

ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)



NEW QUESTION 1

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 2

- (Exam Topic 15)

An organization 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 3

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 4

- (Exam Topic 15)

Which of the following 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 5

- (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 6

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 7

- (Exam Topic 15)

Which of the following 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 8

- (Exam Topic 15)

Which of the following is fundamentally required to address potential security issues when initiating software development?

- A. Implement ongoing security audits in all environments.
- B. Ensure isolation of development from production.
- C. Add information security objectives into development.
- D. Conduct independent source code review.

Answer: C

NEW QUESTION 9

- (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 10

- (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 10

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 15

- (Exam Topic 15)

What is the PRIMARY consideration when testing industrial control systems (ICS) for security weaknesses?

- A. ICS often do not have availability requirements.
- B. ICS are often isolated and difficult to access.
- C. ICS often run on UNIX operating systems.
- D. ICS are often sensitive to unexpected traffic.

Answer: B

NEW QUESTION 16

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 17

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 18

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 21

- (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 22

- (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 25

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 29

- (Exam Topic 15)

Why is authentication by ownership stronger than authentication by knowledge?

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

Answer: B

NEW QUESTION 34

- (Exam Topic 15)

A user is allowed to access the file labeled "Financial Forecast," but only between 9:00 a.m. and 5:00 p.m., Monday through Friday. Which type of access mechanism should be used to accomplish this?

- A. Minimum access control
- B. Rule-based access control
- C. Limited role-based access control (RBAC)
- D. Access control list (ACL)

Answer: B

NEW QUESTION 36

- (Exam Topic 15)

A digitally-signed e-mail was delivered over a wireless network protected with Wired Equivalent Privacy (WEP) protocol. Which of the following principles is at risk?

- A. Availability
- B. Non-Repudiation
- C. Confidentiality
- D. Integrity

Answer: B

NEW QUESTION 38

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 39

- (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 44

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 46

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 50

- (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 53

- (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 55

- (Exam Topic 15)

When developing an external facing web-based system, which of the following would be the MAIN focus of the security assessment prior to implementation and production?

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

Answer: B

NEW QUESTION 58

- (Exam Topic 15)

What is the correct order of execution for security architecture?

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

Answer: A

NEW QUESTION 59

- (Exam Topic 15)

Using the cipher text and resultant clear text message to derive the non-alphabetic cipher key is an example of which method of cryptanalytic attack?

- A. Frequency analysis
- B. Ciphertext-only attack
- C. Probable-plaintext attack
- D. Known-plaintext attack

Answer: D

NEW QUESTION 61

- (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 66

- (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 71

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 74

- (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 76

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 79

- (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 80

- (Exam Topic 15)

A security professional was tasked with rebuilding a company's wireless infrastructure. Which of the following are the MOST important factors to consider while making a decision on which wireless spectrum to deploy?

- A. Hybrid frequency band, service set identifier (SSID), and interpolation
- B. Performance, geographic location, and radio signal interference
- C. Facility size, intermodulation, and direct satellite service
- D. Existing client devices, manufacturer reputation, and electrical interference

Answer: D

NEW QUESTION 85

- (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 89

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 91

- (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 95

- (Exam Topic 15)

When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

- A. Provide links to security policies
- B. Log all activities associated with sensitive systems
- C. Employ strong access controls
- D. Confirm that confidentiality agreements are signed

Answer: C

NEW QUESTION 98

- (Exam Topic 15)

What security principle addresses the issue of "Security by Obscurity"?

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

Answer: D

NEW QUESTION 101

- (Exam Topic 15)

A financial organization that works according to agile principles has developed a new application for their external customer base to request a line of credit. A security analyst has been asked to assess the security risk of the minimum viable product (MVP). Which is the MOST important activity the analyst should assess?

- A. The software has the correct functionality.
- B. The software has been code reviewed.
- C. The software had been branded according to corporate standards,
- D. The software has been signed off for release by the product owner.

Answer: A

NEW QUESTION 103

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 105

- (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 107

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 112

- (Exam Topic 15)

Which of the following is the MAIN difference between a network-based firewall and a host-based firewall?

- A. A network-based firewall is stateful, while a host-based firewall is stateless.
- B. A network-based firewall controls traffic passing through the device, while a host-based firewall controls traffic destined for the device.
- C. A network-based firewall verifies network traffic, while a host-based firewall verifies processes and applications.
- D. A network-based firewall blocks network intrusions, while a host-based firewall blocks malware.

Answer: B

NEW QUESTION 115

- (Exam Topic 15)

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

- A. Parallel
- B. Simulation
- C. Table-top
- D. Cut-over

Answer: C

NEW QUESTION 118

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 120

- (Exam Topic 15)

A security professional has been assigned to assess a web application. The assessment report recommends switching to Security Assertion Markup Language (SAML). What is the PRIMARY security benefit in switching to SAML?

- A. It uses Transport Layer Security (TLS) to address confidentiality.
- B. it enables single sign-on (SSO) for web applications.
- C. The users' password is not passed during authentication.
- D. It limits unnecessary data entry on web forms.

Answer: B

NEW QUESTION 122

- (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 125

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 130

- (Exam Topic 15)

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

- A. Strict integration of application management, configuration management (CM), and phone management
- B. Management application installed on user phones that tracks all application events and cellular traffic
- C. Enterprise-level security information and event management (SIEM) dashboard that provides full visibility of cellular phone activity

D. Routine reports generated by the user's cellular phone provider that detail security events

Answer: B

NEW QUESTION 133

- (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 138

- (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 141

- (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 143

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 144

- (Exam Topic 15)

Data remanence is the biggest threat in which of the following scenarios?

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

Answer: D

NEW QUESTION 148

- (Exam Topic 15)

The acquisition of personal data being obtained by a lawful and fair means is an example of what principle?

- A. Data Quality Principle
- B. Openness Principle
- C. Purpose Specification Principle
- D. Collection Limitation Principle

Answer: D

NEW QUESTION 149

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 153

- (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 158

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 162

- (Exam Topic 15)

Which of the following is the **PRIMARY** goal of logical access controls?

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

Answer: C

NEW QUESTION 164

- (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 168

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 173

- (Exam Topic 15)

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

- A. Intrusion detection system (IDS)
- B. Circuit-Level Proxy
- C. Application-Level Proxy

D. Host-based Firewall

Answer: B

NEW QUESTION 178

- (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 182

- (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 184

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 187

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 191

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 192

- (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 196

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 198

- (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 202

- (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 203

- (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 205

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 210

- (Exam Topic 15)

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

- A. Drill through the device and platters.
- B. Mechanically shred the entire HDD.
- C. Remove the control electronics.
- D. HP iProcess the HDD through a degaussing device.

Answer: D

NEW QUESTION 212

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 215

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 217

- (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 219

- (Exam Topic 15)

What does the result of Cost-Benefit Analysis (C8A) on new security initiatives provide?

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

Answer: A

NEW QUESTION 224

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 226

- (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 227

- (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 232

- (Exam Topic 15)

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

- A. Take photos of the damage
- B. Notify all of the Board of Directors

- C. Communicate with the press following the communications plan
- D. Dispatch personnel to the disaster recovery (DR) site

Answer: A

NEW QUESTION 234

- (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 239

- (Exam Topic 15)

An authentication system that uses challenge and response was recently implemented on an organization's network, because the organization conducted an annual penetration test showing that testers were able to move laterally using authenticated credentials. Which attack method was MOST likely used to achieve this?

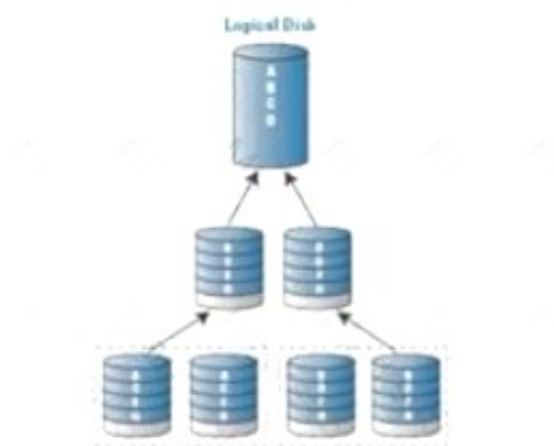
- A. Cross-Site Scripting (XSS)
- B. Pass the ticket
- C. Brute force
- D. Hash collision

Answer: B

NEW QUESTION 240

- (Exam Topic 15)

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



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

Answer: D

NEW QUESTION 244

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 249

- (Exam Topic 15)

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

What is this value called?

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

Answer: C

NEW QUESTION 251

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 253

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 254

- (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 259

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 263

- (Exam Topic 15)

An organization purchased a commercial off-the-shelf (COTS) software several years ago. The information technology (IT) Director has decided to migrate the application into the cloud, but is concerned about the application security of the software in the organization's dedicated environment with a cloud service provider. What is the BEST way to prevent and correct the software's security weakness?

- A. Implement a dedicated COTS sandbox environment
- B. Follow the software end-of-life schedule
- C. Transfer the risk to the cloud service provider
- D. Examine the software updating and patching process

Answer: A

NEW QUESTION 264

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 266

- (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 268

- (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 271

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 275

- (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 280

- (Exam Topic 15)

How should the retention period for an organization's social media content be defined?

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

Answer: B

NEW QUESTION 283

- (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 286

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 291

- (Exam Topic 15)

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

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

Answer: C

NEW QUESTION 293

- (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)² 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 295

- (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 298

- (Exam Topic 15)

Why are packet filtering routers used in low-risk environments?

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

Answer: B

NEW QUESTION 300

- (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 303

- (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 308

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 312

- (Exam Topic 15)

A security professional needs to find a secure and efficient method of encrypting data on an endpoint. Which solution includes a root key?

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

Answer: D

NEW QUESTION 315

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 320

- (Exam Topic 15)

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

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

Answer: D

NEW QUESTION 321

- (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 323

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 325

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 328

- (Exam Topic 15)

An information security professional is reviewing user access controls on a customer-facing application. The application must have multi-factor authentication (MFA) in place. The application currently requires a username and password to login. Which of the following options would BEST implement MFA?

- A. Geolocate the user and compare to previous logins
- B. Require a pre-selected number as part of the login
- C. Have the user answer a secret question that is known to them
- D. Enter an automatically generated number from a hardware token

Answer: C

NEW QUESTION 333

- (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 335

- (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 336

- (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 337

- (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 339

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 344

- (Exam Topic 15)

When are security requirements the LEAST expensive to implement?

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

Answer: D

NEW QUESTION 348

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 352

- (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 356

- (Exam Topic 15)

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

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

Answer: B

NEW QUESTION 357

- (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 361

- (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 365

- (Exam Topic 15)

Who should perform the design review to uncover security design flaws as part of the Software Development Life Cycle (SDLC)?

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

Answer: B

NEW QUESTION 369

- (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 371

- (Exam Topic 15)

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

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

Answer: A

NEW QUESTION 372

- (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 377

- (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 381

- (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 385

- (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 388

- (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 393

- (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 397

- (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 402

- (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 405

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 406

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 409

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 412

- (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 416

- (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 420

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 422

- (Exam Topic 14)

Which of the following is mobile device remote fingerprinting?

- A. Installing an application to retrieve common characteristics of the device
- B. Storing information about a remote device in a cookie file
- C. Identifying a device based on common characteristics shared by all devices of a certain type
- D. Retrieving the serial number of the mobile device

Answer: C

NEW QUESTION 426

- (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 (AUP)
- D. Information classification scheme

Answer: D

NEW QUESTION 427

- (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 429

- (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 433

- (Exam Topic 14)

Which of the following will have the MOST influence on the definition and creation of data classification and data ownership policies?

- A. Data access control policies
- B. Threat modeling
- C. Common Criteria (CC)

D. Business Impact Analysis (BIA)

Answer: A

NEW QUESTION 437

- (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 439

- (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 440

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 444

- (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 445

- (Exam Topic 14)

Which of the below strategies would MOST comprehensively address the risk of malicious insiders leaking sensitive information?

- A. Data Loss Protection (DLP), firewalls, data classification
- B. Least privilege access, Data Loss Protection (DLP), physical access controls
- C. Staff vetting, least privilege access, Data Loss Protection (DLP)
- D. Background checks, data encryption, web proxies

Answer: B

NEW QUESTION 446

- (Exam Topic 14)

An organization discovers that its secure file transfer protocol (SFTP) server has been accessed by an unauthorized person to download an unreleased game. A recent security audit found weaknesses in some of the organization's general information technology (IT) controls, specifically pertaining to software change control and security patch management, but not in other control areas.

Which of the following is the MOST probable attack vector used in the security breach?

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

Answer: A

NEW QUESTION 448

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 453

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 454

- (Exam Topic 14)

Which of the following BEST provides for non-repudiation of user account actions?

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

Answer: D

NEW QUESTION 455

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 460

- (Exam Topic 14)

The core component of Role Based Access control (RBAC) must be constructed of defined data elements. Which elements are required?

- A. Users, permissions, operators, and protected objects
- B. Users, roles, operations, and protected objects
- C. Roles, accounts, permissions, and protected objects
- D. Roles, operations, accounts, and protected objects

Answer: B

NEW QUESTION 461

- (Exam Topic 14)

A financial company has decided to move its main business application to the Cloud. The legal department objects, arguing that the move of the platform should comply with several regulatory obligations such as the General Data Protection (GDPR) and ensure data confidentiality. The Chief Information Security Officer (CISO) says that the cloud provider has met all regulations requirements and even provides its own encryption solution with internally-managed encryption keys to address data confidentiality. Did the CISO address all the legal requirements in this situation?

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

Answer: B

NEW QUESTION 462

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 463

- (Exam Topic 14)

An organization is outsourcing its payroll system and is requesting to conduct a full audit on the third-party information technology (IT) systems. During the due diligence process, the third party provides previous audit report on its IT system.

Which of the following **MUST** be considered by the organization in order for the audit reports to be acceptable?

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

Answer: A

NEW QUESTION 468

- (Exam Topic 14)

Which open standard could a large corporation deploy for authorization services for single sign-on (SSO) use across multiple internal and external application?

- A. Terminal Access Controller Access Control System (TACACS)
- B. Security Assertion Markup Language (SAML)
- C. Lightweight Directory Access Protocol (LDAP)
- D. Active Directory Federation Services (ADFS)

Answer: B

NEW QUESTION 473

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 475

- (Exam Topic 14)

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

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

Answer: A

NEW QUESTION 478

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 482

- (Exam Topic 14)

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

- A. Log of backup administrative actions
- B. Log of the transported media and its classification marking
- C. Log of the transported media and its detailed contents
- D. Log of backed up data and their respective data custodians

Answer: B

NEW QUESTION 484

- (Exam Topic 14)

An organization implements a Remote Access Server (RAS). Once users connect to the server, digital certificates are used to authenticate their identity. What type of Extensible Authentication Protocol (EAP) would the organization use during this authentication?

- A. Transport layer security (TLS)
- B. Message Digest 5 (MD5)
- C. Lightweight Extensible Authentication Protocol (EAP)
- D. Subscriber Identity Module (SIM)

Answer: A

NEW QUESTION 489

- (Exam Topic 14)

What are the roles within a scrum methodology?

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

Answer: B

NEW QUESTION 492

- (Exam Topic 14)

Which of the following management processes allots ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

- A. Compliance
- B. Configuration
- C. Identity
- D. Patch

Answer: B

NEW QUESTION 496

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 497

- (Exam Topic 14)

Assume that a computer was powered off when an information security professional arrived at a crime scene. Which of the following actions should be performed after the crime scene is isolated?

- A. Turn the computer on and collect volatile data.
- B. Turn the computer on and collect network information.
- C. Leave the computer off and prepare the computer for transportation to the laboratory
- D. Remove the hard drive, prepare it for transportation, and leave the hardware at the scene.

Answer: C

NEW QUESTION 499

- (Exam Topic 14)

Which of the following threats exists with an implementation of digital signatures?

- A. Spoofing
- B. Substitution
- C. Content tampering
- D. Eavesdropping

Answer: A

NEW QUESTION 504

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 506

- (Exam Topic 14)

Which of the following phases involves researching a target's configuration from public sources when performing a penetration test?

- A. Information gathering
- B. Social engineering
- C. Target selection
- D. Traffic enumeration

Answer: A

NEW QUESTION 511

- (Exam Topic 14)

Which of the following is a characteristic of a challenge/response authentication process?

- A. Presenting distorted graphics of text for authentication
- B. Transmitting a hash based on the user's password
- C. Using a password history blacklist
- D. Requiring the use of non-consecutive numeric characters

Answer: A

NEW QUESTION 514

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 518

- (Exam Topic 14)

Which of the following will help identify the source internet protocol (IP) address of malware being executed on a computer?

- A. List of open network connections
- B. Display Transmission Control Protocol/Internet Protocol (TCP/IP) network configuration information.
- C. List of running processes
- D. Display the Address Resolution Protocol (ARP) table.

Answer: A

NEW QUESTION 519

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 522

- (Exam Topic 14)

Which of the following provides the GREATEST level of data security for a Virtual Private Network (VPN) connection?

- A. Internet Protocol Payload Compression (IPComp)
- B. Internet Protocol Security (IPSec)
- C. Extensible Authentication Protocol (EAP)
- D. Remote Authentication Dial-In User Service (RADIUS)

Answer: B

NEW QUESTION 524

- (Exam Topic 14)

Change management policies and procedures belong to which of the following types of controls?

- A. Directive
- B. Detective
- C. Corrective

D. Preventative

Answer: A

Explanation:

Reference: <https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA570&lpg=PA570&dq=CISSP+Change+mana>

NEW QUESTION 525

- (Exam Topic 14)

Which type of test suite should be run for fast feedback during application development?

- A. Full recession
- B. End-to-end
- C. Smoke
- D. Specific functionality

Answer: C

NEW QUESTION 527

- (Exam Topic 14)

Match the level of evaluation to the correct common criteria (CC) assurance level.

Drag each level of evaluation on the left to is corresponding CC assurance level on the right

Level of Evaluation	Assurance Level
Structurally tested	1
Methodically tested and checked	2
Methodically designed, tested, and reviewed	3
Functionally tested	4
Semiformally verified design and tested	5
Formally verified design and tested	6
Semiformally designed and tested	7

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Level of Evaluation	Assurance Level
Structurally tested	Functionally tested 1
Methodically tested and checked	Structurally tested 2
Methodically designed, tested, and reviewed	Methodically tested and checked 3
Functionally tested	Methodically designed, tested, and reviewed 4
Semiformally verified design and tested	Semiformally designed and tested 5
Formally verified design and tested	Semiformally verified design and tested 6
Semiformally designed and tested	Formally verified design and tested 7

NEW QUESTION 528

- (Exam Topic 14)

Who is essential for developing effective test scenarios for disaster recovery (DR) test plans?

- A. Business line management and IT staff members
- B. Chief Information Officer (CIO) and DR manager
- C. DR manager and IT staff members
- D. IT staff members and project managers

Answer: B

NEW QUESTION 532

- (Exam Topic 14)

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

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

Answer: C

NEW QUESTION 535

- (Exam Topic 14)

Which of the following is the MOST important action regarding authentication?

- A. Granting access rights
- B. Enrolling in the system
- C. Establishing audit controls
- D. Obtaining executive authorization

Answer: B

NEW QUESTION 537

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 542

- (Exam Topic 14)

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

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

Answer: D

NEW QUESTION 544

- (Exam Topic 14)

Which security architecture strategy could be applied to secure an operating system (OS) baseline for deployment within the corporate enterprise?

- A. Principle of Least Privilege
- B. Principle of Separation of Duty
- C. Principle of Secure Default
- D. principle of Fail Secure

Answer: D

NEW QUESTION 547

- (Exam Topic 14)

The adoption of an enterprise-wide business continuity program requires Which of the following?

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

Answer: D

NEW QUESTION 550

- (Exam Topic 14)

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

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

Answer: B

NEW QUESTION 553

- (Exam Topic 14)

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

- A. When major changes occur on systems
- B. When personnel changes occur
- C. Before and after Disaster Recovery (DR) tests
- D. At planned intervals

Answer: D

NEW QUESTION 554

- (Exam Topic 14)

Which of the following **MUST** an organization do to effectively communicate is security strategy to all affected parties?

- A. Involve representatives from each key organizational area.
- B. Provide regular updates to the board of directors.
- C. Notify staff of changes to the strategy.
- D. Remove potential communication barriers.

Answer: C

NEW QUESTION 559

- (Exam Topic 14)

Which of the following is applicable to a publicly held company concerned about information handling and storage requirement specific to the financial reporting?

- A. Privacy Act of 1974
- B. Clinger-Cohan Act of 1996
- C. Sarbanes-Oxley (SOX) Act of 2002
- D. International Organization for Standardization (ISO) 27001

Answer: C

NEW QUESTION 560

- (Exam Topic 14)

Which of the following is the **MOST** significant benefit to implementing a third-party federated identity architecture?

- A. Attribute assertions as agencies can request a larger set of attributes to fulfill service delivery
- B. Data decrease related to storing personal information
- C. Reduction in operational costs to the agency
- D. Enable business objectives so departments can focus on mission rather than the business of identitymanagement

Answer: C

NEW QUESTION 562

- (Exam Topic 14)

What is maintained by using write blocking devices whan forensic evidence is examined?

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

Answer: B

NEW QUESTION 564

- (Exam Topic 14)

What is the threat modeling order using process for Attack simu-lation and threat analysis (PASTA)?

- A. Application decomposition, threat analysis, vulnerability detection, attack enumeration, risk/impact analysis
- B. Threat analysis, vulnerability detection, application decomposition, attack enumeration, risk/Impact analysis
- C. Risk/impact analysis, application decomposition, threat analysis, vulnerability detection, attack enumeration
- D. Application decomposition, threat analysis, risk/impact analysis, vulnerability detection, attack enumeration

Answer: A

NEW QUESTION 567

- (Exam Topic 14)

Which of the following needs to be taken into account when assessing vulnerability?

- A. Risk identification and validation
- B. Threat mapping
- C. Risk acceptance criteria
- D. Safeguard selection

Answer: A

Explanation:

Reference: <https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA478&lpg=PA478&dq=CISSP+taken+into+acc>

NEW QUESTION 571

- (Exam Topic 14)

Which of the following is the primary advantage of segmenting Virtual Machines (VM) using physical networks?

- A. Simplicity of network configuration and network monitoring
- B. Removes the need for decentralized management solutions
- C. Removes the need for dedicated virtual security controls
- D. Simplicity of network configuration and network redundancy

Answer: A

NEW QUESTION 573

- (Exam Topic 14)

What Is the FIRST step for a digital investigator to perform when using best practices to collect digital evidence from a potential crime scene?

- A. Consult the lead investigate to team the details of the case and required evidence.
- B. Assure that grounding procedures have been followed to reduce the loss of digital data due to static electricity discharge.
- C. Update the Basic Input Output System (BIOS) and Operating System (OS) of any tools used to assure evidence admissibility.
- D. Confirm that the appropriate warrants were issued to the subject of the investigation to eliminate illegal search claims.

Answer: D

NEW QUESTION 574

- (Exam Topic 14)

What is the PRIMARY objective for conducting an internal security audit?

- A. Verify that all systems and Standard Operating Procedures (SOP) are properly documented.
- B. Verify that all personnel supporting a system are knowledgeable of their responsibilities.
- C. Verify that security controls are established following best practices.
- D. Verify that applicable security controls are implemented and effective.

Answer: D

NEW QUESTION 575

- (Exam Topic 14)

Which of the following attacks is dependent upon the compromise of a secondary target in order to reach the primary target?

- A. Watering hole
- B. Brute force
- C. Spear phishing
- D. Address Resolution Protocol (ARP) poisoning

Answer: D

NEW QUESTION 577

- (Exam Topic 14)

Which of the following attributes could be used to describe a protection mechanism of an open design methodology?

- A. It must be tamperproof to protect it from malicious attacks.
- B. It can facilitate independent confirmation of the design security.
- C. It can facilitate blackbox penetration testing.
- D. It exposes the design to vulnerabilities and malicious attacks.

Answer: A

NEW QUESTION 578

- (Exam Topic 14)

As a security manger which of the following is the MOST effective practice for providing value to an organization?

- A. Assess business risk and apply security resources accordingly
- B. Coordinate security implementations with internal audit

- C. Achieve compliance regardless of related technical issues
- D. Identify confidential information and protect it

Answer: D

NEW QUESTION 583

- (Exam Topic 14)

What is the BEST way to establish identity over the internet?

- A. Challenge Handshake Authentication Protocol (CHAP) and strong passwords
- B. Internet Mail Access Protocol (IMAP) with Triple Data Encryption Standard (3DES)
- C. Remote Authentication Dial-In User Service (RADIUS) server with hardware tokens
- D. Remote user authentication via Simple Object Access Protocol (SOAP)

Answer: D

NEW QUESTION 588

- (Exam Topic 14)

What is the most effective form of media sanitization to ensure residual data cannot be retrieved?

- A. Clearing
- B. Destroying
- C. Purging
- D. Disposal

Answer: B

NEW QUESTION 593

- (Exam Topic 13)

Which one of the following is an advantage of an effective release control strategy from a configuration control standpoint?

- A. Ensures that a trace for all deliverables is maintained and auditable
- B. Enforces backward compatibility between releases
- C. Ensures that there is no loss of functionality between releases
- D. Allows for future enhancements to existing features

Answer: A

NEW QUESTION 598

- (Exam Topic 13)

When developing a business case for updating a security program, the security program owner MUST do which of the following?

- A. Identify relevant metrics
- B. Prepare performance test reports
- C. Obtain resources for the security program
- D. Interview executive management

Answer: A

NEW QUESTION 603

- (Exam Topic 14)

Individuals have been identified and determined as having a need-to-know for the information. Which of the following access control methods MUST include a consistent set of rules for controlling and limiting access?

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

Answer: D

NEW QUESTION 604

- (Exam Topic 13)

What is the MAIN reason for testing a Disaster Recovery Plan (DRP)?

- A. To ensure Information Technology (IT) staff knows and performs roles assigned to each of them
- B. To validate backup sites' effectiveness
- C. To find out what does not work and fix it
- D. To create a high level DRP awareness among Information Technology (IT) staff

Answer: B

NEW QUESTION 607

- (Exam Topic 13)

A security analyst for a large financial institution is reviewing network traffic related to an incident. The analyst determines the traffic is irrelevant to the investigation

but in the process of the review, the analyst also finds that an applications data, which included full credit card cardholder data, is transferred in clear text between the server and user's desktop. The analyst knows this violates the Payment Card Industry Data Security Standard (PCI-DSS). Which of the following is the analyst's next step?

- A. Send the log file co-workers for peer review
- B. Include the full network traffic logs in the incident report
- C. Follow organizational processes to alert the proper teams to address the issue.
- D. Ignore data as it is outside the scope of the investigation and the analyst's role.

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 611

- (Exam Topic 13)

What is the PRIMARY role of a scrum master in agile development?

- A. To choose the primary development language
- B. To choose the integrated development environment
- C. To match the software requirements to the delivery plan
- D. To project manage the software delivery

Answer: D

NEW QUESTION 616

- (Exam Topic 13)

A minimal implementation of endpoint security includes which of the following?

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

Answer: B

NEW QUESTION 620

- (Exam Topic 13)

Which of the following access management procedures would minimize the possibility of an organization's employees retaining access to secure work areas after they change roles?

- A. User access modification
- B. user access recertification
- C. User access termination
- D. User access provisioning

Answer: B

NEW QUESTION 621

- (Exam Topic 13)

What capability would typically be included in a commercially available software package designed for access control?

- A. Password encryption
- B. File encryption
- C. Source library control
- D. File authentication

Answer: A

NEW QUESTION 625

- (Exam Topic 13)

Which of the following is the MOST effective practice in managing user accounts when an employee is terminated?

- A. Implement processes for automated removal of access for terminated employees.
- B. Delete employee network and system IDs upon termination.
- C. Manually remove terminated employee user-access to all systems and applications.
- D. Disable terminated employee network ID to remove all access.

Answer: B

NEW QUESTION 630

- (Exam Topic 13)

Which of the following provides the MOST comprehensive filtering of Peer-to-Peer (P2P) traffic?

- A. Application proxy
- B. Port filter
- C. Network boundary router

D. Access layer switch

Answer: D

NEW QUESTION 635

- (Exam Topic 13)

What is the BEST location in a network to place Virtual Private Network (VPN) devices when an internal review reveals network design flaws in remote access?

- A. In a dedicated Demilitarized Zone (DMZ)
- B. In its own separate Virtual Local Area Network (VLAN)
- C. At the Internet Service Provider (ISP)
- D. Outside the external firewall

Answer: B

NEW QUESTION 639

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 641

- (Exam Topic 13)

Within the company, desktop clients receive Internet Protocol (IP) address over Dynamic Host Configuration Protocol (DHCP).

Which of the following represents a valid measure to help protect the network against unauthorized access?

- A. Implement path management
- B. Implement port based security through 802.1x
- C. Implement DHCP to assign IP address to server systems
- D. Implement change management

Answer: B

NEW QUESTION 645

- (Exam Topic 13)

An organization adopts a new firewall hardening standard. How can the security professional verify that the technical staff correct implemented the new standard?

- A. Perform a compliance review
- B. Perform a penetration test
- C. Train the technical staff
- D. Survey the technical staff

Answer: A

Explanation:

Section: Security Operations

NEW QUESTION 650

- (Exam Topic 13)

Which security modes is MOST commonly used in a commercial environment because it protects the integrity of financial and accounting data?

- A. Biba
- B. Graham-Denning
- C. Clark-Wilson
- D. Beil-LaPadula

Answer: C

NEW QUESTION 653

- (Exam Topic 13)

Which one of the following data integrity models assumes a lattice of integrity levels?

- A. Take-Grant
- B. Biba
- C. Harrison-Ruzzo
- D. Bell-LaPadula

Answer: B

NEW QUESTION 658

- (Exam Topic 13)

When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

- A. Log all activities associated with sensitive systems
- B. Provide links to security policies
- C. Confirm that confidentially agreements are signed
- D. Employ strong access controls

Answer: D

NEW QUESTION 663

- (Exam Topic 13)

Which of the following is the BEST reason for writing an information security policy?

- A. To support information security governance
- B. To reduce the number of audit findings
- C. To deter attackers
- D. To implement effective information security controls

Answer: A

NEW QUESTION 665

- (Exam Topic 13)

Even though a particular digital watermark is difficult to detect, which of the following represents a way it might still be inadvertently removed?

- A. Truncating parts of the data
- B. Applying Access Control Lists (ACL) to the data
- C. Appending non-watermarked data to watermarked data
- D. Storing the data in a database

Answer: A

NEW QUESTION 668

- (Exam Topic 13)

Which of the following mandates the amount and complexity of security controls applied to a security risk?

- A. Security vulnerabilities
- B. Risk tolerance
- C. Risk mitigation
- D. Security staff

Answer: C

NEW QUESTION 672

- (Exam Topic 13)

When determining who can accept the risk associated with a vulnerability, which of the following is MOST important?

- A. Countermeasure effectiveness
- B. Type of potential loss
- C. Incident likelihood
- D. Information ownership

Answer: C

NEW QUESTION 674

- (Exam Topic 13)

In a change-controlled environment, which of the following is MOST likely to lead to unauthorized changes to production programs?

- A. Modifying source code without approval
- B. Promoting programs to production without approval
- C. Developers checking out source code without approval
- D. Developers using Rapid Application Development (RAD) methodologies without approval

Answer: A

NEW QUESTION 676

- (Exam Topic 13)

Which of the following is a characteristic of an internal audit?

- A. An internal audit is typically shorter in duration than an external audit.
- B. The internal audit schedule is published to the organization well in advance.
- C. The internal auditor reports to the Information Technology (IT) department
- D. Management is responsible for reading and acting upon the internal audit results

Answer: D

NEW QUESTION 680

- (Exam Topic 13)

Which of the following alarm systems is recommended to detect intrusions through windows in a high-noise, occupied environment?

- A. Acoustic sensor
- B. Motion sensor
- C. Shock sensor
- D. Photoelectric sensor

Answer: C

NEW QUESTION 685

- (Exam Topic 13)

What does electronic vaulting accomplish?

- A. It protects critical files.
- B. It ensures the fault tolerance of Redundant Array of Independent Disks (RAID) systems
- C. It stripes all database records
- D. It automates the Disaster Recovery Process (DRP)

Answer: A

Explanation:

Section: Security Operations

NEW QUESTION 687

- (Exam Topic 13)

The MAIN use of Layer 2 Tunneling Protocol (L2TP) is to tunnel data

- A. through a firewall at the Session layer
- B. through a firewall at the Transport layer
- C. in the Point-to-Point Protocol (PPP)
- D. in the Payload Compression Protocol (PCP)

Answer: C

NEW QUESTION 689

- (Exam Topic 13)

An organization recently conducted a review of the security of its network applications. One of the vulnerabilities found was that the session key used in encrypting sensitive information to a third party server had been hard-coded in the client and server applications. Which of the following would be MOST effective in mitigating this vulnerability?

- A. Diffie-Hellman (DH) algorithm
- B. Elliptic Curve Cryptography (ECC) algorithm
- C. Digital Signature algorithm (DSA)
- D. Rivest-Shamir-Adleman (RSA) algorithm

Answer: D

NEW QUESTION 693

- (Exam Topic 13)

An organization plan on purchasing a custom software product developed by a small vendor to support its business model. Which unique consideration should be made part of the contractual agreement potential long-term risks associated with creating this dependency?

- A. A source code escrow clause
- B. Right to request an independent review of the software source code
- C. Due diligence form requesting statements of compliance with security requirements
- D. Access to the technical documentation

Answer: B

NEW QUESTION 694

- (Exam Topic 13)

Which of the following MUST be scalable to address security concerns raised by the integration of third-party identity services?

- A. Mandatory Access Controls (MAC)
- B. Enterprise security architecture
- C. Enterprise security procedures
- D. Role Based Access Controls (RBAC)

Answer: C

NEW QUESTION 698

- (Exam Topic 13)

Which of the following methods of suppressing a fire is environmentally friendly and the MOST appropriate for a data center?

- A. Inert gas fire suppression system
- B. Halon gas fire suppression system
- C. Dry-pipe sprinklers
- D. Wet-pipe sprinklers

Answer: A

NEW QUESTION 699

- (Exam Topic 13)

Which of the following management process allows ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

- A. Configuration
- B. Identity
- C. Compliance
- D. Patch

Answer: A

NEW QUESTION 704

- (Exam Topic 13)

What can happen when an Intrusion Detection System (IDS) is installed inside a firewall-protected internal network?

- A. The IDS can detect failed administrator logon attempts from servers.
- B. The IDS can increase the number of packets to analyze.
- C. The firewall can increase the number of packets to analyze.
- D. The firewall can detect failed administrator login attempts from servers

Answer: A

NEW QUESTION 707

- (Exam Topic 13)

Which of the following is considered a secure coding practice?

- A. Use concurrent access for shared variables and resources
- B. Use checksums to verify the integrity of libraries
- C. Use new code for common tasks
- D. Use dynamic execution functions to pass user supplied data

Answer: B

NEW QUESTION 710

- (Exam Topic 13)

Drag the following Security Engineering terms on the left to the BEST definition on the right.

<u>Security Engineering Term</u>	<u>Definition</u>
<div>Risk</div>	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
<div>Security Risk Treatment</div>	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
<div>Protection Needs Assessment</div>	The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
<div>Threat Assessment</div>	The method used to identify feasible security risk mitigation options and plans.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Risk - A measure of the extent to which an entity is threatened by a potential circumstance of event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

Protection Needs Assessment - The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should be asset be lost, modified, degraded, disrupted, compromised, or become unavailable.

Threat assessment - The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.

Security Risk Treatment - The method used to identify feasible security risk mitigation options and plans.

NEW QUESTION 714

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 719

- (Exam Topic 12)

When writing security assessment procedures, what is the MAIN purpose of the test outputs and reports?

- A. To force the software to fail and document the process
- B. To find areas of compromise in confidentiality and integrity
- C. To allow for objective pass or fail decisions
- D. To identify malware or hidden code within the test results

Answer: C

NEW QUESTION 720

- (Exam Topic 12)

Which of the following information MUST be provided for user account provisioning?

- A. Full name
- B. Unique identifier
- C. Security question
- D. Date of birth

Answer: B

NEW QUESTION 721

- (Exam Topic 12)

Backup information that is critical to the organization is identified through a

- A. Vulnerability Assessment (VA).
- B. Business Continuity Plan (BCP).
- C. Business Impact Analysis (BIA).
- D. data recovery analysis.

Answer: D

NEW QUESTION 726

- (Exam Topic 12)

Which of the following is the MOST important goal of information asset valuation?

- A. Developing a consistent and uniform method of controlling access on information assets
- B. Developing appropriate access control policies and guidelines
- C. Assigning a financial value to an organization's information assets
- D. Determining the appropriate level of protection

Answer: D

NEW QUESTION 728

- (Exam Topic 12)

Which Radio Frequency Interference (RFI) phenomenon associated with bundled cable runs can create information leakage?

- A. Transference
- B. Covert channel
- C. Bleeding
- D. Cross-talk

Answer: D

NEW QUESTION 730

- (Exam Topic 12)

What balance MUST be considered when web application developers determine how informative application error messages should be constructed?

- A. Risk versus benefit
- B. Availability versus auditability
- C. Confidentiality versus integrity
- D. Performance versus user satisfaction

Answer: A

NEW QUESTION 735

- (Exam Topic 12)

What is a characteristic of Secure Socket Layer (SSL) and Transport Layer Security (TLS)?

- A. SSL and TLS provide a generic channel security mechanism on top of Transmission Control Protocol (TCP).
- B. SSL and TLS provide nonrepudiation by default.
- C. SSL and TLS do not provide security for most routed protocols.
- D. SSL and TLS provide header encapsulation over HyperText Transfer Protocol (HTTP).

Answer: A

NEW QUESTION 740

- (Exam Topic 12)

An organization regularly conducts its own penetration tests. Which of the following scenarios **MUST** be covered for the test to be effective?

- A. Third-party vendor with access to the system
- B. System administrator access compromised
- C. Internal attacker with access to the system
- D. Internal user accidentally accessing data

Answer: B

NEW QUESTION 742

- (Exam Topic 12)

When using Generic Routing Encapsulation (GRE) tunneling over Internet Protocol version 4 (IPv4), where is the GRE header inserted?

- A. Into the options field
- B. Between the delivery header and payload
- C. Between the source and destination addresses
- D. Into the destination address

Answer: B

NEW QUESTION 747

- (Exam Topic 12)

When designing a vulnerability test, which one of the following is likely to give the **BEST** indication of what components currently operate on the network?

- A. Topology diagrams
- B. Mapping tools
- C. Asset register
- D. Ping testing

Answer: B

NEW QUESTION 749

- (Exam Topic 12)

Which of the following is needed to securely distribute symmetric cryptographic keys?

- A. Officially approved Public-Key Infrastructure (PKI) Class 3 or Class 4 certificates
- B. Officially approved and compliant key management technology and processes
- C. An organizationally approved communication protection policy and key management plan
- D. Hardware tokens that protect the user's private key.

Answer: C

NEW QUESTION 753

- (Exam Topic 12)

An application developer is deciding on the amount of idle session time that the application allows before a timeout. The **BEST** reason for determining the session timeout requirement is

- A. organization policy.
- B. industry best practices.
- C. industry laws and regulations.
- D. management feedback.

Answer: A

NEW QUESTION 755

- (Exam Topic 12)

How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

- A. Examines log messages or other indications on the system.
- B. Monitors alarms sent to the system administrator
- C. Matches traffic patterns to virus signature files
- D. Examines the Access Control List (ACL)

Answer: C

NEW QUESTION 758

- (Exam Topic 12)

A company was ranked as high in the following National Institute of Standards and Technology (NIST) functions: Protect, Detect, Respond and Recover. However, a low maturity grade was attributed to the Identify function. In which of the following the controls categories does this company need to improve when analyzing its processes individually?

- A. Asset Management, Business Environment, Governance and Risk Assessment
- B. Access Control, Awareness and Training, Data Security and Maintenance
- C. Anomalies and Events, Security Continuous Monitoring and Detection Processes
- D. Recovery Planning, Improvements and Communications

Answer: A

NEW QUESTION 759

- (Exam Topic 12)

What is the difference between media marking and media labeling?

- A. Media marking refers to the use of human-readable security attributes, while media labeling refers to the use of security attributes in internal data structures.
- B. Media labeling refers to the use of human-readable security attributes, while media marking refers to the use of security attributes in internal data structures.
- C. Media labeling refers to security attributes required by public policy/law, while media marking refers to security required by internal organizational policy.
- D. Media marking refers to security attributes required by public policy/law, while media labeling refers to security attributes required by internal organizational policy.

Answer: D

NEW QUESTION 762

- (Exam Topic 12)

Which of the following is the BEST method to reduce the effectiveness of phishing attacks?

- A. User awareness
- B. Two-factor authentication
- C. Anti-phishing software
- D. Periodic vulnerability scan

Answer: A

NEW QUESTION 764

- (Exam Topic 12)

Which of the following is BEST suited for exchanging authentication and authorization messages in a multi-party decentralized environment?

- A. Lightweight Directory Access Protocol (LDAP)
- B. Security Assertion Markup Language (SAML)
- C. Internet Mail Access Protocol
- D. Transport Layer Security (TLS)

Answer: B

NEW QUESTION 767

- (Exam Topic 12)

Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

- A. Reversal
- B. Gray box
- C. Blind
- D. White box

Answer: C

NEW QUESTION 768

- (Exam Topic 12)

Although code using a specific program language may not be susceptible to a buffer overflow attack,

- A. most calls to plug-in programs are susceptible.
- B. most supporting application code is susceptible.
- C. the graphical images used by the application could be susceptible.
- D. the supporting virtual machine could be susceptible.

Answer: C

NEW QUESTION 772

- (Exam Topic 12)

In general, servers that are facing the Internet should be placed in a demilitarized zone (DMZ). What is MAIN purpose of the DMZ?

- A. Reduced risk to internal systems.
- B. Prepare the server for potential attacks.
- C. Mitigate the risk associated with the exposed server.
- D. Bypass the need for a firewall.

Answer: A

NEW QUESTION 774

- (Exam Topic 12)

Match the access control type to the example of the control type. Drag each access control type net to its corresponding example.

Access Control Type		Example
Administrative		Labeling of sensitive data
Technical		Biometrics for authentication
Logical		Constrained user interface
Physical		Radio Frequency Identification (RFID) badge

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Administrative – labeling of sensitive data
Technical – Constrained user interface
Logical – Biometrics for authentication
Physical – Radio Frequency Identification 9RFID) badge

NEW QUESTION 776

- (Exam Topic 11)

Which of the following PRIMARILY contributes to security incidents in web-based applications?

- A. Systems administration and operating systems
- B. System incompatibility and patch management
- C. Third-party applications and change controls
- D. Improper stress testing and application interfaces

Answer: C

NEW QUESTION 781

- (Exam Topic 11)

Order the below steps to create an effective vulnerability management process.

Step		Order
Identify risks		1
Implement patch deployment		2
Implement recurring scanning schedule		3
Identify assets		4
Implement change management		5

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Step		Order
Identify risks	Identify assets	1
Implement patch deployment	Identify risks	2
Implement recurring scanning schedule	Implement change management	3
Identify assets	Implement patch deployment	4
Implement change management	Implement recurring scanning schedule	5

NEW QUESTION 785

- (Exam Topic 11)

Which of the following could elicit a Denial of Service (DoS) attack against a credential management system?

- A. Delayed revocation or destruction of credentials
B. Modification of Certificate Revocation List
C. Unauthorized renewal or re-issuance
D. Token use after decommissioning

Answer: B

NEW QUESTION 786

- (Exam Topic 11)

An organization has decided to contract with a cloud-based service provider to leverage their identity as a service offering. They will use Open Authentication (OAuth) 2.0 to authenticate external users to the organization's services.

As part of the authentication process, which of the following must the end user provide?

- A. An access token
B. A username and password
C. A username
D. A password

Answer: A

NEW QUESTION 790

- (Exam Topic 11)

Which of the following is a recommended alternative to an integrated email encryption system?

- A. Sign emails containing sensitive data
- B. Send sensitive data in separate emails
- C. Encrypt sensitive data separately in attachments
- D. Store sensitive information to be sent in encrypted drives

Answer: C

NEW QUESTION 793

- (Exam Topic 11)

Which of the following is the BEST example of weak management commitment to the protection of security assets and resources?

- A. poor governance over security processes and procedures
- B. immature security controls and procedures
- C. variances against regulatory requirements
- D. unanticipated increases in security incidents and threats

Answer: A

NEW QUESTION 797

- (Exam Topic 11)

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

- A. Document the system as high risk
- B. Perform a vulnerability assessment
- C. Perform a quantitative threat assessment
- D. Notate the information and move on

Answer: B

NEW QUESTION 801

- (Exam Topic 11)

Which of the following is the PRIMARY benefit of implementing data-in-use controls?

- A. If the data is lost, it must be decrypted to be opened.
- B. If the data is lost, it will not be accessible to unauthorized users.
- C. When the data is being viewed, it can only be printed by authorized users.
- D. When the data is being viewed, it must be accessed using secure protocols.

Answer: C

NEW QUESTION 803

- (Exam Topic 11)

Data leakage of sensitive information is MOST often concealed by which of the following?

- A. Secure Sockets Layer (SSL)
- B. Secure Hash Algorithm (SHA)
- C. Wired Equivalent Privacy (WEP)
- D. Secure Post Office Protocol (POP)

Answer: A

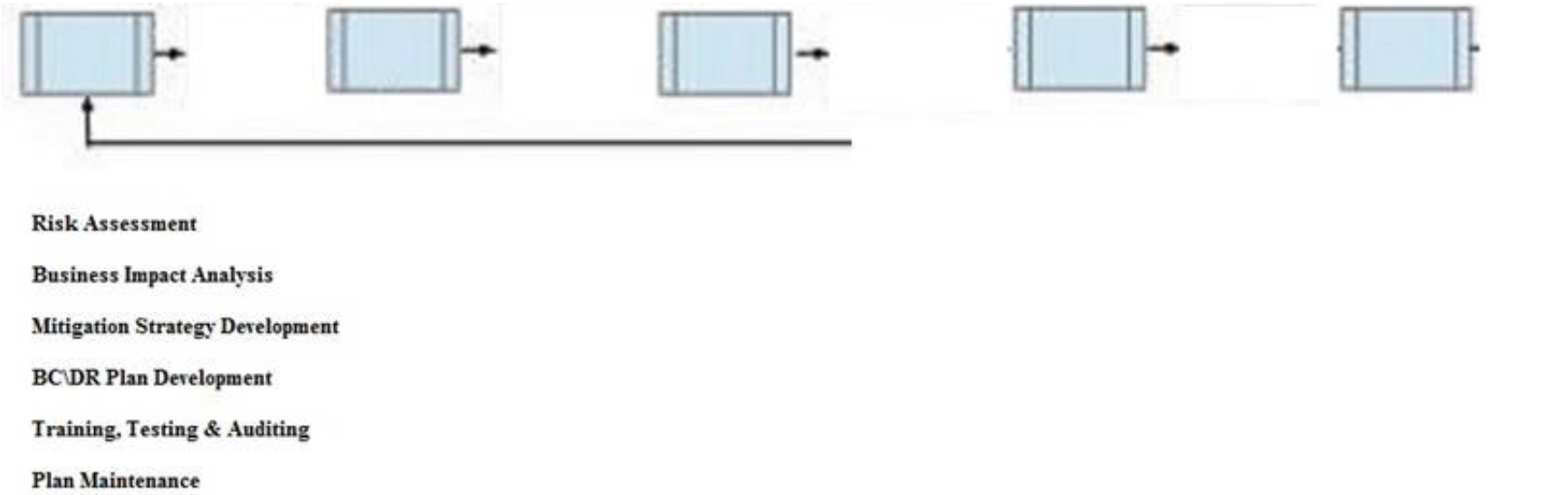
NEW QUESTION 804

- (Exam Topic 11)

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

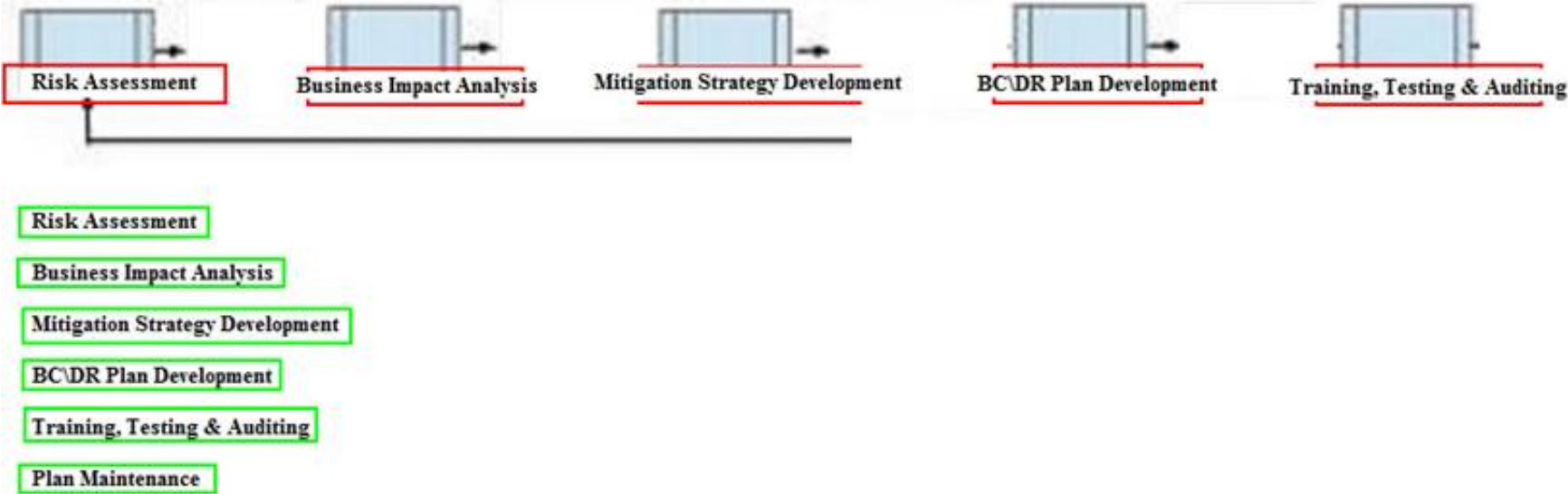
Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 808

.....

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](#)