B. Stops memory resident viruses from propagating their payload
C. Reduces the risk of polymorphic viruses from encrypting their payload
D. Helps prevent certain exploits that store code in buffers

Answer: C

NEW QUESTION 149
- (Exam Topic 15)
In a multi-tenant cloud environment, what approach will secure logical access to assets?

A. Hybrid cloud
B. Transparency/Auditability of administrative access
C. Controlled configuration management (CM)
D. Virtual private cloud (VPC)

Answer: D

NEW QUESTION 150
- (Exam Topic 15)
Which of the following will accomplish Multi-Factor Authentication (MFA)?

A. Issuing a smart card with a user-selected Personal Identification Number (PIN)
B. Requiring users to enter a Personal Identification Number (PIN) and a password
C. Performing a palm and retinal scan
D. Issuing a smart card and a One Time Password (OTP) token

Answer: A

NEW QUESTION 155
- (Exam Topic 15)
A security professional has been assigned to assess a web application. The assessment report recommends switching to Security Assertion Markup Language (SAML). What is the PRIMARY security benefit in switching to SAML?

A. It uses Transport Layer Security (TLS) to address confidentiality.
B. it enables single sign-on (SSO) for web applications.
C. The users' password Is not passed during authentication.
D. It limits unnecessary data entry on web forms.

Answer: B

NEW QUESTION 157
- (Exam Topic 15)
Which of the following would be considered an incident if reported by a security information and event management (SIEM) system?

A. An administrator is logging in on a server through a virtual private network (VPN).
B. A log source has stopped sending data.
C. A web resource has reported a 404 error.
D. A firewall logs a connection between a client on the Internet and a web server using Transmission Control Protocol (TCP) on port 80.

Answer: C

NEW QUESTION 161
- (Exam Topic 15)
Security Software Development Life Cycle (SDLC) expects application code to be written In a consistent manner to allow ease of auditing and which of the following?

A. Protecting
B. Executing
C. Copying
D. Enhancing

Answer: A

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 169
- (Exam Topic 15)
In a large company, a system administrator needs to assign users access to files using Role Based Access Control (RBAC). Which option Is an example of RBAC?

A. Mowing users access to files based on their group membership
B. Allowing users access to files based on username
C. Allowing users access to files based on the users location at time of access
D. Allowing users access to files based on the file type

Answer: A

NEW QUESTION 171
- (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 176
- (Exam Topic 15)
What is the PRIMARY benefit of relying on Security Content Automation Protocol (SCAP)?

A. Save security costs for the organization.
B. Improve vulnerability assessment capabilities.
C. Standardize specifications between software security products.
D. Achieve organizational compliance with international standards.

Answer: C

NEW QUESTION 179
- (Exam Topic 15)
Clothing retailer employees are provisioned with user accounts that provide access to resources at partner businesses. All partner businesses use common identity and access management (IAM) protocols and differing technologies. Under the Extended Identity principle, what is the process flow between partner businesses to allow this TAM action?

A. Clothing retailer acts as identity provider (IdP), confirms identity of user using industry standards, then sends credentials to partner businesses that act as a ServiceProvider and allows access to services.
B. Clothing retailer acts as User Self Service, confirms identity of user using industry standards, then sends credentials to partner businesses that act as a ServiceProvider and allows access to services.
C. Clothing retailer acts as Service Provider, confirms identity of user using industry standards, then sends credentials to partner businesses that act as an identityprovider (IdP) and allows access to resources.
D. Clothing retailer acts as Access Control Provider, confirms access of user using industry standards, then sends credentials to partner businesses that act as a ServiceProvider and allows access to resources.

Answer: A

NEW QUESTION 183
- (Exam Topic 15)
Which of the following would an information security professional use to recognize changes to content, particularly unauthorized changes?

A. File Integrity Checker
B. Security information and event management (SIEM) system
C. Audit Logs
D. Intrusion detection system (IDS)

Answer: A

NEW QUESTION 186
- (Exam Topic 15)
When defining a set of security controls to mitigate a risk, which of the following actions MUST occur?

A. Each control's effectiveness must be evaluated individually.
B. Each control must completely mitigate the risk.
C. The control set must adequately mitigate the risk.
D. The control set must evenly divided the risk.

Answer: A

NEW QUESTION 191
- (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 193
- (Exam Topic 15)
An organization has developed a way for customers to share information from their wearable devices with each other. Unfortunately, the users were not informed as to what information collected would be shared. What technical controls should be put in place to remedy the privacy issue while still trying to accomplish the organization's business goals?

A. Default the user to not share any information.
B. Inform the user of the sharing feature changes after implemented.
C. Share only what the organization decides is best.
D. Stop sharing data with the other users.

Answer: D

NEW QUESTION 194
- (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 198
- (Exam Topic 15)
Which of the following events prompts a review of the disaster recovery plan (DRP)?

A. New members added to the steering committee
B. Completion of the security policy review
C. Change in senior management
D. Organizational merger

Answer: D

NEW QUESTION 202
- (Exam Topic 15)
Which of the following vulnerability assessment activities BEST exemplifies the Examine method of assessment?

A. Ensuring that system audit logs capture all relevant data fields required by the security controls baseline
B. Performing Port Scans of selected network hosts to enumerate active services
C. Asking the Information System Security Officer (ISSO) to describe the organization’s patch management processes
D. Logging into a web server using the default administrator account and a default password

Answer: D

NEW QUESTION 206
- (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 210
- (Exam Topic 15)
Which of the following types of web-based attack is happening when an attacker is able to send a well-crafted, malicious request to an authenticated user without the user realizing it?

A. ross-Site Scripting (XSS)
B. Cross-Site request forgery (CSRF)
C. Cross injection
D. Broken Authentication And Session Management

Answer: B

NEW QUESTION 213
- (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 218
- (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 219
- (Exam Topic 15)
What Is a risk of using commercial off-the-shelf (COTS) products?

A. COTS products may not map directly to an organization’s security requirements.
B. COTS products are typically more expensive than developing software in-house.
C. Cost to implement COTS products is difficult to predict.
D. Vendors are often hesitant to share their source code.

Answer: A

NEW QUESTION 222
- (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 226
- (Exam Topic 15)
A software engineer uses automated tools to review application code and search for application flaws, back doors, or other malicious code. Which of the following is the FIRST Software Development Life Cycle (SDLC) phase where this takes place?

A. Design
B. Test
C. Development
D. Deployment

Answer: C

NEW QUESTION 228
- (Exam Topic 15)
If an employee transfers from one role to another, which of the following actions should this trigger within the identity and access management (IAM) lifecycle?

A. New account creation
B. User access review and adjustment
C. Deprovisioning
D. System account access review and adjustment

Answer: B

NEW QUESTION 232
- (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 236
- (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 241
- (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 245
- (Exam Topic 15)
Which of the following MUST be done before a digital forensics investigator may acquire digital evidence?

A. Inventory the digital evidence.
B. Isolate the digital evidence.
C. Verify that the investigator has the appropriate legal authority to proceed.
D. Perform hashing to verify the integrity of the digital evidence.

Answer: C

NEW QUESTION 250
- (Exam Topic 15)
At what stage of the Software Development Life Cycle (SDLC) does software vulnerability remediation MOST likely cost the least to implement?

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

Answer: D

NEW QUESTION 253
- (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 254
- (Exam Topic 15)
What does the result of Cost-Benefit Analysis (C8A) on new security initiatives provide?

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

Answer: A

NEW QUESTION 256
- (Exam Topic 15)
A recent security audit is reporting several unsuccessful login attempts being repeated at specific times during the day on an Internet facing authentication server. No alerts have been generated by the security information and event management (SIEM) system. What PRIMARY action should be taken to improve SIEM performance?

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

Answer: B

NEW QUESTION 259
- (Exam Topic 15)
The security organization is looking for a solution that could help them determine with a strong level of confidence that attackers have breached their network. Which solution is MOST effective at discovering a successful network breach?

A. Deploying a honeypot
B. Developing a sandbox
C. Installing an intrusion prevention system (IPS)
D. Installing an intrusion detection system (IDS)

Answer: A

NEW QUESTION 260
- (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 262
- (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 263
- (Exam Topic 15)
Which of the following is included in the Global System for Mobile Communications (GSM) security framework?

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

Answer: C

NEW QUESTION 267
- (Exam Topic 15)
Which of the following is the PRIMARY type of cryptography required to support non-repudiation of a digitally signed document?

A. Message digest (MD)
B. Asymmetric
C. Symmetric
D. Hashing

Answer: A

NEW QUESTION 270
- (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 273
- (Exam Topic 15)
An authentication system that uses challenge and response was recently implemented on an organization's network, because the organization conducted an annual penetration test showing that testers were able to move laterally using authenticated credentials. Which attack method was MOST likely used to achieve this?

A. Cross-Site Scripting (XSS)
B. Pass the ticket
C. Brute force
D. Hash collision

Answer: B

NEW QUESTION 275
- (Exam Topic 15)
Which organizational department is ultimately responsible for information governance related to e-mail and other e-records?

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

Answer: C

NEW QUESTION 276
- (Exam Topic 15)
Which of the following BEST ensures the integrity of transactions to intended recipients?

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

Answer: A

NEW QUESTION 281
- (Exam Topic 15)
An organization is preparing to achieve General Data Protection Regulation (GDPR) compliance. The Chief Information Security Officer (CISO) is reviewing data protection methods.
Which of the following is the BEST data protection method?

A. Encryption
B. Backups
C. Data obfuscation
D. Strong authentication

Answer: C

NEW QUESTION 282
- (Exam Topic 15)
Write Once, Read Many (WORM) data storage devices are designed to BEST support which of the following core security concepts?

A. lntegrity
B. Scalability
C. Availability
D. Confidentiality

Answer: A

NEW QUESTION 284
- (Exam Topic 15)
Which software defined networking (SDN) architectural component is responsible for translating network requirements?

A. SDN Application
B. SDN Data path
C. SDN Controller
D. SDN Northbound Interfaces

Answer: D

NEW QUESTION 287
- (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 290
- (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 291
- (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 295
- (Exam Topic 15)
Why would a system be structured to isolate different classes of information from one another and segregate them by user jurisdiction?

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

Answer: C

NEW QUESTION 300
- (Exam Topic 15)
Which of the following has the responsibility of information technology (IT) governance?

A. Chief Information Officer (CIO)
B. Senior IT Management
C. Board of Directors
D. Chief Information Security Officer (CISO)

Answer: A

NEW QUESTION 305
- (Exam Topic 15)
International bodies established a regulatory scheme that defines how weapons are exchanged between the signatories. It also addresses cyber weapons, including malicious software, Command and Control (C2) software, and internet surveillance software. This is a description of which of the following?

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

Answer: C

NEW QUESTION 310
- (Exam Topic 15)
What is considered the BEST explanation when determining whether to provide remote network access to a third-party security service?

A. Contract negotiation
B. Vendor demonstration
C. Supplier request
D. Business need

Answer: D

NEW QUESTION 313

- (Exam Topic 15)
A recent information security risk assessment identified weak system access controls on mobile devices as a high me In order to address this risk and ensure only authorized staff access company information, which of the following should the organization implement?

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

Answer: B

NEW QUESTION 314
- (Exam Topic 15)
A company wants to store data related to users on an offsite server. What method can be deployed to protect the privacy of the user's information while maintaining the field-level configuration of the database?

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

Answer: A

NEW QUESTION 319
- (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 324
- (Exam Topic 15)
A user's credential for an application is stored in a relational database. Which control protects the confidentiality of the credential while it is stored?

A. Validate passwords using a stored procedure.
B. Allow only the application to have access to the password field in order to verify user authentication.
C. Use a salted cryptographic hash of the password.
D. Encrypt the entire database and embed an encryption key in the application.

Answer: C

NEW QUESTION 328
- (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 330
- (Exam Topic 15)
Which of the following is the FIRST step during digital identity provisioning?

A. Authorizing the entity for resource access
B. Synchronizing directories
C. Issuing an initial random password
D. Creating the entity record with the correct attributes

Answer: D

NEW QUESTION 332
- (Exam Topic 15)
A system developer has a requirement for an application to check for a secure digital signature before the application is accessed on a user's laptop. Which security mechanism addresses this requirement?

A. Hardware encryption
B. Certificate revocation list (CRL) policy
C. Trusted Platform Module (TPM)
D. Key exchange

Answer: B

NEW QUESTION 334
- (Exam Topic 15)
An organization implements Network Access Control (NAC) ay Institute of Electrical and Electronics Engineers (IEEE) 802.1x and discovers the printers do not support the IEEE 802.1x standard. Which of the following is the BEST resolution?

A. Implement port security on the switch ports for the printers.
B. Implement a virtual local area network (VLAN) for the printers.
C. Do nothing; IEEE 802.1x is irrelevant to printers.
D. Install an IEEE 802. 1x bridge for the printers.

Answer: A

NEW QUESTION 337
- (Exam Topic 15)
Which of the following security tools will ensure authorized data is sent to the application when implementing a cloud based application?

A. Host-based intrusion prevention system (HIPS)
B. Access control list (ACL)
C. File integrity monitoring (FIM)
D. Data loss prevention (DLP)

Answer: B

NEW QUESTION 339
- (Exam Topic 15)
All hosts on the network are sending logs via syslog-ng to the log collector. The log collector is behind its own firewall, The security professional wants to make sure not to put extra load on the firewall due to the amount of traffic that is passing through it. Which of the following types of filtering would MOST likely be used?

A. Uniform Resource Locator (URL) Filtering
B. Web Traffic Filtering
C. Dynamic Packet Filtering
D. Static Packet Filtering

Answer: C

NEW QUESTION 344
- (Exam Topic 15)
A security engineer is required to integrate security into a software project that is implemented by small groups test quickly, continuously, and independently develop, test, and deploy code to the cloud. The engineer will MOST likely integrate with which software development process'

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

Answer: C

NEW QUESTION 345
- (Exam Topic 15)
Which of the following protects personally identifiable information (PII) used by financial services organizations?

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

Answer: B

NEW QUESTION 349
- (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 351
- (Exam Topic 15)
A security professional can BEST mitigate the risk of using a Commercial Off-The-Shelf (COTS) solution by deploying the application with which of the following controls in ?

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

Answer: A

NEW QUESTION 352
- (Exam Topic 15)
Which security feature fully encrypts code and data as it passes to the servers and only decrypts below the hypervisor layer?

A. File-system level encryption
B. Transport Layer Security (TLS)
C. Key management service
D. Trusted execution environments

Answer: D

NEW QUESTION 357
- (Exam Topic 15)
The application owner of a system that handles confidential data leaves an organization. It is anticipated that a replacement will be hired in approximately six months. During that time, which of the following should the organization do?

A. Gram temporary access to the former application owner's account
B. Assign a temporary application owner to the system.
C. Restrict access to the system until a replacement application owner rs hired.
D. Prevent changes to the confidential data until a replacement application owner is hired.

Answer: B

NEW QUESTION 361
- (Exam Topic 15)
Which of the following is the MOST secure protocol for zremote command access to the firewall?

A. Secure Shell (SSH)
B. Trivial File Transfer Protocol (TFTP)
C. Hypertext Transfer Protocol Secure (HTTPS)
D. Simple Network Management Protocol (SNMP) v1

Answer: A

NEW QUESTION 366
- (Exam Topic 15)
An organization wants to migrate to Session Initiation Protocol (SIP) to save on telephony expenses. Which of the following security related statements should be considered in the decision-making process?

A. Cloud telephony is less secure and more expensive than digital telephony services.
B. SIP services are more secure when used with multi-layer security proxies.
C. H.323 media gateways must be used to ensure end-to-end security tunnels.
D. Given the behavior of SIP traffic, additional security controls would be required.

Answer: C

NEW QUESTION 370
- (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 373
- (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 377

- (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 380
- (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 383
- (Exam Topic 15)
Which of the following BEST describes centralized identity management?

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

Answer: B

NEW QUESTION 385
- (Exam Topic 15)
An application developer receives a report back from the security team showing their automated tools were able to successfully enter unexpected data into the organization's customer service portal, causing the site to crash. This is an example of which type of testing?

A. Non-functional
B. Positive
C. Performance
D. Negative

Answer: D

NEW QUESTION 387
- (Exam Topic 15)
In order to provide dual assurance in a digital signature system, the design MUST include which of the following?

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

Answer: B

NEW QUESTION 389
- (Exam Topic 15)
In which of the following scenarios is locking server cabinets and limiting access to keys preferable to locking the server room to prevent unauthorized access?

A. Server cabinets are located in an unshared workspace.
B. Server cabinets are located in an isolated server farm.
C. Server hardware is located in a remote area.
D. Server cabinets share workspace with multiple projects.

Answer: D

NEW QUESTION 390
- (Exam Topic 15)
What type of risk is related to the sequences of value-adding and managerial activities undertaken in an organization?

A. Demand risk
B. Process risk
C. Control risk
D. Supply risk

Answer: B

NEW QUESTION 393
- (Exam Topic 15)
When are security requirements the LEAST expensive to implement?

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

Answer: D

NEW QUESTION 397
- (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 398
- (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 403
- (Exam Topic 15)
Which of the following is a canon of the (ISC)2 Code of Ethics?

A. Integrity first, association before serf, and excellence in all we do
B. Perform all professional activities and duties in accordance with all applicable laws and the highest ethical standards.
C. Provide diligent and competent service to principals.
D. Cooperate with others in the interchange of knowledge and ideas for mutual security.

Answer: C

NEW QUESTION 408
- (Exam Topic 15)
An organization contracts with a consultant to perform a System Organization Control (SOC) 2 audit on their internal security controls. An auditor documents a finding related to an Application Programming Interface (API) performing an action that is not aligned with the scope or objective of the system. Which trust service principle would be MOST applicable in this situation?

A. Processing Integrity
B. Availability
C. Confidentiality
D. Security

Answer: B

NEW QUESTION 410
- (Exam Topic 15)
Which of the following should exist in order to perform a security audit?

A. Industry framework to audit against
B. External (third-party) auditor
C. Internal certified auditor
D. Neutrality of the auditor

Answer: D

NEW QUESTION 413
- (Exam Topic 15)
The European Union (EU) General Data Protection Regulation (GDPR) requires organizations to implement appropriate technical and organizational measures to ensure a
level of security appropriate to the risk. The Data Owner should therefore consider which of the following requirements?

A. Data masking and encryption of personal data

B. Only to use encryption protocols approved by EU
C. Anonymization of personal data when transmitted to sources outside the EU
D. Never to store personal data of EU citizens outside the EU

Answer: D

NEW QUESTION 417
- (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 421
- (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 426
- (Exam Topic 15)
Which of the following threats would be MOST likely mitigated by monitoring assets containing open source libraries for vulnerabilities?

A. Distributed denial-of-service (DDoS) attack
B. Zero-day attack
C. Phishing attempt
D. Advanced persistent threat (APT) attempt

Answer: A

NEW QUESTION 431
- (Exam Topic 15)
The development team has been tasked with collecting data from biometric devices. The application will support a variety of collection data streams. During the testing phase, the team utilizes data from an old production database in a secure testing environment. What principle has the team taken into consideration?

A. biometric data cannot be changed.
B. Separate biometric data streams require increased security.
C. The biometric devices are unknown.
D. Biometric data must be protected from disclosure.

Answer: A

NEW QUESTION 432
- (Exam Topic 15)
Which of the following are all elements of a disaster recovery plan (DRP)?

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

Answer: C

NEW QUESTION 434
- (Exam Topic 15)
What are the PRIMARY responsibilities of security operations for handling and reporting violations and incidents?

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

Answer: D

NEW QUESTION 439
- (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 441
- (Exam Topic 14)
Which one of the following documentation should be included in a Disaster Recovery (DR) package?

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

Answer: C

NEW QUESTION 442
- (Exam Topic 14)
What should an auditor do when conducting a periodic audit on media retention?

A. Check electronic storage media to ensure records are not retained past their destruction date.
B. Ensure authorized personnel are in possession of paper copies containing Personally Identifiable Information….
C. Check that hard disks containing backup data that are still within a retention cycle are being destroyed….
D. Ensure that data shared with outside organizations is no longer on a retention schedule.

Answer: A

NEW QUESTION 445
- (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 448
- (Exam Topic 14)
Which of the following is used to support the concept of defense in depth during the development phase of a software product?

A. Maintenance hooks
B. Polyinstiation
C. Known vulnerability list
D. Security auditing

Answer: B

NEW QUESTION 452
- (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 456
- (Exam Topic 14)
An organization is considering outsourcing applications and data to a Cloud Service Provider (CSP). Which of the following is the MOST important concern regarding privacy?

A. The CSP determines data criticality.
B. The CSP provides end-to-end encryption services.
C. The CSP's privacy policy may be developer by the organization.
D. The CSP may not be subject to the organization's country legation.

Answer: D

NEW QUESTION 460
- (Exam Topic 14)
If a content management system (CMC) is implemented, which one of the following would occur?

A. Developers would no longer have access to production systems
B. The applications placed into production would be secure
C. Patching the systems would be completed more quickly
D. The test and production systems would be running the same software

Answer: D

NEW QUESTION 462
- (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 465
- (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 467
- (Exam Topic 14)
The Secure Shell (SSH) version 2 protocol supports.

A. availability, accountability, compression, and integrity,
B. authentication, availability, confidentiality, and integrity.
C. accountability, compression, confidentiality, and integrity.
D. authentication, compression, confidentiality, and integrity.

Answer: D

NEW QUESTION 468
- (Exam Topic 14)
Additional padding may be added to toe Encapsulating Security Protocol (ESP) b trailer to provide which of the following?

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

Answer: C

NEW QUESTION 473
- (Exam Topic 14)
When adopting software as a service (Saas), which security responsibility will remain with remain with the adopting organization?

A. Physical security
B. Data classification
C. Network control
D. Application layer control

Answer: B

NEW QUESTION 475
- (Exam Topic 14)
Which of the following is a method of attacking internet (IP) v6 Layer 3 and Layer 4 ?

A. Synchronize sequence numbers (SVN) flooding
B. Internet Control Message Protocol (IOP) flooring
C. Domain Name Server [DNS) cache poisoning
D. Media Access Control (MAC) flooding

Answer: A

NEW QUESTION 478
- (Exam Topic 14)
Which of the following is the MOST important reason for using a chain of custody from?

A. To document those who were In possession of the evidence at every point In time
B. To collect records of all digital forensic professionals working on a case
C. To document collected digital evidence
D. To ensure that digital evidence is not overlooked during the analysis

Answer: A

NEW QUESTION 483
- (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 488
- (Exam Topic 14)
What is the MOST common component of a vulnerability management framework?

A. Risk analysis
B. Patch management
C. Threat analysis
D. Backup management

Answer: B

Explanation:
Reference: https://www.helpnetsecurity.com/2016/10/11/effective-vulnerability-management-process/

NEW QUESTION 489
- (Exam Topic 14)
When should an application invoke re-authentication in addition to initial user authentication?

A. At the application sign-off
B. Periodically during a session
C. After a period of inactivity
D. For each business process

Answer: C

NEW QUESTION 490
- (Exam Topic 14)
During a Disaster Recovery (DR) assessment, additional coverage for assurance is required. What should en assessor do?

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

Answer: A

NEW QUESTION 491
- (Exam Topic 14)
An organization operates a legacy Industrial Control System (ICS) to support its core business service, which carrot be replaced. Its management MUST be performed remotely through an administrative console software, which in tum depends on an old version of the Java Runtime Environment (JPE) known to be vulnerable to a number of attacks, How is this risk BEST managed?

A. Isolate the full ICS by moving It onto its own network segment
B. Air-gap and harden the host used for management purposes
C. Convince the management to decommission the ICS and mitigate to a modem technology
D. Deploy a restrictive proxy between all clients and the vulnerable management station

Answer: B

NEW QUESTION 493
- (Exam Topic 14)
Which of the below strategies would MOST comprehensively address the risk of malicious insiders leaking sensitive information?

A. Data Loss Protection (DIP), firewalls, data classification
B. Least privilege access, Data Loss Protection (DLP), physical access controls
C. Staff vetting, least privilege access, Data Loss Protection (DLP)
D. Background checks, data encryption, web proxies

Answer: B

NEW QUESTION 496
- (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 500
- (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 505
- (Exam Topic 14)
In order for application developers to detect potential vulnerabilities earlier during the Software Development Life Cycle (SDLC), which of the following safeguards should be implemented FIRST as part of a comprehensive testing framework?

A. Source code review
B. Acceptance testing
C. Threat modeling
D. Automated testing

Answer: A

NEW QUESTION 509
- (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 514
- (Exam Topic 14)
Point-to-Point Protocol (PPP) was designed to specifically address what issue?

A. A common design flaw in telephone modems
B. Speed and reliability issues between dial-up users and Internet Service Providers (ISP).
C. Compatibility issues with personal computers and web browsers
D. The security of dial-up connections to remote networks

Answer: B

NEW QUESTION 517
- (Exam Topic 14)
Which of the following is the MOST important activity an organization performs to ensure that securiy is part of the overall organization culture?

A. Ensue security policies are issued to all employees
B. Perform formal reviews of security Incidents.
C. Manage a program of security audits.
D. Work with senior management to meet business goals.

Answer: C

NEW QUESTION 518
- (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 520
- (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 523
- (Exam Topic 14)
Which type of fire alarm system sensor is intended to detect fire at its earliest stage?

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

Answer: A

NEW QUESTION 524
- (Exam Topic 14)
What should be the FIRST action for a security administrator who detects an intrusion on the network based on precursors and other indicators?

A. Isolate and contain the intrusion.
B. Notify system and application owners.
C. Apply patches to the Operating Systems (OS).
D. Document and verify the intrusion.

Answer: C

Explanation:
Reference:
https://securityintelligence.com/dont-dwell-on-it-how-to-detect-a-breach-on-your-network-more-efficiently/

NEW QUESTION 529
- (Exam Topic 14)
Which of the following security testing strategies is BEST suited for companies with low to moderate security maturity?

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

Answer: B

NEW QUESTION 532
- (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 535
- (Exam Topic 14)
Which of the following is the MOST important reason for timely installation of software patches?

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

Answer: C

NEW QUESTION 540
- (Exam Topic 14)
The MAIN task of promoting security for Personal Computers (PC) is

A. understanding the technical controls and ensuring they are correctly installed.
B. understanding the required systems and patching processes for different Operating Systems (OS).
C. making sure that users are using only valid, authorized software, so that the chance of virus infection
D. making users understand the risks to the machines and data, so they will take appropriate steps to project them.

Answer: C

NEW QUESTION 544
- (Exam Topic 14)
Which of the following is an accurate statement when an assessment results in the discovery of vulnerabilities in a critical network component?

A. The fact that every other host is sufficiently hardened does not change the fact frat the network is placed at risk of attack.
B. There is little likelihood that the entire network is being placed at a significant risk of attack.
C. A second assessment should immediately be performed after all vulnerabilities are corrected.
D. There is a low possibility that any adjacently connected components have been compromised by an attacker

Answer: C

NEW QUESTION 545
- (Exam Topic 14)
What are the roles within a scrum methodoligy?

A. System owner, scrum master, and development team
B. prduct owner, scrum master, and scrum team
C. Scrum master, requirements manager, and development team
D. Scrum master, quality assurance team, and scrum team

Answer: B

NEW QUESTION 546
- (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 550
- (Exam Topic 14)
When deploying en Intrusion Detection System (IDS) on a high-volume network, the need to distribute the load across multiple sensors would create which technical problem?

A. Session continuity
B. Proxy authentication failure
C. Sensor overload
D. Synchronized sensor updates

Answer: A

NEW QUESTION 555
- (Exam Topic 14)
Assume that a computer was powered off when an information security professional arrived at a crime scene. Which of the following actions should be performed after the crime scene is isolated?

A. Turn the computer on and collect volatile data.
B. Turn the computer on and collect network information.
C. Leave the computer off and prepare the computer for transportation to the laboratory
D. Remove the hard drive, prepare it for transportation, and leave the hardware ta the scene.

Answer: C

NEW QUESTION 558
- (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 563
- (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 566
- (Exam Topic 14)
Asymmetric algorithms are used for which of the following when using Secure Sockets Layer/Transport Layer Security (SSL/TLS) for implementing network security?

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

Answer: C

NEW QUESTION 567
- (Exam Topic 14)
Which of the following technologies would provide the BEST alternative to anti-malware software?

A. Host-based Intrusion Detection Systems (HIDS)
B. Application whitelisting
C. Host-based firewalls
D. Application sandboxing

Answer: B

NEW QUESTION 568
- (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 571
- (Exam Topic 14)
Which of the following initiates the system recovery phase of a disaster recovery plan?

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

Answer: C

NEW QUESTION 572
- (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 577
- (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 581
- (Exam Topic 14)
Which of the following provides the GREATEST level of data security for a Virtual Private Network (VPN) connection?

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

Answer: B

NEW QUESTION 582
- (Exam Topic 14)
Change management policies and procedures belong to which of the following types of controls?

A. Directive
B. Detective
C. Corrective
D. Preventative

Answer: A

Explanation:
Reference: https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA570&lpg=PA570&dq=CISSP+Change+mana

NEW QUESTION 583
- (Exam Topic 14)
Which type of test suite should be run for fast feedback during application develoment?

A. Full recession
B. End-to-end
C. Smoke
D. Specific functionality

Answer: C

NEW QUESTION 587
- (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 592
- (Exam Topic 14)
Organization A is adding a large collection of confidential data records that it received when it acquired Organization B to its data store. Many of the users and staff from Organization B are no longer available. Which of the following MUST Organization A 0do to property classify and secure the acquired data?

A. Assign data owners from Organization A to the acquired data.
B. Create placeholder accounts that represent former users from Organization B.
C. Archive audit records that refer to users from Organization A.
D. Change the data classification for data acquired from Organization B.

Answer: A

NEW QUESTION 594
- (Exam Topic 14)
What high Availability (HA) option of database allows multiple clients to access multiple database servers simultaneously?

A. Non-Structured Query Language (NoSQL) database
B. Relational database
C. Shadow database
D. Replicated database

Answer: C

NEW QUESTION 595
- (Exam Topic 14)
Why do certificate Authorities (CA) add value to the security of electronic commerce transactions?

A. They maintain the certificate revocation list.
B. They maintain the private keys of transition parties.
C. They verify the transaction parties' private keys.
D. They provide a secure communication enamel to the transaction parties.

Answer: D

NEW QUESTION 597
- (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 601
- (Exam Topic 14)
Which of the following is the BEST way to protect against structured Query language (SQL) injection?

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

Answer: D

NEW QUESTION 604
- (Exam Topic 14)
Which of the following methods MOST efficiently manages user accounts when using a third-party cloud-based application and directory solution?

A. Cloud directory
B. Directory synchronization
C. Assurance framework
D. Lightweight Directory Access Protocol (LDAP)

Answer: B

NEW QUESTION 608
- (Exam Topic 14)
An Intrusion Detection System (IDS) is based on the general hypothesis that a security violation is associated with a pattern of system usage which can be

A. differentiated from a normal usage pattern.
B. used to detect known violations.
C. used to detect a masquerader.
D. differentiated to detect all security violations.

Answer: A

NEW QUESTION 612
- (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 615
- (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 616
- (Exam Topic 14)
Which of the following objects should be removed FIRST prior to uploading code to public code repositories?

A. Security credentials
B. Known vulnerabilities
C. Inefficient algorithms
D. Coding mistakes

Answer: A

NEW QUESTION 620
- (Exam Topic 14)
Why might a network administrator choose distributed virtual switches instead of stand-alone switches for network segmentation?

A. To standardize on a single vendor
B. To ensure isolation of management traffic
C. To maximize data plane efficiency
D. To reduce the risk of configuration errors

Answer: C

NEW QUESTION 625
- (Exam Topic 14)
Individual access to a network is BEST determined based on

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

Answer: C

NEW QUESTION 627
- (Exam Topic 14)
Which of the following activities is MOST likely to be performed during a vulnerability assessment?

A. Establish caller authentication procedures to verify the identities of users.
B. Analyze the environment by conducting interview sessions with relevant parties.
C. Document policy exceptions required to access systems in non-compliant areas.
D. Review professorial credentials of the vulnerability assessment team or vendor.

Answer: D

NEW QUESTION 630
- (Exam Topic 14)
What is the threat modeling order using process for Attack simu-lation and threat analysis (PASTA)?

A. Application decomposition, threat analysis, vulnerability detection, attack enumeration, risk/impact analysis
B. Threat analysis, vulnerability detection, application decomposition, attack enumeration, risk/Impact analysis
C. Risk/impact analysis, application decomposition, threat analysis, vulnerability detection, attack enumeration
D. Application decomposition, threat analysis, risk/impact analysis, vulnerability detection, attack enumeration

Answer: A

NEW QUESTION 634
- (Exam Topic 14)
Which of the following MOST applies to session initiation protocal (SIP) security?

A. It leverages Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS).
B. It requires a Public Key Infrastructure (PKI).
C. It reuses security mechanisms derived from existing protocols.
D. It supports end-to-end security natively.

Answer: C

NEW QUESTION 635
- (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 638
- (Exam Topic 14)
What is a common mistake in records retention?

A. Having the organization legal department create a retention policy
B. Adopting a retention policy based on applicable organization requirements
C. Having the Human Resource (HR) department create a retention policy
D. Adopting a retention policy with the longest requirement period

Answer: C

NEW QUESTION 639
- (Exam Topic 14)
An Internet software application requires authentication before a user is permitted to utilize the resource. Which testing scenario BEST validates the functionality of the application?

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

Answer: B

NEW QUESTION 643
- (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 648
- (Exam Topic 14)
What technique used for spoofing the origin of an email can successfully conceal the sender s Internet Protocol (IP) address?

A. Change In-Reply-To data
B. Web crawling
C. Onion routing
D. Virtual Private Network (VPN)

Answer: C

NEW QUESTION 652
- (Exam Topic 14)
Which one of the following is an advantage of an effective release control strategy from a configuration control standpoint?

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

Answer:

C

NEW QUESTION 655
- (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 659
- (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 664
- (Exam Topic 14)
Why are mobile devices something difficult to investigate in a forensic examination?

A. There are no forensics tools available for examination.
B. They may have proprietary software installed to protect them.
C. They may contain cryptographic protection.
D. They have password-based security at logon.

Answer: B

NEW QUESTION 667
- (Exam Topic 14)
Which of the following was developed to support multiple protocols as well as provide as well as provide login, password, and error correction capabilities?

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

Answer: A

NEW QUESTION 669
- (Exam Topic 14)
When conducting a forensic criminal investigation on a computer had drive, what should be dene PRIOR to analysis?

A. Create a backup copy of all the important files on the drive.
B. Power off the computer and wait for assistance.
C. Create a forensic image of the hard drive.
D. Install forensic analysis software.

Answer: C

NEW QUESTION 672
- (Exam Topic 14)
Which inherent password weakness does a One Time Password (OTP) generator overcome?

A. Static passwords must be changed frequently.
B. Static passwords are too predictable.
C. Static passwords are difficult to generate.
D. Static passwords are easily disclosed.

Answer: D

NEW QUESTION 676

- (Exam Topic 14)
Which of the following presents the PRIMARY concern to an organization when setting up a federated single sign-on (SSO) solution with another

A. Sending assertions to an identity provider
B. Requesting Identity assertions from the partners domain
C. defining the identity mapping scheme
D. Having the resource provider query the Identity provider

Answer: C

NEW QUESTION 681
- (Exam Topic 14)
Which testing method requires very limited or no information about the network infrastructure?

A. While box
B. Static
C. Black box
D. Stress

Answer: C

NEW QUESTION 686
- (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 690
- (Exam Topic 14)
Which of the following is a characteristic of a challenge/response authentication process?

A. Using a password history blacklist
B. Transmitting a hash based on the user's password
C. Presenting distorted gravies of text for authentication
D. Requiring the use of non-consecutive numeric characters

Answer: C

NEW QUESTION 692
- (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 695
- (Exam Topic 14)
For a federated identity solution, a third-party Identity Provider (IdP) is PRIMARILY responsible for which of the following?

A. Access Control
B. Account Management
C. Authentication
D. Authorization

Answer: C

NEW QUESTION 700
- (Exam Topic 14)

What Is the FIRST step for a digital investigator to perform when using best practices to collect digital evidence from a potential crime scene?

A. Consult the lead investigate to team the details of the case and required evidence.
B. Assure that grounding procedures have been followed to reduce the loss of digital data due to static electricity discharge.
C. Update the Basic Input Output System (BIOS) and Operating System (OS) of any tools used to assure evidence admissibility.
D. Confirm that the appropriate warrants were issued to the subject of the investigation to eliminate illegal search claims.

Answer: D

NEW QUESTION 703
- (Exam Topic 14)
Which of the following attributes could be used to describe a protection mechanism of an open design methodology?

A. It 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 707
- (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 708
- (Exam Topic 14)
Which of the following BEST describes the responsibilities of data owner?

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

Answer: B

NEW QUESTION 713
- (Exam Topic 14)
What is the BEST way to establish identity over the internet?

A. Challenge Handshake Authentication Protocol (CHAP) and strong passwords
B. Internet Mail Access Protocol (IMAP) with Triple Data Encryption Standard (3DES)
C. Remote Authentication Dial-In User Service (RADIUS) server with hardware tokens
D. Remote user authentication via Simple Object Access Protocol (SOAP)

Answer: D

NEW QUESTION 714
- (Exam Topic 14)
What is the BEST method if an investigator wishes to analyze a hard drive which may be used as evidence?

A. Leave the hard drive in place and use only verified and authenticated Operating Systems (OS) utilities ...
B. Log into the system and immediately make a copy of all relevant files to a Write Once, Read Many ...
C. Remove the hard drive from the system and make a copy of the hard drive's contents using imaging hardware.
D. Use a separate bootable device to make a copy of the hard drive before booting the system and analyzing the hard drive.

Answer: C

NEW QUESTION 716
- (Exam Topic 13)
When developing a business case for updating a security program, the security program owner MUST do which of the following?

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

Answer: A

NEW QUESTION 721
- (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 724
- (Exam Topic 13)
A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report. In which phase of the assessment was this error MOST likely made?

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

Answer: A

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 729
- (Exam Topic 13)
What is the PRIMARY role of a scrum master in agile development?

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

Answer: D

NEW QUESTION 733
- (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 736
- (Exam Topic 13)
Which of the following access management procedures would minimize the possibility of an organization's employees retaining access to secure werk areas after they change roles?

A. User access modification
B. user access recertification
C. User access termination
D. User access provisioning

Answer: B

NEW QUESTION 740
- (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 743
- (Exam Topic 13)
Which of the following would BEST support effective testing of patch compatibility when patches are applied to an organization’s systems?

A. Standardized configurations for devices
B. Standardized patch testing equipment
C. Automated system patching
D. Management support for patching

Answer: C

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 747
- (Exam Topic 13)
Which of the following is the MOST important security goal when performing application interface testing?

A. Confirm that all platforms are supported and function properly
B. Evaluate whether systems or components pass data and control correctly to one another
C. Verify compatibility of software, hardware, and network connections
D. Examine error conditions related to external interfaces to prevent application details leakage

Answer: B

NEW QUESTION 752
- (Exam Topic 13)
When developing solutions for mobile devices, in which phase of the Software Development Life Cycle (SDLC) should technical limitations related to devices be specified?

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

Answer: A

NEW QUESTION 753
- (Exam Topic 13)
Which of the following entails identification of data and links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

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

Answer: B

NEW QUESTION 755
- (Exam Topic 13)
Within the company, desktop clients receive Internet Protocol (IP) address over Dynamic Host Configuration Protocol (DHCP).
Which of the following represents a valid measure to help protect the network against unauthorized access?

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

Answer: B

NEW QUESTION 759
- (Exam Topic 13)
An organization has outsourced its financial transaction processing to a Cloud Service Provider (CSP) who will provide them with Software as a Service (SaaS). If there was a data breach who is responsible for monetary losses?

A. The Data Protection Authority (DPA)
B. The Cloud Service Provider (CSP)
C. The application developers
D. The data owner

Answer: B

NEW QUESTION 760
- (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 764
- (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 768
- (Exam Topic 13)
Even though a particular digital watermark is difficult to detect, which of the following represents a way it might still be inadvertently removed?

A. Truncating parts of the data
B. Applying Access Control Lists (ACL) to the data
C. Appending non-watermarked data to watermarked data
D. Storing the data in a database

Answer: A

NEW QUESTION 773
- (Exam Topic 13)
Which of the following mandates the amount and complexity of security controls applied to a security risk?

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

Answer: C

NEW QUESTION 778
- (Exam Topic 13)
Which of the following is the BEST metric to obtain when gaining support for an Identify and Access Management (IAM) solution?

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

Answer: D

NEW QUESTION 782
- (Exam Topic 13)
A security compliance manager of a large enterprise wants to reduce the time it takes to perform network, system, and application security compliance audits while increasing quality and effectiveness of the results. What should be implemented to BEST achieve the desired results?

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

Answer: A

NEW QUESTION 784
- (Exam Topic 13)
The core component of Role Based Access Control (RBAC) must be constructed of defined data elements. Which elements are required?

A. Users, permissions, operations, and protected objects
B. Roles, accounts, permissions, and protected objects
C. Users, roles, operations, and protected objects
D. Roles, operations, accounts, and protected objects

Answer: C

NEW QUESTION 788
- (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 792
- (Exam Topic 13)
Which of the following could be considered the MOST significant security challenge when adopting DevOps practices compared to a more traditional control framework?

A. Achieving Service Level Agreements (SLA) on how quickly patches will be released when a security flaw is found.
B. Maintaining segregation of duties.
C. Standardized configurations for logging, alerting, and security metrics.
D. Availability of security teams at the end of design process to perform last-minute manual audits and reviews.

Answer: B

NEW QUESTION 794
- (Exam Topic 13)
A control to protect from a Denial-of-Service (DoS) attach has been determined to stop 50% of attacks, and additionally reduces the impact of an attack by 50%. What is the residual risk?

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

Answer: B

NEW QUESTION 796
- (Exam Topic 13)
In a change-controlled environment, which of the following is MOST likely to lead to unauthorized changes to production programs?

A. Modifying source code without approval
B. Promoting programs to production without approval
C. Developers checking out source code without approval
D. Developers using Rapid Application Development (RAD) methodologies without approval

Answer: A

NEW QUESTION 800
- (Exam Topic 13)
Who has the PRIMARY responsibility to ensure that security objectives are aligned with organization goals?

A. Senior management
B. Information security department
C. Audit committee
D. All users

Answer: C

NEW QUESTION 804
- (Exam Topic 13)
A security practitioner is tasked with securing the organization's Wireless Access Points (WAP). Which of these is the MOST effective way of restricting this environment to authorized users?

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

Answer: D

NEW QUESTION 807
- (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 809

- (Exam Topic 13)
An organization plan on purchasing a custom software product developed by a small vendor to support its business model. Which unique consideration should be made part of the contractual agreement potential
long-term risks associated with creating this dependency?

A. A source code escrow clause
B. Right to request an independent review of the software source code
C. Due diligence form requesting statements of compliance with security requirements
D. Access to the technical documentation

Answer: B

NEW QUESTION 810
- (Exam Topic 13)
Which of the following methods of suppressing a fire is environmentally friendly and the MOST appropriate for a data center?

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

Answer: A

NEW QUESTION 814
- (Exam Topic 13)
Which of the following management process allows ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

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

Answer: A

NEW QUESTION 819
- (Exam Topic 13)
An organization's security policy delegates to the data owner the ability to assign which user roles have access to a particular resource. What type of authorization mechanism is being used?

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

Answer: A

NEW QUESTION 821
- (Exam Topic 13)
Which of the following is considered a secure coding practice?

A. Use concurrent access for shared variables and resources
B. Use checksums to verify the integrity of libraries
C. Use new code for common tasks
D. Use dynamic execution functions to pass user supplied data

Answer: B

NEW QUESTION 823
- (Exam Topic 13)
What is the expected outcome of security awareness in support of a security awareness program?

A. Awareness activities should be used to focus on security concerns and respond to those concerns accordingly
B. Awareness is not an activity or part of the training but rather a state of persistence to support the program
C. Awareness is trainin
D. The purpose of awareness presentations is to broaden attention of security.
E. Awareness is not trainin
F. The purpose of awareness presentation is simply to focus attention on security.

Answer: C

NEW QUESTION 825
- (Exam Topic 13)
A company seizes a mobile device suspected of being used in committing fraud. What would be the BEST method used by a forensic examiner to isolate the powered-on device from the network and preserve the evidence?

A. Put the device in airplane mode

B. Suspend the account with the telecommunication provider
C. Remove the SIM card
D. Turn the device off

Answer: A

NEW QUESTION 827
- (Exam Topic 13)
The design review for an application has been completed and is ready for release. What technique should an organization use to assure application integrity?

A. Application authentication
B. Input validation
C. Digital signing
D. Device encryption

Answer: B

NEW QUESTION 831
- (Exam Topic 12)
During the Security Assessment and Authorization process, what is the PRIMARY purpose for conducting a hardware and software inventory?

A. Calculate the value of assets being accredited.
B. Create a list to include in the Security Assessment and Authorization package.
C. Identify obsolete hardware and software.
D. Define the boundaries of the information system.

Answer: A

NEW QUESTION 836
- (Exam Topic 13)
Digital certificates used in Transport Layer Security (TLS) support which of the following?

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

Answer: D

NEW QUESTION 841
- (Exam Topic 12)
Reciprocal backup site agreements are considered to be

A. a better alternative than the use of warm sites.
B. difficult to test for complex systems.
C. easy to implement for similar types of organizations.
D. easy to test and implement for complex systems.

Answer: B

NEW QUESTION 842
- (Exam Topic 12)
In which identity management process is the subject's identity established?

A. Trust
B. Provisioning
C. Authorization
D. Enrollment

Answer: D

NEW QUESTION 846
- (Exam Topic 12)
An organization's information security strategic plan MUST be reviewed

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

Answer: C

NEW QUESTION 849
- (Exam Topic 12)
Which of the following is a characteristic of the initialization vector when using Data Encryption Standard (DES)?

A. It must be known to both sender and receiver.
B. It can be transmitted in the clear as a random number.
C. It must be retained until the last block is transmitted.
D. It can be used to encrypt and decrypt information.

Answer: B

NEW QUESTION 850
- (Exam Topic 12)
The application of a security patch to a product previously validate at Common Criteria (CC) Evaluation Assurance Level (EAL) 4 would

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

Answer: B

NEW QUESTION 851
.....

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