

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)

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 3

- (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 4

- (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 5

- (Exam Topic 15)

In the common criteria, which of the following is a formal document that expresses an implementation-independent set of security requirements?

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

Answer: C

NEW QUESTION 6

- (Exam Topic 15)

In which process MUST security be considered during the acquisition of new software?

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

Answer: B

NEW QUESTION 7

- (Exam Topic 15)

Which of the following is the MOST effective way to ensure the endpoint devices used by remote users are compliant with an organization's approved policies before being allowed on the network?

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

D. Privileged Access Management (PAM)

Answer: B

NEW QUESTION 8

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 9

- (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 10

- (Exam Topic 15)

Wireless users are reporting intermittent Internet connectivity. Connectivity is restored when the users disconnect and reconnect, utilizing the web authentication process each time.

The network administrator can see the devices connected to the APs at all times. Which of the following steps will MOST likely determine the cause of the issue?

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

Answer: A

NEW QUESTION 10

- (Exam Topic 15)

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 11

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 12

- (Exam Topic 15)

What is a use for mandatory access control (MAC)?

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

Answer: D

NEW QUESTION 15

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 16

- (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 19

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 20

- (Exam Topic 15)

An organization wants to define its physical perimeter. What primary device should be used to accomplish this objective if the organization's perimeter MUST cost-efficiently deter casual trespassers?

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

Answer: A

NEW QUESTION 23

- (Exam Topic 15)

When reviewing vendor certifications for handling and processing of company data, which of the following is the BEST Service Organization Controls (SOC) certification for the vendor to possess?

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

Answer: C

NEW QUESTION 24

- (Exam Topic 15)

When reviewing the security logs, the password shown for an administrative login event was ' OR '1'=1' --. This is an example of which of the following kinds of attack?

- A. Brute Force Attack
- B. Structured Query Language (SQL) Injection
- C. Cross-Site Scripting (XSS)
- D. Rainbow Table Attack

Answer: B

NEW QUESTION 25

- (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 27

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 31

- (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 36

- (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 37

- (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 40

- (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 43

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 46

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 50

- (Exam Topic 15)

What is the P R I M A R Y reason criminal law is difficult to enforce when dealing with cyber-crime?

- A. Extradition treaties are rarely enforced.
- B. Numerous language barriers exist.
- C. Law enforcement agencies are understaffed.
- D. Jurisdiction is hard to define.

Answer: D

NEW QUESTION 54

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 56

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 57

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 58

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 63

- (Exam Topic 15)

What type of attack sends Internet Control Message Protocol (ICMP) echo requests to the target machine with a larger payload than the target can handle?

- A. Man-in-the-Middle (MITM)
- B. Denial of Service (DoS)

- C. Domain Name Server (DNS) poisoning
- D. Buffer overflow

Answer: B

NEW QUESTION 65

- (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 70

- (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 75

- (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 80

- (Exam Topic 15)

Why is authentication by ownership stronger than authentication by knowledge?

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

Answer: B

NEW QUESTION 84

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 89

- (Exam Topic 15)

What method could be used to prevent passive attacks against secure voice communications between an organization and its vendor?

- A. Encryption in transit
- B. Configure a virtual private network (VPN)
- C. Configure a dedicated connection
- D. Encryption at rest

Answer: A

NEW QUESTION 90

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 93

- (Exam Topic 15)

Which of the following regulations dictates how data breaches are handled?

- A. Sarbanes-Oxley (SOX)
- B. National Institute of Standards and Technology (NIST)
- C. Payment Card Industry Data Security Standard (PCI-DSS)
- D. General Data Protection Regulation (GDPR)

Answer: D

NEW QUESTION 96

- (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 98

- (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 103

- (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 107

- (Exam Topic 15)

A technician is troubleshooting a client's report about poor wireless performance. Using a client monitor, the technician notes the following information:

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

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

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

Answer: A

NEW QUESTION 109

- (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 113

- (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 118

- (Exam Topic 15)

Which of the following phases in the software acquisition process does developing evaluation criteria take place?

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

Answer: D

NEW QUESTION 120

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 123

- (Exam Topic 15)

A network administrator is designing a new datacenter in a different region that will need to communicate to the old datacenter with a secure connection. Which of the following access methods would provide the BEST security for this new datacenter?

- A. Virtual network computing
- B. Secure Socket Shell
- C. in-band connection
- D. Site-to-site VPN

Answer: D

NEW QUESTION 126

- (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 128

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 131

- (Exam Topic 15)

Which of the following is the MOST common cause of system or security failures?

- A. Lack of system documentation
- B. Lack of physical security controls
- C. Lack of change control
- D. Lack of logging and monitoring

Answer: D

NEW QUESTION 136

- (Exam Topic 15)

Which of the following is MOST important to follow when developing information security controls for an organization?

- A. Exercise due diligence with regard to all risk management information to tailor appropriate controls.
- B. Perform a risk assessment and choose a standard that addresses existing gaps.
- C. Use industry standard best practices for security controls in the organization.
- D. Review all local and international standards and choose the most stringent based on location.

Answer: C

NEW QUESTION 138

- (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 143

- (Exam Topic 15)

In the last 15 years a company has experienced three electrical failures. The cost associated with each failure is listed below.

Which of the following would be a reasonable annual loss expectation?

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

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

Answer: B

NEW QUESTION 148

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 153

- (Exam Topic 15)

Which of the following is the MOST effective countermeasure against data remanence?

- A. Destruction
- B. Clearing
- C. Purging
- D. Encryption

Answer: A

NEW QUESTION 158

- (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 162

- (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 164

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

Answer: A

NEW QUESTION 166

- (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 171

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 172

- (Exam Topic 15)

Which Open Systems Interconnection (OSI) layer(s) BEST corresponds to the network access layer in the Transmission Control Protocol/Internet Protocol (TCP/IP) model?

- A. Transport Layer
- B. Data Link and Physical Layers
- C. Application, Presentation, and Session Layers
- D. Session and Network Layers

Answer: B

NEW QUESTION 175

- (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 178

- (Exam Topic 15)

Computer forensics requires which of the following MAIN steps?

- A. Announce the incident to responsible sections, analyze the data, assimilate the data for correlation
- B. Take action to contain the damage, announce the incident to responsible sections, analyze the data
- C. Acquire the data without altering, authenticate the recovered data, analyze the data
- D. Access the data before destruction, assimilate the data for correlation, take action to contain the damage

Answer: B

NEW QUESTION 183

- (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 186

- (Exam Topic 15)

Which one of the following BEST protects vendor accounts that are used for emergency maintenance?

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

Answer: B

NEW QUESTION 191

- (Exam Topic 15)

Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

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

Answer: B

NEW QUESTION 192

- (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 196

- (Exam Topic 15)

Which type of disaster recovery plan (DRP) testing carries the MOST operational risk?

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

Answer: C

NEW QUESTION 201

- (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 205

- (Exam Topic 15)

Using Address Space Layout Randomization (ASLR) reduces the potential for which of the following attacks?

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

Answer: D

NEW QUESTION 208

- (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 209

- (Exam Topic 15)

When assessing the audit capability of an application, which of the following activities is MOST important?

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

Answer: C

NEW QUESTION 214

- (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 216

- (Exam Topic 15)

Which of the following will accomplish Multi-Factor Authentication (MFA)?

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

Answer: A

NEW QUESTION 218

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 220

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 221

- (Exam Topic 15)

What is the MOST important goal of conducting security assessments?

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

Answer: B

NEW QUESTION 224

- (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 228

- (Exam Topic 15)

What is the FINAL step in the waterfall method for contingency planning?

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

Answer: A

NEW QUESTION 232

- (Exam Topic 15)

What is static analysis intended to do when analyzing an executable file?

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

Answer: D

NEW QUESTION 236

- (Exam Topic 15)

Commercial off-the-shelf (COTS) software presents which of the following additional security concerns?

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

Answer: C

NEW QUESTION 241

- (Exam Topic 15)

Which of the following would be considered an incident if reported by a security information and event management (SIEM) system?

- A. An administrator is logging in on a server through a virtual private network (VPN).
- B. A log source has stopped sending data.

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

Answer: C

NEW QUESTION 245

- (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 247

- (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 250

- (Exam Topic 15)

Which of the following is the PRIMARY purpose of due diligence when an organization embarks on a merger or acquisition?

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

Answer: A

NEW QUESTION 251

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 256

- (Exam Topic 15)

What is the PRIMARY benefit of relying on Security Content Automation Protocol (SCAP)?

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

Answer: C

NEW QUESTION 260

- (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 262

- (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 263

- (Exam Topic 15)

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

- A. Application firewall
- B. Port security
- C. Strong passwords
- D. Two-factor authentication (2FA)

Answer: D

NEW QUESTION 264

- (Exam Topic 15)

Which of the following is the PRIMARY reason for selecting the appropriate level of detail for audit record generation?

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

Answer: B

NEW QUESTION 268

- (Exam Topic 15)

Which of the following is the BEST approach to implement multiple servers on a virtual system?

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

Answer: C

NEW QUESTION 272

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 273

- (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 277

- (Exam Topic 15)

Which event magnitude is defined as deadly, destructive, and disruptive when a hazard interacts with human vulnerability?

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

Answer: B

NEW QUESTION 278

- (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 279

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 284

- (Exam Topic 15)

Which of the following needs to be tested to achieve a Cat 6a certification for a company's data cabling?

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

Answer: C

NEW QUESTION 289

- (Exam Topic 15)

The security team plans on using automated account reconciliation in the corporate user access review process. Which of the following must be implemented for the BEST results with fewest errors when running the audit?

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

Answer: C

NEW QUESTION 294

- (Exam Topic 15)

The Open Web Application Security Project's (OWASP) Software Assurance Maturity Model (SAMM) allows organizations to implement a flexible software security strategy to measure organizational impact based on what risk management aspect?

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

Answer: D

NEW QUESTION 297

- (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 302

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 306

- (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 307

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 312

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 317

- (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 318

- (Exam Topic 15)

When resolving ethical conflicts, the information security professional MUST consider many factors. In what order should these considerations be prioritized?

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

Answer: C

NEW QUESTION 322

- (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 325

- (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 328

- (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 330

- (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 334

- (Exam Topic 15)

Which change management role is responsible for the overall success of the project and supporting the change throughout the organization?

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

Answer: D

NEW QUESTION 336

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 341

- (Exam Topic 15)

An organization is implementing security review as part of system development. Which of the following is the BEST technique to follow?

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

Answer: C

NEW QUESTION 346

- (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 351

- (Exam Topic 15)

The security operations center (SOC) has received credible intelligence that a threat actor is planning to attack with multiple variants of a destructive virus. After obtaining a sample set of this virus' variants and reverse engineering them to understand how they work, a commonality was found. All variants are coded to write to a specific memory location. It is determined this virus is of no threat to the organization because they had the foresight to enable what feature on all endpoints?

- A. Process isolation
- B. Trusted Platform Module (TPM)
- C. Address Space Layout Randomization (ASLR)
- D. Virtualization

Answer: C

NEW QUESTION 355

- (Exam Topic 15)

Which of the following are the three MAIN categories of security controls?

- A. Administrative, technical, physical
- B. Corrective, detective, recovery
- C. Confidentiality, integrity, availability
- D. Preventative, corrective, detective

Answer: A

NEW QUESTION 360

- (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 365

- (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 368

- (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 371

- (Exam Topic 15)

What does the result of Cost-Benefit Analysis (CBA) on new security initiatives provide?

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

Answer: A

NEW QUESTION 372

- (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 373

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 374

- (Exam Topic 15)

What is the FIRST step in developing a patch management plan?

- A. Subscribe to a vulnerability subscription service.
- B. Develop a patch testing procedure.
- C. Inventory the hardware and software used.
- D. Identify unnecessary services installed on systems.

Answer: B

NEW QUESTION 375

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 380

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 381

- (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 383

- (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 388

- (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 390

- (Exam Topic 15)

Which of the following should be done at a disaster site before any item is removed, repaired, or replaced?

- A. Take photos of the damage
- B. Notify all of the Board of Directors
- C. Communicate with the press following the communications plan
- D. Dispatch personnel to the disaster recovery (DR) site

Answer: A

NEW QUESTION 391

- (Exam Topic 15)

A company is attempting to enhance the security of its user authentication processes. After evaluating several options, the company has decided to utilize Identity as a Service (IDaaS).

Which of the following factors leads the company to choose an IDaaS as their solution?

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

Answer: B

NEW QUESTION 393

- (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 398

- (Exam Topic 15)

The adoption of an enterprise-wide Business Continuity (BC) program requires which of the following?

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

Answer: D

NEW QUESTION 402

- (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 406

- (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 409

- (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 411

- (Exam Topic 15)

Which organizational department is ultimately responsible for information governance related to e-mail and other e-records?

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

Answer: C

NEW QUESTION 415

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 417

- (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?

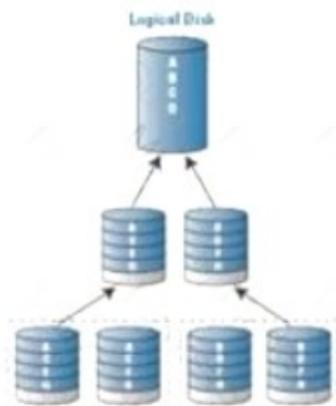
- A. Federation authorities
- B. Proxied federation
- C. Static registration
- D. Dynamic registration

Answer: D

NEW QUESTION 420

- (Exam Topic 15)

Which Redundant Array of Independent Disks (RAID) Level does the following diagram represent?



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

Answer: D

NEW QUESTION 423

- (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 428

- (Exam Topic 15)

Before allowing a web application into the production environment, the security practitioner performs multiple types of tests to confirm that the web application performs as expected. To test the username field, the security practitioner creates a test that enters more characters into the field than is allowed. Which of the following BEST describes the type of test performed?

- A. Misuse case testing
- B. Penetration testing
- C. Web session testing
- D. Interface testing

Answer: A

NEW QUESTION 429

- (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 431

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 433

- (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 438

- (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 443

- (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 448

- (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 450

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 454

- (Exam Topic 15)

An employee's home address should be categorized according to which of the following references?

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

Answer: B

NEW QUESTION 456

- (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 461

- (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 464

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 468

- (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 471

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 473

- (Exam Topic 15)

When conducting a remote access session using Internet Protocol Security (IPSec), which Open Systems Interconnection (OSI) model layer does this connection use?

- A. Transport
- B. Network
- C. Data link
- D. Presentation

Answer: B

NEW QUESTION 478

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 481

- (Exam Topic 15)

Which type of access control includes a system that allows only users that are type=managers and department=sales to access employee records?

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

Answer: C

NEW QUESTION 482

- (Exam Topic 15)

The security team is notified that a device on the network is infected with malware. Which of the following is MOST effective in enabling the device to be quickly located and remediated?

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

Answer: D

NEW QUESTION 484

- (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 487

- (Exam Topic 15)

To monitor the security of buried data lines inside the perimeter of a facility, which of the following is the MOST effective control?

- A. Fencing around the facility with closed-circuit television (CCTV) cameras at all entry points
- B. Ground sensors installed and reporting to a security event management (SEM) system
- C. Steel casing around the facility ingress points
- D. regular sweeps of the perimeter, including manual inspection of the cable ingress points

Answer: D

NEW QUESTION 489

- (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 493

- (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 495

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 496

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 498

- (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 500

- (Exam Topic 15)

Which of the following describes the BEST method of maintaining the inventory of software and hardware within the organization?

- A. Maintaining the inventory through a combination of desktop configuration, administration management, and procurement management tools
- B. Maintaining the inventory through a combination of asset owner interviews, open-source system management, and open-source management tools

- C. Maintaining the inventory through a combination of on-premise storage configuration, cloud management, and partner management tools
- D. Maintaining the inventory through a combination of system configuration, network management, and license management tools

Answer: C

NEW QUESTION 504

- (Exam Topic 15)

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

- A. Increase logging levels.
- B. Implement bi-annual reviews.
- C. Create policies for system access.
- D. Implement and review risk-based alerts.

Answer: D

NEW QUESTION 505

- (Exam Topic 15)

Which algorithm gets its security from the difficulty of calculating discrete logarithms in a finite field and is used to distribute keys, but cannot be used to encrypt or decrypt messages?

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

Answer: C

NEW QUESTION 508

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 511

- (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 513

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 517

- (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 519

- (Exam Topic 15)

Which of the following is used to ensure that data mining activities Will NOT reveal sensitive data?

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

Answer: D

NEW QUESTION 522

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 526

- (Exam Topic 15)

Which of the following BEST describes centralized identity management?

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

Answer: B

NEW QUESTION 529

- (Exam Topic 15)

How is it possible to extract private keys securely stored on a cryptographic smartcard?

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

Answer: D

NEW QUESTION 532

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 537

- (Exam Topic 15)

A company-wide penetration test result shows customers could access and read files through a web browser. Which of the following can be used to mitigate this vulnerability?

- A. Enforce the chmod of files to 755.
- B. Enforce the control of file directory listings.
- C. Implement access control on the web server.
- D. Implement Secure Sockets Layer (SSL) certificates throughout the web server.

Answer: B

NEW QUESTION 542

- (Exam Topic 15)

Which of the following is a covert channel type?

- A. Storage
- B. Pipe
- C. Memory
- D. Monitoring

Answer: A

NEW QUESTION 547

- (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 551

- (Exam Topic 15)

Which of the following activities should a forensic examiner perform FIRST when determining the priority of digital evidence collection at a crime scene?

- A. Gather physical evidence,
- B. Establish order of volatility.
- C. Assign responsibilities to personnel on the scene.
- D. Establish a list of files to examine.

Answer: C

NEW QUESTION 555

- (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 556

- (Exam Topic 15)

Which of the following should be included in a good defense-in-depth strategy provided by object-oriented programming for software deployment?

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

Answer: A

NEW QUESTION 559

- (Exam Topic 15)

The Chief Information Officer (CIO) has decided that as part of business modernization efforts the organization will move towards a cloud architecture. All business-critical data will be migrated to either internal or external cloud services within the next two years. The CIO has a PRIMARY obligation to work with personnel in which role in order to ensure proper protection of data during and after the cloud migration?

- A. Information owner
- B. General Counsel
- C. Chief Information Security Officer (CISO)
- D. Chief Security Officer (CSO)

Answer: A

NEW QUESTION 564

- (Exam Topic 15)

A hospital's building controls system monitors and operates the environmental equipment to maintain a safe and comfortable environment. Which of the following could be used to minimize the risk of utility supply interruption?

- A. Digital devices that can turn equipment off and continuously cycle rapidly in order to increase supplies and conceal activity on the hospital network
- B. Standardized building controls system software with high connectivity to hospital networks
- C. Lock out maintenance personnel from the building controls system access that can impact critical utility supplies
- D. Digital protection and control devices capable of minimizing the adverse impact to critical utility

Answer: D

NEW QUESTION 566

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

Answer: C

NEW QUESTION 570

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 573

- (Exam Topic 15)

What is the MOST appropriate hierarchy of documents when implementing a security program?

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

Answer: C

NEW QUESTION 576

- (Exam Topic 15)

Which of the following is a risk matrix?

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

Answer: C

NEW QUESTION 579

- (Exam Topic 15)

Which of the following should exist in order to perform a security audit?

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

Answer: D

NEW QUESTION 583

- (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 587

- (Exam Topic 15)

When MUST an organization's information security strategic plan be reviewed?

- A. Quarterly, when the organization's strategic plan is updated
- B. Whenever there are significant changes to a major application
- C. Every three years, when the organization's strategic plan is updated
- D. Whenever there are major changes to the business

Answer: D

NEW QUESTION 589

- (Exam Topic 15)

How does Radio-Frequency Identification (RFID) assist with asset management?

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

Answer: B

NEW QUESTION 594

- (Exam Topic 15)

The initial security categorization should be done early in the system life cycle and should be reviewed periodically. Why is it important for this to be done correctly?

- A. It determines the security requirements.
- B. It affects other steps in the certification and accreditation process.
- C. It determines the functional and operational requirements.
- D. The system engineering process works with selected security controls.

Answer: B

NEW QUESTION 597

- (Exam Topic 15)

Which of the following features is MOST effective in mitigating against theft of data on a corporate mobile device which has been stolen?

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

Answer: A

NEW QUESTION 602

- (Exam Topic 15)

A company developed a web application which is sold as a Software as a Service (SaaS) solution to the customer. The application is hosted by a web server running on a 'specific operating system (OS) on a virtual machine (VM). During the transition phase of the service, it is determined that the support team will need access to the application logs. Which of the following privileges would be the MOST suitable?

- A. Administrative privileges on the OS
- B. Administrative privileges on the web server
- C. Administrative privileges on the hypervisor
- D. Administrative privileges on the application folders

Answer: D

NEW QUESTION 604

- (Exam Topic 15)

What is the BEST approach to anonymizing personally identifiable information (PII) in a test environment?

- A. Randomizing data
- B. Swapping data
- C. Encrypting data
- D. Encoding data

Answer: C

NEW QUESTION 607

- (Exam Topic 15)

A cloud hosting provider would like to provide a Service Organization Control (SOC) report relevant to its security program. This report should be an abbreviated report that can be freely distributed. Which type of report BEST meets this requirement?

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

Answer: D

NEW QUESTION 609

- (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 613

- (Exam Topic 15)

Which of the following statements is MOST accurate regarding information assets?

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

Answer: B

NEW QUESTION 618

- (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 621

- (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 626

- (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 628

- (Exam Topic 15)

What process facilitates the balance of operational and economic costs of protective measures with gains in mission capability?

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

Answer: D

NEW QUESTION 630

- (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 631

- (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 636

- (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 637

- (Exam Topic 14)

In a dispersed network that lacks central control, which of the following is die PRIMARY course of action to mitigate exposure?

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

Answer: C

NEW QUESTION 640

- (Exam Topic 14)

Which one of the following documentation should be included in a Disaster Recovery (DR) package?

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

Answer: C

NEW QUESTION 641

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 644

- (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 648

- (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 649

- (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 650

- (Exam Topic 14)

Internet protocol security (IPSec), point-to-point tunneling protocol (PPTP), and secure sockets Layer (SSL) all use Which of the following to prevent replay attacks?

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

Answer: C

NEW QUESTION 653

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 654

- (Exam Topic 14)

Which of the following value comparisons MOST accurately reflects the agile development approach?

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

Answer: D

NEW QUESTION 655

- (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 658

- (Exam Topic 14)

Vulnerability scanners may allow for the administrator to assign which of the following in order to assist in prioritizing remediation activities?

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

Answer: C

NEW QUESTION 663

- (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 666

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 671

- (Exam Topic 14)

What should be used immediately after a Business Continuity Plan (BCP) has been invoked?

- A. Resumption procedures describing the actions to be taken to return to normal business operations
- B. Emergency procedures describing the necessary actions to be taken following an incident jeopardizes business operations
- C. Fallback procedures describing what action are to be taken to more essential business activities to alternative temporary locations
- D. Maintain schedule how and the plan will be tested and the process for maintaining the plan

Answer: B

NEW QUESTION 672

- (Exam Topic 14)

Additional padding may be added to the Encapsulating Security Protocol (ESP) trailer to provide which of the following?

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

Answer: C

NEW QUESTION 675

- (Exam Topic 14)

What are the roles within a scrum methodology?

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

Answer: D

NEW QUESTION 676

- (Exam Topic 14)

A security practitioner has been tasked with establishing organizational asset handling procedures. What should be considered that would have the GREATEST impact to the development of these procedures?

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

Answer: D

NEW QUESTION 678

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 683

- (Exam Topic 14)

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

- A. Investigate, Evaluate, Respond, Monitor

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

Answer: C

NEW QUESTION 687

- (Exam Topic 14)

Limiting the processor, memory, and Input/output (I/O) capabilities of mobile code is known as

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

Answer: C

NEW QUESTION 689

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 691

- (Exam Topic 14)

Which of the following is the BEST definition of Cross-Site Request Forgery (CSRF)?

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

Answer: A

Explanation:

Reference: <https://portswigger.net/web-security/csrf>

NEW QUESTION 694

- (Exam Topic 14)

What testing technique enables the designer to develop mitigation strategies for potential vulnerabilities?

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

Answer: C

NEW QUESTION 698

- (Exam Topic 14)

Which of the following authorization standards is built to handle Application Programming Interface (API) access for Federated Identity Management (FIM)?

- A. Security Assertion Markup Language (SAML)
- B. Open Authentication (OAUTH)
- C. Remote Authentication Dial-in User service (RADIUS)
- D. Terminal Access Control Access Control System Plus (TACACS+)

Answer: B

NEW QUESTION 700

- (Exam Topic 14)

Which is the RECOMMENDED configuration mode for sensors for an intrusion prevention system (IPS) if the prevention capabilities will be used?

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

Answer: C

NEW QUESTION 702

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 706

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 707

- (Exam Topic 14)

Which of the following is the MOST effective countermeasure against Man-in-the Middle (MITM) attacks while using online banking?

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

Answer: A

NEW QUESTION 711

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 715

- (Exam Topic 14)

Which of the following is the MOST critical success factor in the security patch management process?

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

Answer: A

NEW QUESTION 716

- (Exam Topic 14)

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

- A. Exercise due diligence when deciding to circumvent host government requests.
- B. Become familiar with the means in which the code of ethics is applied and considered.
- C. Complete the assignment based on the customer's wishes.
- D. Execute according to the professional's comfort level with the code of ethics.

Answer: B

NEW QUESTION 718

- (Exam Topic 14)

An organization that has achieved a Capability Maturity model Integration (CMMI) level of 4 has done which of the following?

- A. Addressed continuous innovative process improvement
- B. Addressed the causes of common process variance
- C. Achieved optimized process performance
- D. Achieved predictable process performance

Answer: C

NEW QUESTION 721

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 723

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 726

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 729

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 731

- (Exam Topic 14)

Point-to-Point Protocol (PPP) was designed to specifically address what issue?

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

Answer: B

NEW QUESTION 732

- (Exam Topic 14)

Which of the following controls is the most for a system identified as critical in terms of data and function to the organization?

- A. Preventive controls
- B. Monitoring control
- C. Cost controls
- D. Compensating controls

Answer: B

NEW QUESTION 734

- (Exam Topic 14)

Which of the following is the BEST statement for a professional to include as part of business continuity (BC) procedure?

- A. A full data backup must be done upon management request.
- B. An incremental data backup must be done upon management request.
- C. A full data backup must be done based on the needs of the business.

D. In incremental data backup must be done after each system change.

Answer: D

NEW QUESTION 737

- (Exam Topic 14)

Which of the following is the MOST important activity an organization performs to ensure that security is part of the overall organization culture?

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

Answer: C

NEW QUESTION 741

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 743

- (Exam Topic 14)

What is the document that describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls?

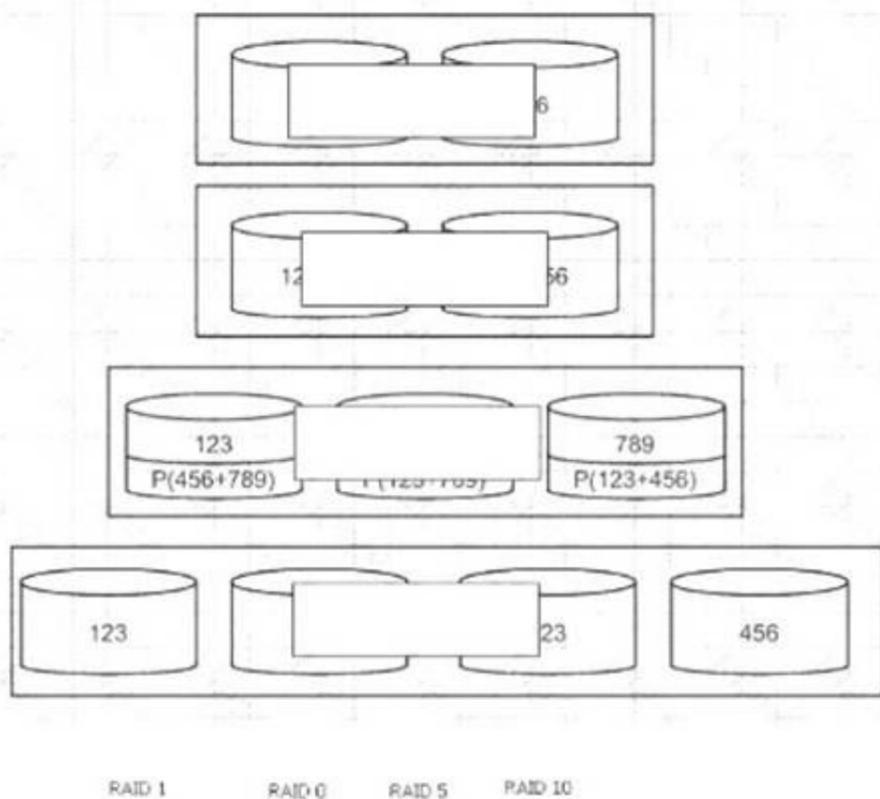
- A. Business Impact Analysis (BIA)
- B. Security Assessment Report (SAR)
- C. Plan of Action and Milestones (POA&M)
- D. Security Assessment Plan (SAP)

Answer: C

NEW QUESTION 748

- (Exam Topic 14)

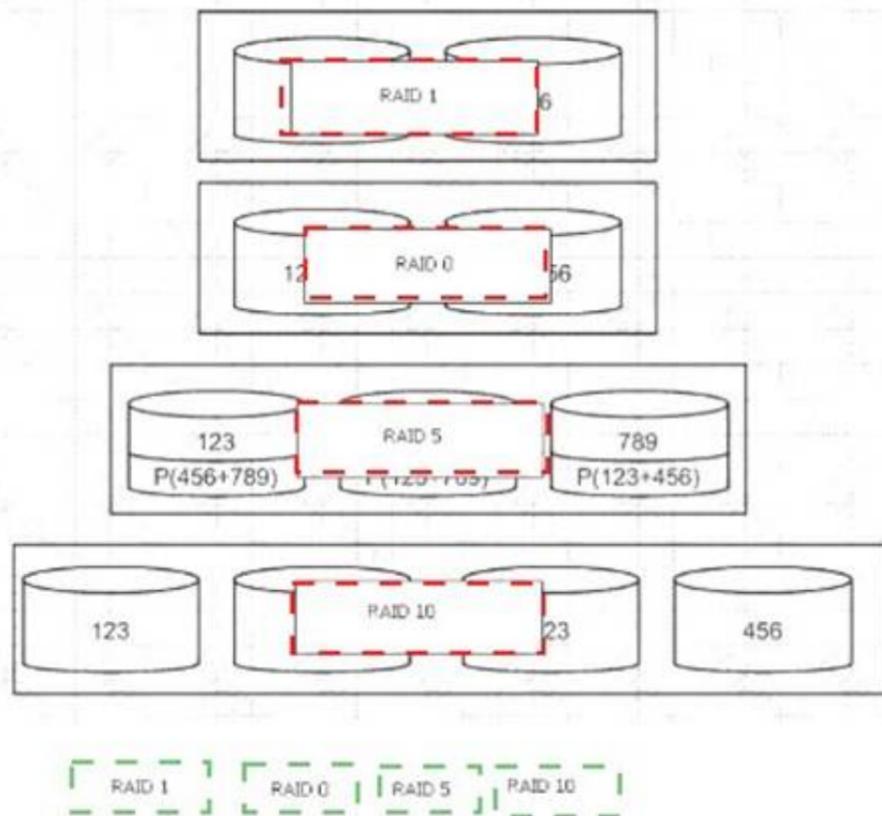
Given a file containing ordered number, i.e. "123456789," match each of the following redundant Array of independent Disks (RAID) levels to the corresponding visual representation. Note: P() = parity.
 Drag each level to the appropriate place on the diagram.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 749

- (Exam Topic 14)

Which of the following is the PRIMARY reason a sniffer operating on a network is collecting packets only from its own host?

- A. An Intrusion Detection System (IDS) has dropped the packets.
- B. The network is connected using switches.
- C. The network is connected using hubs.
- D. The network's firewall does not allow sniffing.

Answer: A

NEW QUESTION 750

- (Exam Topic 14)

How can a security engineer maintain network separation from a secure environment while allowing remote users to work in the secure environment?

- A. Use a Virtual Local Area Network (VLAN) to segment the network
- B. Implement a bastion host
- C. Install anti-virus on all enceinte
- D. Enforce port security on access switches

Answer: A

NEW QUESTION 754

- (Exam Topic 14)

What is the FIRST step required in establishing a records retention program?

- A. Identify and inventory all records.
- B. Identify and inventory all records storage locations
- C. Classify records based on sensitivity.
- D. Draft a records retention policy.

Answer: D

NEW QUESTION 757

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 758

- (Exam Topic 14)

Which of the following security testing strategies is BEST suited for companies with low to moderate security maturity?

- A. Load Testing
- B. White-box testing

- C. Black -box testing
- D. Performance testing

Answer: B

NEW QUESTION 760

- (Exam Topic 14)

Which of the following models uses unique groups contained in unique conflict classes?

- A. Chinese Wall
- B. Bell-LaPadula
- C. Clark-Wilson
- D. Biba

Answer: C

NEW QUESTION 765

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 767

- (Exam Topic 14)

In fault-tolerant systems, what do rollback capabilities permit?

- A. Restoring the system to a previous functional state
- B. Identifying the error that caused the problem
- C. Allowing the system to run in a reduced manner
- D. Isolating the error that caused the problem

Answer: A

NEW QUESTION 768

- (Exam Topic 14)

The MAIN task of promoting security for Personal Computers (PC) is

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

Answer: C

NEW QUESTION 771

- (Exam Topic 14)

What are the roles within a scrum methodology?

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

Answer: B

NEW QUESTION 772

- (Exam Topic 14)

Which of the following is the BEST identity-as-a-service (IDaaS) solution for validating users?

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

Answer: A

NEW QUESTION 774

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 775

- (Exam Topic 14)

Which of the following practices provides the development of security and identification of threats in designing software?

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

Answer: D

NEW QUESTION 778

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 780

- (Exam Topic 14)

Which is the second phase of public key Infrastructure (pk1) key/certificate life-cycle management?

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

Answer: C

NEW QUESTION 781

- (Exam Topic 14)

Asymmetric algorithms are used for which of the following when using Secure Sockets Layer/Transport Layer Security (SSL/TLS) for implementing network security?

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

Answer: C

NEW QUESTION 784

- (Exam Topic 14)

What is the MAIN reason to ensure the appropriate retention periods are enforced for data stored on electronic media?

- A. To reduce the carbon footprint by eliminating paper
- B. To create an inventory of data assets stored on disk for backup and recovery
- C. To declassify information that has been improperly classified
- D. To reduce the risk of loss, unauthorized access, use, modification, and disclosure

Answer: D

NEW QUESTION 787

- (Exam Topic 14)

Which of the following media is least problematic with data remanence?

- A. Magnetic disk
- B. Electrically Erasable Programming read-only Memory (EEPROM)
- C. Dynamic Random Access Memory (DRAM)
- D. Flash memory

Answer: C

NEW QUESTION 789

- (Exam Topic 14)

Which of the following initiates the system recovery phase of a disaster recovery plan?

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

Answer: C

NEW QUESTION 790

- (Exam Topic 14)

During a recent assessment an organization has discovered that the wireless signal can be detected outside the campus area. What logical control should be implemented in order to BEST protect the confidentiality of information traveling over wireless transmission media?

- A. Configure a firewall to logically separate the data at the boundary.
- B. Configure the Access Points (AP) to use Wi-Fi Protected Access 2 (WPA2) encryption.
- C. Disable the Service Set Identifier (SSID) broadcast on the Access Points (AP).
- D. Perform regular technical assessments on the Wireless Local Area Network (WLAN).

Answer: B

NEW QUESTION 793

- (Exam Topic 14)

Which of the following steps should be conducted during the FIRST phase of software assurance in a generic acquisition process?

- A. Establishing and consenting to the contract work schedule
- B. Issuing a Request for proposal (RFP) with a work statement
- C. Developing software requirements to be included in work statement
- D. Reviewing and accepting software deliverables

Answer: C

NEW QUESTION 796

- (Exam Topic 14)

Organization A is adding a large collection of confidential data records that it received when it acquired Organization B to its data store. Many of the users and staff from Organization B are no longer available. Which of the following MUST Organization A do to properly classify and secure the acquired data?

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

Answer: A

NEW QUESTION 800

- (Exam Topic 14)

When can a security program be considered effective?

- A. Audits are regularly performed and reviewed.
- B. Vulnerabilities are proactively identified.
- C. Risk is lowered to an acceptable level.
- D. Badges are regularly performed and validated

Answer: C

NEW QUESTION 804

- (Exam Topic 14)

An audit of an application reveals that the current configuration does not match the configuration of the originally implemented application. Which of the following is the FIRST action to be taken?

- A. Recommend an update to the change control process.
- B. Verify the approval of the configuration change.
- C. Roll back the application to the original configuration.
- D. Document the changes to the configuration.

Answer: B

NEW QUESTION 809

- (Exam Topic 14)

An employee receives a promotion that entitles them to access higher-level functions on the company's accounting system, as well as keeping their access to the previous system that is no longer needed or applicable. What is the name of the process that tries to remove this excess privilege?

- A. Access provisioning
- B. Segregation of Duties (SoD)
- C. Access certification
- D. Access aggregation

Answer: B

NEW QUESTION 813

- (Exam Topic 14)

Which of the following is the PRIMARY security consideration for how an organization should handle Information Technology (IT) assets?

- A. The monetary value of the asset
- B. The controls implemented on the asset
- C. The physical form factor of the asset
- D. The classification of the data on the asset

Answer: D

NEW QUESTION 814

- (Exam Topic 14)

Which would result in the GREATEST impact following a breach to a cloud environment?

- A. The hypervisor host is poorly secured
- B. The same Logical Unit Number (LUN) is used for all VMs
- C. Insufficient network segregation
- D. Insufficient hardening of Virtual Machines (VM)

Answer: C

NEW QUESTION 816

- (Exam Topic 14)

Why do certificate Authorities (CA) add value to the security of electronic commerce transactions?

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

Answer: D

NEW QUESTION 820

- (Exam Topic 14)

A development operations team would like to start building new applications delegating the cybersecurity responsibility as much as possible to the service provider. Which of the following environments BEST fits their need?

- A. Cloud Virtual Machines (VM)
- B. Cloud application container within a Virtual Machine (VM)
- C. On premises Virtual Machine (VM)
- D. Self-hosted Virtual Machine (VM)

Answer: A

NEW QUESTION 822

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 825

- (Exam Topic 14)

Why is lexical obfuscation in software development discouraged by many organizations?

- A. Problems writing test cases
- B. Problems recovering systems after disaster
- C. Problems compiling the code
- D. Problems maintaining data connections

Answer: C

NEW QUESTION 828

- (Exam Topic 14)

When would an organization review a Business Continuity Management (BCM) system?

- A. When major changes occur on systems
- B. When personnel changes occur

- C. Before and after Disaster Recovery (DR) tests
- D. At planned intervals

Answer: D

NEW QUESTION 832

.....

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