ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

NEW QUESTION 1
- (Exam Topic 15)
An organization plans to acquire @ commercial off-the-shelf (COTS) system to replace their aging home-built reporting system. When should the organization's security team FIRST get involved in this acquisition's life cycle?

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

Answer: D

NEW QUESTION 2
- (Exam Topic 15)
An organization 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)
In the common criteria, which of the following is a formal document that expresses an implementation-independent set of security requirements?

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

Answer: C

NEW QUESTION 4
- (Exam Topic 15)
In which process MUST security be considered during the acquisition of new software?

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

Answer: B

NEW QUESTION 5
- (Exam Topic 15)
Which of the following is the MOST effective way to ensure the endpoint devices used by remote users are compliant with an organization's approved policies before being allowed on the network?

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

Answer: B

NEW QUESTION 6
- (Exam Topic 15)
Which of the following virtual network configuration options is BEST to protect virtual machines (VM)?

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

Answer: D

NEW QUESTION 7
- (Exam Topic 15)
Two computers, each with a single connection on the same physical 10 gigabit Ethernet network segment, need to communicate with each other. The first machine has a single Internet Protocol (IP) Classless
Inter-Domain Routing (CIDR) address of 192.168.1.3/30 and the second machine has an IP/CIDR address 192.168.1.6/30. Which of the following is correct?

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

Answer: B

NEW QUESTION 8
- (Exam Topic 15)
A database server for a financial application is scheduled for production deployment. Which of the following controls will BEST prevent tampering?

A. Service accounts removal
B. Data validation
C. Logging and monitoring
D. Data sanitization

Answer: B

NEW QUESTION 9
- (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 10
- (Exam Topic 15)
An organization has implemented a password complexity and an account lockout policy enforcing five incorrect logins tries within ten minutes. Network users have reported significantly increased account lockouts. Which of the following security principles is this company affecting?

A. Availability
B. Integrity
C. Confidentiality
D. Authentication

Answer: A

NEW QUESTION 10
- (Exam Topic 15)
Which of the following is a PRIMARY security weakness in the design of Domain Name System (DNS)?

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

Answer: A

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

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

Answer: B

NEW QUESTION 17
- (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 18
- (Exam Topic 15)
During a penetration test, what are the three PRIMARY objectives of the planning phase?

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

Answer: D

NEW QUESTION 21
- (Exam Topic 15)
A new employee formally reported suspicious behavior to the organization security team. The report claims that someone not affiliated with the organization was inquiring about the member's work location, length of employment, and building access controls. The employee's reporting is MOST likely the result of which of the following?

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

Answer: C

NEW QUESTION 23
- (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 25
- (Exam Topic 15)
An organization wants to define its physical perimeter. What primary device should be used to accomplish this objective if the organization's perimeter MUST cost-efficiently deter casual trespassers?

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

Answer: A

NEW QUESTION 26
- (Exam Topic 15)
When reviewing vendor certifications for handling and processing of company data, which of the following is the BEST Service Organization Controls (SOC) certification for the vendor to possess?

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

Answer: C

NEW QUESTION 27
- (Exam Topic 15)
A customer continues to experience attacks on their email, web, and File Transfer Protocol (FTP) servers. These attacks are impacting their business operations. Which of the following is the BEST recommendation to make?

A. Configure an intrusion detection system (IDS).
B. Create a demilitarized zone (DMZ).
C. Deploy a bastion host.
D. Setup a network firewall.

Answer: C

NEW QUESTION 32
- (Exam Topic 15)
Which of the following is the BEST method to identify security controls that should be implemented for a web-based application while in development?

A. Application threat modeling
B. Secure software development.

C. Agile software development
D. Penetration testing

Answer: A

NEW QUESTION 35
- (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 36
- (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 38
- (Exam Topic 15)
Which of the following is performed to determine a measure of success of a security awareness training program designed to prevent social engineering attacks?

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

Answer: B

NEW QUESTION 42
- (Exam Topic 15)
Which of the following factors should be considered characteristics of Attribute Based Access Control (ABAC) in terms of the attributes used?

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

Answer: D

NEW QUESTION 44
- (Exam Topic 15)
What is the FIRST step for an organization to take before allowing personnel to access social media from a corporate device or user account?

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

Answer: A

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

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

Answer: D

NEW QUESTION 50

- (Exam Topic 15)
Which of the following is the MOST effective preventative method to identify security flaws in software?

A. Monitor performance in production environments.
B. Perform a structured code review.
C. Perform application penetration testing.
D. Use automated security vulnerability testing tods.

Answer: B

NEW QUESTION 52
- (Exam Topic 15)
Information security practitioners are in the midst of implementing a new firewall. Which of the following failure methods would BEST prioritize security in the event of failure?

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

Answer: A

NEW QUESTION 57
- (Exam Topic 15)
An organization recently upgraded to a Voice over Internet Protocol (VoIP) phone system. Management is concerned with unauthorized phone usage. Security consultant is responsible for putting together a plan to secure these phones. Administrators have assigned unique personal identification number codes for each person in the organization. What is the BEST solution?

A. Use phone locking software to enforce usage and PIN policies.
B. Inform the user to change the PIN regularl
C. Implement call detail records (CDR) reports to track usage.
D. Have the administrator enforce a policy to change the PIN regularl
E. Implement call detail records (CDR) reports to track usage.
F. Have the administrator change the PIN regularl
G. Implement call detail records (CDR) reports to track usage.

Answer: C

NEW QUESTION 62
- (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 64
- (Exam Topic 15)
Why is data classification control important to an organization?

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

Answer: A

NEW QUESTION 67
- (Exam Topic 15)
Why is authentication by ownership stronger than authentication by knowledge?

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

Answer: B

NEW QUESTION 71
- (Exam Topic 15)
What level of Redundant Array of Independent Disks (RAID) is configured PRIMARILY for high-performance data reads and writes?

A. RAID-0
B. RAID-1

C. RAID-5
D. RAID-6

Answer: A

NEW QUESTION 73
- (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 74
- (Exam Topic 15)
A project manager for a large software firm has acquired a government contract that generates large amounts of Controlled Unclassified Information (CUI). The organization's information security manager has received a request to transfer project-related CUI between systems of differing security classifications. What role provides
the authoritative guidance for this transfer?

A. Information owner
B. PM
C. Data Custodian
D. Mission/Business Owner

Answer: C

NEW QUESTION 75
- (Exam Topic 15)
Which of the following BEST describes the objectives of the Business Impact Analysis (BIA)?

A. Identifying the events and environmental factors that can adversely affect an organization
B. Identifying what is important and critical based on disruptions that can affect the organization.
C. Establishing the need for a Business Continuity Plan (BCP) based on threats that can affect an organization
D. Preparing a program to create an organizational awareness for executing the Business Continuity Plan (BCP)

Answer: B

NEW QUESTION 78
- (Exam Topic 15)
Which of the following implementations will achieve high availability in a website?

A. Multiple Domain Name System (DNS) entries resolving to the same web server and large amounts of bandwidth
B. Disk mirroring of the web server with redundant disk drives in a hardened data center
C. Disk striping of the web server hard drives and large amounts of bandwidth
D. Multiple geographically dispersed web servers that are configured for failover

Answer: D

NEW QUESTION 82
- (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 83
- (Exam Topic 15)
What type of investigation applies when malicious behavior is suspected between two organizations?

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

Answer: A

NEW QUESTION 86

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

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

Answer: B

NEW QUESTION 89
- (Exam Topic 15)
A technician is troubleshooting a client's report about poor wireless performance. Using a client monitor, the technician notes the following information:

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

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

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

Answer: A

NEW QUESTION 90
- (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 91
- (Exam Topic 15)
Which of the following is a term used to describe maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions?

A. Information Security Management System (ISMS)
B. Information Sharing & Analysis Centers (ISAC)
C. Risk Management Framework (RMF)
D. Information Security Continuous Monitoring (ISCM)

Answer: D

NEW QUESTION 95
- (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 98
- (Exam Topic 15)

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

Answer: D

NEW QUESTION 102

- (Exam Topic 15)
The disaster recovery (DR) process should always include

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

Answer: A

NEW QUESTION 104
- (Exam Topic 15)
Which of the following is security control volatility?

A. A reference to the stability of the security control.
B. A reference to how unpredictable the security control is.
C. A reference to the impact of the security control.
D. A reference to the likelihood of change in the security control.

Answer: D

NEW QUESTION 106
- (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 110
- (Exam Topic 15)
Which of the following phases in the software acquisition process does developing evaluation criteria take place?

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

Answer: D

NEW QUESTION 112
- (Exam Topic 15)
A financial services organization has employed a security consultant to review processes used by employees across various teams. The consultant interviewed a member of the application development practice and found gaps in their threat model. Which of the following correctly represents a trigger for when a threat model should be revised?

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

Answer: D

NEW QUESTION 115
- (Exam Topic 15)
When developing an external facing web-based system, which of the following would be the MAIN focus of the security assessment prior to implementation and production?

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

Answer: B

NEW QUESTION 116
- (Exam Topic 15)
What is the FIRST step that should be considered in a Data Loss Prevention (DLP) program?

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

Answer: D

NEW QUESTION 120
- (Exam Topic 15)
A client server infrastructure that provides user-to-server authentication describes which one of the following?

A. Secure Sockets Layer (SSL)
B. Kerberos
C. 509
D. User-based authorization

Answer: B

NEW QUESTION 124
- (Exam Topic 15)
In which of the following system life cycle processes should security requirements be developed?

A. Risk management
B. Business analysis
C. Information management
D. System analysis

Answer: B

NEW QUESTION 129
- (Exam Topic 15)
An application is used for funds transfer between an organization and a third-party. During a security audit, an issue with the business continuity/disaster recovery policy and procedures for this application. Which of the following reports should the audit file with the organization?

A. Service Organization Control (SOC) 1
B. Statement on Auditing Standards (SAS) 70
C. Service Organization Control (SOC) 2
D. Statement on Auditing Standards (SAS) 70-1

Answer: C

NEW QUESTION 130
- (Exam Topic 15)
Which of the following determines how traffic should flow based on the status of the infrastructure layer?

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

Answer: A

NEW QUESTION 135
- (Exam Topic 15)
Which of the following BEST represents a defense in depth concept?

A. Network-based data loss prevention (DLP), Network Access Control (NAC), network-based Intrusion prevention system (NIPS), Port security on core switches
B. Host-based data loss prevention (DLP), Endpoint anti-malware solution, Host-based integrity checker, Laptop locks, hard disk drive (HDD) encryption
C. Endpoint security management, network intrusion detection system (NIDS), Network Access Control (NAC), Privileged Access Management (PAM), security informationand event management (SIEM)
D. Web application firewall (WAF), Gateway network device tuning, Database firewall, Next-Generation Firewall (NGFW), Tier-2 demilitarized zone (DMZ) tuning

Answer: C

NEW QUESTION 136
- (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 140
- (Exam Topic 15)
What security principle addresses the issue of "Security by Obscurity"?

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

Answer: D

NEW QUESTION 142
- (Exam Topic 15)
Which of the following would qualify as an exception to the "right to be forgotten" of the General Data Protection Regulation's (GDPR)?

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

Answer: C

NEW QUESTION 143
- (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 148
- (Exam Topic 15)
Which of the following is a Key Performance Indicator (KPI) for a security training and awareness program?

A. The number of security audits performed
B. The number of attendees at security training events
C. The number of security training materials created
D. The number of security controls implemented

Answer: B

NEW QUESTION 152
- (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 155
- (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 157
- (Exam Topic 15)
Which of the following is the MOST secure password technique?

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

Answer: A

NEW QUESTION 162

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

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

Answer: A

NEW QUESTION 166
- (Exam Topic 15)
In software development, which of the following entities normally signs the code to protect the code integrity?

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

Answer: B

NEW QUESTION 167
- (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 168
- (Exam Topic 15)
Which type of disaster recovery plan (DRP) testing carries the MOST operational risk?

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

Answer: C

NEW QUESTION 170
- (Exam Topic 15)
Which of the following poses the GREATEST privacy risk to personally identifiable information (PII) when disposing of an office printer or copier?

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

Answer: B

NEW QUESTION 173
- (Exam Topic 15)
In systems security engineering, what does the security principle of modularity provide?

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

Answer: A

NEW QUESTION 175
- (Exam Topic 15)
Dumpster diving is a technique used in which stage of penetration testing methodology?

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

Answer: B

NEW QUESTION 176
- (Exam Topic 15)
Using Address Space Layout Randomization (ASLR) reduces the potential for which of the following attacks?

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

Answer: D

NEW QUESTION 181
- (Exam Topic 15)
When assessing the audit capability of an application, which of the following activities is MOST important?

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

Answer: C

NEW QUESTION 184
- (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 186
- (Exam Topic 15)
In a multi-tenant cloud environment, what approach will secure logical access to assets?

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

Answer: D

NEW QUESTION 191
- (Exam Topic 15)
While classifying credit card data related to Payment Card Industry Data Security Standards (PCI-DSS), which of the following is a PRIMARY security requirement?

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

Answer: C

NEW QUESTION 195
- (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 198
- (Exam Topic 15)
Which of the following is the MOST significant key management problem due to the number of keys created?

A. Keys are more difficult to provision and
B. Storage of the keys require increased security
C. Exponential growth when using asymmetric keys
D. Exponential growth when using symmetric keys

Answer: B

NEW QUESTION 200
- (Exam Topic 15)
An enterprise is developing a baseline cybersecurity standard its suppliers must meet before being awarded a contract. Which of the following statements is TRUE about the baseline cybersecurity standard?

A. It should be expressed as general requirements.
B. It should be expressed in legal terminology.
C. It should be expressed in business terminology.
D. It should be expressed as technical requirements.

Answer: D

NEW QUESTION 202
- (Exam Topic 15)
What BEST describes the confidentiality, integrity, availability triad?

A. A tool used to assist in understanding how to protect the organization's data
B. The three-step approach to determine the risk level of an organization
C. The implementation of security systems to protect the organization's data
D. A vulnerability assessment to see how well the organization's data is protected

Answer: C

NEW QUESTION 204
- (Exam Topic 15)
A small office is running WiFi 4 APs, and neighboring offices do not want to increase the throughput to associated devices. Which of the following is the MOST cost-efficient way for the office to increase network performance?

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

Answer: C

NEW QUESTION 207
- (Exam Topic 15)
What is the FINAL step in the waterfall method for contingency planning?

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

Answer: A

NEW QUESTION 212
- (Exam Topic 15)
What is static analysis intended to do when analyzing an executable file?

A. Collect evidence of the executable file's usage, including dates of creation and last use.
B. Search the documents and files associated with the executable file.
C. Analyze the position of the file in the file system and the executable file's libraries.
D. Disassemble the file to gather information about the executable file's function.

Answer: D

NEW QUESTION 214
- (Exam Topic 15)
Commercial off-the-shelf (COTS) software presents which of the following additional security concerns?

A. Vendors take on the liability for COTS software vulnerabilities.
B. In-house developed software is inherently less secure.
C. Exploits for COTS software are well documented and publicly available.
D. COTS software is inherently less secure.

Answer: C

NEW QUESTION 215
- (Exam Topic 15)
Which of the following would be considered an incident if reported by a security information and event management (SIEM) system?

A. An administrator is logging in on a server through a virtual private network (VPN).

B. A log source has stopped sending data.
C. A web resource has reported a 404 error.
D. A firewall logs a connection between a client on the Internet and a web server using Transmission Control Protocol (TCP) on port 80.

Answer: C

NEW QUESTION 217
- (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 221
- (Exam Topic 15)
Which of the following is the reason that transposition ciphers are easily recognizable?

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

Answer: B

NEW QUESTION 223
- (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 225
- (Exam Topic 15)
A hospital has allowed virtual private networking (VPN) access to remote database developers. Upon auditing the internal firewall configuration, the network administrator discovered that split-tunneling was enabled. What is the concern with this configuration?

A. Remote sessions will not require multi-layer authentication.
B. Remote clients are permitted to exchange traffic with the public and private network.
C. Multiple Internet Protocol Security (IPSec) tunnels may be exploitable in specific circumstances.
D. The network intrusion detection system (NIDS) will fail to inspect Secure Sockets Layer (SSL) traffic.

Answer: C

NEW QUESTION 226
- (Exam Topic 15)
What is the benefit of using Network Admission Control (NAC)?

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

Answer: C

NEW QUESTION 227
- (Exam Topic 15)
Which of the following minimizes damage to information technology (IT) equipment stored in a data center when a false fire alarm event occurs?

A. A pre-action system is installed.
B. An open system is installed.
C. A dry system is installed.
D. A wet system is installed.

Answer: C

NEW QUESTION 232

- (Exam Topic 15)
Which of the following is the PRIMARY purpose of due diligence when an organization embarks on a merger or acquisition?

A. Assess the business risks.
B. Formulate alternative strategies.
C. Determine that all parties are equally protected.
D. Provide adequate capability for all parties.
E. Strategy and program management, project delivery, governance, operations

Answer: A

NEW QUESTION 236
- (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 241
- (Exam Topic 15)
What is the PRIMARY benefit of relying on Security Content Automation Protocol (SCAP)?

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

Answer: C

NEW QUESTION 245
- (Exam Topic 15)
Which of the following is the BEST way to protect privileged accounts?

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

Answer: D

NEW QUESTION 248
- (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 253
- (Exam Topic 15)
Which of the following measures serves as the BEST means for protecting data on computers, smartphones, and external storage devices when traveling to high-risk countries?

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

Answer: D

NEW QUESTION 256
- (Exam Topic 15)
An organization has implemented a protection strategy to secure the network from unauthorized external access. The new Chief Information Security Officer (CISO) wants to increase security by better protecting the network from unauthorized internal access. Which Network Access Control (NAC) capability BEST meets this objective?

A. Application firewall
B. Port security

C. Strong passwords
D. Two-factor authentication (2FA)

Answer: D

NEW QUESTION 259
- (Exam Topic 15)
Data remanence is the biggest threat in which of the following scenarios?

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

Answer: D

NEW QUESTION 261
- (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 265
- (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 266
- (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 269
- (Exam Topic 15)
A Distributed Denial of Service (DDoS) attack was carried out using malware called Mirai to create a large-scale command and control system to launch a botnet. Which of the following devices were the PRIMARY sources used to generate the attack traffic?

A. Internet of Things (IoT) devices
B. Microsoft Windows hosts
C. Web servers running open source operating systems (OS)
D. Mobile devices running Android

Answer: A

NEW QUESTION 274
- (Exam Topic 15)
An organization has developed a way for customers to share information from their wearable devices with each other. Unfortunately, the users were not informed as to what information collected would be shared. What technical controls should be put in place to remedy the privacy issue while still trying to accomplish the organization's business goals?

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

Answer: D

NEW QUESTION 275

- (Exam Topic 15)
An international organization has decided to use a Software as a Service (SaaS) solution to support its business operations. Which of the following compliance standards should the organization use to assess the international code security and data privacy of the solution?

A. Health Insurance Portability and Accountability Act (HIPAA)
B. Service Organization Control (SOC) 2
C. Payment Card Industry (PCI)
D. Information Assurance Technical Framework (IATF)

Answer: B

NEW QUESTION 280
- (Exam Topic 15)
Which of the following is the BEST approach to implement multiple servers on a virtual system?

A. Implement multiple functions per virtual server and apply the same security configuration for each virtual server.
B. Implement one primary function per virtual server and apply high security configuration on the host operating system.
C. Implement one primary function per virtual server and apply individual security configuration for each virtual server.
D. Implement multiple functions within the same virtual server and apply individual security configurations to each function.

Answer: C

NEW QUESTION 281
- (Exam Topic 15)
An organization has determined that its previous waterfall approach to software development is not keeping pace with business demands. To adapt to the rapid changes required for product delivery, the organization has decided to move towards an Agile software development and release cycle. In order to ensure the success of the Agile methodology, who is MOST critical in creating acceptance tests or acceptance criteria for each release?

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

Answer: D

NEW QUESTION 284
- (Exam Topic 15)
What documentation is produced FIRST when performing an effective physical loss control process?

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

Answer: C

NEW QUESTION 287
- (Exam Topic 15)
Which of the following is the PRIMARY goal of logical access controls?

A. Restrict access to an information asset.
B. Ensure integrity of an information asset.
C. Restrict physical access to an information asset.
D. Ensure availability of an information asset.

Answer: C

NEW QUESTION 292
- (Exam Topic 15)
Which of the following attacks, if successful, could give an intruder complete control of a software-defined networking (SDN) architecture?

A. Sniffing the traffic of a compromised host inside the network
B. Sending control messages to open a flow that does not pass a firewall from a compromised host within the network
C. A brute force password attack on the Secure Shell (SSH) port of the controller
D. Remote Authentication Dial-In User Service (RADIUS) token replay attack

Answer: B

NEW QUESTION 294
- (Exam Topic 15)
Which of the following would be the BEST mitigation practice for man-in-the-middle (MITM) Voice over Internet Protocol (VoIP) attacks?

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

Answer: B

NEW QUESTION 297
- (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 298
- (Exam Topic 15)
Where can the Open Web Application Security Project (OWASP) list of associated vulnerabilities be found?

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

Answer: A

NEW QUESTION 299
- (Exam Topic 15)
Which of the following is considered the FIRST step when designing an internal security control assessment?

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

Answer: D

NEW QUESTION 304
- (Exam Topic 15)
Which of the following types of web-based attack is happening when an attacker is able to send a well-crafted, malicious request to an authenticated user without the user realizing it?

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

Answer: B

NEW QUESTION 308
- (Exam Topic 15)
Which of the following frameworks provides vulnerability metrics and characteristics to support the National Vulnerability Database (NVD)?

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

Answer: D

NEW QUESTION 309
- (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 313
- (Exam Topic 15)
Which Wide Area Network (WAN) technology requires the first router in the path to determine the full path the packet will travel, removing the need for other

routers in the path to make independent determinations?

A. Multiprotocol Label Switching (MPLS)
B. Synchronous Optical Networking (SONET)
C. Session Initiation Protocol (SIP)
D. Fiber Channel Over Ethernet (FCoE)

Answer: A

NEW QUESTION 315
- (Exam Topic 15)
Which of the following needs to be tested to achieve a Cat 6a certification for a company's data cabling?

A. RJ11
B. LC ports
C. Patch panel
D. F-type connector

Answer: C

NEW QUESTION 320
- (Exam Topic 15)
A company is enrolled in a hard drive reuse program where decommissioned equipment is sold back to the vendor when it is no longer needed. The vendor pays more money for functioning drives than equipment that is no longer operational. Which method of data sanitization would provide the most secure means of preventing unauthorized data loss, while also receiving the most money from the vendor?

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

Answer: C

NEW QUESTION 325
- (Exam Topic 15)
Which of the following explains why classifying data is an important step in performing a Risk assessment?

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

Answer: D

NEW QUESTION 330
- (Exam Topic 15)
An organization's internal audit team performed a security audit on the company's system and reported that the manufacturing application is rarely updated along with other issues categorized as minor. Six months later, an external audit team reviewed the same system with the same scope, but identified severe weaknesses in the manufacturing application's security controls. What is MOST likely to be the root cause of the internal audit team's failure in detecting these security issues?

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

Answer: A

NEW QUESTION 333
- (Exam Topic 15)
What Is a risk of using commercial off-the-shelf (COTS) products?

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

Answer: A

NEW QUESTION 337
- (Exam Topic 15)
The Open Web Application Security Project’s (OWASP) Software Assurance Maturity Model (SAMM) allows organizations to implement a flexible software security strategy to measure organizational impact based on what risk management aspect?

A. Risk tolerance
B. Risk exception
C. Risk treatment
D. Risk response

Answer: D

NEW QUESTION 338
- (Exam Topic 15)
Which of the following is the MOST common use of the Online Certificate Status Protocol (OCSP)?

A. To obtain the expiration date of an X.509 digital certificate
B. To obtain the revocation status of an X.509 digital certificate
C. To obtain the author name of an X.509 digital certificate
D. To verify the validity of an X.509 digital certificate

Answer: D

NEW QUESTION 343
- (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 347
- (Exam Topic 15)
Upon commencement of an audit within an organization, which of the following actions is MOST important for the auditor(s) to take?

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

Answer: C

NEW QUESTION 349
- (Exam Topic 15)
When resolving ethical conflicts, the information security professional MUST consider many factors. In what order should these considerations be prioritized?

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

Answer: C

NEW QUESTION 351
- (Exam Topic 15)
Which of the following BEST obtains an objective audit of security controls?

A. The security audit is measured against a known standard.
B. The security audit is performed by a certified internal auditor.
C. The security audit is performed by an independent third-party.
D. The security audit produces reporting metrics for senior leadership.

Answer: A

NEW QUESTION 355
- (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 357
- (Exam Topic 15)
The security team has been tasked with performing an interface test against a frontend external facing application and needs to verify that all input fields protect against

invalid input. Which of the following BEST assists this process?

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

Answer: A

NEW QUESTION 362
- (Exam Topic 15)
Which of the following is a key responsibility for a data steward assigned to manage an enterprise data lake?

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

Answer: A

NEW QUESTION 364
- (Exam Topic 15)
Which of the (ISC)? Code of Ethics canons is MOST reflected when preserving the value of systems, applications, and entrusted information while avoiding conflicts of interest?

A. Act honorably, honestly, justly, responsibly, and legally.
B. Protect society, the commonwealth, and the infrastructure.
C. Provide diligent and competent service to principles.
D. Advance and protect the profession.

Answer: B

NEW QUESTION 369
- (Exam Topic 15)
Which change management role is responsible for the overall success of the project and supporting the change throughout the organization?

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

Answer: D

NEW QUESTION 374
- (Exam Topic 15)
What is the FIRST step in risk management?

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

Answer: C

NEW QUESTION 379
- (Exam Topic 15)
A subscription service which provides power, climate control, raised flooring, and telephone wiring but NOT the computer and peripheral equipment is BEST described as a:

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

Answer: C

NEW QUESTION 381
- (Exam Topic 15)
Which of the following factors is á PRIMARY reason to drive changes in an Information Security Continuous Monitoring (ISCM) strategy?

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

Answer: B

NEW QUESTION 386
- (Exam Topic 15)
An organization is implementing security review as part of system development. Which of the following is the BEST technique to follow?

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

Answer: C

NEW QUESTION 387
- (Exam Topic 15)
Which of the following would be the BEST guideline to follow when attempting to avoid the exposure of sensitive data?

A. Store sensitive data only when necessary.
B. Educate end-users on methods of attacks on sensitive data.
C. Establish report parameters for sensitive data.
D. Monitor mail servers for sensitive data being exfilltrated.

Answer: A

NEW QUESTION 388
- (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 390
- (Exam Topic 15)
A company wants to implement two-factor authentication (2FA) to protect their computers from unauthorized users. Which solution provides the MOST secure means of authentication and meets the criteria they have set?

A. Username and personal identification number (PIN)
B. Fingerprint and retinal scanners
C. Short Message Services (SMS) and smartphone authenticator
D. Hardware token and password

Answer: D

NEW QUESTION 391
- (Exam Topic 15)
A software developer wishes to write code that will execute safely and only as intended. Which of the following programming language types is MOST likely to achieve this goal?

A. Statically typed
B. Weakly typed
C. Strongly typed
D. Dynamically typed

Answer: D

NEW QUESTION 396
- (Exam Topic 15)
Which of the following attack types can be used to compromise the integrity of data during transmission?

A. Keylogging
B. Packet sniffing
C. Synchronization flooding
D. Session hijacking

Answer: B

NEW QUESTION 401
- (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 403
- (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 404
- (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 408
- (Exam Topic 15)
Which of the following statements is TRUE about Secure Shell (SSH)?

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

Answer: B

NEW QUESTION 411
- (Exam Topic 15)
When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner's first consideration?

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

Answer: B

NEW QUESTION 415
- (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 416
- (Exam Topic 15)
The quality assurance (QA) department is short-staffed and is unable to test all modules before the anticipated release date of an application. What security control is MOST likely to be violated?

A. Separation of environments
B. Program management
C. Mobile code controls
D. Change management

Answer: D

NEW QUESTION 419
- (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 424
- (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 428
- (Exam Topic 15)
Which evidence collecting technique would be utilized when it is believed an attacker is employing a rootkit and a quick analysis is needed?

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

Answer: A

NEW QUESTION 431
- (Exam Topic 15)
The adoption of an enterprise-wide Business Continuity (BC) program requires which of the following?

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

Answer: D

NEW QUESTION 436
- (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 441
- (Exam Topic 15)
Of the following, which BEST provides non- repudiation with regards to access to a server room?

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

Answer: C

NEW QUESTION 445
- (Exam Topic 15)
An attacker has intruded into the source code management system and is able to download but not modify the code. Which of the following aspects of the code theft has the HIGHEST security impact?

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

Answer: A

NEW QUESTION 448
- (Exam Topic 15)
Which organizational department is ultimately responsible for information governance related to e-mail and other e-records?

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

Answer: C

NEW QUESTION 450
- (Exam Topic 15)
Which of the following BEST describes the purpose of Border Gateway Protocol (BGP)?

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

Answer: B

NEW QUESTION 454
- (Exam Topic 15)
A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

A. nslookup
B. netstat -a
C. ipeonfig /a
D. arp -a

Answer: B

NEW QUESTION 459
- (Exam Topic 15)
Which of the following BEST ensures the integrity of transactions to intended recipients?

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

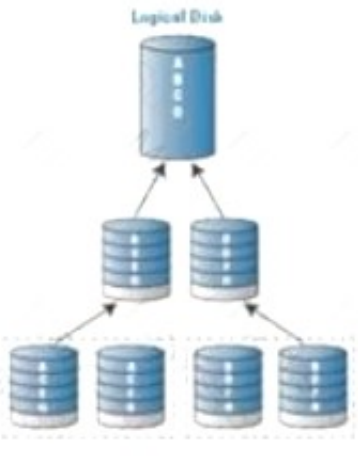
Answer: A

NEW QUESTION 461
- (Exam Topic 15)
What are the first two components of logical access control?

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

Answer: B

NEW QUESTION 464
- (Exam Topic 15)
Which Redundant Array c/ Independent Disks (RAID) Level does the following diagram represent?



A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 10

Answer: D

NEW QUESTION 468
- (Exam Topic 15)
An organization is preparing to achieve General Data Protection Regulation (GDPR) compliance. The Chief Information Security Officer (CISO) is reviewing data protection methods.
Which of the following is the BEST data protection method?

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

Answer: C

NEW QUESTION 473
- (Exam Topic 15)
Write Once, Read Many (WORM) data storage devices are designed to BEST support which of the following core security concepts?

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

Answer: A

NEW QUESTION 474
- (Exam Topic 15)
The security architect has been assigned the responsibility of ensuring integrity of the organization's electronic records. Which of the following methods provides the strongest level of integrity?

A. Time stamping
B. Encryption
C. Hashing
D. Digital signature

Answer: D

NEW QUESTION 477
- (Exam Topic 15)
A large manufacturing organization arranges to buy an industrial machine system to produce a new line of products. The system includes software provided to the vendor by a thirdparty organization. The financial risk to the manufacturing organization starting production is high. What step should the manufacturing organization take to minimize its financial risk in the new venture prior to the purchase?

A. Hire a performance tester to execute offline tests on a system.
B. Calculate the possible loss in revenue to the organization due to software bugs and vulnerabilities, and compare that to the system's overall price.
C. Place the machine behind a Layer 3 firewall.
D. Require that the software be thoroughly tested by an accredited independent software testing company.

Answer: B

NEW QUESTION 482
- (Exam Topic 15)
Which of the following BEST describes the standard used to exchange authorization information between different identity management systems?

A. Security Assertion Markup Language (SAML)
B. Service Oriented Architecture (SOA)
C. Extensible Markup Language (XML)
D. Wireless Authentication Protocol (WAP)

Answer: A

NEW QUESTION 487
- (Exam Topic 15)
What is the MOST common security risk of a mobile device?

A. Insecure communications link
B. Data leakage
C. Malware infection
D. Data spoofing

Answer: C

NEW QUESTION 492
- (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 494
- (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 498
- (Exam Topic 15)
Which of the following has the responsibility of information technology (IT) governance?

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

Answer: A

NEW QUESTION 500
- (Exam Topic 15)
What is the second phase of public key infrastructure (PKI) key/certificate life-cycle management?

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

Answer: A

NEW QUESTION 501
- (Exam Topic 15)
Which of the following vulnerabilities can be BEST detected using automated analysis?

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

Answer: D

NEW QUESTION 502
- (Exam Topic 15)
International bodies established a regulatory scheme that defines how weapons are exchanged between the signatories. It also addresses cyber weapons, including malicious software, Command and Control (C2) software, and internet surveillance software. This is a description of which of the following?

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

Answer: C

NEW QUESTION 504
- (Exam Topic 15)
What is considered the BEST explanation when determining whether to provide remote network access to a third-party security service?

A. Contract negotiation
B. Vendor demonstration
C. Supplier request

D. Business need

Answer: D

NEW QUESTION 508
- (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 513
- (Exam Topic 15)
An employee's home address should be categorized according to which of the following references?

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

Answer: B

NEW QUESTION 515
- (Exam Topic 15)
When developing an organization's information security budget, it is important that the

A. expected risk can be managed appropriately with the funds allocated.
B. requested funds are at an equal amount to the expected cost of breaches.
C. requested funds are part of a shared funding pool with other areas.
D. expected risk to the organization does not exceed the funds allocated.

Answer: A

NEW QUESTION 518
- (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 522
- (Exam Topic 15)
How should the retention period for an organization's social media content be defined?

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

Answer: B

NEW QUESTION 526
- (Exam Topic 15)
Which of the following is the MOST important consideration in selecting a security testing method based on different Radio-Frequency Identification (RFID) vulnerability types?

A. The performance and resource utilization of tools
B. The quality of results and usability of tools
C. An understanding of the attack surface
D. Adaptability of testing tools to multiple technologies

Answer: C

NEW QUESTION 530
- (Exam Topic 15)
A manager identified two conflicting sensitive user functions that were assigned to a single user account that had the potential to result in financial and regulatory

risk to the company. The manager MOST likely discovered this during which of the following?

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

Answer: B

NEW QUESTION 535
- (Exam Topic 15)
A scan report returned multiple vulnerabilities affecting several production servers that are mission critical. Attempts to apply the patches in the development environment have caused the servers to crash. What is the BEST course of action?

A. Upgrade the software affected by the vulnerability.
B. Inform management of possible risks.
C. Mitigate the risks with compensating controls.
D. Remove the affected software from the servers.

Answer: C

NEW QUESTION 538
- (Exam Topic 15)
Which is the BEST control to meet the Statement on Standards for Attestation Engagements 18 (SSAE-18) confidentiality category?

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

Answer: C

NEW QUESTION 540
- (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 541
- (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 542
- (Exam Topic 15)
The security team is notified that a device on the network is infected with malware. Which of the following is MOST effective in enabling the device to be quickly located and remediated?

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

Answer: D

NEW QUESTION 544
- (Exam Topic 15)
Why are packet filtering routers used in low-risk environments?

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

Answer: B

NEW QUESTION 548
- (Exam Topic 15)
A system developer has a requirement for an application to check for a secure digital signature before the application is accessed on a user's laptop. Which security mechanism addresses this requirement?

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

Answer: B

NEW QUESTION 550
- (Exam Topic 15)
Which of the following is the name of an individual or group that is impacted by a change?

A. Change agent
B. Stakeholder
C. Sponsor
D. End User

Answer: B

NEW QUESTION 554
- (Exam Topic 15)
An organization implements Network Access Control (NAC) ay Institute of Electrical and Electronics Engineers (IEEE) 802.1x and discovers the printers do not support the IEEE 802.1x standard. Which of the following is the BEST resolution?

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

Answer: A

NEW QUESTION 558
- (Exam Topic 15)
The Industrial Control System (ICS) Computer Emergency Response Team (CERT) has released an alert regarding ICS-focused malware specifically propagating through Windows-based business networks. Technicians at a local water utility note that their dams, canals, and locks controlled by an internal Supervisory Control and Data Acquisition (SCADA) system have been malfunctioning. A digital forensics professional is consulted in the Incident Response (IR) and recovery. Which of the following is the
MOST challenging aspect of this investigation?

A. SCADA network latency
B. Group policy implementation
C. Volatility of data
D. Physical access to the system

Answer: C

NEW QUESTION 561
- (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 562
- (Exam Topic 15)
Which of the following protects personally identifiable information (PII) used by financial services organizations?

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

Answer: B

NEW QUESTION 563
- (Exam Topic 15)
What is the overall goal of software security testing?

A. Identifying the key security features of the software

B. Ensuring all software functions perform as specified
C. Reducing vulnerabilities within a software system
D. Making software development more agile

Answer: B

NEW QUESTION 565
- (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 567
- (Exam Topic 15)
A security professional can BEST mitigate the risk of using a Commercial Off-The-Shelf (COTS) solution by deploying the application with which of the following controls in ?

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

Answer: A

NEW QUESTION 572
- (Exam Topic 15)
A security professional needs to find a secure and efficient method of encrypting data on an endpoint. Which solution includes a root key?

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

Answer: D

NEW QUESTION 575
- (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 579
- (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 583
- (Exam Topic 15)
What is the FIRST step prior to executing a test of an organisation’s disaster recovery (DR) or business continuity plan (BCP)?

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

Answer: D

NEW QUESTION 588

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

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

Answer: D

NEW QUESTION 590
- (Exam Topic 15)
The application owner of a system that handles confidential data leaves an organization. It is anticipated that a replacement will be hired in approximately six months. During that time, which of the following should the organization do?

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

Answer: B

NEW QUESTION 594
- (Exam Topic 15)
Which algorithm gets its security from the difficulty of calculating discrete logarithms in a finite field and is used to distribute keys, but cannot be used to encrypt or decrypt messages?

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

Answer: C

NEW QUESTION 599
- (Exam Topic 15)
What is the BEST design for securing physical perimeter protection?

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

Answer: B

NEW QUESTION 603
- (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 606
- (Exam Topic 15)
Which of the following BEST describes when an organization should conduct a black box security audit on a new software product?

A. When the organization wishes to check for non-functional compliance
B. When the organization wants to enumerate known security vulnerabilities across their infrastructure
C. When the organization has experienced a security incident
D. When the organization is confident the final source code is complete

Answer: B

NEW QUESTION 610
- (Exam Topic 15)
Which of the following determines how traffic should flow based on the status of the infrastructure true?

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

Answer: D

NEW QUESTION 611
- (Exam Topic 15)
A security professional has reviewed a recent site assessment and has noted that a server room on the second floor of a building has Heating, Ventilation, and Air Conditioning (HVAC) intakes on the ground level that have ultraviolet light filters installed, Aero-K Fire suppression in the server room, and pre-action fire suppression on floors above the server room. Which of the following changes can the security professional recommend to reduce risk associated with these conditions?

A. Remove the ultraviolet light filters on the HVAC intake and replace the fire suppression system on the upper floors with a dry system
B. Add additional ultraviolet light filters to the HVAC intake supply and return ducts and change server room fire suppression to FM-200
C. Apply additional physical security around the HVAC intakes and update upper floor fire suppression to FM-200.
D. Elevate the HVAC intake by constructing a plenum or external shaft over it and convert the server room fire suppression to a pre-action system

Answer: C

NEW QUESTION 612
- (Exam Topic 15)
An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex.
Which of the following is the MOST likely cause of this issue?

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

Answer: A

NEW QUESTION 614
- (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 617
- (Exam Topic 15)
Which media sanitization methods should be used for data with a high security categorization?

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

Answer: D

NEW QUESTION 621
- (Exam Topic 15)
Which of the following is used to ensure that data mining activities Will NOT reveal sensitive data?

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

Answer: D

NEW QUESTION 623
- (Exam Topic 15)
Which of the following protection is provided when using a Virtual Private Network (VPN) with Authentication Header (AH)?

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

Answer: C

NEW QUESTION 627
- (Exam Topic 15)
A cloud service accepts Security Assertion Markup Language (SAML) assertions from users to on and security However, an attacker was able to spoof a registered account on the network and query the SAML provider.
What is the MOST common attack leverage against this flaw?

A. Attacker forges requests to authenticate as a different user.
B. Attacker leverages SAML assertion to register an account on the security domain.
C. Attacker conducts denial-of-service (DoS) against the security domain by authenticating as the same user repeatedly.
D. Attacker exchanges authentication and authorization data between security domains.

Answer: A

NEW QUESTION 631
- (Exam Topic 15)
How is it possible to extract private keys securely stored on a cryptographic smartcard?

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

Answer: D

NEW QUESTION 636
- (Exam Topic 15)
An organization is considering partnering with a third-party supplier of cloud services. The organization will only be providing the data and the third-party supplier will be providing the security controls. Which of the following BEST describes this service offering?

A. Platform as a Service (PaaS)
B. Infrastructure as a Service (IaaS)
C. Software as a Service (SaaS)
D. Anything as a Service (XaaS)

Answer: D

NEW QUESTION 639
- (Exam Topic 15)
An application developer receives a report back from the security team showing their automated tools were able to successfully enter unexpected data into the organization's customer service portal, causing the site to crash. This is an example of which type of testing?

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

Answer: D

NEW QUESTION 643
- (Exam Topic 15)
Which one of the following can be used to detect an anomaly in a system by keeping track of the state of files that do not normally change?\

A. System logs
B. Anti-spyware
C. Integrity checker
D. Firewall logs

Answer: C

NEW QUESTION 647
- (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 650
- (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 655

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

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

Answer: B

NEW QUESTION 658
- (Exam Topic 15)
Which of the following should be included in a good defense-in-depth strategy provided by object-oriented programming for software deployment?

A. Polyinstantiation
B. Polymorphism
C. Encapsulation
D. Inheritance

Answer: A

NEW QUESTION 661
- (Exam Topic 15)
In an environment where there is not full administrative control over all network connected endpoints, such as a university where non-corporate devices are used, what is
the BEST way to restrict access to the network?

A. Use switch port security to limit devices connected to a particular switch port.
B. Use of virtual local area networks (VLAN) to segregate users.
C. Use a client-based Network Access Control (NAC) solution.
D. Use a clientless Network Access Control (NAC) solution

Answer: A

NEW QUESTION 663
- (Exam Topic 15)
When are security requirements the LEAST expensive to implement?

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

Answer: D

NEW QUESTION 667
- (Exam Topic 15)
What part of an organization’s strategic risk assessment MOST likely includes information on items affecting the success of the organization?

A. Key Risk Indicator (KRI)
B. Threat analysis
C. Vulnerability analysis
D. Key Performance Indicator (KPI)

Answer: A

NEW QUESTION 671
- (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 672
- (Exam Topic 15)
Which of the following should exist in order to perform a security audit?

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

Answer: D

NEW QUESTION 674
- (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 679
- (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 683
- (Exam Topic 15)
Which of the following is the MOST effective strategy to prevent an attacker from disabling a network?

A. Test business continuity and disaster recovery (DR) plans.
B. Design networks with the ability to adapt, reconfigure, and fail over.
C. Implement network segmentation to achieve robustness.
D. Follow security guidelines to prevent unauthorized network access.

Answer: D

NEW QUESTION 687
- (Exam Topic 15)
Who should perform the design review to uncover security design flaws as part of the Software Development Life Cycle (SDLC)?

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

Answer: B

NEW QUESTION 692
- (Exam Topic 15)
At which phase of the software assurance life cycle should risks associated with software acquisition strategies be identified?

A. Follow-on phase
B. Planning phase
C. Monitoring and acceptance phase
D. Contracting phase

Answer: C

NEW QUESTION 695
- (Exam Topic 15)
How should the retention period for an organization's social media content be defined?

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

Answer: C

NEW QUESTION 698
- (Exam Topic 15)
Which of the following features is MOST effective in mitigating against theft of data on a corporate mobile device which has been stolen?

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

Answer:

A

NEW QUESTION 700
- (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 705
- (Exam Topic 15)
A healthcare insurance organization chose a vendor to develop a software application. Upon review of the draft contract, the information security professional notices that software security is not addressed. What is the BEST approach to address the issue?

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

Answer: C

NEW QUESTION 708
- (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 711
- (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 712
- (Exam Topic 15)
The development team has been tasked with collecting data from biometric devices. The application will support a variety of collection data streams. During the testing phase, the team utilizes data from an old production database in a secure testing environment. What principle has the team taken into consideration?

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

Answer: A

NEW QUESTION 716
- (Exam Topic 15)
What process facilitates the balance of operational and economic costs of protective measures with gains in mission capability?

A. Risk assessment
B. Performance testing
C. Security audit
D. Risk management

Answer: D

NEW QUESTION 720
- (Exam Topic 14)
What is the MOST effective way to determine a mission critical asset in an organization?

A. Vulnerability analysis

B. business process analysis
C. Threat analysis
D. Business risk analysis

Answer: B

NEW QUESTION 722
- (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 725
- (Exam Topic 14)
In a dispersed network that lacks central control, which of the following is die PRIMARY course of action to mitigate exposure?

A. Implement management policies, audit control, and data backups
B. Implement security policies and standards, access controls, and access limitations
C. Implement security policies and standards, data backups, and audit controls
D. Implement remote access policies, shared workstations, and log management

Answer: C

NEW QUESTION 730
- (Exam Topic 14)
What is a warn site when conducting Business continuity planning (BCP)

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

Answer: B

NEW QUESTION 735
- (Exam Topic 14)
What type of access control determines the authorization to resource based on pre-defined job titles within an organization?

A. Role-Based Access Control (RBAC)
B. Role-based access control
C. Non-discretionary access control
D. Discretionary Access Control (DAC)

Answer: A

NEW QUESTION 739
- (Exam Topic 14)
Which of the following is the PRIMARY risk associated with Extensible Markup Language (XML) applications?

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

Answer: A

NEW QUESTION 740
- (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 742
- (Exam Topic 14)

For the purpose of classification, which of the following is used to divide trust domain and trust boundaries?

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

Answer: A

NEW QUESTION 745
- (Exam Topic 14)
What access control scheme uses fine-grained rules to specify the conditions under which access to each data item or applications is granted?

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

Answer: D

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

NEW QUESTION 748
- (Exam Topic 14)
A large corporation is looking for a solution to automate access based on where the request is coming from, who the user is, what device they are connecting with, and what and time of day they are attempting this access. What type of solution would suit their needs?

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

Answer: B

NEW QUESTION 752
- (Exam Topic 14)
Vulnerability scanners may allow for the administrator to assign which of the following in order to assist in prioritizing remediation activities?

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

Answer: C

NEW QUESTION 753
- (Exam Topic 14)
Which of the following encryption types is used in Hash Message Authentication Code (HMAC) for key distribution?

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

Answer: A

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

NEW QUESTION 755
- (Exam Topic 14)
A corporate security policy specifies that all devices on the network must have updated operating system patches and anti-malware software. Which technology should be used to enforce this policy?

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

Answer: D

NEW QUESTION 756
- (Exam Topic 14)
Which of the following is the GREATEST security risk associated with the user of identity as a service (IDaaS) when an organization its own software?

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

Answer: B

NEW QUESTION 760
- (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 765
- (Exam Topic 14)
Compared with hardware cryptography, software cryptography is generally

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

Answer: A

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

NEW QUESTION 767
- (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 769
- (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 773
- (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 778
- (Exam Topic 14)
An organization has a short-term agreement with a public Cloud Service Provider (CSP). Which of the following BEST protects sensitive data once the agreement expires and the assets are reused?

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

Answer: C

NEW QUESTION 783
- (Exam Topic 14)
Limiting the processor, memory, and Input/output (I/O) capabilities of mobile code is known as

A. code restriction.
B. on-demand compile.
C. sandboxing.
D. compartmentalization.

Answer: C

NEW QUESTION 784
- (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 789
- (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 794
- (Exam Topic 14)
Which of the following is the MOST effective countermeasure against Man-in-the Middle (MITM) attacks while using online banking?

A. Transport Layer Security (TLS)
B. Secure Sockets Layer (SSL)
C. Pretty Good Privacy (PGP)
D. Secure Shell (SSH)

Answer: A

NEW QUESTION 795
- (Exam Topic 14)
When conducting a security assessment of access controls , Which activity is port of the data analysis phase?

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

Answer: C

NEW QUESTION 799
- (Exam Topic 14)
Which of the following is the MOST critical success factor in the security patch management process?

A. Tracking and reporting on inventory
B. Supporting documentation
C. Management review of reports
D. Risk and impact analysis

Answer: A

NEW QUESTION 801
- (Exam Topic 14)
An organization discovers that its secure file transfer protocol (SFTP) server has been accessed by an unauthorized person to download an unreleased game. A recent security audit found weaknesses in some of the organization’s general information technology (IT) controls, specifically pertaining to software change control and security patch management, but not in other control areas.
Which of the following is the MOST probable attack vector used in the security breach?

A. Buffer overflow
B. Weak password able to lack of complexity rules
C. Distributed Denial of Service (DDoS)
D. Cross-Site Scripting (XSS)

Answer: A

NEW QUESTION 805
- (Exam Topic 14)
In order for application developers to detect potential vulnerabilities earlier during the Software Development Life Cycle (SDLC), which of the following safeguards should be implemented FIRST as part of a comprehensive testing framework?

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

Answer: A

NEW QUESTION 810
- (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 812
- (Exam Topic 14)
Which of the following open source software issues pose the MOST risk to an application?

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

Answer: D

NEW QUESTION 814
- (Exam Topic 14)
Which of the following BEST provides for non-repudiation od user account actions?

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

Answer: D

NEW QUESTION 819
- (Exam Topic 14)
Point-to-Point Protocol (PPP) was designed to specifically address what issue?

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

Answer: B

NEW QUESTION 824
- (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 829

- (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 832
- (Exam Topic 14)
An organization is outsourcing its payroll system and is requesting to conduct a full audit on the third-party information technology (IT) systems. During the due diligence process, the third party provides previous audit report on its IT system.
Which of the following MUST be considered by the organization in order for the audit reports to be acceptable?

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

Answer: A

NEW QUESTION 837
- (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 842
- (Exam Topic 14)
Which layer of the Open systems Interconnection (OSI) model is being targeted in the event of a Synchronization (SYN) flood attack?

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

Answer: B

NEW QUESTION 844
- (Exam Topic 14)
Which of the following is a process in the access provisioning lifecycle that will MOST likely identify access aggregation issues?

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

Answer: C

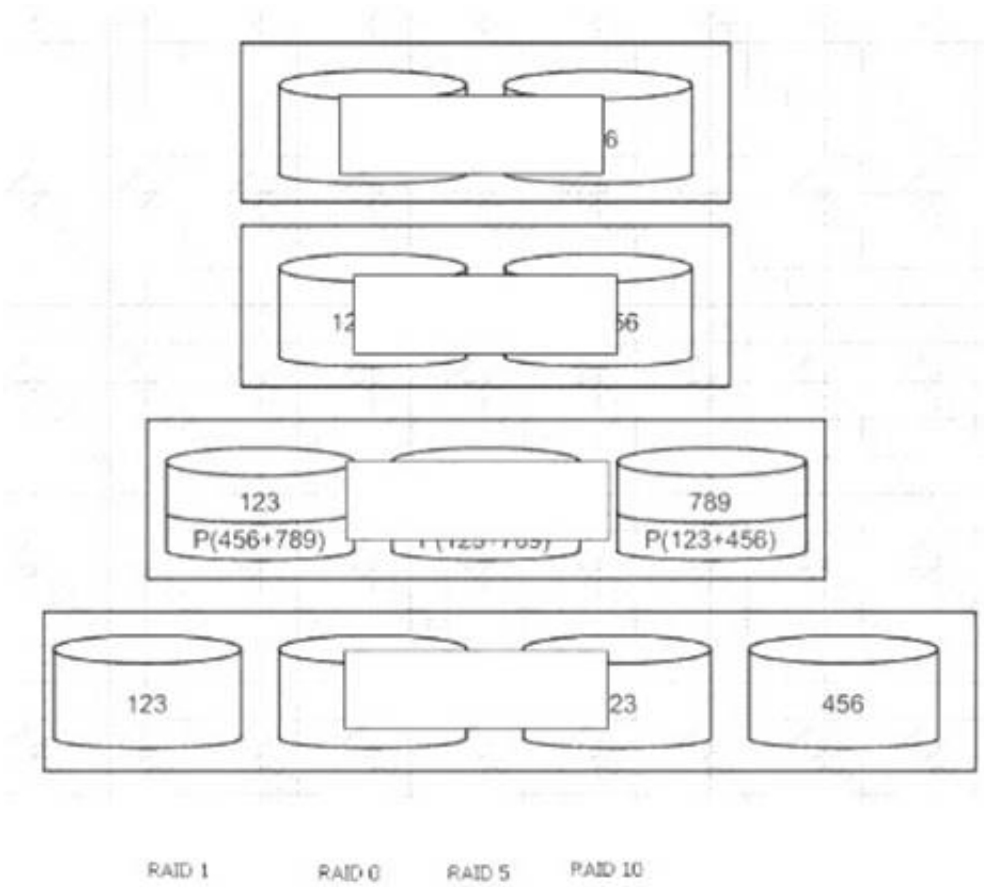
Explanation:
Reference: https://books.google.com.pk/books?id=W2TvAgAAQBAJ&pg=PA256&lpg=PA256&dq=process+in+the+acce

NEW QUESTION 845
- (Exam Topic 14)
What is the document that describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls?

A. Business Impact Analysis (BIA)
B. Security Assessment Report (SAR)
C. Plan of Action and Milestones {POA&M)
D. Security Assessment Plan (SAP)

Answer: C

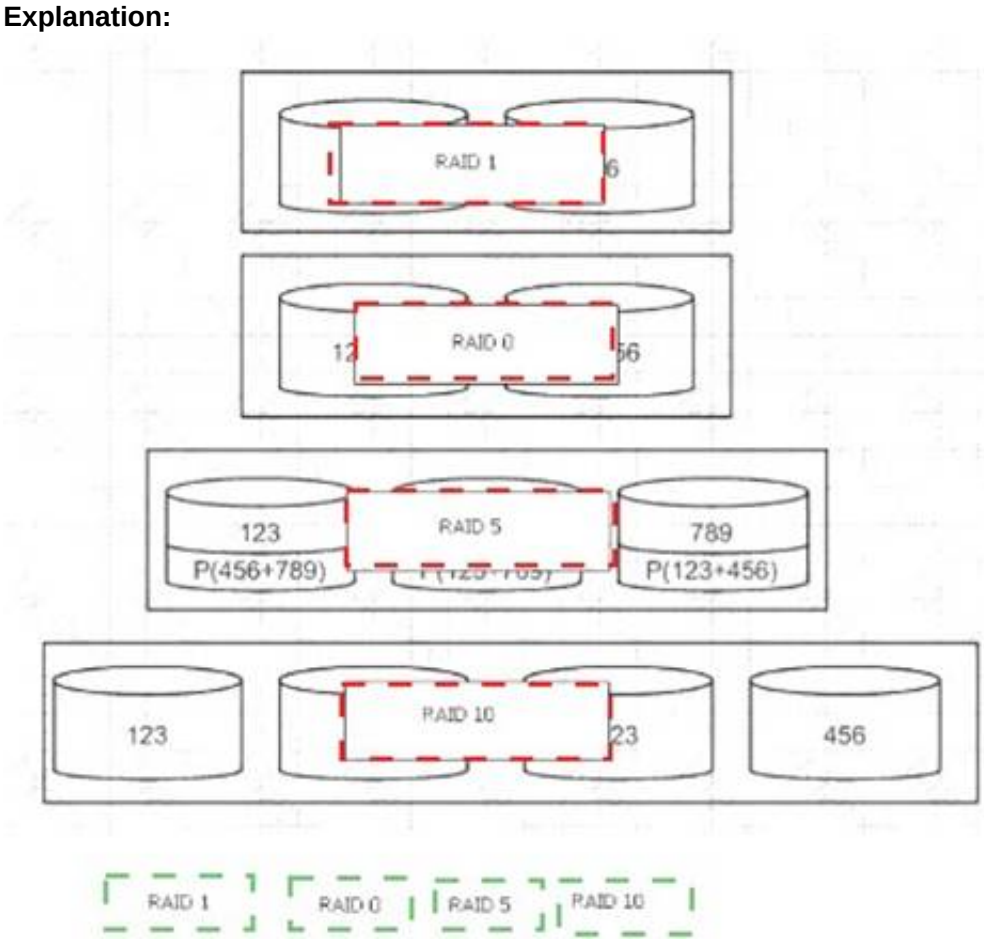
NEW QUESTION 846
- (Exam Topic 14)
Given a file containing ordered number, i.e. “123456789,” match each of the following redundant Array of independent Disks (RAID) levels to the corresponding visual representation visual representation. Note: P() = parity.
Drag each level to the appropriate place on the diagram.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 851
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISSP Practice Exam Features:

* CISSP Questions and Answers Updated Frequently

* CISSP Practice Questions Verified by Expert Senior Certified Staff

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

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