

## Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

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



#### 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)

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

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

**Answer: D**

#### NEW QUESTION 3

- (Exam Topic 15)

In addition to life, protection of which of the following elements is MOST important when planning a data center site?

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

**Answer: D**

#### NEW QUESTION 4

- (Exam Topic 15)

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

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

**Answer: B**

#### NEW QUESTION 5

- (Exam Topic 15)

Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site. Which of the following will BEST provide this functionality?

- A. Client-to-site VPN
- B. Third-party VPN service
- C. Site-to-site VPN
- D. Split-tunnel VPN

**Answer: C**

#### NEW QUESTION 6

- (Exam Topic 15)

An organization is planning a penetration test that simulates the malicious actions of a former network administrator. What kind of penetration test is needed?

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

**Answer: C**

#### NEW QUESTION 7

- (Exam Topic 15)

Which of the following virtual network configuration options is BEST to protect virtual machines (VM)?

- A. Traffic filtering
- B. Data encryption

- C. Data segmentation
- D. Traffic throttling

**Answer:** D

#### NEW QUESTION 8

- (Exam Topic 15)

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

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

**Answer:** B

#### NEW QUESTION 9

- (Exam Topic 15)

A database server for a financial application is scheduled for production deployment. Which of the following controls will BEST prevent tampering?

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

**Answer:** B

#### NEW QUESTION 10

- (Exam Topic 15)

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

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

**Answer:** A

#### NEW QUESTION 10

- (Exam Topic 15)

Which of the following 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 14

- (Exam Topic 15)

Which of the following access control models is MOST restrictive?

- A. Discretionary Access Control (DAC)
- B. Mandatory Access Control (MAC)
- C. Role Based Access Control (RBAC)
- D. Rule based access control

**Answer:** B

#### NEW QUESTION 19

- (Exam Topic 15)

Which of the following is established to collect information Se eee ee ee nation readily available in part through implemented security controls?

- A. Security Assessment Report (SAR)
- B. Organizational risk tolerance
- C. Information Security Continuous Monitoring (ISCM)
- D. Risk assessment report

**Answer:** D

#### NEW QUESTION 22

- (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 25

- (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 29

- (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 33

- (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 35

- (Exam Topic 15)

A cybersecurity engineer has been tasked to research and implement an ultra-secure communications channel to protect the organization's most valuable intellectual property (IP). The primary directive in this initiative is to ensure there is no possible way the communications can be intercepted without detection.

Which of the following is the only way to ensure this 'outcome'?

- A. Diffie-Hellman key exchange
- B. Symmetric key cryptography
- C. [Public key infrastructure (PKI)
- D. Quantum Key Distribution

**Answer:** C

#### NEW QUESTION 36

- (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 37

- (Exam Topic 15)

During a penetration test, what are the three PRIMARY objectives of the planning phase?

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

**Answer:** D

**NEW QUESTION 38**

- (Exam Topic 15)

An international trading organization that holds an International Organization for Standardization (ISO) 27001 certification is seeking to outsource their security monitoring to a managed security service provider (MSSP). The trading organization's security officer is tasked with drafting the requirements that need to be included in the outsourcing contract.

Which of the following **MUST** be included in the contract?

- A. A detailed overview of all equipment involved in the outsourcing contract
- B. The MSSP having an executive manager responsible for information security
- C. The right to perform security compliance tests on the MSSP's equipment
- D. The right to audit the MSSP's security process

**Answer:** C

**NEW QUESTION 43**

- (Exam Topic 15)

Which of the following ensures old log data is not overwritten?

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

**Answer:** D

**NEW QUESTION 45**

- (Exam Topic 15)

Which of the following is the strongest physical access control?

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

**Answer:** D

**NEW QUESTION 46**

- (Exam Topic 15)

What type of database attack would allow a customer service employee to determine quarterly sales results before they are publically announced?

- A. Polyinstantiation
- B. Inference
- C. Aggregation
- D. Data mining

**Answer:** A

**NEW QUESTION 50**

- (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 53**

- (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 55**

- (Exam Topic 15)

Which of the following is the BEST method to identify security controls that should be implemented for a web-based application while in development?

- A. Application threat modeling
- B. Secure software development.
- C. Agile software development
- D. Penetration testing

**Answer:** A

#### NEW QUESTION 60

- (Exam Topic 15)

An organization needs a general purpose document to prove that its internal controls properly address security, availability, processing integrity, confidentiality or privacy risks. Which of the following reports is required?

- A. A Service Organization Control (SOC) 3 report
- B. The Statement on Standards for Attestation Engagements N
- C. 18 (SSAE 18)
- D. A Service Organization Control (SOC) 2 report
- E. The International Organization for Standardization (ISO) 27001

**Answer:** C

#### NEW QUESTION 61

- (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 64

- (Exam Topic 15)

Which of the following is performed to determine a measure of success of a security awareness training program designed to prevent social engineering attacks?

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

**Answer:** B

#### NEW QUESTION 66

- (Exam Topic 15)

Which of the following factors should be considered characteristics of Attribute Based Access Control (ABAC) in terms of the attributes used?

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

**Answer:** D

#### NEW QUESTION 68

- (Exam Topic 15)

An attacker is able to remain indefinitely logged into a exploiting to remain on the web service?

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

**Answer:** C

#### NEW QUESTION 69

- (Exam Topic 15)

Which of the following is the MOST effective preventative method to identify security flaws in software?

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



**Answer:** B

#### NEW QUESTION 71

- (Exam Topic 15)

Information security practitioners are in the midst of implementing a new firewall. Which of the following failure methods would BEST prioritize security in the event of failure?

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

**Answer:** A

#### NEW QUESTION 74

- (Exam Topic 15)

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

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

**Answer:** C

#### NEW QUESTION 79

- (Exam Topic 15)

Which of the following is the BEST way to protect against Structured Query language (SQL) injection?

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

**Answer:** D

#### NEW QUESTION 80

- (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 84

- (Exam Topic 15)

Which of the following uses the destination IP address to forward packets?

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

**Answer:** C

#### NEW QUESTION 89

- (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 90

- (Exam Topic 15)

Which of the following security objectives for industrial control systems (ICS) can be adapted to securing any Internet of Things (IoT) system?

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

**Answer:** D

#### NEW QUESTION 94

- (Exam Topic 15)

Why is data classification control important to an organization?

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

**Answer:** A

#### NEW QUESTION 98

- (Exam Topic 15)

What level of Redundant Array of Independent Disks (RAID) is configured PRIMARILY for high-performance data reads and writes?

- A. RAID-0
- B. RAID-1
- C. RAID-5
- D. RAID-6

**Answer:** A

#### NEW QUESTION 100

- (Exam Topic 15)

Which of the following MUST the administrator of a security information and event management (SIEM) system ensure?

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

**Answer:** C

#### NEW QUESTION 102

- (Exam Topic 15)

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

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

**Answer:** C

#### NEW QUESTION 103

- (Exam Topic 15)

Which audit type is MOST appropriate for evaluating the effectiveness of a security program?

- A. Threat
- B. Assessment
- C. Analysis
- D. Validation

**Answer:** B

#### NEW QUESTION 106

- (Exam Topic 15)

Which of the following BEST describes the objectives of the Business Impact Analysis (BIA)?

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



**Answer:** B

**NEW QUESTION 109**

- (Exam Topic 15)

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

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

**Answer:** B

**NEW QUESTION 113**

- (Exam Topic 15)

A security practitioner needs to implementation 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 116**

- (Exam Topic 15)

What type of investigation applies when malicious behavior is suspected between two organizations?

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

**Answer:** A

**NEW QUESTION 119**

- (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 124**

- (Exam Topic 15)

Physical Access Control Systems (PACS) allow authorized security personnel to manage and monitor access control for subjects through which function?

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

**Answer:** B

**NEW QUESTION 127**

- (Exam Topic 15)

Which of the following is a term used to describe maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions?

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

**Answer:** D

**NEW QUESTION 131**

- (Exam Topic 15)

What is the BEST control to be implemented at a login page in a web application to mitigate the ability to enumerate users?

- A. Implement a generic response for a failed login attempt.

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

**Answer:** A

#### NEW QUESTION 136

- (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 141

- (Exam Topic 15)

The disaster recovery (DR) process should always include

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

**Answer:** A

#### NEW QUESTION 144

- (Exam Topic 15)

Which of the following is security control volatility?

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

**Answer:** D

#### NEW QUESTION 145

- (Exam Topic 15)

In supervisory control and data acquisition (SCADA) systems, which of the following controls can be used to reduce device exposure to malware?

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

**Answer:** B

#### NEW QUESTION 146

- (Exam Topic 15)

Spyware is BEST described as

- A. data mining for advertising.
- B. a form of cyber-terrorism,
- C. an information gathering technique,
- D. a web-based attack.

**Answer:** B

#### NEW QUESTION 150

- (Exam Topic 15)

What is the correct order of execution for security architecture?

- A. Governance, strategy and program management, project delivery, operations
- B. Strategy and program management, governance, project delivery, operations
- C. Governance, strategy and program management, operations, project delivery
- D. Strategy and program management, project delivery, governance, operations

**Answer:** A

#### NEW QUESTION 155

- (Exam Topic 15)

Which of the following is the MOST important rule for digital investigations?

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

**Answer:** C

#### NEW QUESTION 156

- (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 158

- (Exam Topic 15)

A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

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

**Answer:** A

#### NEW QUESTION 160

- (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 165

- (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 167

- (Exam Topic 15)

Which of the following addresses requirements of security assessment during software acquisition?

- A. Software assurance policy
- B. Continuous monitoring
- C. Software configuration management (SCM)
- D. Data loss prevention (DLP) policy

**Answer:** B

#### NEW QUESTION 168

- (Exam Topic 15)

An organization is setting a security assessment scope with the goal of developing a Security Management Program (SMP). The next step is to select an approach for conducting the risk assessment. Which of the following approaches is MOST effective for the SMP?

- A. Data driven risk assessment with a focus on data
- B. Security controls driven assessment that focuses on controls management
- C. Business processes based risk assessment with a focus on business goals
- D. Asset driven risk assessment with a focus on the assets

**Answer:** A

#### NEW QUESTION 170

- (Exam Topic 15)

A developer begins employment with an information technology (IT) organization. On the first day, the developer works through the list of assigned projects and finds that some files within those projects aren't accessible. Other developers working on the same project have no trouble locating and working on the. What is the MOST likely explanation for the discrepancy in access?

- A. The IT administrator had failed to grant the developer privileged access to the servers.
- B. The project files were inadvertently deleted.
- C. The new developer's computer had not been added to an access control list (ACL).
- D. The new developer's user account was not associated with the right roles needed for the projects.

**Answer:** A

#### NEW QUESTION 172

- (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 177

- (Exam Topic 15)

What is the MOST important criterion that needs to be adhered to during the data collection process of an active investigation?

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

**Answer:** A

#### NEW QUESTION 180

- (Exam Topic 15)

In which of the following system life cycle processes should security requirements be developed?

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

**Answer:** B

#### NEW QUESTION 184

- (Exam Topic 15)

What is the BEST way to restrict access to a file system on computing systems?

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

**Answer:** C

#### NEW QUESTION 188

- (Exam Topic 15)

Which of the following determines how traffic should flow based on the status of the infrastructure layer?

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

**Answer:** A

#### NEW QUESTION 192

- (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 respons
- E. It may be necessary to collect additional information to clarify or supplement existing monitoring data.

**Answer:** A

#### NEW QUESTION 197

- (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 202

- (Exam Topic 15)

Which of the following is the MOST comprehensive Business Continuity (BC) test?

- A. Full functional drill
- B. Full table top
- C. Full simulation
- D. Full interruption

**Answer:** C

#### NEW QUESTION 203

- (Exam Topic 15)

Which of the following BEST represents a defense in depth concept?

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

**Answer:** C

#### NEW QUESTION 207

- (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 208

- (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 210

- (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 214

- (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 215

- (Exam Topic 15)

Which of the following is a common risk with fiber optical communications, and what is the associated mitigation measure?

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

**Answer:** B

#### NEW QUESTION 219

- (Exam Topic 15)

Which of the following is the MOST appropriate control for asset data labeling procedures?

- A. Logging data media to provide a physical inventory control
- B. Reviewing audit trails of logging records
- C. Categorizing the types of media being used
- D. Reviewing off-site storage access controls

**Answer:** C

#### NEW QUESTION 223

- (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 224

- (Exam Topic 15)

Which of the following is the MOST secure password technique?

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

**Answer:** A

#### NEW QUESTION 227

- (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 229

- (Exam Topic 15)

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

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

**Answer:** C



#### NEW QUESTION 230

- (Exam Topic 15)

A colleague who recently left the organization asked a security professional for a copy of the organization's confidential incident management policy. Which of the following is the BEST response to this request?

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

**Answer: B**

#### NEW QUESTION 234

- (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 236

- (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 239

- (Exam Topic 15)

In systems security engineering, what does the security principle of modularity provide?

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

**Answer: A**

#### NEW QUESTION 242

- (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 247

- (Exam Topic 15)

When designing a business continuity plan (BCP), what is the formula to determine the Maximum Tolerable Downtime (MTD)?

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

**Answer: C**

#### NEW QUESTION 251

- (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 254**

- (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 256**

- (Exam Topic 15)

After the INITIAL input of a user identification (ID) and password, what is an authentication system that prompts the user for a different response each time the user logs on?

- A. Persons Identification Number (PIN)
- B. Secondary password
- C. Challenge response
- D. Voice authentication

**Answer:** C

**NEW QUESTION 257**

- (Exam Topic 15)

The personal laptop of an organization executive is stolen from the office, complete with personnel and project records. Which of the following should be done FIRST to mitigate future occurrences?

- A. Encrypt disks on personal laptops.
- B. Issue cable locks for use on personal laptops.
- C. Create policies addressing critical information on personal laptops.
- D. Monitor personal laptops for critical information.

**Answer:** A

**NEW QUESTION 260**

- (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 263**

- (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 266**

- (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 268**

- (Exam Topic 15)

A corporation does not have a formal data destruction policy. During which phase of a criminal legal proceeding will this have the MOST impact?

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

**Answer:** D

#### NEW QUESTION 273

- (Exam Topic 15)

Which of the following security tools monitors devices and records the information in a central database for further analysis?

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

**Answer:** A

#### NEW QUESTION 277

- (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 278

- (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 283

- (Exam Topic 15)

A developer is creating an application that requires secure logging of all user activity. What is the BEST permission the developer should assign to the log file to ensure requirements are met?

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

**Answer:** C

#### NEW QUESTION 284

- (Exam Topic 15)

Which of the following is the reason that transposition ciphers are easily recognizable?

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

**Answer:** B

#### NEW QUESTION 288

- (Exam Topic 15)

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

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

**Answer:** B

#### NEW QUESTION 293

- (Exam Topic 15)

What is the benefit of using Network Admission Control (NAC)?

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

**Answer:** C

#### NEW QUESTION 294

- (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 295

- (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 296

- (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 298

- (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 299

- (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 300

- (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 305

- (Exam Topic 15)

Which of the following would an information security professional use to recognize changes to content, particularly unauthorized changes?

A. File Integrity Checker

B. Security information and event management (SIEM) system

C. Audit Logs

D. Intrusion detection system (IDS)

**Answer:** A

#### NEW QUESTION 306

- (Exam Topic 15)

Which of the following measures serves as the BEST means for protecting data on computers, smartphones, and external storage devices when traveling to high-risk countries?

A. Review applicable destination country laws, forensically clean devices prior to travel, and only download sensitive data over a virtual private network (VPN) upon arriving at the destination.

B. Keep laptops, external storage devices, and smartphones in the hotel room when not in use.

C. Leverage a Secure Socket Layer (SSL) connection over a virtual private network (VPN) to download sensitive data upon arriving at the destination.

D. Use multi-factor authentication (MFA) to gain access to data stored on laptops or external storage devices and biometric fingerprint access control isms to unlock smartphones.

**Answer:** D

#### NEW QUESTION 307

- (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 308

- (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 312

- (Exam Topic 15)

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

A. Health Insurance Portability and Accountability Act (HIPAA)

B. Service Organization Control (SOC) 2

C. Payment Card Industry (PCI)

D. Information Assurance Technical Framework (IATF)

**Answer:** B

#### NEW QUESTION 316

- (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 319**

- (Exam Topic 15)

A company hired an external vendor to perform a penetration test of a new payroll system. The company's internal test team had already performed an in-depth application and security test of the system and determined that it met security requirements. However, the external vendor uncovered significant security weaknesses where sensitive personal data was being sent unencrypted to the tax processing systems. What is the MOST likely cause of the security issues?

- A. Failure to perform interface testing
- B. Failure to perform negative testing
- C. Inadequate performance testing
- D. Inadequate application level testing

**Answer:** A

**NEW QUESTION 324**

- (Exam Topic 15)

Which of the following events prompts a review of the disaster recovery plan (DRP)?

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

**Answer:** D

**NEW QUESTION 325**

- (Exam Topic 15)

Where can the Open Web Application Security Project (OWASP) list of associated vulnerabilities be found?

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

**Answer:** A

**NEW QUESTION 330**

- (Exam Topic 15)

Which of the following vulnerability assessment activities BEST exemplifies the Examine method of assessment?

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

**Answer:** D

**NEW QUESTION 335**

- (Exam Topic 15)

Which of the following is considered the FIRST step when designing an internal security control assessment?

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

**Answer:** D

**NEW QUESTION 339**

- (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 343**

- (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 344

- (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 347

- (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 348

- (Exam Topic 15)

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

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

**Answer:** B

#### NEW QUESTION 349

- (Exam Topic 15)

Which of the following types of hosts should be operating in the demilitarized zone (DMZ)?

- A. Hosts intended to provide limited access to public resources
- B. Database servers that can provide useful information to the public
- C. Hosts that store unimportant data such as demographical information
- D. File servers containing organizational data

**Answer:** A

#### NEW QUESTION 350

- (Exam Topic 15)

An organization's retail website provides its only source of revenue, so the disaster recovery plan (DRP) must document an estimated time for each step in the plan.

Which of the following steps in the DRP will list the GREATEST duration of time for the service to be fully operational?

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

**Answer:** B

#### NEW QUESTION 354

- (Exam Topic 15)

Upon commencement of an audit within an organization, which of the following actions is MOST important for the auditor(s) to take?

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

**Answer:** C

#### NEW QUESTION 355

- (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 357

- (Exam Topic 15)

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

- A. Jamming
- B. Man-in-the-Middle (MITM)
- C. War driving
- D. Internet Protocol (IP) spoofing

**Answer:** B

#### NEW QUESTION 362

- (Exam Topic 15)

Which of the following is a key responsibility for a data steward assigned to manage an enterprise data lake?

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

**Answer:** A

#### NEW QUESTION 367

- (Exam Topic 15)

In a disaster recovery (DR) test, which of the following would be a trait of crisis management?

- A. Wide focus
- B. Strategic
- C. Anticipate
- D. Process

**Answer:** D

#### NEW QUESTION 369

- (Exam Topic 15)

An access control list (ACL) on a router is a feature MOST similar to which type of firewall?

- A. Packet filtering firewall
- B. Application gateway firewall
- C. Heuristic firewall
- D. Stateful firewall

**Answer:** B

#### NEW QUESTION 370

- (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 375

- (Exam Topic 15)

Which of the (ISC)? Code of Ethics canons is MOST reflected when preserving the value of systems, applications, and entrusted information while avoiding conflicts of interest?

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

**Answer:** B

**NEW QUESTION 380**

- (Exam Topic 15)

Which of the following is a correct feature of a virtual local area network (VLAN)?

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

**Answer:** A

**NEW QUESTION 384**

- (Exam Topic 15)

Which of the following BEST describes why software assurance is critical in helping prevent an increase in business and mission risk for an organization?

- A. Software that does not perform as intended may be exploitable which makes it vulnerable to attack.
- B. Request for proposals (RFP) avoid purchasing software that does not meet business needs.
- C. Contracting processes eliminate liability for security vulnerabilities for the purchaser.
- D. Decommissioning of old software reduces long-term costs related to technical debt.

**Answer:** B

**NEW QUESTION 388**

- (Exam Topic 15)

Which of the following MUST be done before a digital forensics investigator may acquire digital evidence?

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

**Answer:** C

**NEW QUESTION 392**

- (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 395**

- (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 398**

- (Exam Topic 15)

Which of the following would be the BEST guideline to follow when attempting to avoid the exposure of sensitive data?

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

**Answer:** A

**NEW QUESTION 402**

- (Exam Topic 15)

During an internal audit of an organizational Information Security Management System (ISMS), nonconformities are identified. In which of the following management stages are nonconformities reviewed, assessed and/or corrected by the organization?

- A. Planning

- B. Operation
- C. Assessment
- D. Improvement

**Answer:** B

#### NEW QUESTION 405

- (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 408

- (Exam Topic 15)

When determining data and information asset handling, regardless of the specific toolset being used, which of the following is one of the common components of big data?

- A. Consolidated data collection
- B. Distributed storage locations
- C. Distributed data collection
- D. Centralized processing location

**Answer:** C

#### NEW QUESTION 411

- (Exam Topic 15)

A software developer wishes to write code that will execute safely and only as intended. Which of the following programming language types is MOST likely to achieve this goal?

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

**Answer:** D

#### NEW QUESTION 415

- (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 416

- (Exam Topic 15)

Which of the following attack types can be used to compromise the integrity of data during transmission?

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

**Answer:** B

#### NEW QUESTION 417

- (Exam Topic 15)

Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

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

**Answer:** C

#### NEW QUESTION 422

- (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 424

- (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 426

- (Exam Topic 15)

Which of the following statements is TRUE about Secure Shell (SSH)?

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

**Answer:** B

#### NEW QUESTION 428

- (Exam Topic 15)

How does security in a distributed file system using mutual authentication differ from file security in a multi-user host?

- A. Access control can rely on the Operating System (OS), but eavesdropping is
- B. Access control cannot rely on the Operating System (OS), and eavesdropping
- C. Access control can rely on the Operating System (OS), and eavesdropping is
- D. Access control cannot rely on the Operating System (OS), and eavesdropping

**Answer:** C

#### NEW QUESTION 432

- (Exam Topic 15)

Which of the following is included in the Global System for Mobile Communications (GSM) security framework?

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

**Answer:** C

#### NEW QUESTION 435

- (Exam Topic 15)

Digital non-repudiation requires which of the following?

- A. A trusted third-party
- B. Appropriate corporate policies
- C. Symmetric encryption
- D. Multifunction access cards

**Answer:** A

#### NEW QUESTION 439

- (Exam Topic 15)

Which of the following is the PRIMARY type of cryptography required to support non-repudiation of a digitally signed document?

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

**Answer:**

A

#### NEW QUESTION 440

- (Exam Topic 15)

Which of the following statements BEST describes least privilege principle in a cloud environment?

- A. Network segments remain private if unneeded to access the internet.
- B. Internet traffic is inspected for all incoming and outgoing packets.
- C. A single cloud administrator is configured to access core functions.
- D. Routing configurations are regularly updated with the latest routes.

**Answer:** B

#### NEW QUESTION 444

- (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 447

- (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 450

- (Exam Topic 15)

Which technique helps system designers consider potential security concerns of their systems and applications?

- A. Penetration testing
- B. Threat modeling
- C. Manual inspections and reviews
- D. Source code review

**Answer:** B

#### NEW QUESTION 451

- (Exam Topic 15)

Which of the following is a limitation of the Bell-LaPadula model?

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

**Answer:** A

#### NEW QUESTION 452

- (Exam Topic 15)

An attacker has intruded into the source code management system and is able to download but not modify the code. Which of the following aspects of the code theft has the HIGHEST security impact?

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

**Answer:** A

#### NEW QUESTION 456

- (Exam Topic 15)

A web-based application known to be susceptible to attacks is now under review by a senior developer. The organization would like to ensure this application is less susceptible to injection attacks specifically, What strategy will work BEST for the organization's situation?

- A. Do not store sensitive unencrypted data on the back end.



- B. Whitelist input and encode or escape output before it is processed for rendering.
- C. Limit privileged access or hard-coding logon credentials,
- D. Store sensitive data in a buffer that retains data in operating system (OS) cache or memory.

**Answer:** B

#### NEW QUESTION 458

- (Exam Topic 15)

A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

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

**Answer:** B

#### NEW QUESTION 460

- (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 465

- (Exam Topic 15)

Which of the following is the BEST option to reduce the network attack surface of a system?

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

**Answer:** C

#### NEW QUESTION 470

- (Exam Topic 15)

a large organization uses biometrics to allow access to its facilities. It adjusts the biometric value for incorrectly granting or denying access so that the two numbers are the same.

What is this value called?

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

**Answer:** C

#### NEW QUESTION 475

- (Exam Topic 15)

An organization is preparing to achieve General Data Protection Regulation (GDPR) compliance. The Chief Information Security Officer (CISO) is reviewing data protection methods.

Which of the following is the BEST data protection method?

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

**Answer:** C

#### NEW QUESTION 478

- (Exam Topic 15)

An organization is looking to include mobile devices in its asset management system for better tracking. In which system tier of the reference architecture would mobile devices be tracked?

- A. 1
- B. 2
- C. 3

**Answer:** A

#### NEW QUESTION 480

- (Exam Topic 15)

Write Once, Read Many (WORM) data storage devices are designed to BEST support which of the following core security concepts?

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

**Answer:** A

#### NEW QUESTION 484

- (Exam Topic 15)

What is the MOST common security risk of a mobile device?

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

**Answer:** C

#### NEW QUESTION 486

- (Exam Topic 15)

When telephones in a city are connected by a single exchange, the caller can only connect with the switchboard operator. The operator then manually connects the call.

This is an example of which type of network topology?

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

**Answer:** A

#### NEW QUESTION 488

- (Exam Topic 15)

Which of the following protocols will allow the encrypted transfer of content on the Internet?

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

**Answer:** B

#### NEW QUESTION 493

- (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 498

- (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 503

- (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 508**

- (Exam Topic 15)

What is the second phase of public key infrastructure (PKI) key/certificate life-cycle management?

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

**Answer:** A

**NEW QUESTION 511**

- (Exam Topic 15)

Which of the following vulnerabilities can be BEST detected using automated analysis?

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

**Answer:** D

**NEW QUESTION 516**

- (Exam Topic 15)

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

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

**Answer:** C

**NEW QUESTION 519**

- (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 524**

- (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 529**

- (Exam Topic 15)

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

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

**Answer:** B

**NEW QUESTION 530**

- (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 531

- (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 534

- (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 538

- (Exam Topic 15)

In software development, developers should use which type of queries to prevent a Structured Query Language (SQL) injection?

- A. Parameterised
- B. Dynamic
- C. Static
- D. Controlled

**Answer:** A

#### NEW QUESTION 543

- (Exam Topic 15)

An organization wants a service provider to authenticate users via the users' organization domain credentials. Which markup language should the organization's security personnel use to support the integration?

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

**Answer:** A

#### NEW QUESTION 548

- (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 549

- (Exam Topic 15)

A manager identified two conflicting sensitive user functions that were assigned to a single user account that had the potential to result in financial and regulatory risk to the company. The manager MOST likely discovered this during which of the following?

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

**Answer:** B

#### NEW QUESTION 552

- (Exam Topic 15)

A scan report returned multiple vulnerabilities affecting several production servers that are mission critical. Attempts to apply the patches in the development environment have caused the servers to crash. What is the BEST course of action?

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

**Answer:** C

#### NEW QUESTION 553

- (Exam Topic 15)

Which is the BEST control to meet the Statement on Standards for Attestation Engagements 18 (SSAE-18) confidentiality category?

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

**Answer:** C

#### NEW QUESTION 557

- (Exam Topic 15)

Which of the following technologies can be used to monitor and dynamically respond to potential threats on web applications?

- A. Security Assertion Markup Language (SAML)
- B. Web application vulnerability scanners
- C. Runtime application self-protection (RASP)
- D. Field-level tokenization

**Answer:** C

#### NEW QUESTION 561

- (Exam Topic 15)

Which of the following is the FIRST requirement a data owner should consider before implementing a data retention policy?

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

**Answer:** B

#### NEW QUESTION 563

- (Exam Topic 15)

Which of the following is the BEST method to gather evidence from a computer's hard drive?

- A. Disk duplication
- B. Disk replacement
- C. Forensic signature
- D. Forensic imaging

**Answer:** D

#### NEW QUESTION 566

- (Exam Topic 15)

A security engineer is assigned to work with the patch and vulnerability management group. The deployment of a new patch has been approved and needs to be applied.

The research is complete, and the security engineer has provided recommendations. Where should the patch be applied FIRST?

- A. Server environment
- B. Desktop environment
- C. Lower environment
- D. Production environment

**Answer:** C

#### NEW QUESTION 568

- (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 570**

- (Exam Topic 15)

A system developer has a requirement for an application to check for a secure digital signature before the application is accessed on a user's laptop. Which security mechanism addresses this requirement?

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

**Answer:** B

**NEW QUESTION 574**

- (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 578**

- (Exam Topic 15)

Which of the following is the name of an individual or group that is impacted by a change?

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

**Answer:** B

**NEW QUESTION 579**

- (Exam Topic 15)

An organization implements Network Access Control (NAC) by Institute of Electrical and Electronics Engineers (IEEE) 802.1x and discovers the printers do not support the IEEE 802.1x standard. Which of the following is the BEST resolution?

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

**Answer:** A

**NEW QUESTION 583**

- (Exam Topic 15)

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

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

**Answer:** C

**NEW QUESTION 586**

- (Exam Topic 15)

Which of the following security tools will ensure authorized data is sent to the application when implementing a cloud based application?

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

**Answer:** B

**NEW QUESTION 587**



- (Exam Topic 15)

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

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

**Answer:** C

#### NEW QUESTION 592

- (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 597

- (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 598

- (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 603

- (Exam Topic 15)

Which application type is considered high risk and provides a common way for malware and viruses to enter a network?

- A. Instant messaging or chat applications
- B. E-mail applications
- C. Peer-to-Peer (P2P) file sharing applications
- D. End-to-end applications

**Answer:** A

#### NEW QUESTION 606

- (Exam Topic 15)

What industry-recognized document could be used as a baseline reference that is related to data security and business operations for conducting a security assessment?

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

**Answer:** D

#### NEW QUESTION 611

- (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 612**

- (Exam Topic 15)

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

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

**Answer:** C

**NEW QUESTION 613**

- (Exam Topic 15)

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

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

**Answer:** A

**NEW QUESTION 615**

- (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 620**

- (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 623**

- (Exam Topic 15)

Which of the following techniques evaluates the secure Bet principles of network or software architectures?

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

**Answer:** A

**NEW QUESTION 625**

- (Exam Topic 15)

Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

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

**Answer:** B

**NEW QUESTION 629**

- (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 630

- (Exam Topic 15)

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

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

**Answer:** A

#### NEW QUESTION 631

- (Exam Topic 15)

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

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

**Answer:** D

#### NEW QUESTION 632

- (Exam Topic 15)

Which of the following is an important design feature for the outer door of a mantrap?

- A. Allow it to be opened by an alarmed emergency button.
- B. Do not allow anyone to enter it alone.
- C. Do not allow it to be observed by closed-circuit television (CCTV) cameras.
- D. Allow it be opened when the inner door of the mantrap is also open

**Answer:** D

#### NEW QUESTION 637

- (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 639

- (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 642

- (Exam Topic 15)

In which of the following scenarios is locking server cabinets and limiting access to keys preferable to locking the server room to prevent unauthorized access?

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

**Answer:** D

#### NEW QUESTION 645

- (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 646

- (Exam Topic 15)

When are security requirements the LEAST expensive to implement?

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

**Answer:** D

#### NEW QUESTION 648

- (Exam Topic 15)

Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

- A. Trusted Computing Base (TCB)
- B. Time separation
- C. Security kernel
- D. Reference monitor

**Answer:** C

#### NEW QUESTION 649

- (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 653

- (Exam Topic 15)

Which combination of cryptographic algorithms are compliant with Federal Information Processing Standard (FIPS) Publication 140-2 for non-legacy systems?

- A. Diffie-hellman (DH) key exchange: DH ( $\geq 2048$  bits) Symmetric Key: Advanced Encryption Standard (AES)  $> 128$  bits Digital Signature: Rivest-Shamir-Adleman (RSA) (1024 bits)
- B. Diffie-hellman (DH) key exchange: DH ( $\geq 2048$  bits) Symmetric Key: Advanced Encryption Standard (AES)  $> 128$  bits Digital Signature: Digital Signature Algorithm (DSA) ( $\geq 2048$  bits)
- C. Diffie-hellman (DH) key exchange: DH ( $\leq 1024$  bits) Symmetric Key: Blowfish Digital Signature: Rivest-Shamir-Adleman (RSA) ( $\geq 2048$  bits)
- D. Diffie-hellman (DH) key exchange: DH ( $\geq 2048$  bits) Symmetric Key: Advanced Encryption Standard (AES)  $< 128$  bits Digital Signature: Elliptic Curve Digital Signature Algorithm (ECDSA) ( $\geq 256$  bits)

**Answer:** C

#### NEW QUESTION 656

- (Exam Topic 15)

An organization would like to ensure that all new users have a predefined departmental access template applied upon creation. The organization would also like additional access for users to be granted on a per-project basis. What type of user access administration is BEST suited to meet the organization's needs?

- A. Hybrid
- B. Federated
- C. Decentralized
- D. Centralized

**Answer:** A

#### NEW QUESTION 658

- (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 662

- (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 666

- (Exam Topic 15)

While performing a security review for a new product, an information security professional discovers that the organization's product development team is proposing to collect government-issued identification (ID) numbers from customers to use as unique customer identifiers. Which of the following recommendations should be made to the product development team?

- A. Customer identifiers should be a variant of the user's government-issued ID number.
- B. Customer identifiers that do not resemble the user's government-issued ID number should be used.
- C. Customer identifiers should be a cryptographic hash of the user's government-issued ID number.
- D. Customer identifiers should be a variant of the user's name, for example, "jdoe" or "john.doe."

**Answer:** C

#### NEW QUESTION 670

- (Exam Topic 15)

What is the FIRST step in reducing the exposure of a network to Internet Control Message Protocol (ICMP) based attacks?

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

**Answer:** B

#### NEW QUESTION 672

- (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 676

- (Exam Topic 15)

Which of the following techniques evaluates the secure design principles of network OF software architectures?

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

**Answer:** B

#### NEW QUESTION 680

- (Exam Topic 15)

What should be used to determine the risks associated with using Software as a Service (SaaS) for collaboration and email?

- A. Cloud access security broker (CASB)
- B. Open Web Application Security Project (OWASP)
- C. Process for Attack Simulation and Threat Analysis (PASTA)
- D. Common Security Framework (CSF)



**Answer:** A

**NEW QUESTION 683**

- (Exam Topic 15)

Which of the following is the MOST effective strategy to prevent an attacker from disabling a network?

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

**Answer:** D

**NEW QUESTION 686**

- (Exam Topic 15)

At which phase of the software assurance life cycle should risks associated with software acquisition strategies be identified?

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

**Answer:** C

**NEW QUESTION 687**

- (Exam Topic 15)

What are the three key benefits that application developers should derive from the northbound application programming interface (API) of software defined networking (SDN)?

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

**Answer:** C

**NEW QUESTION 690**

- (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 695**

- (Exam Topic 15)

Which of the following threats would be MOST likely mitigated by monitoring assets containing open source libraries for vulnerabilities?

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

**Answer:** A

**NEW QUESTION 700**

- (Exam Topic 15)

In an IDEAL encryption system, who has sole access to the decryption key?

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

**Answer:** B

**NEW QUESTION 702**

- (Exam Topic 15)

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



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

**Answer:** B

#### NEW QUESTION 706

- (Exam Topic 15)

A retail company is looking to start a development project that will utilize open source components in its code for the first time. The development team has already acquired several 'open source components and utilized them in proof of concept (POC) code. The team recognizes that the legal and operational risks are outweighed by the benefits of open-source software use. What MUST the organization do next?

- A. Mandate that all open-source components be approved by the Information Security Manager (ISM).
- B. Scan all open-source components for security vulnerabilities.
- C. Establish an open-source compliance policy.
- D. Require commercial support for all open-source components.

**Answer:** C

#### NEW QUESTION 710

- (Exam Topic 15)

Which of the following is a secure design principle for a new product?

- A. Build in appropriate levels of fault tolerance.
- B. Utilize obfuscation whenever possible.
- C. Do not rely on previously used code.
- D. Restrict the use of modularization.

**Answer:** A

#### NEW QUESTION 713

- (Exam Topic 15)

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

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

**Answer:** A

#### NEW QUESTION 715

- (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 720

- (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 725

- (Exam Topic 15)

What are the PRIMARY responsibilities of security operations for handling and reporting violations and incidents?

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

**Answer:** D

**NEW QUESTION 729**

- (Exam Topic 15)

Which of the following system components enforces access controls on an object?

- A. Security perimeter
- B. Access control matrix
- C. Trusted domain
- D. Reference monitor

**Answer:** B

**NEW QUESTION 734**

- (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 738**

- (Exam Topic 14)

Which of the following is the BEST technique to facilitate secure software development?

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

**Answer:** A

**NEW QUESTION 742**

- (Exam Topic 14)

What is the MOST effective way to determine a mission critical asset in an organization?

- A. Vulnerability analysis
- B. business process analysis
- C. Threat analysis
- D. Business risk analysis

**Answer:** B

**NEW QUESTION 745**

- (Exam Topic 15)

Building blocks for software-defined networks (SDN) require which of the following?

- A. The SDN is mostly composed of virtual machines (VM).
- B. The SDN is composed entirely of client-server pairs.
- C. Virtual memory is used in preference to random-access memory (RAM).
- D. Random-access memory (RAM) is used in preference to virtual memory.

**Answer:** C

**NEW QUESTION 746**

- (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 749**

- (Exam Topic 14)

Which of the following are core categories of malicious attack against Internet of Things (IOT) devices?

- A. Packet capture and false data injection
- B. Packet capture and brute force attack
- C. Node capture 3rd Structured Query Language (SQL) injection
- D. Node capture and false data injection

**Answer:** D

**NEW QUESTION 751**

- (Exam Topic 14)

What steps can be taken to prepare personally identifiable information (PII) for processing by a third party?

- A. It is not necessary to protect PII as long as it is in the hands of the provider.
- B. A security agreement with a Cloud Service Provider (CSP) was required so there is no concern.
- C. The personal information should be maintained separately connected with a one-way reference.
- D. The personal information can be hashed and then the data can be sent to an outside processor.

**Answer:** C

**NEW QUESTION 756**

- (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 758**

- (Exam Topic 14)

What is a warm site when conducting Business continuity planning (BCP)?

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

**Answer:** B

**NEW QUESTION 762**

- (Exam Topic 14)

Activity to baseline, tailor, and scope security controls takes place during which National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) step?

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

**Answer:** D

**NEW QUESTION 763**

- (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. Polyinstantiation
- C. Known vulnerability list
- D. Security auditing

**Answer:** B

**NEW QUESTION 767**

- (Exam Topic 14)

What type of access control determines the authorization to resource based on pre-defined job titles within an organization?

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

**Answer:** A

**NEW QUESTION 770**

- (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 772

- (Exam Topic 14)

An organization wants to enable users to authenticate across multiple security domains. To accomplish this they have decided to use Federated Identity Management (FIM). Which of the following is used behind the scenes in a FIM deployment?

- A. Standard Generalized Markup Language (SGML)
- B. Extensible Markup Language (XML)
- C. Security Assertion Markup Language (SAML)
- D. Transaction Authority Markup Language (XAML)

**Answer:** C

#### NEW QUESTION 776

- (Exam Topic 14)

Continuity of operations is BEST supported by which of the following?

- A. Confidentiality, availability, and reliability
- B. Connectivity, reliability, and redundancy
- C. Connectivity, reliability, and recovery
- D. Confidentiality, integrity, and availability

**Answer:** B

#### NEW QUESTION 779

- (Exam Topic 14)

Which of the following is the PRIMARY risk associated with Extensible Markup Language (XML) applications?

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

**Answer:** A

#### NEW QUESTION 783

- (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 developed by the organization.
- D. The CSP may not be subject to the organization's country legislation.

**Answer:** D

#### NEW QUESTION 784

- (Exam Topic 14)

An organization has implemented a new backup process which protects confidential data by encrypting the information stored on backup tapes. Which of the following is a MAJOR data confidentiality concern after the implementation of this new backup process?

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

**Answer:** D

#### NEW QUESTION 786

- (Exam Topic 14)

copyright provides protection for which of the following?

- A. Discoveries of natural phenomena
- B. New and non-obvious invention
- C. A particular expression of an idea
- D. Ideas expressed in literary works

**Answer:** C

#### NEW QUESTION 788

- (Exam Topic 14)

Physical assets defined in an organization's Business Impact Analysis (BIA) could include which of the following?

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

**Answer:** B

#### NEW QUESTION 792

- (Exam Topic 14)

How long should the records on a project be retained?

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

**Answer:** B

#### NEW QUESTION 797

- (Exam Topic 14)

What access control scheme uses fine-grained rules to specify the conditions under which access to each data item or applications is granted?

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

**Answer:** D

#### Explanation:

Reference: [https://en.wikipedia.org/wiki/Attribute-based\\_access\\_control](https://en.wikipedia.org/wiki/Attribute-based_access_control)

#### NEW QUESTION 799

- (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 804

- (Exam Topic 14)

Functional security testing is MOST critical during which phase of the system development life cycle (SDLC)?

- A. Operations / Maintenance
- B. Implementation
- C. Acquisition / Development
- D. Initiation

**Answer:** B

#### NEW QUESTION 805

- (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 806

- (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 811**

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

## Money Back Guarantee

### CISSP Practice Exam Features:

- \* CISSP Questions and Answers Updated Frequently
- \* CISSP Practice Questions Verified by Expert Senior Certified Staff
- \* CISSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CISSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year