Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

https://www.2passeasy.com/dumps/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)
An organization has been collecting a large amount of redundant and unusable data and filling up the storage area network (SAN). Management has requested the identification of a solution that will address ongoing storage problems. Which is the BEST technical solution?

A. Deduplication
B. Compression
C. Replication
D. Caching

Answer: B

NEW QUESTION 3
- (Exam Topic 15)
What is a use for mandatory access control (MAC)?

A. Allows for labeling of sensitive user accounts for access control
B. Allows for mandatory user identity and passwords based on sensitivity
C. Allows for mandatory system administrator access control over objects
D. Allows for object security based on sensitivity represented by a label

Answer: D

NEW QUESTION 4
- (Exam Topic 15)
Which of the following is fundamentally required to address potential security issues when initiating software development?

A. Implement ongoing security audits in all environments.
B. Ensure isolation of development from production.
C. Add information security objectives into development.
D. Conduct independent source code review.

Answer: C

NEW QUESTION 5
- (Exam Topic 15)
A breach investigation …… a website was exploited through an open soured …..Is The FIRB Stan In the Process that could have prevented this breach?

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

Answer: B

NEW QUESTION 6
- (Exam Topic 15)
Which of the following is the FIRST step for defining Service Level Requirements (SLR)?

A. Creating a prototype to confirm or refine the customer requirements
B. Drafting requirements for the service level agreement (SLA)
C. Discussing technology and solution requirements with the customer
D. Capturing and documenting the requirements of the customer

Answer: D

NEW QUESTION 7
- (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 8
- (Exam Topic 15)
Which of the following actions should be undertaken prior to deciding on a physical baseline Protection Profile (PP)?

A. Check the technical design.
B. Conduct a site survey.
C. Categorize assets.
D. Choose a suitable location.

Answer: A

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

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

Answer: D

NEW QUESTION 10
- (Exam Topic 15)
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 10
- (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 13
- (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 15
- (Exam Topic 15)
During a Disaster Recovery (DR) simulation, it is discovered that the shared recovery site lacks adequate data restoration capabilities to support the implementation of multiple plans simultaneously. What would be impacted by this fact if left unchanged?

A. Recovery Point Objective (RPO)
B. Recovery Time Objective (RTO)
C. Business Impact Analysis (BIA)
D. Return on Investment (ROI)
E. A

Answer: E

NEW QUESTION 18
- (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 23
- (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 28
- (Exam Topic 15)
The Rivest-Shamir-Adleman (RSA) algorithm is BEST suited for which of the following operations?

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

Answer: C

NEW QUESTION 29
- (Exam Topic 15)
What type of attack sends Internet Control Message Protocol (ICMP) echo requests to the target machine with a larger payload than the target can handle?

A. Man-in-the-Middle (MITM)
B. Denial of Service (DoS)
C. Domain Name Server (DNS) poisoning
D. Buffer overflow

Answer: B

NEW QUESTION 30
- (Exam Topic 15)
Which of the following security objectives for industrial control systems (ICS) can be adapted to securing any Internet of Things (IoT) system?

A. Prevent unauthorized modification of data.
B. Restore the system after an incident.
C. Detect security events and incidents.
D. Protect individual components from exploitation

Answer: D

NEW QUESTION 32
- (Exam Topic 15)
Which of the following MUST the administrator of a security information and event management (SIEM) system ensure?

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

Answer: C

NEW QUESTION 36
- (Exam Topic 15)
A digitally-signed e-mail was delivered over a wireless network protected with Wired Equivalent Privacy (WEP) protocol. Which of the following principles is at risk?

A. Availability
B. Non-Repudiation
C. Confidentiality
D. Integrity

Answer: B

NEW QUESTION 37
- (Exam Topic 15)

Which of the following is an indicator that a company's new user security awareness training module has been effective?

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

Answer: B

NEW QUESTION 42
- (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 44
- (Exam Topic 15)
Which of the following actions should be taken by a security professional when a mission critical computer network attack is suspected?

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

Answer: C

NEW QUESTION 45
- (Exam Topic 15)
A security architect is reviewing plans for an application with a Recovery Point Objective (RPO) of 15 minutes. The current design has all of the application infrastructure located within one co-location data center. Which security principle is the architect currently assessing?

A. Availability
B. Disaster recovery (DR)
C. Redundancy
D. Business continuity (BC)

Answer: D

NEW QUESTION 50
- (Exam Topic 15)
As a design principle, which one of the following actors is responsible for identifying and approving data security requirements in a cloud ecosystem?

A. Cloud broker
B. Cloud provider
C. Cloud consumer
D. Cloud auditor

Answer: C

NEW QUESTION 51
- (Exam Topic 15)
An establish information technology (IT) consulting firm is considering acquiring a successful local startup. To gain a comprehensive understanding of the startup's security posture' which type of assessment provides the BEST information?

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

Answer: A

NEW QUESTION 55
- (Exam Topic 15)
Which of the following is an example of a vulnerability of full-disk encryption (FDE)?

A. Data at rest has been compromised when the user has authenticated to the device.
B. Data on the device cannot be restored from backup.
C. Data in transit has been compromised when the user has authenticated to the device.
D. Data on the device cannot be backed up.

Answer: A

NEW QUESTION 56
- (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 61
- (Exam Topic 15)
Which of the following is the MOST important rule for digital investigations?

A. Ensure event logs are rotated.
B. Ensure original data is never modified.
C. Ensure individual privacy is protected.
D. Ensure systems are powered on.

Answer: C

NEW QUESTION 63
- (Exam Topic 15)
Using the cipher text and resultant clear text message to derive the non-alphabetic cipher key is an example of which method of cryptanalytic attack?

A. Frequency analysis
B. Ciphertext-only attack
C. Probable-plaintext attack
D. Known-plaintext attack

Answer: D

NEW QUESTION 66
- (Exam Topic 15)
Information Security Continuous Monitoring (1SCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management
decisions. Which of the following is the FIRST step in developing an ISCM strategy and implementing an ISCM program?

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

Answer: A

NEW QUESTION 71
- (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 75
- (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 77
- (Exam Topic 15)
Which Open Systems Interconnection (OSI) layer(s) BEST corresponds to the network access layer in the Transmission Control Protocol/Internet Protocol (TCP/IP) model?

A. Transport Layer

B. Data Link and Physical Layers
C. Application, Presentation, and Session Layers
D. Session and Network Layers

Answer: B

NEW QUESTION 79
- (Exam Topic 15)
A financial organization that works according to agile principles has developed a new application for their external customer base to request a line of credit. A security analyst has been asked to assess the security risk of the minimum viable product (MVP). Which is the MOST important activity the analyst should assess?

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

Answer: A

NEW QUESTION 82
- (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 85
- (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 89
- (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 92
- (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 96
- (Exam Topic 15)
Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

A. Scope options
B. Reservation
C. Dynamic assignment
D. Exclusion
E. Static assignment

Answer: B

NEW QUESTION 97

- (Exam Topic 15)
Which of the following is the MAIN difference between a network-based firewall and a host-based firewall?

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

Answer: B

NEW QUESTION 100
- (Exam Topic 15)
If the wide area network (WAN) is supporting converged applications like Voice over Internet Protocol (VoIP), which of the following becomes even MORE essential to the assurance of network?

A. Classless Inter-Domain Routing (CIDR)
B. Deterministic routing
C. Internet Protocol (IP) routing lookups
D. Boundary routing

Answer: C

NEW QUESTION 104
- (Exam Topic 15)
A colleague who recently left the organization asked a security professional for a copy of the organization's confidential incident management policy. Which of the following is the BEST response to this request?

A. Email the policy to the colleague as they were already part of the organization and familiar with it.
B. Do not acknowledge receiving the request from the former colleague and ignore them.
C. Access the policy on a company-issued device and let the former colleague view the screen.
D. Submit the request using company official channels to ensure the policy is okay to distribute.

Answer: B

NEW QUESTION 109
- (Exam Topic 15)
When designing a business continuity plan (BCP), what is the formula to determine the Maximum Tolerable Downtime (MTD)?

A. Annual Loss Expectancy (ALE) + Work Recovery Time (WRT)
B. Business impact analysis (BIA) + Recovery Point Objective (RPO)
C. Recovery Time Objective (RTO) + Work Recovery Time (WRT)
D. Estimated Maximum Loss (EML) + Recovery Time Objective (RTO)

Answer: C

NEW QUESTION 111
- (Exam Topic 15)
When designing a new Voice over Internet Protocol (VoIP) network, an organization's top concern is preventing unauthorized users accessing the VoIP network. Which of the following will BEST help secure the VoIP network?

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

Answer: A

NEW QUESTION 114
- (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 118
- (Exam Topic 15)
An organization has discovered that organizational data is posted by employees to data storage accessible to the general public. What is the PRIMARY step an organization must take
to ensure data is properly protected from public release?

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

D. Implement a user reporting policy.

Answer: C

NEW QUESTION 121
- (Exam Topic 15)
An information security administrator wishes to block peer-to-peer (P2P) traffic over Hypertext Transfer Protocol (HTTP) tunnels. Which of the following layers of the Open Systems Interconnection (OSI) model requires inspection?

A. Presentation
B. Transport
C. Session
D. Application

Answer: A

NEW QUESTION 123
- (Exam Topic 15)
A corporation does not have a formal data destruction policy. During which phase of a criminal legal proceeding will this have the MOST impact?

A. Arraignment
B. Trial
C. Sentencing
D. Discovery

Answer: D

NEW QUESTION 127
- (Exam Topic 15)
Which of the following security tools monitors devices and records the information in a central database for further analysis?

A. Security orchestration automation and response
B. Host-based intrusion detection system (HIDS)
C. Antivirus
D. Endpoint detection and response (EDR)

Answer: A

NEW QUESTION 132
- (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 137
- (Exam Topic 15)
A developer is creating an application that requires secure logging of all user activity. What is the BEST permission the developer should assign to the log file to ensure requirements are met?

A. Read
B. Execute
C. Write
D. Append

Answer: C

NEW QUESTION 141
- (Exam Topic 15)
A security architect is developing an information system for a client. One of the requirements is to deliver a platform that mitigates against common vulnerabilities and attacks, What is the MOST efficient option used to prevent buffer overflow attacks?

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

Answer: B

NEW QUESTION 144

- (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 145
- (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 149
- (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 154
- (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 157
- (Exam Topic 15)
At the destination host, which of the following OSI model layers will discard a segment with a bad checksum in the UDP header?

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

Answer: C

NEW QUESTION 160
- (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 161
- (Exam Topic 15)
Which of the following is the PRIMARY reason for selecting the appropriate level of detail for audit record generation?

A. Lower costs throughout the System Development Life Cycle (SDLC)
B. Facilitate a root cause analysis (RCA)
C. Enable generation of corrective action reports
D. Avoid lengthy audit reports

Answer: B

NEW QUESTION 164
- (Exam Topic 15)
When conducting a third-party risk assessment of a new supplier, which of the following reports should be reviewed to confirm the operating effectiveness of the security, availability, confidentiality, and privacy trust principles?

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

Answer: B

NEW QUESTION 165
- (Exam Topic 15)
Which event magnitude is defined as deadly, destructive, and disruptive when a hazard interacts with human vulnerability?

A. Disaster
B. Catastrophe
C. Crisis
D. Accident

Answer: B

NEW QUESTION 168
- (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 171
- (Exam Topic 15)
The Chief Information Security Officer (CISO) is concerned about business application availability. The organization was recently subject to a ransomware attack that resulted in the unavailability of applications and services for 10 working days that required paper-based running of all main business processes. There are now aggressive plans to enhance the Recovery Time Objective (RTO) and cater for more frequent data captures. Which of the following solutions should be implemented to fully comply to the new business requirements?

A. Virtualization
B. Antivirus
C. Process isolation
D. Host-based intrusion prevention system (HIPS)

Answer: A

NEW QUESTION 173
- (Exam Topic 15)
An organization recently suffered from a web-application attack that resulted in stolen user session cookie information. The attacker was able to obtain the information when a user's browser executed a script upon visiting a compromised website. What type of attack MOST likely occurred?

A. Cross-Site Scripting (XSS)
B. Extensible Markup Language (XML) external entities
C. SQL injection (SQLI)
D. Cross-Site Request Forgery (CSRF)

Answer: A

NEW QUESTION 178
- (Exam Topic 15)
The security team plans on using automated account reconciliation in the corporate user access review process. Which of the following must be implemented for the BEST results with fewest errors when running the audit?

A. Removal of service accounts from review
B. Segregation of Duties (SoD)
C. Clear provisioning policies
D. Frequent audits

Answer: C

NEW QUESTION 180
- (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 183
- (Exam Topic 15)
Which of the following types of datacenter architectures will MOST likely be used in a large SDN and can be extended beyond the datacenter?

A. iSCSI
B. FCoE
C. Three-tiered network
D. Spine and leafE Top-of-rack switching

Answer: B

NEW QUESTION 185
- (Exam Topic 15)
A hospital enforces the Code of Fair Information Practices. What practice applies to a patient requesting their medical records from a web portal?

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

Answer: D

NEW QUESTION 190
- (Exam Topic 15)
An organization's retail website provides its only source of revenue, so the disaster recovery plan (DRP) must document an estimated time for each step in the plan.
Which of the following steps in the DRP will list the GREATEST duration of time for the service to be fully operational?

A. Update the Network Address Translation (NAT) table.
B. Update Domain Name System (DNS) server addresses with domain registrar.
C. Update the Border Gateway Protocol (BGP) autonomous system number.
D. Update the web server network adapter configuration.

Answer: B

NEW QUESTION 191
- (Exam Topic 15)
Configuring a Wireless Access Point (WAP) with the same Service Set Identifier (SSID) as another WAP in order to have users unknowingly connect is referred to as which of the following?

A. Jamming
B. Man-irHht-Middk (MITM)
C. War driving
D. Internet Protocol (IP) spoofing

Answer: B

NEW QUESTION 193
- (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 197
- (Exam Topic 15)
During an internal audit of an organizational Information Security Management System (ISMS), nonconformities are identified. In which of the following

management stages are nonconformities reviewed, assessed and/or corrected by the organization?

A. Planning
B. Operation
C. Assessment
D. Improvement

Answer: B

NEW QUESTION 200
- (Exam Topic 15)
An organization is implementing data encryption using symmetric ciphers and the Chief Information Officer (CIO) is concerned about the risk of using one key to protect all sensitive data, The security practitioner has been tasked with recommending a solution to address the CIO's concerns, Which of the following is the BEST approach to achieving the objective by encrypting all sensitive data?

A. Use a Secure Hash Algorithm 256 (SHA-256).
B. Use a hierarchy of encryption keys.
C. Use Hash Message Authentication Code (HMAC) keys.
D. Use Rivest-Shamir-Adleman (RSA) keys.

Answer: D

NEW QUESTION 203
- (Exam Topic 15)
Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

A. Layer 3 switch
B. VPN headend
C. Next-generation firewall
D. Proxy server
E. Intrusion prevention

Answer: C

NEW QUESTION 207
- (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 211
- (Exam Topic 15)
Which of the following documents specifies services from the client's viewpoint?

A. Service level report
B. Business impact analysis (BIA)
C. Service level agreement (SLA)
D. Service Level Requirement (SLR)

Answer: C

NEW QUESTION 215
- (Exam Topic 15)
In Identity Management (IdM), when is the verification stage performed?

A. As part of system sign-on
B. Before creation of the identity
C. After revocation of the identity
D. During authorization of the identity

Answer: A

NEW QUESTION 220
- (Exam Topic 15)
A Chief Information Officer (CIO) has delegated responsibility of their system security to the head of the information technology (IT) department. While corporate policy dictates that only the CIO can make decisions on the level of data protection required, technical implementation decisions are done by the head of the IT department. Which of the following BEST describes the security role filled by the head of the IT department?

A. System analyst
B. System security officer

C. System processor
D. System custodian

Answer: D

NEW QUESTION 222
- (Exam Topic 15)
Which of the following is the MOST effective measure for dealing with rootkit attacks?

A. Turing off unauthorized services and rebooting the system
B. Finding and replacing the altered binaries with legitimate ones
C. Restoring the system from the last backup
D. Reinstalling the system from trusted sources

Answer: D

NEW QUESTION 226
- (Exam Topic 15)
Which of the following is the MOST important first step in preparing for a security audit?

A. Identify team members.
B. Define the scope.
C. Notify system administrators.
D. Collect evidence.

Answer: B

NEW QUESTION 229
- (Exam Topic 15)
Which of the following is the PRIMARY purpose of installing a mantrap within a facility?

A. Control traffic
B. Prevent rapid movement
C. Prevent plggybacking
D. Control air flow

Answer: C

NEW QUESTION 230
- (Exam Topic 15)
A company is attempting to enhance the security of its user authentication processes. After evaluating several options, the company has decided to utilize Identity as a Service (IDaaS).
Which of the following factors leads the company to choose an IDaaS as their solution?

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

Answer: B

NEW QUESTION 235
- (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 237
- (Exam Topic 15)
When assessing web vulnerabilities, how can navigating the dark web add value to a penetration test?

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

Answer: D

NEW QUESTION 240

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

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

Answer: D

NEW QUESTION 242
- (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 247
- (Exam Topic 15)
When telephones in a city are connected by a single exchange, the caller can only connect with the switchboard operator. The operator then manually connects the call.
This is an example of which type of network topology?

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

Answer: A

NEW QUESTION 248
- (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 252
- (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 256
- (Exam Topic 15)
The Chief Information Security Officer (CISO) of a small organization is making a case for building a security operations center (SOC). While debating between an in-house, fully outsourced, or a hybrid capability, which of the following would be the MAIN consideration, regardless of the model?

A. Skill set and training
B. Headcount and capacity
C. Tools and technologies
D. Scope and service catalog

Answer: C

NEW QUESTION 261
- (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 264
- (Exam Topic 15)
A hacker can use a lockout capability to start which of the following attacks?

A. Denial of service (DoS)
B. Dictionary
C. Ping flood
D. Man-in-the-middle (MITM)

Answer: A

NEW QUESTION 267
- (Exam Topic 15)
An organization wants a service provider to authenticate users via the users' organization domain credentials. Which markup language should the organization's security personnel use to support the integration?

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

Answer: A

NEW QUESTION 271
- (Exam Topic 15)
A firm within the defense industry has been directed to comply with contractual requirements for encryption of a government client's Controlled Unclassified Information (CUI). What encryption strategy represents how to protect data at rest in the MOST efficient and cost-effective manner?

A. Perform physical separation of program information and encrypt only information deemed critical by the defense client
B. Perform logical separation of program information, using virtualized storage solutions with built-in encryption at the virtualization layer
C. Perform logical separation of program information, using virtualized storage solutions with encryption management in the back-end disk systems
D. Implement data at rest encryption across the entire storage area network (SAN)

Answer: C

NEW QUESTION 275
- (Exam Topic 15)
Which of the following is the FIRST step an organization's security professional performs when defining a cyber-security program based upon industry standards?

A. Map the organization's current security practices to industry standards and frameworks.
B. Define the organization's objectives regarding security and risk mitigation.
C. Select from a choice of security best practices.
D. Review the past security assessments.

Answer: A

NEW QUESTION 277
- (Exam Topic 15)
What is considered a compensating control for not having electrical surge protectors installed?

A. Having dual lines to network service providers built to the site
B. Having backup diesel generators installed to the site
C. Having a hot disaster recovery (DR) environment for the site
D. Having network equipment in active-active clusters at the site

Answer: D

NEW QUESTION 279
- (Exam Topic 15)
Which type of access control includes a system that allows only users that are type=managers and department=sales to access employee records?

A. Discretionary access control (DAC)
B. Mandatory access control (MAC)
C. Role-based access control (RBAC)
D. Attribute-based access control (ABAC)

Answer: C

NEW QUESTION 282
- (Exam Topic 15)

Which of the following BEST describes the use of network architecture in reducing corporate risks associated with mobile devices?

A. Maintaining a "closed applications model on all mobile devices depends on demilitarized 2one (DM2) servers
B. Split tunneling enabled for mobile devices improves demilitarized zone (DMZ) security posture
C. Segmentation and demilitarized zone (DMZ) monitoring are implemented to secure a virtual private network (VPN) access for mobile devices
D. Applications that manage mobile devices are located in an Internet demilitarized zone (DMZ)

Answer: C

NEW QUESTION 285
- (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 290
- (Exam Topic 15)
What industry-recognized document could be used as a baseline reference that is related to data security and business operations for conducting a security assessment?

A. Service Organization Control (SOC) 1 Type 2
B. Service Organization Control (SOC) 2 Type 1
C. Service Organization Control (SOC) 1 Type 1
D. Service Organization Control (SOC) 2 Type 2

Answer: D

NEW QUESTION 291
- (Exam Topic 15)
What is the PRIMARY reason that a bit-level copy is more desirable than a file-level copy when replicating a hard drive's contents for an e-discovery investigation?

A. Files that have been deleted will be transferred.
B. The file and directory structure is retained.
C. File-level security settings will be preserved.
D. The corruption of files is less likely.

Answer: A

NEW QUESTION 292
- (Exam Topic 15)
What is a security concern when considering implementing software-defined networking (SDN)?

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

Answer: C

NEW QUESTION 295
- (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 299
- (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 304
- (Exam Topic 15)
Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

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

Answer: B

NEW QUESTION 307
- (Exam Topic 15)
An organization outgrew its internal data center and is evaluating third-party hosting facilities. In this evaluation, which of the following is a PRIMARY factor for selection?

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

Answer: C

NEW QUESTION 310
- (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 314
- (Exam Topic 15)
Which of the following is a standard Access Control List (ACL) element that enables a router to filter Internet traffic?

A. Media Access Control (MAC) address
B. Internet Protocol (IP) address
C. Security roles
D. Device needs

Answer: B

NEW QUESTION 315
- (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 320
- (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 325
- (Exam Topic 15)
What is the MOST appropriate hierarchy of documents when implementing a security program?

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

Answer:

C

NEW QUESTION 329
- (Exam Topic 15)
Which of the following is a risk matrix?

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

Answer: C

NEW QUESTION 332
- (Exam Topic 15)
What is the BEST reason to include supply chain risks in a corporate risk register?

A. Risk registers help fund corporate supply chain risk management (SCRM) systems.
B. Risk registers classify and categorize risk and allow risks to be compared to corporate risk appetite.
C. Risk registers can be used to illustrate residual risk across the company.
D. Risk registers allow for the transfer of risk to third parties.

Answer: B

NEW QUESTION 334
- (Exam Topic 15)
Which of the following techniques evaluates the secure design principles of network OF software architectures?

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

Answer: B

NEW QUESTION 337
- (Exam Topic 15)
How does Radio-Frequency Identification (RFID) assist with asset management?

A. It uses biometric information for system identification.
B. It uses two-factor authentication (2FA) for system identification.
C. It transmits unique Media Access Control (MAC) addresses wirelessly.
D. It transmits unique serial numbers wirelessly.

Answer: B

NEW QUESTION 342
- (Exam Topic 15)
What are the three key benefits that application developers should derive from the northbound application programming interface (API) of software defined networking (SDN)?

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

Answer: C

NEW QUESTION 343
- (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 345
- (Exam Topic 15)
In an IDEAL encryption system, who has sole access to the decryption key?

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

D. System administrator

Answer: B

NEW QUESTION 349
- (Exam Topic 15)
Which security audit standard provides the BEST way for an organization to understand a vendor's Information Systems (IS) in relation to confidentiality, integrity, and availability?

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

Answer: B

NEW QUESTION 350
- (Exam Topic 15)
Which of the fallowing statements is MOST accurate regarding information assets?

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

Answer: B

NEW QUESTION 355
- (Exam Topic 15)
An internal audit for an organization recently identified malicious actions by a user account. Upon further investigation, it was determined the offending user account was used by multiple people at multiple locations simultaneously for various services and applications. What is the BEST method to prevent this problem in the future?

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

Answer: A

NEW QUESTION 358
- (Exam Topic 15)
Which of the following BEST describes botnets?

A. Computer systems on the Internet that are set up to trap people who attempt to penetrate other computer system
B. Set of related programs that protects the resources of a private network from other networks
C. Small network inserted in a neutral zone between an organization's private network and the outside public network
D. Groups of computers that are used to launch destructive attacks

Answer: D

NEW QUESTION 361
- (Exam Topic 15)
Which of the following is the MAIN benefit of off-site storage?

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

Answer: A

NEW QUESTION 362
- (Exam Topic 14)
Which of the following media is LEAST problematic with data remanence?

A. Dynamic Random Access Memory (DRAM)
B. Electrically Erasable Programming Read-Only Memory (BPRCM)
C. Flash memory
D. Magnetic disk

Answer: A

NEW QUESTION 366
- (Exam Topic 14)

Which of the following is TRUE regarding equivalence class testing?

A. It is characterized by the stateless behavior of a process implemented In a function.
B. An entire partition can be covered by considering only one representative value from that partition.
C. Test inputs are obtained from the derived boundaries of the given functional specifications.
D. It is useful for testing communications protocols and graphical user interfaces.

Answer: C

NEW QUESTION 371
- (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 375
- (Exam Topic 14)
Internet protocol security (IPSec), point-to-point tunneling protocol (PPTP), and secure sockets Layer (SSL) all use Which of the following to prevent replay attacks?

A. Large Key encryption
B. Single integrity protection
C. Embedded sequence numbers
D. Randomly generated nonces

Answer: C

NEW QUESTION 379
- (Exam Topic 14)
Which of the following value comparisons MOST accurately reflects the agile development approach?

A. Processes and toots over individuals and interactions
B. Contract negotiation over customer collaboration
C. Following a plan over responding to change
D. Working software over comprehensive documentation

Answer: D

NEW QUESTION 380
- (Exam Topic 14)
Physical assets defined in an organization's Business Impact Analysis (BIA) could include which of the following?

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

Answer: B

NEW QUESTION 384
- (Exam Topic 14)
How long should the records on a project be retained?

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

Answer: B

NEW QUESTION 385
- (Exam Topic 14)
Which of the following is a MAJOR concern when there is a need to preserve or retain information for future retrieval?

A. Laws and regulations may change in the interim, making it unnecessary to retain the information.
B. The expense of retaining the information could become untenable for the organization.
C. The organization may lose track of the information and not dispose of it securely.
D. The technology needed to retrieve the information may not be available in the future.

Answer: C

NEW QUESTION 387
- (Exam Topic 14)
Which of the following System and Organization Controls (SOC) report types should an organization request if they require a period of time report covering security and availability for a particular system?

A. SOC 1 Type1
B. SOC 1Type2
C. SOC 2 Type 1
D. SOC 2 Type 2

Answer: D

NEW QUESTION 388
- (Exam Topic 14)

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

Answer: D

NEW QUESTION 389
- (Exam Topic 14)
What are the roles within a scrum methodology?

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

Answer: D

NEW QUESTION 390
- (Exam Topic 14)
A security practitioner has been tasked with establishing organizational asset handling procedures. What should be considered that would have the GRFATEST impact to the development of these procedures?

A. Media handling procedures
B. User roles and responsibilities
C. Acceptable Use Policy (ALP)
D. Information classification scheme

Answer: D

NEW QUESTION 394
- (Exam Topic 14)
How can an attacker exploit overflow to execute arbitrary code?

A. Modify a function's return address.
B. Alter the address of the stack.
C. Substitute elements in the stack.
D. Move the stack pointer.

Answer: A

NEW QUESTION 397
- (Exam Topic 14)
Which of the following is the PRIMARY mechanism used to limit the range of objects available to a given subject within different execution domains?

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

Answer: C

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

NEW QUESTION 402
- (Exam Topic 14)
Which is the MOST critical aspect of computer-generated evidence?

A. Objectivity
B. Integrity

C. Timeliness
D. Relevancy

Answer: B

NEW QUESTION 407
- (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 410
- (Exam Topic 14)
Which of the following will have the MOST influence on the definition and creation of data classification and data ownership policies?

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

Answer: A

NEW QUESTION 415
- (Exam Topic 14)
Which of the following is the BEST definition of Cross-Site Request Forgery (CSRF)?

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

Answer: A

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

NEW QUESTION 419
- (Exam Topic 14)
Which of the following is the PRIMARY consideration when determining the frequency an automated control should be assessed or monitored?

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

Answer: B

NEW QUESTION 421
- (Exam Topic 14)
Which is the RECOMMENDED configuration mode for sensors for an intrusion prevention system (IPS) if the prevention capabilities will be used?

A. Active
B. Passive
C. Inline
D. Span

Answer: C

NEW QUESTION 426
- (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 427

- (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 428
- (Exam Topic 14)
Which of the following is considered the last line defense in regard to a Governance, Risk managements, and compliance (GRC) program?

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

Answer: B

NEW QUESTION 431
- (Exam Topic 14)
The core component of Role Based Access control (RBAC) must be constructed of defined data elements. Which elements are required?

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

Answer: B

NEW QUESTION 433
- (Exam Topic 14)
When a flaw in Industrial control (ICS) software is discovered, what is the GREATEST impediment to deploying a patch?

A. Many IG systems have software that is no longer being maintained by the venders.
B. Compensating controls may impact IG performance.
C. Testing a patch in an IG may require more resources than the organization can commit.
D. vendors are required to validate the operability patches.

Answer: D

NEW QUESTION 437
- (Exam Topic 14)
Which of the following would an internal technical security audit BEST validate?

A. Whether managerial controls are in place
B. Support for security programs by executive management
C. Appropriate third-party system hardening
D. Implementation of changes to a system

Answer: D

NEW QUESTION 439
- (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 440
- (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 442
- (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 444
- (Exam Topic 14)
According to the Capability Maturity Model Integration (CMMI), which of the following levels is identified by a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines?

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

Answer: D

NEW QUESTION 449
- (Exam Topic 14)
An organization implements a Remote Access Server (RAS). Once users correct to the server, digital certificates are used to authenticate their identity. What type of Extensible Authentication Protocol (EAP) would the organization use dring this authentication?

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

Answer: A

NEW QUESTION 452
- (Exam Topic 14)
As users switch roles within an organization, their accounts are given additional permissions to perform the duties of their new position. After a recent audit, it was discovered that many of these accounts maintained their old permissions as well. The obsolete permissions identified by the audit have been remediated and accounts have only the appropriate permissions to complete their jobs.
Which of the following is the BEST way to prevent access privilege creep?

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

Answer: A

NEW QUESTION 457
- (Exam Topic 14)
Which of the following management processes allots ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

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

Answer: B

NEW QUESTION 462
- (Exam Topic 14)
What is the BEST way to correlate large volumes of disparate data sources in a Security Operations Center (SOC) environment?

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

Answer: B

NEW QUESTION 464
- (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 467
- (Exam Topic 14)
Which of the following practices provides the development of security and identification of threats in designing software?

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

Answer: D

NEW QUESTION 471
- (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 475
- (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 479
- (Exam Topic 14)
Which is the MOST effective countermeasure to prevent electromagnetic emanations on unshielded data cable?

A. Move cable are away from exterior facing windows
B. Encase exposed cable runs in metal conduit
C. Enable Power over Ethernet (PoE) to increase voltage
D. Bundle exposed cables together to disguise their signals

Answer: B

NEW QUESTION 481
- (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 482
- (Exam Topic 14)
When designing on Occupent Emergency plan (OEP) for United states (US) Federal government facilities, what factor must be considered?

A. location of emergency exits in building
B. Average age of the agency employees
C. Geographical location and structural design of building
D. Federal agency for which plan is being drafted

Answer: A

NEW QUESTION 486

- (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 489
- (Exam Topic 14)
Who is essential for developing effective test scenarios for disaster recovery (DR) test plans?

A. Business line management and IT staff members
B. Chief Information Officer (CIO) and DR manager
C. DR manager end IT staff members
D. IT staff members and project managers

Answer: B

NEW QUESTION 493
- (Exam Topic 14)
Directive controls are a form of change management policy and procedures. Which of the following subsections are recommended as part of the change management process?

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

Answer: A

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

NEW QUESTION 498
- (Exam Topic 14)
Which of the following is applicable to a publicly held company concerned about information handling and storage requirement specific to the financial reporting?

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

Answer: C

NEW QUESTION 501
- (Exam Topic 14)
Why is planning the MOST critical phase of a Role Based Access Control (RBAC) implementation?

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

Answer: B

NEW QUESTION 505
- (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 507
- (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 509
- (Exam Topic 14)
How does identity as a service (IDaaS) provide an easy mechanism for integrating identity service into individual applications with minimal development effort?

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

Answer: D

NEW QUESTION 511
- (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 515
- (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 516
- (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 520
- (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 521
- (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 524
- (Exam Topic 14)
Which of the following findings would MOST likely indicate a high risk in a vulnerability assessment report?

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

Answer: A

NEW QUESTION 526
- (Exam Topic 14)
Company A is evaluating new software to replace an in-house developed application. During the acquisition process. Company A specified the security retirement, as well as the functional requirements. Company B responded to the acquisition request with their flagship product that runs on an Operating System (OS) that Company A has never used nor evaluated. The flagship product meets all security -and functional requirements as defined by Company A.
Based upon Company B's response, what step should Company A take?

A. Move ahead with the acpjisition process, and purchase the flagship software
B. Conduct a security review of the OS
C. Perform functionality testing
D. Enter into contract negotiations ensuring Service Level Agreements (SLA) are established to include security patching

Answer: B

NEW QUESTION 531
- (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 532
- (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 536
- (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 540
- (Exam Topic 14)
Which of the following is the BEST approach for a forensic examiner to obtain the greatest amount of relevant information form malicious software?

A. Analyze the behavior of the program.
B. Examine the file properties and permissions.
C. Review the code to identify its origin.
D. Analyze the logs generated by the software.

Answer: A

NEW QUESTION 545
- (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 547
- (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 erra MOST likely occur?

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

Answer: A

NEW QUESTION 548
- (Exam Topic 14)
Which of the following attacks is dependent upon the compromise of a secondary target in order to reach the primary target?

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

Answer: D

NEW QUESTION 553
- (Exam Topic 14)
A security professional should consider the protection of which of the following elements FIRST when developing a defense-in-depth strategy for a mobile workforce?

A. Network perimeters
B. Demilitarized Zones (DM2)
C. Databases and back-end servers
D. End-user devices

Answer: D

NEW QUESTION 557
- (Exam Topic 14)
Which of the following is critical if an employee is dismissed due to violation of an organization's Acceptable Use Policy (ALP)?

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

Answer: B

NEW QUESTION 562
- (Exam Topic 14)
Which of the following attributes could be used to describe a protection mechanism of an open design methodology?
A. lt must be tamperproof to protect it from malicious attacks.
B. It can facilitate independent confirmation of the design security.
C. It can facilitate blackbox penetration testing.
D. It exposes the design to vulnerabilities and malicious attacks.

Answer: A

NEW QUESTION 567
- (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 572
- (Exam Topic 14)
Which of the following is the weakest form of protection for an application that handles Personally Identifiable Information (PII)?

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

D. Multifactor authentication

Answer: B

NEW QUESTION 577
- (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 582
- (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 586
- (Exam Topic 13)
Access to which of the following is required to validate web session management?

A. Log timestamp
B. Live session traffic
C. Session state variables
D. Test scripts

Answer: B

NEW QUESTION 589
- (Exam Topic 13)
What is the MAIN reason for testing a Disaster Recovery Plan (DRP)?

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

Answer: B

NEW QUESTION 593
- (Exam Topic 13)
Who would be the BEST person to approve an organizations information security policy?

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

Answer: B

Explanation:
Section: Security Operations

NEW QUESTION 597
- (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 602

- (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 607
- (Exam Topic 13)
What capability would typically be included in a commercially available software package designed for access control?

A. Password encryption
B. File encryption
C. Source library control
D. File authentication

Answer: A

NEW QUESTION 612
- (Exam Topic 13)
Why is planning in Disaster Recovery (DR) an interactive process?

A. It details off-site storage plans
B. It identifies omissions in the plan
C. It defines the objectives of the plan
D. It forms part of the awareness process

Answer: C

NEW QUESTION 617
- (Exam Topic 13)
Which of the following provides the MOST comprehensive filtering of Peer-to-Peer (P2P) traffic?

A. Application proxy
B. Port filter
C. Network boundary router
D. Access layer switch

Answer: D

NEW QUESTION 618
- (Exam Topic 13)
Which security access policy contains fixed security attributes that are used by the system to determine a user’s access to a file or object?

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

Answer: A

NEW QUESTION 619
- (Exam Topic 13)
Which of the following is a common characteristic of privacy?

A. Provision for maintaining an audit trail of access to the private data
B. Notice to the subject of the existence of a database containing relevant credit card data
C. Process for the subject to inspect and correct personal data on-site
D. Database requirements for integration of privacy data

Answer: C

NEW QUESTION 622
- (Exam Topic 13)
Which of the following is a benefit in implementing an enterprise Identity and Access Management (IAM) solution?

A. Password requirements are simplified.
B. Risk associated with orphan accounts is reduced.
C. Segregation of duties is automatically enforced.
D. Data confidentiality is increased.

Answer: A

NEW QUESTION 623
- (Exam Topic 13)
Who is accountable for the information within an Information System (IS)?

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

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 624
- (Exam Topic 13)
Which of the following is a direct monetary cost of a security incident?

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

Answer: C

NEW QUESTION 628
- (Exam Topic 13)
Which of the following is the BEST Identity-as-a-Service (IDaaS) solution for validating users?

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

Answer: B

NEW QUESTION 632
- (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 636
- (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 641
- (Exam Topic 13)
Unused space in a disk cluster is important in media analysis because it may contain which of the following?

A. Residual data that has not been overwritten
B. Hidden viruses and Trojan horses
C. Information about the File Allocation table (FAT)
D. Information about patches and upgrades to the system

Answer: A

NEW QUESTION 645
- (Exam Topic 13)
Which of the following alarm systems is recommended to detect intrusions through windows in a high-noise, occupied environment?

A. Acoustic sensor
B. Motion sensor

C. Shock sensor
D. Photoelectric sensor

Answer: C

NEW QUESTION 650
- (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 652
- (Exam Topic 13)
Which of the following is the BEST way to reduce the impact of an externally sourced flood attack?

A. Have the service provider block the soiree address.
B. Have the soiree service provider block the address.
C. Block the source address at the firewall.
D. Block all inbound traffic until the flood ends.

Answer: C

NEW QUESTION 656
- (Exam Topic 13)
After following the processes defined within the change management plan, a super user has upgraded a device within an Information system.
What step would be taken to ensure that the upgrade did NOT affect the network security posture?

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

Answer: B

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 657
- (Exam Topic 13)
Which factors MUST be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?

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

Answer: B

NEW QUESTION 660
- (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 662
- (Exam Topic 13)
“Stateful” differs from “Static” packet filtering firewalls by being aware of which of the following?

A. Difference between a new and an established connection
B. Originating network location
C. Difference between a malicious and a benign packet payload
D. Originating application session

Answer: A

NEW QUESTION 664
- (Exam Topic 13)
Which of the following is the GREATEST benefit of implementing a Role Based Access Control (RBAC) system?

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

Answer: D

NEW QUESTION 669
- (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 673
- (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 676
- (Exam Topic 12)
When writing security assessment procedures, what is the MAIN purpose of the test outputs and reports?

A. To force the software to fail and document the process
B. To find areas of compromise in confidentiality and integrity
C. To allow for objective pass or fail decisions
D. To identify malware or hidden code within the test results

Answer: C

NEW QUESTION 681
- (Exam Topic 12)
At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

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

Answer: C

NEW QUESTION 686
- (Exam Topic 12)
Which of the following is MOST important when deploying digital certificates?

A. Validate compliance with X.509 digital certificate standards
B. Establish a certificate life cycle management framework
C. Use a third-party Certificate Authority (CA)
D. Use no less than 256-bit strength encryption when creating a certificate

Answer: B

NEW QUESTION 688
- (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 689
- (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 693
- (Exam Topic 12)
Which of the following is the MAIN reason for using configuration management?

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

Answer: D

NEW QUESTION 694
- (Exam Topic 12)
Which of the following is the MOST important goal of information asset valuation?

A. Developing a consistent and uniform method of controlling access on information assets
B. Developing appropriate access control policies and guidelines
C. Assigning a financial value to an organization's information assets
D. Determining the appropriate level of protection

Answer: D

NEW QUESTION 697
- (Exam Topic 12)
A user sends an e-mail request asking for read-only access to files that are not considered sensitive. A Discretionary Access Control (DAC) methodology is in place. Which is the MOST suitable approach that the administrator should take?

A. Administrator should request data owner approval to the user access
B. Administrator should request manager approval for the user access
C. Administrator should directly grant the access to the non-sensitive files
D. Administrator should assess the user access need and either grant or deny the access

Answer: A

NEW QUESTION 700
- (Exam Topic 12)
A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

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

Answer: A

NEW QUESTION 702
- (Exam Topic 12)
An organization regularly conducts its own penetration tests. Which of the following scenarios MUST be covered for the test to be effective?

A. Third-party vendor with access to the system
B. System administrator access compromised
C. Internal attacker with access to the system
D. Internal user accidentally accessing data

Answer: B

NEW QUESTION 706
- (Exam Topic 12)
Which of the following is the PRIMARY reason for employing physical security personnel at entry points in facilities where card access is in operation?

A. To verify that only employees have access to the facility.
B. To identify present hazards requiring remediation.
C. To monitor staff movement throughout the facility.
D. To provide a safe environment for employees.

Answer: D

NEW QUESTION 710
- (Exam Topic 12)
A database administrator is asked by a high-ranking member of management to perform specific changes to the accounting system database. The administrator is specifically instructed to not track or evidence the change in a ticket. Which of the following is the BEST course of action?

A. Ignore the request and do not perform the change.
B. Perform the change as requested, and rely on the next audit to detect and report the situation.
C. Perform the change, but create a change ticket regardless to ensure there is complete traceability.
D. Inform the audit committee or internal audit directly using the corporate whistleblower process.

Answer: D

NEW QUESTION 714
- (Exam Topic 12)
A proxy firewall operates at what layer of the Open System Interconnection (OSI) model?

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

Answer: D

NEW QUESTION 716
- (Exam Topic 12)
In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of

A. systems integration.
B. risk management.
C. quality assurance.
D. change management.

Answer: D

NEW QUESTION 719
- (Exam Topic 12)
A vulnerability in which of the following components would be MOST difficult to detect?

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

Answer: C

NEW QUESTION 721
- (Exam Topic 12)
Which of the following is BEST suited for exchanging authentication and authorization messages in a multi-party decentralized environment?

A. Lightweight Directory Access Protocol (LDAP)
B. Security Assertion Markup Language (SAML)
C. Internet Mail Access Protocol
D. Transport Layer Security (TLS)

Answer: B

NEW QUESTION 723
- (Exam Topic 12)
Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

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

Answer: C

NEW QUESTION 728
- (Exam Topic 12)
Match the name of access control model with its associated restriction.
Drag each access control model to its appropriate restriction access on the right.

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 733
- (Exam Topic 11)
Which of the following BEST describes the purpose of performing security certification?

A. To identify system threats, vulnerabilities, and acceptable level of risk
B. To formalize the confirmation of compliance to security policies and standards
C. To formalize the confirmation of completed risk mitigation and risk analysis
D. To verify that system architecture and interconnections with other systems are effectively implemented

Answer: B

NEW QUESTION 737
- (Exam Topic 11)
Which of the following roles has the obligation to ensure that a third party provider is capable of processing and handling data in a secure manner and meeting the standards set by the organization?

A. Data Custodian
B. Data Owner
C. Data Creator
D. Data User

Answer: B

NEW QUESTION 739
- (Exam Topic 11)
Which of the following PRIMARILY contributes to security incidents in web-based applications?

A. Systems administration and operating systems
B. System incompatibility and patch management
C. Third-party applications and change controls
D. Improper stress testing and application interfaces

Answer: C

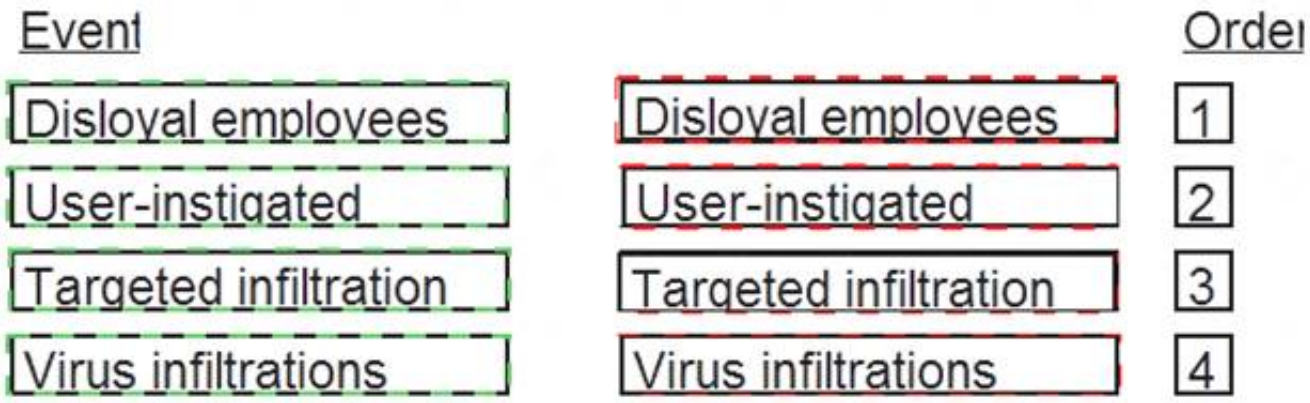
NEW QUESTION 742
- (Exam Topic 11)
In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?

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

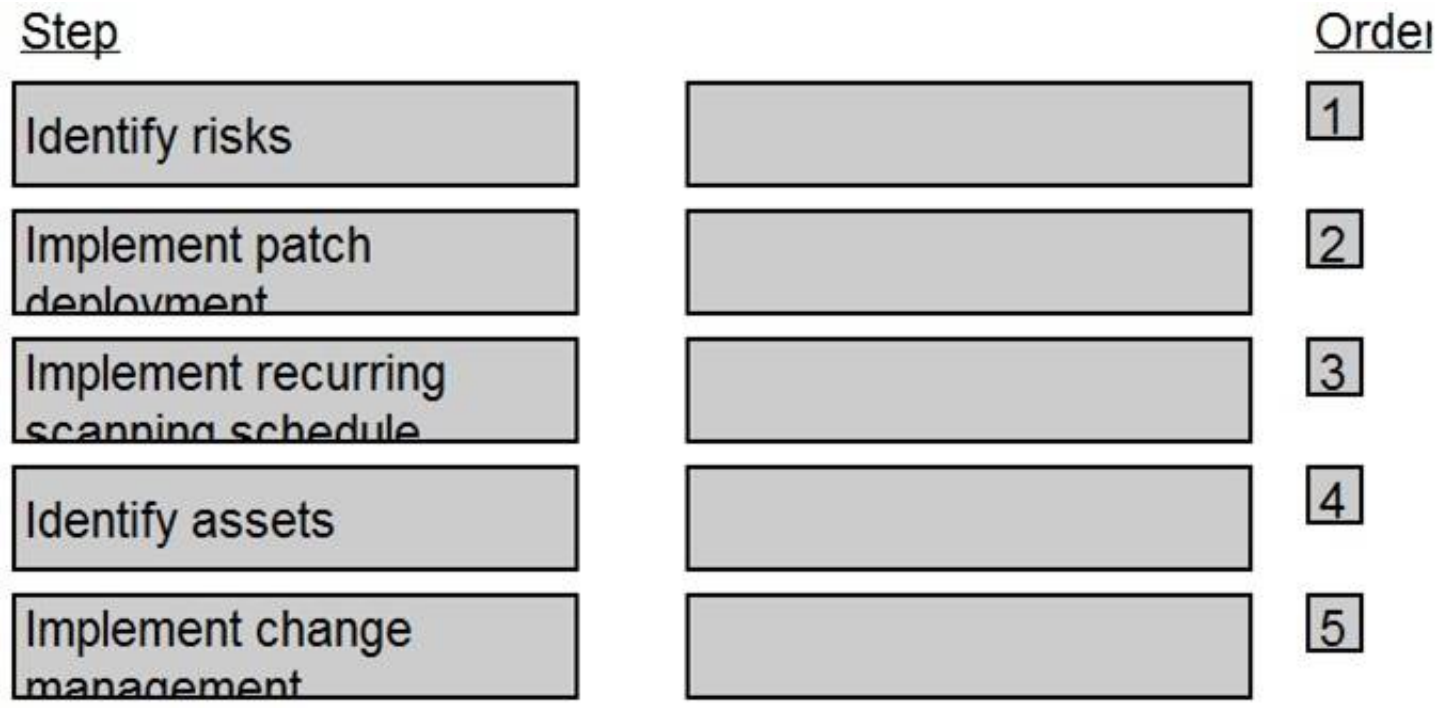
A. Mastered
B. Not Mastered

Answer: A

Explanation:



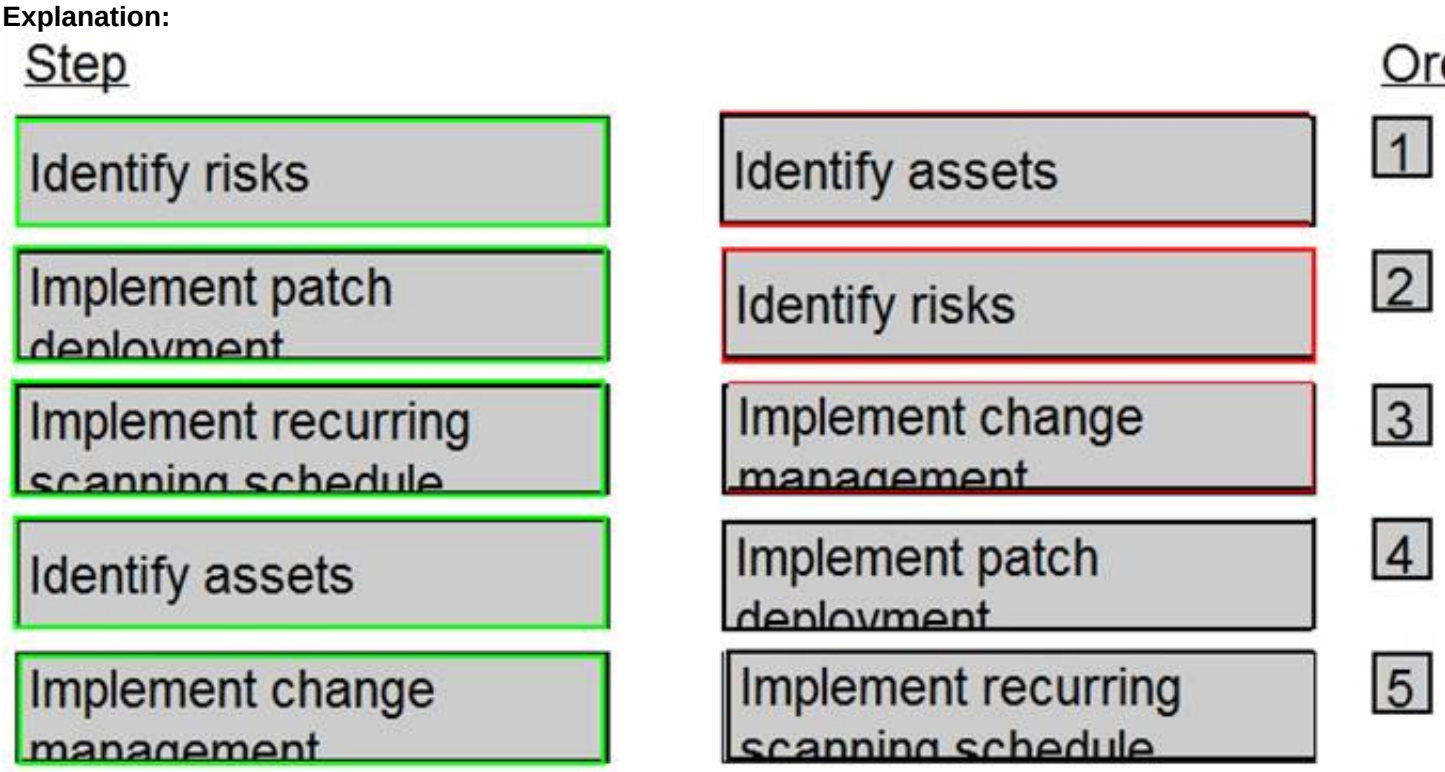
NEW QUESTION 745
- (Exam Topic 11)
Order the below steps to create an effective vulnerability management process.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 746
- (Exam Topic 11)
How can lessons learned from business continuity training and actual recovery incidents BEST be used?

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

Answer: A

NEW QUESTION 751
- (Exam Topic 11)
Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?

A. Policy documentation review
B. Authentication validation
C. Periodic log reviews
D. Interface testing

Answer: C

NEW QUESTION 753
- (Exam Topic 11)
Which of the following entities is ultimately accountable for data remanence vulnerabilities with data replicated by a cloud service provider?

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

Answer: A

NEW QUESTION 755
- (Exam Topic 11)
By carefully aligning the pins in the lock, which of the following defines the opening of a mechanical lock without the proper key?

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

Answer: B

NEW QUESTION 757
- (Exam Topic 11)
Which of the following is a recommended alternative to an integrated email encryption system?

A. Sign emails containing sensitive data
B. Send sensitive data in separate emails
C. Encrypt sensitive data separately in attachments
D. Store sensitive information to be sent in encrypted drives

Answer: C

NEW QUESTION 762
- (Exam Topic 11)
Which of the following is the BEST example of weak management commitment to the protection of security assets and resources?

A. poor governance over security processes and procedures
B. immature security controls and procedures
C. variances against regulatory requirements
D. unanticipated increases in security incidents and threats

Answer: A

NEW QUESTION 766
- (Exam Topic 11)
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.
What is the best approach for the CISO?
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.
What is the best approach for the CISO?

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

Answer: B

NEW QUESTION 771
- (Exam Topic 11)
Data remanence refers to which of the following?

A. The remaining photons left in a fiber optic cable after a secure transmission.
B. The retention period required by law or regulation.
C. The magnetic flux created when removing the network connection from a server or personal computer.
D. The residual information left on magnetic storage media after a deletion or erasure.

Answer: D

NEW QUESTION 773
- (Exam Topic 11)
Which of the following BEST describes a rogue Access Point (AP)?

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

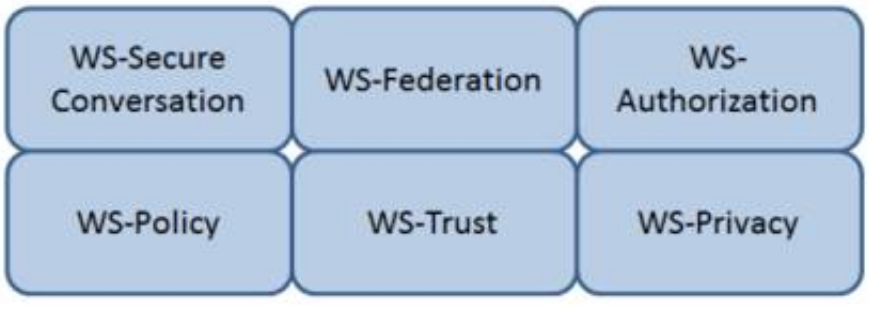
Answer: C

NEW QUESTION 778
- (Exam Topic 11)
Which of the following is the MOST likely cause of a non-malicious data breach when the source of the data breach was an un-marked file cabinet containing sensitive documents?

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

Answer: A

NEW QUESTION 780
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
WS-Federation
Reference: Java Web Services: Up and Running" By Martin Kalin page 228

NEW QUESTION 782
- (Exam Topic 11)
When planning a penetration test, the tester will be MOST interested in which information?

A. Places to install back doors
B. The main network access points
C. Job application handouts and tours
D. Exploits that can attack weaknesses

Answer: D

NEW QUESTION 784
- (Exam Topic 11)
Disaster Recovery Plan (DRP) training material should be

A. consistent so that all audiences receive the same training.
B. stored in a fire proof safe to ensure availability when needed.
C. only delivered in paper format.
D. presented in a professional looking manner.

Answer: A

NEW QUESTION 786
- (Exam Topic 11)
Which of the following is the BEST method to assess the effectiveness of an organization's vulnerability management program?

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

Answer: B

NEW QUESTION 788
- (Exam Topic 11)
After a thorough analysis, it was discovered that a perpetrator compromised a network by gaining access to the network through a Secure Socket Layer (SSL) Virtual Private Network (VPN) gateway. The perpetrator guessed a username and brute forced the password to gain access. Which of the following BEST mitigates this issue?

A. Implement strong passwords authentication for VPN
B. Integrate the VPN with centralized credential stores
C. Implement an Internet Protocol Security (IPSec) client
D. Use two-factor authentication mechanisms

Answer: D

NEW QUESTION 789
- (Exam Topic 11)
An organization lacks a data retention policy. Of the following, who is the BEST person to consult for such requirement?

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

Answer: C

NEW QUESTION 792
- (Exam Topic 11)
Drag the following Security Engineering terms on the left to the BEST definition on the right.

Security Engineering		Definition
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**
Threat Assessment		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**
Protection Needs		The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**
Risk		The method used to identify feasible security **risk mitigation options and plans.**

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Security Engineering		Definition
Security Risk Treatment	Protection Needs	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**
Threat Assessment	Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**
Protection Needs	Threat Assessment	The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**
Risk	Security Risk Treatment	The method used to identify feasible security **risk mitigation options and plans.**

NEW QUESTION 794
- (Exam Topic 11)
Which of the following is the BIGGEST weakness when using native Lightweight Directory Access Protocol (LDAP) for authentication?

A. Authorizations are not included in the server response
B. Unsalted hashes are passed over the network
C. The authentication session can be replayed
D. Passwords are passed in cleartext

Answer: D

NEW QUESTION 796
- (Exam Topic 11)
To protect auditable information, which of the following MUST be configured to only allow read access?

A. Logging configurations
B. Transaction log files
C. User account configurations
D. Access control lists (ACL)

Answer: B

NEW QUESTION 801
- (Exam Topic 11)
The MAIN reason an organization conducts a security authorization process is to

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

Answer: A

NEW QUESTION 805
- (Exam Topic 11)
A Simple Power Analysis (SPA) attack against a device directly observes which of the following?

A. Static discharge
B. Consumption
C. Generation
D. Magnetism

Answer: B

NEW QUESTION 810
- (Exam Topic 11)
The 802.1x standard provides a framework for what?

A. Network authentication for only wireless networks
B. Network authentication for wired and wireless networks
C. Wireless encryption using the Advanced Encryption Standard (AES)
D. Wireless network encryption using Secure Sockets Layer (SSL)

Answer: B

NEW QUESTION 815
- (Exam Topic 11)
How does an organization verify that an information system's current hardware and software match the standard system configuration?

A. By reviewing the configuration after the system goes into production
B. By running vulnerability scanning tools on all devices in the environment
C. By comparing the actual configuration of the system against the baseline
D. By verifying all the approved security patches are implemented

Answer: C

NEW QUESTION 816
- (Exam Topic 11)
Which of the following is an advantage of on-premise Credential Management Systems?

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

Answer: B

NEW QUESTION 821
- (Exam Topic 10)
Which of the following secure startup mechanisms are PRIMARILY designed to thwart attacks?

A. Timing
B. Cold boot
C. Side channel
D. Acoustic cryptanalysis

Answer: B

NEW QUESTION 822
- (Exam Topic 10)
According to best practice, which of the following is required when implementing third party software in a production environment?

A. Scan the application for vulnerabilities
B. Contract the vendor for patching
C. Negotiate end user application training
D. Escrow a copy of the software

Answer: A

NEW QUESTION 824
- (Exam Topic 10)
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization’s network. A plan will be necessary to address these concerns.
What MUST the plan include in order to reduce client-side exploitation?

A. Approved web browsers
B. Network firewall procedures
C. Proxy configuration
D. Employee education

Answer: D

NEW QUESTION 829
- (Exam Topic 10)
What do Capability Maturity Models (CMM) serve as a benchmark for in an organization?

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

Answer: D

NEW QUESTION 830
- (Exam Topic 10)
Which of the following actions MUST be taken if a vulnerability is discovered during the maintenance stage in a System Development Life Cycle (SDLC)?

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

Answer: C

NEW QUESTION 833
- (Exam Topic 10)
Which of the following assures that rules are followed in an identity management architecture?

A. Policy database
B. Digital signature
C. Policy decision point
D. Policy enforcement point

Answer: D

NEW QUESTION 834
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?

A. Severity of risk
B. Complexity of strategy
C. Frequency of incidents
D. Ongoing awareness

Answer: A

NEW QUESTION 838
- (Exam Topic 10)
When using third-party software developers, which of the following is the MOST effective method of providing software development Quality Assurance (QA)?

A. Retain intellectual property rights through contractual wording.
B. Perform overlapping code reviews by both parties.
C. Verify that the contractors attend development planning meetings.
D. Create a separate contractor development environment.

Answer: B

NEW QUESTION 843
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Which of the following is considered the MOST important priority for the information security officer?

A. Formal acceptance of the security strategy
B. Disciplinary actions taken against unethical behavior
C. Development of an awareness program for new employees
D. Audit of all organization system configurations for faults

Answer: A

NEW QUESTION 846

- (Exam Topic 10)
What is a common challenge when implementing Security Assertion Markup Language (SAML) for identity integration between on-premise environment and an external identity provider service?

A. Some users are not provisioned into the service.
B. SAML tokens are provided by the on-premise identity provider.
C. Single users cannot be revoked from the service.
D. SAML tokens contain user information.

Answer: A

NEW QUESTION 847
- (Exam Topic 10)
Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?

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

Answer: A

NEW QUESTION 850
- (Exam Topic 10)
Which of the following are required components for implementing software configuration management systems?

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

Answer: C

NEW QUESTION 851
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
Which of the following BEST describes the access control methodology used?

A. Least privilege
B. Lattice Based Access Control (LBAC)
C. Role Based Access Control (RBAC)
D. Lightweight Directory Access Control (LDAP)

Answer: C

NEW QUESTION 855
- (Exam Topic 10)
Which of the following is the MOST crucial for a successful audit plan?

A. Defining the scope of the audit to be performed
B. Identifying the security controls to be implemented
C. Working with the system owner on new controls
D. Acquiring evidence of systems that are not compliant

Answer: A

NEW QUESTION 858
- (Exam Topic 10)
What is the MOST critical factor to achieve the goals of a security program?

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

Answer: B

NEW QUESTION 859
- (Exam Topic 10)
A system is developed so that its business users can perform business functions but not user administration functions. Application administrators can perform administration functions but not user business functions. These capabilities are BEST described as

A. least privilege.
B. rule based access controls.

C. Mandatory Access Control (MAC).
D. separation of duties.

Answer: D

NEW QUESTION 861
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

CISSP Practice Exam Features:

* CISSP Questions and Answers Updated Frequently

* CISSP Practice Questions Verified by Expert Senior Certified Staff

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

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