

ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)



NEW QUESTION 1

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 2

- (Exam Topic 15)

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)

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

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

Answer: B

NEW QUESTION 4

- (Exam Topic 15)

Which of the following is an important requirement when designing a secure remote access system?

- A. Configure a Demilitarized Zone (DMZ) to ensure that user and service traffic is separated.
- B. Provide privileged access rights to computer files and systems.
- C. Ensure that logging and audit controls are included.
- D. Reduce administrative overhead through password self service.

Answer: C

NEW QUESTION 5

- (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 6

- (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 7

- (Exam Topic 15)

Wi-Fi Protected Access 2 (WPA2) provides users with a higher level of assurance that their data will remain protected by using which protocol?

- A. Secure Shell (SSH)
- B. Internet Protocol Security (IPsec)
- C. Secure Sockets Layer (SSL)
- D. Extensible Authentication Protocol (EAP)

Answer: A

NEW QUESTION 8

- (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 9

- (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 10

- (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 11

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 13

- (Exam Topic 15)

Which of the following access control models is MOST restrictive?

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

Answer: B

NEW QUESTION 17

- (Exam Topic 15)

A large human resources organization wants to integrate their identity management with a trusted partner organization. The human resources organization wants to maintain the creation and management of the identities and may want to share with other partners in the future. Which of the following options BEST serves

their needs?

- A. Federated identity
- B. Cloud Active Directory (AD)
- C. Security Assertion Markup Language (SAML)
- D. Single sign-on (SSO)

Answer: A

NEW QUESTION 22

- (Exam Topic 15)

An organization has implemented a password complexity and an account lockout policy enforcing five incorrect logins tries within ten minutes. Network users have reported significantly increased account lockouts. Which of the following security principles is this company affecting?

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

Answer: A

NEW QUESTION 26

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 30

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 35

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 36

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 41

- (Exam Topic 15)

A breach investigation a website was exploited through an open sourcedIs The FIRB Stan In the Process that could have prevented this breach?

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

Answer: B

NEW QUESTION 46

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 50

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 55

- (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 60

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 64

- (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 66

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 68

- (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 72

- (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 74

- (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 78

- (Exam Topic 15)

In order to support the least privilege security principle when a resource is transferring within the organization from a production support system administration role to a developer role, what changes should be made to the resource's access to the production operating system (OS) directory structure?

- A. From Read Only privileges to No Access Privileges
- B. From Author privileges to Administrator privileges
- C. From Administrator privileges to No Access privileges
- D. From No Access Privileges to Author privileges

Answer: C

NEW QUESTION 81

- (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 85

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 90

- (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 94

- (Exam Topic 15)

What is the PRIMARY benefit of incident reporting and computer crime investigations?

- A. Providing evidence to law enforcement
- B. Repairing the damage and preventing future occurrences
- C. Appointing a computer emergency response team
- D. Complying with security policy

Answer: D

NEW QUESTION 96

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 98

- (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 99

- (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 103

- (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 108

- (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 109

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 110

- (Exam Topic 15)

In a DevOps environment, which of the following actions is MOST necessary to have confidence in the quality of the changes being made?

- A. Prepare to take corrective actions quickly.
- B. Receive approval from the change review board.
- C. Review logs for any anomalies.
- D. Automate functionality testing.

Answer: B

NEW QUESTION 115

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 118

- (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 123

- (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 128

- (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 130

- (Exam Topic 15)

Which of the following actions should be taken by a security professional when a mission critical computer network attack is suspected?

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

Answer: C

NEW QUESTION 131

- (Exam Topic 15)

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

- A. Information Security Management System (ISMS)
- B. Information Sharing & Analysis Centers (ISAC)

- C. Risk Management Framework (RMF)
- D. Information Security Continuous Monitoring (ISCM)

Answer: D

NEW QUESTION 132

- (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 137

- (Exam Topic 15)

As a design principle, which one of the following actors is responsible for identifying and approving data security requirements in a cloud ecosystem?

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

Answer: C

NEW QUESTION 141

- (Exam Topic 15)

What is the MOST effective response to a hacker who has already gained access to a network and will attempt to pivot to other resources?

- A. Reset all passwords.
- B. Shut down the network.
- C. Warn users of a breach.
- D. Segment the network.

Answer: D

NEW QUESTION 142

- (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 145

- (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 149

- (Exam Topic 15)

Which of the following is an example of a vulnerability of full-disk encryption (FDE)?

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

Answer: A

NEW QUESTION 151

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 156

- (Exam Topic 15)

Which of the following services can be deployed via a cloud service or on-premises to integrate with Identity as a Service (IDaaS) as the authoritative source of user identities?

- A. Directory
- B. User database
- C. Multi-factor authentication (MFA)
- D. Single sign-on (SSO)

Answer: A

NEW QUESTION 160

- (Exam Topic 15)

What is the FIRST step that should be considered in a Data Loss Prevention (DLP) program?

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

Answer: D

NEW QUESTION 164

- (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 167

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 169

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 171

- (Exam Topic 15)

Which of the following is included in change management?

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

Answer: A

NEW QUESTION 174

- (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 175

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 179

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 184

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 186

- (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 189

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 192

- (Exam Topic 15)

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

organizational risk management

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

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

Answer: A

NEW QUESTION 195

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 199

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 200

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 203

- (Exam Topic 15)

Which of the following are the BEST characteristics of security metrics?

- A. They are generalized and provide a broad overview
- B. They use acronyms and abbreviations to be concise
- C. They use bar charts and Venn diagrams
- D. They are consistently measured and quantitatively expressed

Answer: D

NEW QUESTION 208

- (Exam Topic 15)

Which of the following would qualify as an exception to the "right to be forgotten" of the General Data Protection Regulation's (GDPR)?

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

Answer: C

NEW QUESTION 210

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 213

- (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 215

- (Exam Topic 15)

Why is it important that senior management clearly communicates the formal Maximum Tolerable Downtime (MTD) decision?

- A. To provide each manager with precise direction on selecting an appropriate recovery alternative
- B. To demonstrate to the regulatory bodies that the company takes business continuity seriously
- C. To demonstrate to the board of directors that senior management is committed to continuity recovery efforts
- D. To provide a formal declaration from senior management as required by internal audit to demonstrate sound business practices

Answer: D

NEW QUESTION 220

- (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 224

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 226

- (Exam Topic 15)

Which of the following is the MOST secure password technique?

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

Answer: A

NEW QUESTION 230

- (Exam Topic 15)

Which of the following departments initiates the request, approval, and provisioning business process?

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

Answer: A

NEW QUESTION 233

- (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 234

- (Exam Topic 15)

Before implementing an internet-facing router, a network administrator ensures that the equipment is baselined/hardened according to approved configurations and settings. This action provides protection against which of the following attacks?

- A. Blind spoofing
- B. Media Access Control (MAC) flooding
- C. SQL injection (SQLI)
- D. Ransomware

Answer: B

NEW QUESTION 236

- (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 239

- (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 243

- (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 247

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 248

- (Exam Topic 15)

An enterprise is developing a baseline cybersecurity standard its suppliers must meet before being awarded a contract. Which of the following statements is TRUE about the baseline cybersecurity standard?

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

Answer: D

NEW QUESTION 250

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 251

- (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 256

- (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 259

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 260

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 263

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 267

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 268

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 271

- (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 275

- (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 279

- (Exam Topic 15)

Which of the following will an organization's network vulnerability testing process BEST enhance?

- A. Firewall log review processes
- B. Asset management procedures
- C. Server hardening processes
- D. Code review procedures

Answer: C

NEW QUESTION 284

- (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 285

- (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 287

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 289

- (Exam Topic 15)

At the destination host, which of the following OSI model layers will discard a segment with a bad checksum in the UDP header?

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

Answer: C

NEW QUESTION 293

- (Exam Topic 15)

When defining a set of security controls to mitigate a risk, which of the following actions MUST occur?

- A. Each control's effectiveness must be evaluated individually.
- B. Each control must completely mitigate the risk.
- C. The control set must adequately mitigate the risk.
- D. The control set must evenly divided the risk.

Answer: A

NEW QUESTION 298

- (Exam Topic 15)

An organization is planning to have an it audit of its as a Service (SaaS) application to demonstrate to external parties that the security controls around availability are designed. The audit report must also cover a certain period of time to show the operational effectiveness of the controls. Which Service Organization Control (SOC) report would BEST fit their needs?

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

Answer: D

NEW QUESTION 303

- (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 307

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 310

- (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 315

- (Exam Topic 15)

What documentation is produced FIRST when performing an effective physical loss control process?

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

Answer: C

NEW QUESTION 316

- (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 318

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 321

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 325

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 329

- (Exam Topic 15)

Within a large organization, what business unit is BEST positioned to initiate provisioning and deprovisioning of user accounts?

- A. Training department
- B. Internal audit
- C. Human resources
- D. Information technology (IT)

Answer: C

NEW QUESTION 334

- (Exam Topic 15)

Which of the following types of web-based attack is happening when an attacker is able to send a well-crafted, malicious request to an authenticated user without the user realizing it?

- A. Cross-Site Scripting (XSS)
- B. Cross-Site request forgery (CSRF)

- C. Cross injection
- D. Broken Authentication And Session Management

Answer: B

NEW QUESTION 337

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 342

- (Exam Topic 15)

Which of the following explains why classifying data is an important step in performing a Risk assessment?

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

Answer: D

NEW QUESTION 345

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 346

- (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 349

- (Exam Topic 15)

What is a risk of using commercial off-the-shelf (COTS) products?

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

Answer: A

NEW QUESTION 350

- (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 354

- (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 357

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 362

- (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 363

- (Exam Topic 15)

What is the MOST significant benefit of role-based access control (RBAC)?

- A. Reduction in authorization administration overhead
- B. Reduces inappropriate access
- C. Management of least privilege
- D. Most granular form of access control

Answer: A

NEW QUESTION 367

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 370

- (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 372

- (Exam Topic 15)

Which of the following BEST obtains an objective audit of security controls?

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

Answer:

A

NEW QUESTION 376

- (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 379

- (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 380

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 384

- (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 388

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 391

- (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 395

- (Exam Topic 15)

Which section of the assessment report addresses separate vulnerabilities, weaknesses, and gaps?

- A. Key findings section
- B. Executive summary with full details

- C. Risk review section
- D. Findings definition section

Answer: A

NEW QUESTION 398

- (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 401

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 402

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 405

- (Exam Topic 15)

Which of the following factors is a PRIMARY reason to drive changes in an Information Security Continuous Monitoring (ISCM) strategy?

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

Answer: B

NEW QUESTION 406

- (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 411

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 413

- (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 418

- (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 420

- (Exam Topic 15)

Which of the following documents specifies services from the client's viewpoint?

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

Answer: C

NEW QUESTION 421

- (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 423

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 428

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 429

- (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 430

- (Exam Topic 15)

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

- A. System analyst
- B. System security officer
- C. System processor
- D. System custodian

Answer: D

NEW QUESTION 431

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 433

- (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 434

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 436

- (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 437

- (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 439

- (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 442

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 445

- (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 447

- (Exam Topic 15)

Of the following, which BEST provides non- repudiation with regards to access to a server room?

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

Answer: C

NEW QUESTION 451

- (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 455

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 457

- (Exam Topic 15)

When performing an investigation with the potential for legal action, what should be the analyst's FIRST consideration?

- A. Chain-of-custody
- B. Authorization to collect
- C. Court admissibility
- D. Data decryption

Answer: A

NEW QUESTION 459

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 461

- (Exam Topic 15)

The security architect has been assigned the responsibility of ensuring integrity of the organization's electronic records. Which of the following methods provides the strongest level of integrity?

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

Answer: D

NEW QUESTION 466

- (Exam Topic 15)

What is the BEST method to use for assessing the security impact of acquired software?

- A. Common vulnerability review
- B. Software security compliance validation
- C. Threat modeling
- D. Vendor assessment

Answer: B

NEW QUESTION 470

- (Exam Topic 15)

Which of the following BEST describes the standard used to exchange authorization information between different identity management systems?

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

Answer: A

NEW QUESTION 471

- (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 474

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 479

- (Exam Topic 15)

Why would a system be structured to isolate different classes of information from one another and segregate them by user jurisdiction?

- A. The organization can avoid e-discovery processes in the event of litigation.
- B. The organization's infrastructure is clearly arranged and scope of responsibility is simplified.

- C. The organization can vary its system policies to comply with conflicting national laws.
- D. The organization is required to provide different services to various third-party organizations.

Answer: C

NEW QUESTION 482

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 484

- (Exam Topic 15)

Which of the following has the responsibility of information technology (IT) governance?

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

Answer: A

NEW QUESTION 489

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 490

- (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 494

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 498

- (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 503

- (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 507

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 508

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 513

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 518

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 523

- (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 527

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 531

- (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 536

- (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 540

- (Exam Topic 15)

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

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

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

Answer: C

NEW QUESTION 543

- (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 545

- (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 549

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 554

- (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 557

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 560

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 564

- (Exam Topic 15)

What is the MAIN purpose of a security assessment plan?

- A. Provide guidance on security requirements, to ensure the identified security risks are properly addressed based on the recommendation
- B. Provide the objectives for the security and privacy control assessments and a detailed roadmap of how to conduct such assessments.
- C. Provide technical information to executives to help them understand information security postures and secure funding.
- D. Provide education to employees on security and privacy, to ensure their awareness on policies and procedures

Answer: B

NEW QUESTION 566

- (Exam Topic 15)

Which of the following protects personally identifiable information (PII) used by financial services organizations?

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

Answer: B

NEW QUESTION 570

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 574

- (Exam Topic 15)

What is the FIRST step prior to executing a test of an organisation's disaster recovery (DR) or business continuity plan (BCP)?

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

Answer: D

NEW QUESTION 575

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 580

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 582

- (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 587

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 592

- (Exam Topic 15)

What is the BEST design for securing physical perimeter protection?

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

Answer: B

NEW QUESTION 595

- (Exam Topic 15)

Which of the following BEST describes when an organization should conduct a black box security audit on a new software product?

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

Answer: B

NEW QUESTION 597

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 602

- (Exam Topic 15)

A security professional is assessing the risk in an application and does not take into account any mitigating or compensating controls. This type of risk rating is an example of which of the following?

- A. Transferred risk
- B. Inherent risk
- C. Residual risk
- D. Avoided risk

Answer: B

NEW QUESTION 604

- (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 607

- (Exam Topic 15)

Which of the following protection is provided when using a Virtual Private Network (VPN) with Authentication Header (AH)?

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

Answer: C

NEW QUESTION 608

- (Exam Topic 15)

How is Remote Authentication Dial-In User Service (RADIUS) authentication accomplished?

- A. It uses clear text and firewall rules.
- B. It relies on Virtual Private Networks (VPN).
- C. It uses clear text and shared secret keys.
- D. It relies on asymmetric encryption keys.

Answer: C

NEW QUESTION 609

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 614

- (Exam Topic 15)

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

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

D. Data Owner

Answer: D

NEW QUESTION 615

- (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 618

- (Exam Topic 15)

What is the HIGHEST priority in agile development?

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

Answer: C

NEW QUESTION 621

- (Exam Topic 15)

The security architect has been mandated to assess the security of various brands of mobile devices. At what phase of the product lifecycle would this be MOST likely to occur?

- A. Disposal
- B. Implementation
- C. Development
- D. Operations and maintenance

Answer: C

NEW QUESTION 626

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 627

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 630

- (Exam Topic 15)

Which one of the following can be used to detect an anomaly in a system by keeping track of the state of files that do not normally change?

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

Answer: C

NEW QUESTION 631

- (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 636

- (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 641

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 646

- (Exam Topic 15)

A criminal organization is planning an attack on a government network. Which of the following scenarios presents the HIGHEST risk to the organization?

- A. Network is flooded with communication traffic by the attacker.
- B. Organization loses control of their network devices.
- C. Network management communications is disrupted.
- D. Attacker accesses sensitive information regarding the network topology.

Answer: B

NEW QUESTION 651

- (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 656

- (Exam Topic 15)

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

- A. Integrity first, association before self, and excellence in all we do
- B. Perform all professional activities and duties in accordance with all applicable laws and the highest ethical standards.
- C. Provide diligent and competent service to principals.
- D. Cooperate with others in the interchange of knowledge and ideas for mutual security.

Answer: C

NEW QUESTION 660

- (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 662

- (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 666

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 670

- (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 672

- (Exam Topic 15)

When recovering from an outage, what is the Recovery Point Objective (RPO), in terms of data recovery?

- A. The RPO is the maximum amount of time for which loss of data is acceptable.
- B. The RPO is the minimum amount of data that needs to be recovered.
- C. The RPO is a goal to recover a targeted percentage of data lost.
- D. The RPO is the amount of time it takes to recover an acceptable percentage of data lost.

Answer: B

NEW QUESTION 673

- (Exam Topic 15)

What is the BEST reason to include supply chain risks in a corporate risk register?

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

Answer: B

NEW QUESTION 674

- (Exam Topic 15)

To comply with industry requirements, a security assessment on the cloud server should identify which protocols and weaknesses are being exposed to attackers on the Internet.

Which of the following tools is the MOST appropriate to complete the assessment?

- A. Use tcpdump and parse the output file in a protocol analyzer.
- B. Use an IP scanner and target the cloud WAN network addressing
- C. Run netstat in each cloud server and retrieve the running processes.
- D. Use nmap and set the servers' public IPs as the target

Answer: D

NEW QUESTION 675

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 678

- (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 681

- (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 686

- (Exam Topic 15)

A healthcare insurance organization chose a vendor to develop a software application. Upon review of the draft contract, the information security professional notices that software security is not addressed. What is the BEST approach to address the issue?

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

Answer: C

NEW QUESTION 691

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 695

- (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 700

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 703

- (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 706

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 709

- (Exam Topic 15)

A security professional has been requested by the Board of Directors and Chief Information Security Officer (CISO) to perform an internal and external penetration test. What is the BEST course of action?

- A. Review data localization requirements and regulations.
- B. Review corporate security policies and procedures,
- C. With notice to the Configuring a Wireless Access Point (WAP) with the same Service Set Identifier external test.
- D. With notice to the organization, perform an external penetration test first, then an internal test.

Answer: D

NEW QUESTION 711

- (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 714

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 719

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 721

- (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 724

- (Exam Topic 14)

When developing the entitlement review process, which of the following roles is responsible for determining who has a need for the information?

- A. Data Custodian
- B. Data Owner
- C. Database Administrator
- D. Information Technology (IT) Director

Answer: B

NEW QUESTION 727

- (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 728

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 733

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 738

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 743

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 746

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 749

- (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 753

- (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 754

- (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 755

- (Exam Topic 14)

If a content management system (CMC) is implemented, which one of the following would occur?

- A. Developers would no longer have access to production systems
- B. The applications placed into production would be secure
- C. Patching the systems would be completed more quickly
- D. The test and production systems would be running the same software

Answer: D

NEW QUESTION 756

- (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 761

- (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 766

- (Exam Topic 14)

How long should the records on a project be retained?

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

Answer:

B

NEW QUESTION 768

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 770

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 772

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 774

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 776

- (Exam Topic 14)

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

Answer: D

NEW QUESTION 779

- (Exam Topic 14)

What are the roles within a scrum methodology?

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

Answer: D

NEW QUESTION 783

- (Exam Topic 14)

Compared with hardware cryptography, software cryptography is generally

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

D. less expensive and faster.

Answer: A

Explanation:

Reference:

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

NEW QUESTION 785

- (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 787

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 791

- (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 793

- (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 798

- (Exam Topic 14)

What is the PRIMARY purpose for an organization to conduct a security audit?

- A. To ensure the organization is adhering to a well-defined standard
- B. To ensure the organization is applying security controls to mitigate identified risks
- C. To ensure the organization is configuring information systems efficiently
- D. To ensure the organization is documenting findings

Answer: A

NEW QUESTION 800

- (Exam Topic 14)

Which of the following is used to detect steganography?

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

Answer: C

NEW QUESTION 803

- (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 804

- (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 807

- (Exam Topic 14)

When dealing with shared, privileged accounts, especially those for emergencies, what is the BEST way to assure non-repudiation of logs?

- A. Regularly change the passwords,
- B. implement a password vaulting solution.
- C. Lock passwords in tamperproof envelopes in a safe.
- D. Implement a strict access control policy.

Answer: B

NEW QUESTION 810

- (Exam Topic 14)

Which of the following is the PRIMARY consideration when determining the frequency an automated control should be assessed or monitored?

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

Answer: B

NEW QUESTION 813

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 818

- (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 820

- (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 825

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 828

- (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 829

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 833

- (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 834

- (Exam Topic 14)

From an asset security perspective, what is the BEST countermeasure to prevent data theft due to data remanence when a sensitive data storage media is no longer needed?

- A. Return the media to the system owner.
- B. Delete the sensitive data from the media.
- C. Physically destroy the retired media.
- D. Encrypt data before it is stored on the media.

Answer: C

NEW QUESTION 837

- (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 839

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CISSP Practice Exam Features:

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

100% Actual & Verified — Instant Download, Please Click
[Order The CISSP Practice Test Here](#)