

CISSP Dumps

Certified Information Systems Security Professional (CISSP)

<https://www.certleader.com/CISSP-dumps.html>



NEW QUESTION 1

- (Exam Topic 15)

What is the MAIN objective of risk analysis in Disaster Recovery (DR) planning?

- A. Establish Maximum Tolerable Downtime (MTD) Information Systems (IS).
- B. Define the variable cost for extended downtime scenarios.
- C. Identify potential threats to business availability.
- D. Establish personnel requirements for various downtime scenarios.

Answer: C

NEW QUESTION 2

- (Exam Topic 15)

What is the FIRST step when developing an Information Security Continuous Monitoring (ISCM) program?

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

Answer: D

NEW QUESTION 3

- (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 4

- (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 5

- (Exam Topic 15)

Which of the following does the security design process ensure within the System Development Life Cycle (SDLC)?

- A. Proper security controls, security goals, and fault mitigation are properly conducted.
- B. Proper security controls, security objectives, and security goals are properly initiated.
- C. Security goals, proper security controls, and validation are properly initiated.
- D. Security objectives, security goals, and system test are properly conducted.

Answer: B

NEW QUESTION 6

- (Exam Topic 15)

A company is planning to implement a private cloud infrastructure. Which of the following recommendations will support the move to a cloud infrastructure?

- A. Implement a virtual local area network (VLAN) for each department and create a separate subnet for each VLAN.
- B. Implement software-defined networking (SDN) to provide the ability for the network infrastructure to be integrated with the control and data planes.
- C. Implement a virtual local area network (VLAN) to logically separate the local area network (LAN) from the physical switches.
- D. implement software-defined networking (SDN) to provide the ability to apply high-level policies to shape and reorder network traffic based on users, devices and applications.

Answer: D

NEW QUESTION 7

- (Exam Topic 15)

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

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

D. Acceptance testing

Answer: B

NEW QUESTION 8

- (Exam Topic 15)

he security organization is looking for a solution that could help them determine with a strong level of confidence that attackers have breached their network. Which solution is MOST effective at discovering successful network breach?

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

Answer: B

NEW QUESTION 9

- (Exam Topic 15)

Which of the following routing protocols is used to exchange route information between public autonomous systems?

- A. OSPF
- B. BGP
- C. EIGRP
- D. RIP

Answer: B

NEW QUESTION 10

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 10

- (Exam Topic 15)

A 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 15

- (Exam Topic 15)

Which security evaluation model assesses a product's Security Assurance Level (SAL) in comparison to similar solutions?

- A. Payment Card Industry Data Security Standard (PCI-DSS)
- B. International Organization for Standardization (ISO) 27001
- C. Common criteria (CC)
- D. Control Objectives for Information and Related Technology (COBIT)

Answer: C

NEW QUESTION 18

- (Exam Topic 15)

Which of the following is the FIRST step for defining Service Level Requirements (SLR)?

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

Answer: D

NEW QUESTION 21

- (Exam Topic 15)

Which of the following provides the MOST secure method for Network Access Control (NAC)?

- A. Media Access Control (MAC) filtering
- B. 802.1X authentication
- C. Application layer filtering
- D. Network Address Translation (NAT)

Answer: B

NEW QUESTION 26

- (Exam Topic 15)

Which of the following actions should be undertaken prior to deciding on a physical baseline Protection Profile (PP)?

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

Answer: A

NEW QUESTION 27

- (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 29

- (Exam Topic 15)

To minimize the vulnerabilities of a web-based application, which of the following FIRST actions will lock down the system and minimize the risk of an attack?

- A. Install an antivirus on the server
- B. Run a vulnerability scanner
- C. Review access controls
- D. Apply the latest vendor patches and updates

Answer: D

NEW QUESTION 32

- (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 34

- (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 37

- (Exam Topic 15)

A company is moving from the V model to Agile development. How can the information security department BEST ensure that secure design principles are implemented in the new methodology?

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

D. Information security requirements are captured in mandatory user stories.

Answer: D

NEW QUESTION 39

- (Exam Topic 15)

What is the MAIN purpose of conducting a business impact analysis (BIA)?

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

Answer: B

NEW QUESTION 40

- (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 45

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 50

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 55

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 60

- (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 62

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 65

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 66

- (Exam Topic 15)

Which of the following is the BEST way to mitigate circumvention of access controls?

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

Answer: D

NEW QUESTION 70

- (Exam Topic 15)

A security practitioner needs to implement solution to verify endpoint security protections and operating system (OS) versions. Which of the following is the BEST solution to implement?

- A. An intrusion prevention system (IPS)
- B. An intrusion prevention system (IPS)
- C. Network Access Control (NAC)
- D. A firewall

Answer: B

NEW QUESTION 72

- (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 73

- (Exam Topic 15)

Who should formulate conclusions from a particular digital fore Ball, Submit a Toper Of Tags, and the results?

- A. The information security professional's supervisor
- B. Legal counsel for the information security professional's employer
- C. The information security professional who conducted the analysis
- D. A peer reviewer of the information security professional

Answer: B

NEW QUESTION 78

- (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 router off, perform forensic analysis, apply the appropriate fin, and log incidents.

Answer: C

NEW QUESTION 80

- (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 82

- (Exam Topic 15)

Which reporting type requires a service organization to describe its system and define its control objectives and controls that are relevant to users internal control over financial reporting?

- A. Statement on Auditing Standards (SAS)70
- B. Service Organization Control 1 (SOC1)
- C. Service Organization Control 2 (SOC2)
- D. Service Organization Control 3 (SOC3)

Answer: B

NEW QUESTION 85

- (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 89

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 92

- (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 95

- (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 100

- (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 102

- (Exam Topic 15)

When configuring Extensible Authentication Protocol (EAP) in a Voice over Internet Protocol (VoIP) network, which of the following authentication types is the MOST secure?

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

Answer: C

NEW QUESTION 105

- (Exam Topic 15)

What is the term used to define where data is geographically stored in the cloud?

- A. Data warehouse
- B. Data privacy rights
- C. Data subject rights
- D. Data sovereignty

Answer: D

NEW QUESTION 107

- (Exam Topic 15)

Which of the following is included in change management?

- A. Business continuity testing
- B. User Acceptance Testing (UAT) before implementation
- C. Technical review by business owner
- D. Cost-benefit analysis (CBA) after implementation

Answer: A

NEW QUESTION 111

- (Exam Topic 15)

Which of the following are mandatory canons for the (ISC)* Code of Ethics?

- A. Develop comprehensive security strategies for the organization.
- B. Perform is, honestly, fairly, responsibly, and lawfully for the organization.
- C. Create secure data protection policies to principals.
- D. Provide diligent and competent service to principals.

Answer: D

NEW QUESTION 116

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 118

- (Exam Topic 15)

In the last 15 years a company has experienced three electrical failures. The cost associated with each failure is listed below. Which of the following would be a reasonable annual loss expectation?

Availability	60,000
Integrity	10,000
Confidentiality	0
<hr/>	
Total Impact	70,000

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

Answer: B

NEW QUESTION 120

- (Exam Topic 15)

When testing password strength, which of the following is the BEST method for brute forcing passwords?

- A. Conduct an offline attack on the hashed password information.
- B. Conduct an online password attack until the account being used is locked.
- C. Use a comprehensive list of words to attempt to guess the password.
- D. Use social engineering methods to attempt to obtain the password.

Answer: C

NEW QUESTION 124

- (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 128

- (Exam Topic 15)

Information Security Continuous Monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management

decisions. Which of the following is the FIRST step in developing an ISCM strategy and implementing an ISCM program?

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

Answer: A

NEW QUESTION 132

- (Exam Topic 15)

Which of the following goals represents a modern shift in risk management according to National Institute of Standards and Technology (NIST)?

- A. Focus on operating environments that are changing, evolving, and full of emerging threats.
- B. Secure information technology (IT) systems that store, process, or transmit organizational information.
- C. Enable management to make well-informed risk-based decisions justifying security expenditure.
- D. Provide an improved mission accomplishment approach.

Answer: C

NEW QUESTION 134

- (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 information and 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 138

- (Exam Topic 15)

Which of the following is an open standard for exchanging authentication and authorization data between parties?

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

Answer: D

NEW QUESTION 140

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 142

- (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 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 144

- (Exam Topic 15)

A security professional should ensure that clients support which secondary algorithm for digital signatures when a Secure Multipurpose Internet Mail Extension (S/MIME) is used?

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

Answer: C

NEW QUESTION 149

- (Exam Topic 15)

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

Answer: D

NEW QUESTION 153

- (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 158

- (Exam Topic 15)

The existence of physical barriers, card and personal identification number (PIN) access systems, cameras, alarms, and security guards BEST describes this security approach?

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

Answer: B

NEW QUESTION 159

- (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 162

- (Exam Topic 15)

Which of the following is the BEST way to determine the success of a patch management process?

- A. Analysis and impact assessment
- B. Auditing and assessment
- C. Configuration management (CM)
- D. Change management

Answer: A

NEW QUESTION 164

- (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 171

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 172

- (Exam Topic 15)

Which of the following Disaster recovery (DR) testing processes is LEAST likely to disrupt normal business operations?

- A. Parallel
- B. Simulation
- C. Table-top

D. Cut-over

Answer: C

NEW QUESTION 177

- (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 179

- (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 181

- (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 185

- (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 187

- (Exam Topic 15)

An organization is trying to secure instant messaging (IM) communications through its network perimeter. Which of the following is the MOST significant challenge?

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

Answer: B

NEW QUESTION 192

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 197

- (Exam Topic 15)

What is the MOST important goal of conducting security assessments?

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

Answer: B

NEW QUESTION 201

- (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 202

- (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 203

- (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 206

- (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 209

- (Exam Topic 15)

Management has decided that a core application will be used on personal cellular phones. As an implementation requirement, regularly scheduled analysis of the security posture needs to be conducted. Management has also directed that continuous monitoring be implemented. Which of the following is required to accomplish management's directive?

- A. Strict integration of application management, configuration management (CM), and phone management
- B. Management application installed on user phones that tracks all application events and cellular traffic
- C. Enterprise-level security information and event management (SIEM) dashboard that provides full visibility of cellular phone activity
- D. Routine reports generated by the user's cellular phone provider that detail security events

Answer: B

NEW QUESTION 210

- (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 215

- (Exam Topic 15)

In setting expectations when reviewing the results of a security test, which of the following statements is MOST important to convey to reviewers?

- A. The target's security posture cannot be further compromised.
- B. The results of the tests represent a point-in-time assessment of the target(s).
- C. The accuracy of testing results can be greatly improved if the target(s) are properly hardened.
- D. The deficiencies identified can be corrected immediately

Answer: C

NEW QUESTION 217

- (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 222

- (Exam Topic 15)

Which of the following is the PRIMARY issue when analyzing detailed log information?

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

Answer: D

NEW QUESTION 223

- (Exam Topic 15)

Which of the following describes the order in which a digital forensic process is usually conducted?

- A. Ascertain legal authority, agree upon examination strategy, conduct examination, and report results
- B. Ascertain legal authority, conduct investigation, report results, and agree upon examination strategy
- C. Agree upon examination strategy, ascertain legal authority, conduct examination, and report results
- D. Agree upon examination strategy, ascertain legal authority, report results, and conduct examination

Answer: A

NEW QUESTION 228

- (Exam Topic 15)

Which of the following outsourcing agreement provisions has the HIGHEST priority from a security operations perspective?

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

Answer: D

NEW QUESTION 229

- (Exam Topic 15)

A Chief Information Security Officer (CISO) of a firm which decided to migrate to cloud has been tasked with ensuring an optimal level of security. Which of the following would be the FIRST consideration?

- A. Define the cloud migration roadmap and set out which applications and data repositories should be moved into the cloud.
- B. Ensure that the contract between the cloud vendor and the firm clearly defines responsibilities for operating security controls.
- C. Analyze the firm's applications and data repositories to determine the relevant control requirements.
- D. Request a security risk assessment of the cloud vendor be completed by an independent third-party.

Answer: A

NEW QUESTION 231

- (Exam Topic 15)

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

- A. Mowing users access to files based on their group membership

- B. Allowing users access to files based on username
- C. Allowing users access to files based on the users location at time of access
- D. Allowing users access to files based on the file type

Answer: A

NEW QUESTION 235

- (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 237

- (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 238

- (Exam Topic 15)

An attack utilizing social engineering and a malicious Uniform Resource Locator (URL) link to take advantage of a victim's existing browser session with a web application is an example of which of the following types of attack?

- A. Cross-Site Scripting (XSS)
- B. Cross-site request forgery (CSRF)
- C. Injection
- D. Click jacking

Answer: B

NEW QUESTION 241

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 243

- (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 244

- (Exam Topic 15)

What are the essential elements of a Risk Assessment Report (RAR)?

- A. Table of contents, testing criteria, and index
- B. Table of contents, chapters, and executive summary
- C. Executive summary, graph of risks, and process

D. Executive summary, body of the report, and appendices

Answer: D

NEW QUESTION 249

- (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 250

- (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 251

- (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 256

- (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 257

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 262

- (Exam Topic 15)

A network security engineer needs to ensure that a security solution analyzes traffic for protocol manipulation and various sorts of common attacks. In addition, all Uniform Resource Locator (URL) traffic must be inspected and users prevented from browsing inappropriate websites. Which of the following solutions should be implemented to enable administrators the capability to analyze traffic, blacklist external sites, and log user traffic for later analysis?

- A. Intrusion detection system (IDS)
- B. Circuit-Level Proxy
- C. Application-Level Proxy
- D. Host-based Firewall

Answer: B

NEW QUESTION 266

- (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 267

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

Answer: B

NEW QUESTION 268

- (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 273

- (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 277

- (Exam Topic 15)

Which of the following BEST describes the purpose of the reference monitor when defining access control to enforce the security model?

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

Answer: B

NEW QUESTION 280

- (Exam Topic 15)

What requirement MUST be met during internal security audits to ensure that all information provided is expressed as an objective assessment without risk of retaliation?

- A. The auditor must be independent and report directly to the management.
- B. The auditor must utilize automated tools to back their findings.
- C. The auditor must work closely with both the information Technology (IT) and security sections of an organization.
- D. The auditor must perform manual reviews of systems and processes.

Answer: A

NEW QUESTION 283

- (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 284

- (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 289

- (Exam Topic 15)

According to the (ISC)? ethics canon "act honorably, honestly, justly, responsibly, and legally," which order should be used when resolving conflicts?

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

Answer: A

NEW QUESTION 292

- (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 297

- (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 302

- (Exam Topic 15)

A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

- A. OTDR
- B. Tone generator
- C. Fusion splicer
- D. Cable tester
- E. PoE injector

Answer: A

NEW QUESTION 305

- (Exam Topic 15)

Which of the following BEST describes the purpose of software forensics?

- A. To perform cyclic redundancy check (CRC) verification and detect changed applications
- B. To review program code to determine the existence of backdoors
- C. To analyze possible malicious intent of malware
- D. To determine the author and behavior of the code

Answer: D

NEW QUESTION 306

- (Exam Topic 15)

Which of the following types of datacenter architectures will MOST likely be used in a large SDN and can be extended beyond the datacenter?

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

Answer: B

NEW QUESTION 307

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 310

- (Exam Topic 15)

A hospital enforces the Code of Fair Information Practices. What practice applies to a patient requesting their medical records from a web portal?

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

Answer: D

NEW QUESTION 315

- (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 316

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 321

- (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 323

- (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 324

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 326

- (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 329

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 334

- (Exam Topic 15)

Which of the following factors is a 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 338

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 339

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 343

- (Exam Topic 15)

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

- A. Drill through the device and platters.
- B. Mechanically shred the entire HDD.
- C. Remove the control electronics.

D. HP iProcess the HDD through a degaussing device.

Answer: D

NEW QUESTION 344

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 348

- (Exam Topic 15)

An organization wants to share data securely with their partners via the Internet. Which standard port is typically used to meet this requirement?

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

Answer: C

NEW QUESTION 351

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 353

- (Exam Topic 15)

What action should be taken by a business line that is unwilling to accept the residual risk in a system after implementing compensating controls?

- A. Notify the audit committee of the situation.
- B. Purchase insurance to cover the residual risk.
- C. Implement operational safeguards.
- D. Find another business line willing to accept the residual risk.

Answer: B

NEW QUESTION 357

- (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 360

- (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 361

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 362

- (Exam Topic 15)

The security organization is looking for a solution that could help them determine with a strong level of confidence that attackers have breached their network. Which solution is MOST effective at discovering a successful network breach?

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

Answer: A

NEW QUESTION 365

- (Exam Topic 15)

A malicious user gains access to unprotected directories on a web server. Which of the following is MOST likely the cause for this information disclosure?

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

Answer: A

NEW QUESTION 367

- (Exam Topic 15)

In Identity Management (IdM), when is the verification stage performed?

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

Answer: A

NEW QUESTION 368

- (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 369

- (Exam Topic 15)

A software development company found odd behavior in some recently developed software, creating a need for a more thorough code review. What is the MOST effective argument for a more thorough code review?

- A. It will increase flexibility of the applications developed.
- B. It will increase accountability with the customers.
- C. It will impede the development process.
- D. It will reduce the potential for vulnerabilities.

Answer: D

NEW QUESTION 370

- (Exam Topic 15)

When auditing the Software Development Life Cycle (SDLC) which of the following is one of the high-level audit phases?

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

Answer: B

NEW QUESTION 375

- (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 380

- (Exam Topic 15)

Which of the following is the MOST important first step in preparing for a security audit?

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

Answer: B

NEW QUESTION 382

- (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 386

- (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 389

- (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 394

- (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 397

- (Exam Topic 15)

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

- A. The actual origin and tools used for the test can be hidden.

- B. Information may be found on related breaches and hacking.
- C. Vulnerabilities can be tested without impact on the tested environment.
- D. Information may be found on hidden vendor patches.

Answer: D

NEW QUESTION 400

- (Exam Topic 15)

A company needs to provide shared access of sensitive data on a cloud storage to external business partners. Which of the following identity models is the BEST to blind identity providers (IdP) and relying parties (RP) so that subscriber lists of other parties are not disclosed?

- A. Federation authorities
- B. Proxied federation
- C. Static registration
- D. Dynamic registration

Answer: D

NEW QUESTION 403

- (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 405

- (Exam Topic 15)

What are the first two components of logical access control?

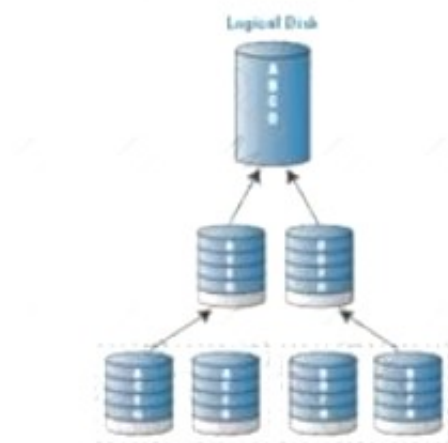
- A. Confidentiality and authentication
- B. Authentication and identification
- C. Identification and confidentiality
- D. Authentication and availability

Answer: B

NEW QUESTION 406

- (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 410

- (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 412

- (Exam Topic 15)

What is the PRIMARY purpose of creating and reporting metrics for a security awareness, training, and education program?

- A. Make all stakeholders aware of the program's progress.
- B. Measure the effect of the program on the organization's workforce.
- C. Facilitate supervision of periodic training events.
- D. Comply with legal regulations and document due diligence in security practices.

Answer: C

NEW QUESTION 414

- (Exam Topic 15)

Which of the following is considered the PRIMARY security issue associated with encrypted e-mail messages?

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

Answer: C

NEW QUESTION 415

- (Exam Topic 15)

Secure coding can be developed by applying which one of the following?

- A. Applying the organization's acceptable use guidance
- B. Applying the industry best practice coding guidelines
- C. Applying rapid application development (RAD) coding
- D. Applying the organization's web application firewall (WAF) policy

Answer: B

NEW QUESTION 419

- (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 424

- (Exam Topic 15)

What term is commonly used to describe hardware and software assets that are stored in a configuration management database (CMDB)?

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

Answer: D

NEW QUESTION 425

- (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 429

- (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 432

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 434

- (Exam Topic 15)

A user's credential for an application is stored in a relational database. Which control protects the confidentiality of the credential while it is stored?

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

Answer: C

NEW QUESTION 438

- (Exam Topic 15)

If traveling abroad and a customs official demands to examine a personal computer, which of the following should be assumed?

- A. The hard drive has been stolen.
- B. The Internet Protocol (IP) address has been copied.
- C. The hard drive has been copied.
- D. The Media Access Control (MAC) address was stolen

Answer: C

NEW QUESTION 442

- (Exam Topic 15)

While dealing with the consequences of a security incident, which of the following security controls are MOST appropriate?

- A. Detective and recovery controls
- B. Corrective and recovery controls
- C. Preventative and corrective controls
- D. Recovery and proactive controls

Answer: C

NEW QUESTION 447

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 450

- (Exam Topic 15)

An Internet media company produces and broadcasts highly popular television shows. The company is suffering a huge revenue loss due to piracy. What technique should be used to track the distribution of content?

- A. Install the latest data loss prevention (DLP) software at every server used to distribute content.
- B. Log user access to server
- C. Every day those log records are going to be audited by a team of specialized investigators.
- D. Hire several investigators to identify sources of pirated content and report people sharing the content.
- E. Use watermarking to hide a signature into the digital media such that it can be used to find who is using the company's content.

Answer: D

NEW QUESTION 454

- (Exam Topic 15)

Assuming an individual has taken all of the steps to keep their internet connection private, which of the following is the BEST to browse the web privately?

- A. Prevent information about browsing activities from being stored in the cloud.

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

Answer: A

NEW QUESTION 457

- (Exam Topic 15)

What is considered a compensating control for not having electrical surge protectors installed?

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

Answer: D

NEW QUESTION 462

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 464

- (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 467

- (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 log generation.

Answer: B

NEW QUESTION 468

- (Exam Topic 15)

A web developer is completing a new web application security checklist before releasing the application to production. The task of disabling unnecessary services is on the checklist. Which web application threat is being mitigated by this action?

- A. Security misconfiguration
- B. Sensitive data exposure
- C. Broken access control
- D. Session hijacking

Answer: B

NEW QUESTION 473

- (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 Zone (DMZ) 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 478

- (Exam Topic 15)

A cloud service provider requires its customer organizations to enable maximum audit logging for its data storage service and to retain the logs for the period of three months. The audit logging generates extremely high amount of logs. What is the MOST appropriate strategy for the log retention?

- A. Keep last week's logs in an online storage and the rest in a near-line storage.
- B. Keep all logs in an online storage.
- C. Keep all logs in an offline storage.
- D. Keep last week's logs in an online storage and the rest in an offline storage.

Answer: D

NEW QUESTION 479

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 484

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 486

- (Exam Topic 15)

An organization with divisions in the United States (US) and the United Kingdom (UK) processes data comprised of personal information belonging to subjects living in the European Union (EU) and in the US. Which data MUST be handled according to the privacy protections of General Data Protection Regulation (GDPR)?

- A. Only the EU citizens' data
- B. Only the EU residents' data
- C. Only the UK citizens' data
- D. Only data processed in the UK

Answer: A

NEW QUESTION 491

- (Exam Topic 15)

What is the PRIMARY objective of the post-incident phase of the incident response process in the security operations center (SOC)?

- A. improve the IR process.
- B. Communicate the IR details to the stakeholders.
- C. Validate the integrity of the IR.
- D. Finalize the IR.

Answer: A

NEW QUESTION 495

- (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 497

- (Exam Topic 15)

In a quarterly system access review, an active privileged account was discovered that did not exist in the prior review on the production system. The account was created one hour after the previous access review. Which of the following is the BEST option to reduce overall risk in addition to quarterly access reviews?

- A. Increase logging levels.
- B. Implement bi-annual reviews.

- C. Create policies for system access.
- D. Implement and review risk-based alerts.

Answer: D

NEW QUESTION 499

- (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 501

- (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. Grant 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 is hired.
- D. Prevent changes to the confidential data until a replacement application owner is hired.

Answer: B

NEW QUESTION 502

- (Exam Topic 15)

A company needs to provide employee access to travel services, which are hosted by a third-party service provider. Employee experience is important, and when users are already authenticated, access to the travel portal is seamless. Which of the following methods is used to share information and grant user access to the travel portal?

- A. Security Assertion Markup Language (SAML) access
- B. Single sign-on (SSO) access
- C. Open Authorization (OAuth) access
- D. Federated access

Answer: D

NEW QUESTION 506

- (Exam Topic 15)

employee training, risk management, and data handling procedures and policies could be characterized as which type of security measure?

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

Answer: D

NEW QUESTION 510

- (Exam Topic 15)

Which of the following is the MOST secure protocol for remote command access to the firewall?

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

Answer: A

NEW QUESTION 514

- (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 517

- (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 518

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 519

- (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 523

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 528

- (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 529

- (Exam Topic 15)

Which of the following VPN configurations should be used to separate Internet and corporate traffic?

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

Answer: A

NEW QUESTION 533

- (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 535

- (Exam Topic 15)

An organization outgrew its internal data center and is evaluating third-party hosting facilities. In this evaluation, which of the following is a PRIMARY factor for selection?

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

Answer: C

NEW QUESTION 539

- (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 541

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 544

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 546

- (Exam Topic 15)

What is the HIGHEST priority in agile development?

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

Answer: C

NEW QUESTION 548

- (Exam Topic 15)

During testing, where are the requirements to inform parent organizations, law enforcement, and a computer incident response team documented?

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

Answer: D

NEW QUESTION 553

- (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 558

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 560

- (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 561

- (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 564

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 568

- (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 569

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 573

- (Exam Topic 15)

Which of the following is a canon of the (ISC)2 Code of Ethics?

- A. Integrity first, association before self, 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 575

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 577

- (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 578

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 579

- (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 580

- (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 582

- (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 586

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 588

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 590

- (Exam Topic 15)

Which of the following BEST describes botnets?

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

Answer: D

NEW QUESTION 594

- (Exam Topic 15)

Which of the following is the BEST method to validate secure coding techniques against injection and overflow attacks?

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

Answer: B

NEW QUESTION 597

- (Exam Topic 15)

Which of the following is the MAIN benefit of off-site storage?

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

Answer: A

NEW QUESTION 602

- (Exam Topic 14)

Which of the following is the MOST important consideration that must be taken into account when deploying an enterprise patching solution that includes mobile devices?

- A. Service provider(s) utilized by the organization
- B. Whether it will impact personal use
- C. Number of mobile users in the organization
- D. Feasibility of downloads due to available bandwidth

Answer: C

NEW QUESTION 606

- (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 607

- (Exam Topic 14)

Which of the following entails identification of data end links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

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

Answer: A

NEW QUESTION 612

- (Exam Topic 14)

What should an auditor do when conducting a periodic audit on media retention?

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

Answer: A

NEW QUESTION 616

- (Exam Topic 14)

Which of the following is TRUE regarding equivalence class testing?

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

Answer: C

NEW QUESTION 618

- (Exam Topic 14)

Which of the following is used to support the concept of defense in depth during the development phase of a software product?

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

Answer: B

NEW QUESTION 620

- (Exam Topic 14)

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

- A. Size, nature, and complexity of the organization
- B. Business needs of the security organization
- C. All possible risks
- D. Adaptation model for future recovery planning

Answer: B

NEW QUESTION 625

- (Exam Topic 14)

An organization is considering outsourcing applications and data to a Cloud Service Provider (CSP). Which of the following is the MOST important concern regarding privacy?

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

Answer: D

NEW QUESTION 629

- (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 630

- (Exam Topic 14)

Which of the following techniques is effective to detect taps in fiber optic cables?

- A. Taking baseline signal level of the cable
- B. Measuring signal through external oscillator solution devices
- C. Outlining electromagnetic field strength
- D. Performing network vulnerability scanning

Answer: B

NEW QUESTION 633

- (Exam Topic 14)

Which of the following is a characteristic of the independent testing of a program?

- A. Independent testing increases the likelihood that a test will expose the effect of a hidden feature.
- B. Independent testing decreases the likelihood that a test will expose the effect of a hidden feature.
- C. Independent testing teams help decrease the cost of creating test data and system design specification.
- D. Independent testing teams help identify functional requirements and Service Level Agreements (SLA)

Answer: A

NEW QUESTION 637

- (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 640

- (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 645

- (Exam Topic 14)

The Secure Shell (SSH) version 2 protocol supports.

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

Answer: D

NEW QUESTION 649

- (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 650

- (Exam Topic 14)

Which of the following is a MAJOR concern when there is a need to preserve or retain information for future retrieval?

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

Answer: C

NEW QUESTION 654

- (Exam Topic 14)

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

Answer: D

NEW QUESTION 657

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 662

- (Exam Topic 14)

Which of the following is a method of attacking internet (IP) v6 Layer 3 and Layer 4 ?

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

Answer: A

NEW QUESTION 667

- (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 672

- (Exam Topic 14)

Which of the following four iterative steps are conducted on third-party vendors in an on-going basis?

- A. Investigate, Evaluate, Respond, Monitor
- B. Frame, Assess, Respond, Monitor
- C. Frame, Assess, Remediate, Monitor
- D. Investigate, Assess, Remediate, Monitor

Answer: C

NEW QUESTION 677

- (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 679

- (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 683

- (Exam Topic 14)

Which of the following is used to detect steganography?

- A. Audio analysis
- B. Statistical analysis
- C. Reverse engineering
- D. Cryptanalysis

Answer: C

NEW QUESTION 685

- (Exam Topic 14)

Which of the following practices provides the development team with a definition of security and identification of threats in designing software?

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

Answer: C

NEW QUESTION 690

- (Exam Topic 14)

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

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

Answer: A

Explanation:

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

NEW QUESTION 691

- (Exam Topic 14)

When should an application invoke re-authentication in addition to initial user authentication?

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

Answer: C

NEW QUESTION 696

- (Exam Topic 14)

A criminal organization is planning an attack on a government network. Which of the following is the MOST severe attack to the network availability?

- A. Network management communications is disrupted by attacker
- B. Operator loses control of network devices to attacker
- C. Sensitive information is gathered on the network topology by attacker
- D. Network is flooded with communication traffic by attacker

Answer: B

NEW QUESTION 698

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 703

- (Exam Topic 14)

Which of the following is held accountable for the risk to organizational systems and data that result from outsourcing Information Technology (IT) systems and services?

- A. The acquiring organization
- B. The service provider
- C. The risk executive (function)
- D. The IT manager

Answer: C

NEW QUESTION 704

- (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 705

- (Exam Topic 14)

When selecting a disk encryption technology, which of the following MUST also be assured to be encrypted?

- A. Master Boot Record (MBR)
- B. Pre-boot environment
- C. Basic Input Output System (BIOS)
- D. Hibernation file

Answer: A

NEW QUESTION 706

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 708

- (Exam Topic 14)

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

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

Answer: B

Explanation:

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

NEW QUESTION 712

- (Exam Topic 14)

What is the BEST approach for maintaining ethics when a security professional is unfamiliar with the culture of a country and is asked to perform a questionable task?

- A. Exercise due diligence when deciding to circumvent host government requests.

- B. Become familiar with the means in which the code of ethics is applied and considered.
- C. Complete the assignment based on the customer's wishes.
- D. Execute according to the professional's comfort level with the code of ethics.

Answer: B

NEW QUESTION 713

- (Exam Topic 14)

Which of the following MUST a security professional do in order to quantify the value of a security program to organization management?

- A. Report using metrics.
- B. Rank priorities as high, medium, or low.
- C. Communicate compliance obstacles.
- D. Report on employee activities

Answer: A

NEW QUESTION 715

- (Exam Topic 14)

Who determines the required level of independence for security control Assessors (SCA)?

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

Answer: B

NEW QUESTION 716

- (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 720

- (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 723

- (Exam Topic 14)

Which layer handle packet fragmentation and reassembly in the Open system interconnection (OSI) Reference model?

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

Answer: B

NEW QUESTION 726

- (Exam Topic 14)

What is the MOST effective way to protect privacy?

- A. Eliminate or reduce collection of personal information.
- B. Encrypt all collected personal information.
- C. Classify all personal information at the highest information classification level.
- D. Apply tokenization to all personal information records.

Answer: D

NEW QUESTION 729

- (Exam Topic 14)

A financial company has decided to move its main business application to the Cloud. The legal department objects, arguing that the move of the platform should

comply with several regulatory obligations such as the General Data Protection (GDPR) and ensure data confidentiality. The Chief Information Security Officer (CISO) says that the cloud provider has met all regulations requirements and even provides its own encryption solution with internally-managed encryption keys to address data confidentiality. Did the CISO address all the legal requirements in this situation?

- A. No, because the encryption solution is internal to the cloud provider.
- B. Yes, because the cloud provider meets all regulations requirements.
- C. Yes, because the cloud provider is GDPR compliant.
- D. No, because the cloud provider is not certified to host government data.

Answer: B

NEW QUESTION 734

- (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 737

- (Exam Topic 14)

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

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

Answer: C

Explanation:

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

NEW QUESTION 739

- (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 743

- (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 746

- (Exam Topic 14)

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

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

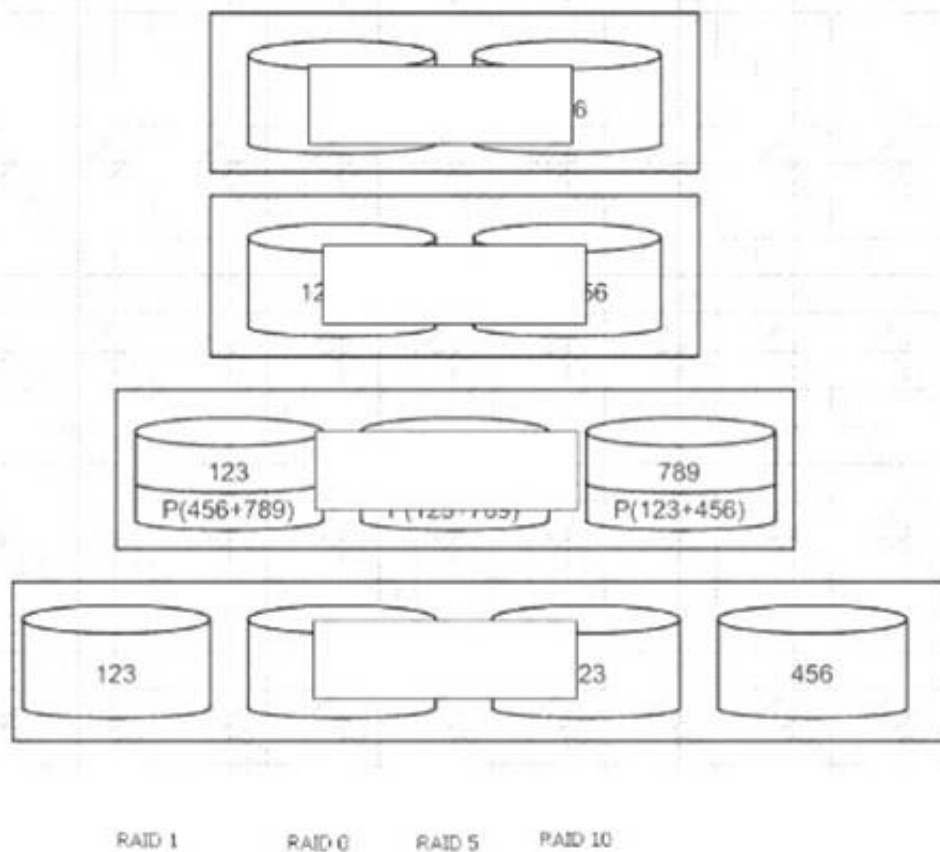
Answer: D

NEW QUESTION 748

- (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.

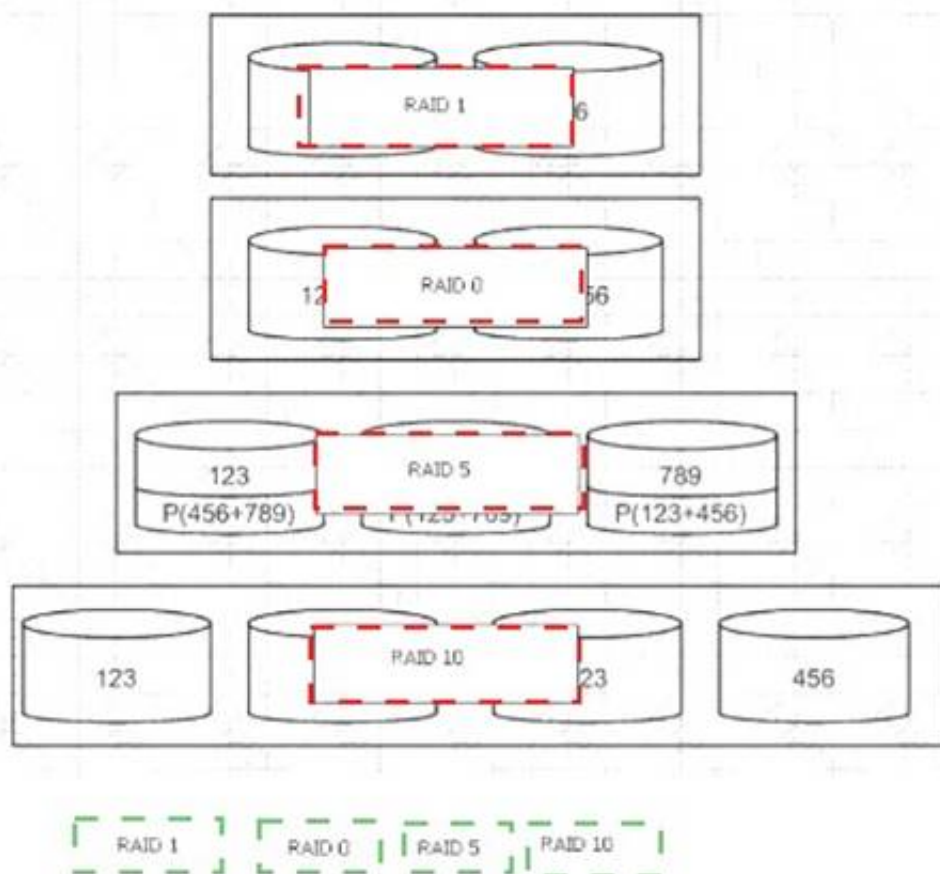
Drag each level to the appropriate place on the diagram.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 753

- (Exam Topic 14)

If virus infection is suspected, which of the following is the FIRST step for the user to take?

- A. Unplug the computer from the network.
- B. Save the opened files and shutdown the computer.
- C. Report the incident to service desk.
- D. Update the antivirus to the latest version.

Answer: C

NEW QUESTION 757

- (Exam Topic 14)

A vehicle of a private courier company that transports backup data for offsite storage was robbed while in transport backup data for offsite was robbed while in transit. The incident management team is now responsible to estimate the robbery, which of the following would help the incident management team to MOST effectively analyze the business impact of the robbery?

- A. Log of backup administrative actions
- B. Log of the transported media and its classification marking

- C. Log of the transported media and its detailed contents
- D. Log of backed up data and their respective data custodians

Answer: B

NEW QUESTION 761

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 764

- (Exam Topic 14)

What are the roles within a scrum methodology?

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

Answer: B

NEW QUESTION 765

- (Exam Topic 14)

Which of the following is MOST critical in a contract for data disposal on a hard drive with a third party?

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

Answer: C

NEW QUESTION 770

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 774

- (Exam Topic 14)

Digital certificates used transport layer security (TLS) support which of the following?

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

Answer: A

NEW QUESTION 779

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISSP Exam with Our Prep Materials Via below:

<https://www.certleader.com/CISSP-dumps.html>