

# ISC2

## Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)



#### NEW QUESTION 1

- (Exam Topic 1)

An important principle of defense in depth is that achieving information security requires a balanced focus on which PRIMARY elements?

- A. Development, testing, and deployment
- B. Prevention, detection, and remediation
- C. People, technology, and operations
- D. Certification, accreditation, and monitoring

Answer: C

#### NEW QUESTION 2

- (Exam Topic 1)

When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined?

- A. Only when assets are clearly defined
- B. Only when standards are defined
- C. Only when controls are put in place
- D. Only procedures are defined

Answer: A

#### NEW QUESTION 3

- (Exam Topic 1)

All of the following items should be included in a Business Impact Analysis (BIA) questionnaire EXCEPT questions that

- A. determine the risk of a business interruption occurring
- B. determine the technological dependence of the business processes
- C. Identify the operational impacts of a business interruption
- D. Identify the financial impacts of a business interruption

Answer: B

#### NEW QUESTION 4

- (Exam Topic 1)

Which of the following actions will reduce risk to a laptop before traveling to a high risk area?

- A. Examine the device for physical tampering
- B. Implement more stringent baseline configurations
- C. Purge or re-image the hard disk drive
- D. Change access codes

Answer: D

#### NEW QUESTION 5

- (Exam Topic 1)

Which of the following types of technologies would be the MOST cost-effective method to provide a reactive control for protecting personnel in public areas?

- A. Install mantraps at the building entrances
- B. Enclose the personnel entry area with polycarbonate plastic
- C. Supply a duress alarm for personnel exposed to the public
- D. Hire a guard to protect the public area

Answer: D

#### NEW QUESTION 6

- (Exam Topic 1)

What is the MOST important consideration from a data security perspective when an organization plans to relocate?

- A. Ensure the fire prevention and detection systems are sufficient to protect personnel
- B. Review the architectural plans to determine how many emergency exits are present
- C. Conduct a gap analysis of a new facilities against existing security requirements
- D. Revise the Disaster Recovery and Business Continuity (DR/BC) plan

Answer: C

#### NEW QUESTION 7

- (Exam Topic 2)

In a data classification scheme, the data is owned by the

- A. system security managers
- B. business managers
- C. Information Technology (IT) managers
- D. end users

Answer: B

**NEW QUESTION 8**

- (Exam Topic 2)

Which of the following is an effective control in preventing electronic cloning of Radio Frequency Identification (RFID) based access cards?

- A. Personal Identity Verification (PIV)
- B. Cardholder Unique Identifier (CHUID) authentication
- C. Physical Access Control System (PACS) repeated attempt detection
- D. Asymmetric Card Authentication Key (CAK) challenge-response

Answer: C

**NEW QUESTION 9**

- (Exam Topic 2)

When implementing a data classification program, why is it important to avoid too much granularity?

- A. The process will require too many resources
- B. It will be difficult to apply to both hardware and software
- C. It will be difficult to assign ownership to the data
- D. The process will be perceived as having value

Answer: A

**NEW QUESTION 10**

- (Exam Topic 2)

Which of the following is MOST important when assigning ownership of an asset to a department?

- A. The department should report to the business owner
- B. Ownership of the asset should be periodically reviewed
- C. Individual accountability should be ensured
- D. All members should be trained on their responsibilities

Answer: B

**NEW QUESTION 10**

- (Exam Topic 3)

Which component of the Security Content Automation Protocol (SCAP) specification contains the data required to estimate the severity of vulnerabilities identified automated vulnerability assessments?

- A. Common Vulnerabilities and Exposures (CVE)
- B. Common Vulnerability Scoring System (CVSS)
- C. Asset Reporting Format (ARF)
- D. Open Vulnerability and Assessment Language (OVAL)

Answer: B

**NEW QUESTION 11**

- (Exam Topic 3)

Which technique can be used to make an encryption scheme more resistant to a known plaintext attack?

- A. Hashing the data before encryption
- B. Hashing the data after encryption
- C. Compressing the data after encryption
- D. Compressing the data before encryption

Answer: A

**NEW QUESTION 14**

- (Exam Topic 4)

An external attacker has compromised an organization's network security perimeter and installed a sniffer onto an inside computer. Which of the following is the MOST effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information?

- A. Implement packet filtering on the network firewalls
- B. Install Host Based Intrusion Detection Systems (HIDS)
- C. Require strong authentication for administrators
- D. Implement logical network segmentation at the switches

Answer: D

**NEW QUESTION 19**

- (Exam Topic 4)

Which of the following is used by the Point-to-Point Protocol (PPP) to determine packet formats?

- A. Layer 2 Tunneling Protocol (L2TP)

- B. Link Control Protocol (LCP)
- C. Challenge Handshake Authentication Protocol (CHAP)
- D. Packet Transfer Protocol (PTP)

**Answer:** B

**NEW QUESTION 20**

- (Exam Topic 4)

Which of the following factors contributes to the weakness of Wired Equivalent Privacy (WEP) protocol?

- A. WEP uses a small range Initialization Vector (IV)
- B. WEP uses Message Digest 5 (MD5)
- C. WEP uses Diffie-Hellman
- D. WEP does not use any Initialization Vector (IV)

**Answer:** A

**NEW QUESTION 25**

- (Exam Topic 5)

Which of the following BEST describes an access control method utilizing cryptographic keys derived from a smart card private key that is embedded within mobile devices?

- A. Derived credential
- B. Temporary security credential
- C. Mobile device credentialing service
- D. Digest authentication

**Answer:** A

**NEW QUESTION 30**

- (Exam Topic 7)

Recovery strategies of a Disaster Recovery planning (DRIP) MUST be aligned with which of the following?

- A. Hardware and software compatibility issues
- B. Applications' critically and downtime tolerance
- C. Budget constraints and requirements
- D. Cost/benefit analysis and business objectives

**Answer:** D

**NEW QUESTION 34**

- (Exam Topic 7)

What would be the MOST cost effective solution for a Disaster Recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours?

- A. Warm site
- B. Hot site
- C. Mirror site
- D. Cold site

**Answer:** A

**NEW QUESTION 38**

- (Exam Topic 7)

What is the MOST important step during forensic analysis when trying to learn the purpose of an unknown application?

- A. Disable all unnecessary services
- B. Ensure chain of custody
- C. Prepare another backup of the system
- D. Isolate the system from the network

**Answer:** D

**NEW QUESTION 43**

- (Exam Topic 7)

With what frequency should monitoring of a control occur when implementing Information Security Continuous Monitoring (ISCM) solutions?

- A. Continuously without exception for all security controls
- B. Before and after each change of the control
- C. At a rate concurrent with the volatility of the security control
- D. Only during system implementation and decommissioning

**Answer:** B

**NEW QUESTION 46**

- (Exam Topic 7)

When is a Business Continuity Plan (BCP) considered to be valid?

- A. When it has been validated by the Business Continuity (BC) manager
- B. When it has been validated by the board of directors
- C. When it has been validated by all threat scenarios
- D. When it has been validated by realistic exercises

**Answer: D**

#### **NEW QUESTION 48**

- (Exam Topic 7)

Which of the following is the FIRST step in the incident response process?

- A. Determine the cause of the incident
- B. Disconnect the system involved from the network
- C. Isolate and contain the system involved
- D. Investigate all symptoms to confirm the incident

**Answer: D**

#### **NEW QUESTION 50**

- (Exam Topic 8)

What is the BEST approach to addressing security issues in legacy web applications?

- A. Debug the security issues
- B. Migrate to newer, supported applications where possible
- C. Conduct a security assessment
- D. Protect the legacy application with a web application firewall

**Answer: D**

#### **NEW QUESTION 55**

- (Exam Topic 9)

What is the FIRST step in developing a security test and its evaluation?

- A. Determine testing methods
- B. Develop testing procedures
- C. Identify all applicable security requirements
- D. Identify people, processes, and products not in compliance

**Answer: C**

#### **NEW QUESTION 58**

- (Exam Topic 9)

Which of the following is a method used to prevent Structured Query Language (SQL) injection attacks?

- A. Data compression
- B. Data classification
- C. Data warehousing
- D. Data validation

**Answer: D**

#### **NEW QUESTION 60**

- (Exam Topic 9)

The three PRIMARY requirements for a penetration test are

- A. A defined goal, limited time period, and approval of management
- B. A general objective, unlimited time, and approval of the network administrator
- C. An objective statement, disclosed methodology, and fixed cost
- D. A stated objective, liability waiver, and disclosed methodology

**Answer: A**

#### **NEW QUESTION 65**

- (Exam Topic 9)

Which of the following is the FIRST action that a system administrator should take when it is revealed during a penetration test that everyone in an organization has unauthorized access to a server holding sensitive data?

- A. Immediately document the finding and report to senior management.
- B. Use system privileges to alter the permissions to secure the server
- C. Continue the testing to its completion and then inform IT management
- D. Terminate the penetration test and pass the finding to the server management team

**Answer: A**

**NEW QUESTION 66**

- (Exam Topic 9)

Which of the following MUST be part of a contract to support electronic discovery of data stored in a cloud environment?

- A. Integration with organizational directory services for authentication
- B. Tokenization of data
- C. Accommodation of hybrid deployment models
- D. Identification of data location

**Answer: D**

**NEW QUESTION 69**

- (Exam Topic 9)

To prevent inadvertent disclosure of restricted information, which of the following would be the LEAST effective process for eliminating data prior to the media being discarded?

- A. Multiple-pass overwriting
- B. Degaussing
- C. High-level formatting
- D. Physical destruction

**Answer: C**

**NEW QUESTION 72**

- (Exam Topic 9)

Which one of the following is a threat related to the use of web-based client side input validation?

- A. Users would be able to alter the input after validation has occurred
- B. The web server would not be able to validate the input after transmission
- C. The client system could receive invalid input from the web server
- D. The web server would not be able to receive invalid input from the client

**Answer: A**

**NEW QUESTION 76**

- (Exam Topic 9)

Contingency plan exercises are intended to do which of the following?

- A. Train personnel in roles and responsibilities
- B. Validate service level agreements
- C. Train maintenance personnel
- D. Validate operation metrics

**Answer: A**

**NEW QUESTION 80**

- (Exam Topic 9)

Which of the following is a physical security control that protects Automated Teller Machines (ATM) from skimming?

- A. Anti-tampering
- B. Secure card reader
- C. Radio Frequency (RF) scanner
- D. Intrusion Prevention System (IPS)

**Answer: A**

**NEW QUESTION 81**

- (Exam Topic 9)

What technique BEST describes antivirus software that detects viruses by watching anomalous behavior?

- A. Signature
- B. Inference
- C. Induction
- D. Heuristic

**Answer: D**

**NEW QUESTION 82**

- (Exam Topic 9)

An internal Service Level Agreement (SLA) covering security is signed by senior managers and is in place. When should compliance to the SLA be reviewed to ensure that a good security posture is being delivered?

- A. As part of the SLA renewal process
- B. Prior to a planned security audit
- C. Immediately after a security breach
- D. At regularly scheduled meetings

**Answer:** D

**NEW QUESTION 86**

- (Exam Topic 9)

The overall goal of a penetration test is to determine a system's

- A. ability to withstand an attack.
- B. capacity management.
- C. error recovery capabilities.
- D. reliability under stress.

**Answer:** A

**NEW QUESTION 91**

- (Exam Topic 9)

Including a Trusted Platform Module (TPM) in the design of a computer system is an example of a technique to what?

- A. Interface with the Public Key Infrastructure (PKI)
- B. Improve the quality of security software
- C. Prevent Denial of Service (DoS) attacks
- D. Establish a secure initial state

**Answer:** D

**NEW QUESTION 92**

- (Exam Topic 9)

Which one of these risk factors would be the LEAST important consideration in choosing a building site for a new computer facility?

- A. Vulnerability to crime
- B. Adjacent buildings and businesses
- C. Proximity to an airline flight path
- D. Vulnerability to natural disasters

**Answer:** C

**NEW QUESTION 96**

- (Exam Topic 9)

An advantage of link encryption in a communications network is that it

- A. makes key management and distribution easier.
- B. protects data from start to finish through the entire network.
- C. improves the efficiency of the transmission.
- D. encrypts all information, including headers and routing information.

**Answer:** D

**NEW QUESTION 99**

- (Exam Topic 9)

Which of the following is the best practice for testing a Business Continuity Plan (BCP)?

- A. Test before the IT Audit
- B. Test when environment changes
- C. Test after installation of security patches
- D. Test after implementation of system patches

**Answer:** B

**NEW QUESTION 104**

- (Exam Topic 9)

As one component of a physical security system, an Electronic Access Control (EAC) token is BEST known for its ability to

- A. overcome the problems of key assignments.
- B. monitor the opening of windows and doors.
- C. trigger alarms when intruders are detected.
- D. lock down a facility during an emergency.

**Answer:** A

**NEW QUESTION 107**

- (Exam Topic 9)

Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

- A. Standards, policies, and procedures
- B. Tactical, strategic, and financial
- C. Management, operational, and technical

D. Documentation, observation, and manual

**Answer: C**

**NEW QUESTION 108**

- (Exam Topic 9)

The PRIMARY purpose of a security awareness program is to

- A. ensure that everyone understands the organization's policies and procedures.
- B. communicate that access to information will be granted on a need-to-know basis.
- C. warn all users that access to all systems will be monitored on a daily basis.
- D. comply with regulations related to data and information protection.

**Answer: A**

**NEW QUESTION 112**

- (Exam Topic 9)

The BEST method of demonstrating a company's security level to potential customers is

- A. a report from an external auditor.
- B. responding to a customer's security questionnaire.
- C. a formal report from an internal auditor.
- D. a site visit by a customer's security team.

**Answer: A**

**NEW QUESTION 117**

- (Exam Topic 9)

Which of the following does the Encapsulating Security Payload (ESP) provide?

- A. Authorization and integrity
- B. Availability and integrity
- C. Integrity and confidentiality
- D. Authorization and confidentiality

**Answer: C**

**NEW QUESTION 119**

- (Exam Topic 9)

Which one of the following is the MOST important in designing a biometric access system if it is essential that no one other than authorized individuals are admitted?

- A. False Acceptance Rate (FAR)
- B. False Rejection Rate (FRR)
- C. Crossover Error Rate (CER)
- D. Rejection Error Rate

**Answer: A**

**NEW QUESTION 121**

- (Exam Topic 9)

A practice that permits the owner of a data object to grant other users access to that object would usually provide

- A. Mandatory Access Control (MAC).
- B. owner-administered control.
- C. owner-dependent access control.
- D. Discretionary Access Control (DAC).

**Answer: D**

**NEW QUESTION 125**

- (Exam Topic 9)

Which of the following is a security feature of Global Systems for Mobile Communications (GSM)?

- A. It uses a Subscriber Identity Module (SIM) for authentication.
- B. It uses encrypting techniques for all communications.
- C. The radio spectrum is divided with multiple frequency carriers.
- D. The signal is difficult to read as it provides end-to-end encryption.

**Answer: A**

**NEW QUESTION 130**

- (Exam Topic 9)

Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?

- A. Transparent Database Encryption (TDE)
- B. Column level database encryption
- C. Volume encryption
- D. Data tokenization

**Answer: D**

**NEW QUESTION 132**

- (Exam Topic 9)

An auditor carrying out a compliance audit requests passwords that are encrypted in the system to verify that the passwords are compliant with policy. Which of the following is the BEST response to the auditor?

- A. Provide the encrypted passwords and analysis tools to the auditor for analysis.
- B. Analyze the encrypted passwords for the auditor and show them the results.
- C. Demonstrate that non-compliant passwords cannot be created in the system.
- D. Demonstrate that non-compliant passwords cannot be encrypted in the system.

**Answer: C**

**NEW QUESTION 135**

- (Exam Topic 9)

The use of strong authentication, the encryption of Personally Identifiable Information (PII) on database servers, application security reviews, and the encryption of data transmitted across networks provide

- A. data integrity.
- B. defense in depth.
- C. data availability.
- D. non-repudiation.

**Answer: B**

**NEW QUESTION 139**

- (Exam Topic 9)

Which of the following is the MOST important consideration when storing and processing Personally Identifiable Information (PII)?

- A. Encrypt and hash all PII to avoid disclosure and tampering.
- B. Store PII for no more than one year.
- C. Avoid storing PII in a Cloud Service Provider.
- D. Adherence to collection limitation laws and regulations.

**Answer: D**

**NEW QUESTION 144**

- (Exam Topic 9)

What would be the PRIMARY concern when designing and coordinating a security assessment for an Automatic Teller Machine (ATM) system?

- A. Physical access to the electronic hardware
- B. Regularly scheduled maintenance process
- C. Availability of the network connection
- D. Processing delays

**Answer: A**

**NEW QUESTION 148**

- (Exam Topic 9)

Which of the following is the MAIN reason that system re-certification and re-accreditation are needed?

- A. To assist data owners in making future sensitivity and criticality determinations
- B. To assure the software development team that all security issues have been addressed
- C. To verify that security protection remains acceptable to the organizational security policy
- D. To help the security team accept or reject new systems for implementation and production

**Answer: C**

**NEW QUESTION 149**

- (Exam Topic 9)

Which of the following is a security limitation of File Transfer Protocol (FTP)?

- A. Passive FTP is not compatible with web browsers.
- B. Anonymous access is allowed.
- C. FTP uses Transmission Control Protocol (TCP) ports 20 and 21.
- D. Authentication is not encrypted.

**Answer: D**

**NEW QUESTION 154**

- (Exam Topic 9)

Which one of the following effectively obscures network addresses from external exposure when implemented on a firewall or router?

- A. Network Address Translation (NAT)
- B. Application Proxy
- C. Routing Information Protocol (RIP) Version 2
- D. Address Masking

**Answer: A**

#### **NEW QUESTION 157**

- (Exam Topic 9)

In Business Continuity Planning (BCP), what is the importance of documenting business processes?

- A. Provides senior management with decision-making tools
- B. Establishes and adopts ongoing testing and maintenance strategies
- C. Defines who will perform which functions during a disaster or emergency
- D. Provides an understanding of the organization's interdependencies

**Answer: D**

#### **NEW QUESTION 162**

- (Exam Topic 9)

What principle requires that changes to the plaintext affect many parts of the ciphertext?

- A. Diffusion
- B. Encapsulation
- C. Obfuscation
- D. Permutation

**Answer: A**

#### **NEW QUESTION 167**

- (Exam Topic 9)

The birthday attack is MOST effective against which one of the following cipher technologies?

- A. Chaining block encryption
- B. Asymmetric cryptography
- C. Cryptographic hash
- D. Streaming cryptography

**Answer: C**

#### **NEW QUESTION 168**

- (Exam Topic 9)

A disadvantage of an application filtering firewall is that it can lead to

- A. a crash of the network as a result of user activities.
- B. performance degradation due to the rules applied.
- C. loss of packets on the network due to insufficient bandwidth.
- D. Internet Protocol (IP) spoofing by hackers.

**Answer: B**

#### **NEW QUESTION 171**

- (Exam Topic 9)

What is an effective practice when returning electronic storage media to third parties for repair?

- A. Ensuring the media is not labeled in any way that indicates the organization's name.
- B. Disassembling the media and removing parts that may contain sensitive data.
- C. Physically breaking parts of the media that may contain sensitive data.
- D. Establishing a contract with the third party regarding the secure handling of the media.

**Answer: D**

#### **NEW QUESTION 172**

- (Exam Topic 9)

Which of the following elements MUST a compliant EU-US Safe Harbor Privacy Policy contain?

- A. An Explanation: of how long the data subject's collected information will be retained for and how it will be eventually disposed.
- B. An Explanation: of who can be contacted at the organization collecting the information if corrections are required by the data subject.
- C. An Explanation: of the regulatory frameworks and compliance standards the information collecting organization adheres to.
- D. An Explanation: of all the technologies employed by the collecting organization in gathering information on the data subject.

**Answer: B**

**NEW QUESTION 174**

- (Exam Topic 9)

In a basic SYN flood attack, what is the attacker attempting to achieve?

- A. Exceed the threshold limit of the connection queue for a given service
- B. Set the threshold to zero for a given service
- C. Cause the buffer to overflow, allowing root access
- D. Flush the register stack, allowing hijacking of the root account

**Answer: A**

**NEW QUESTION 179**

- (Exam Topic 9)

Which of the following is a network intrusion detection technique?

- A. Statistical anomaly
- B. Perimeter intrusion
- C. Port scanning
- D. Network spoofing

**Answer: A**

**NEW QUESTION 182**

- (Exam Topic 9)

In a data classification scheme, the data is owned by the

- A. Information Technology (IT) managers.
- B. business managers.
- C. end users.
- D. system security managers.

**Answer: B**

**NEW QUESTION 187**

- (Exam Topic 9)

While impersonating an Information Security Officer (ISO), an attacker obtains information from company employees about their User IDs and passwords. Which method of information gathering has the attacker used?

- A. Trusted path
- B. Malicious logic
- C. Social engineering
- D. Passive misuse

**Answer: C**

**NEW QUESTION 188**

- (Exam Topic 9)

Which of the following actions should be performed when implementing a change to a database schema in a production system?

- A. Test in development, determine dates, notify users, and implement in production
- B. Apply change to production, run in parallel, finalize change in production, and develop a back-out strategy
- C. Perform user acceptance testing in production, have users sign off, and finalize change
- D. Change in development, perform user acceptance testing, develop a back-out strategy, and implement change

**Answer: D**

**NEW QUESTION 189**

- (Exam Topic 9)

Who must approve modifications to an organization's production infrastructure configuration?

- A. Technical management
- B. Change control board
- C. System operations
- D. System users

**Answer: B**

**NEW QUESTION 191**

- (Exam Topic 9)

What is the MOST important purpose of testing the Disaster Recovery Plan (DRP)?

- A. Evaluating the efficiency of the plan
- B. Identifying the benchmark required for restoration
- C. Validating the effectiveness of the plan
- D. Determining the Recovery Time Objective (RTO)

**Answer:**

C

**NEW QUESTION 195**

- (Exam Topic 9)

Which of the following is a potential risk when a program runs in privileged mode?

- A. It may serve to create unnecessary code complexity
- B. It may not enforce job separation duties
- C. It may create unnecessary application hardening
- D. It may allow malicious code to be inserted

**Answer: D**

**NEW QUESTION 199**

- (Exam Topic 9)

Passive Infrared Sensors (PIR) used in a non-climate controlled environment should

- A. reduce the detected object temperature in relation to the background temperature.
- B. increase the detected object temperature in relation to the background temperature.
- C. automatically compensate for variance in background temperature.
- D. detect objects of a specific temperature independent of the background temperature.

**Answer: C**

**NEW QUESTION 200**

- (Exam Topic 9)

Which of the following **MUST** be done when promoting a security awareness program to senior management?

- A. Show the need for security; identify the message and the audience
- B. Ensure that the security presentation is designed to be all-inclusive
- C. Notify them that their compliance is mandatory
- D. Explain how hackers have enhanced information security

**Answer: A**

**NEW QUESTION 205**

- (Exam Topic 9)

What is the **MOST** effective countermeasure to a malicious code attack against a mobile system?

- A. Sandbox
- B. Change control
- C. Memory management
- D. Public-Key Infrastructure (PKI)

**Answer: A**

**NEW QUESTION 206**

- (Exam Topic 9)

An organization is designing a large enterprise-wide document repository system. They plan to have several different classification level areas with increasing levels of controls. The **BEST** way to ensure document confidentiality in the repository is to

- A. encrypt the contents of the repository and document any exceptions to that requirement.
- B. utilize Intrusion Detection System (IDS) set drop connections if too many requests for documents are detected.
- C. keep individuals with access to high security areas from saving those documents into lower security areas.
- D. require individuals with access to the system to sign Non-Disclosure Agreements (NDA).

**Answer: C**

**NEW QUESTION 210**

- (Exam Topic 9)

Which of the following does Temporal Key Integrity Protocol (TKIP) support?

- A. Multicast and broadcast messages
- B. Coordination of IEEE 802.11 protocols
- C. Wired Equivalent Privacy (WEP) systems
- D. Synchronization of multiple devices

**Answer: C**

**NEW QUESTION 214**

- (Exam Topic 9)

Why must all users be positively identified prior to using multi-user computers?

- A. To provide access to system privileges
- B. To provide access to the operating system
- C. To ensure that unauthorized persons cannot access the computers

D. To ensure that management knows what users are currently logged on

**Answer: C**

**NEW QUESTION 216**

- (Exam Topic 9)

An engineer in a software company has created a virus creation tool. The tool can generate thousands of polymorphic viruses. The engineer is planning to use the tool in a controlled environment to test the company's next generation virus scanning software. Which would BEST describe the behavior of the engineer and why?

- A. The behavior is ethical because the tool will be used to create a better virus scanner.
- B. The behavior is ethical because any experienced programmer could create such a tool.
- C. The behavior is not ethical because creating any kind of virus is bad.
- D. The behavior is not ethical because such a tool could be leaked on the Internet.

**Answer: A**

**NEW QUESTION 219**

- (Exam Topic 9)

Which of the following Disaster Recovery (DR) sites is the MOST difficult to test?

- A. Hot site
- B. Cold site
- C. Warm site
- D. Mobile site

**Answer: B**

**NEW QUESTION 222**

- (Exam Topic 9)

Which of the following statements is TRUE of black box testing?

- A. Only the functional specifications are known to the test planner.
- B. Only the source code and the design documents are known to the test planner.
- C. Only the source code and functional specifications are known to the test planner.
- D. Only the design documents and the functional specifications are known to the test planner.

**Answer: A**

**NEW QUESTION 224**

- (Exam Topic 9)

Two companies wish to share electronic inventory and purchase orders in a supplier and client relationship. What is the BEST security solution for them?

- A. Write a Service Level Agreement (SLA) for the two companies.
- B. Set up a Virtual Private Network (VPN) between the two companies.
- C. Configure a firewall at the perimeter of each of the two companies.
- D. Establish a File Transfer Protocol (FTP) connection between the two companies.

**Answer: B**

**NEW QUESTION 228**

- (Exam Topic 9)

At a MINIMUM, a formal review of any Disaster Recovery Plan (DRP) should be conducted

- A. monthly.
- B. quarterly.
- C. annually.
- D. bi-annually.

**Answer: C**

**NEW QUESTION 230**

- (Exam Topic 10)

Refer to the information below to answer the question.

A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.

Which of the following solutions would have MOST likely detected the use of peer-to-peer programs when the computer was connected to the office network?

- A. Anti-virus software
- B. Intrusion Prevention System (IPS)
- C. Anti-spyware software
- D. Integrity checking software

**Answer: B**

**NEW QUESTION 234**

- (Exam Topic 10)

Which of the following violates identity and access management best practices?

- A. User accounts
- B. System accounts
- C. Generic accounts
- D. Privileged accounts

**Answer: C**

**NEW QUESTION 239**

- (Exam Topic 10)

Which of the following is the BEST reason to review audit logs periodically?

- A. Verify they are operating properly
- B. Monitor employee productivity
- C. Identify anomalies in use patterns
- D. Meet compliance regulations

**Answer: C**

**NEW QUESTION 242**

- (Exam Topic 10)

When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?

- A. Perform a service provider PCI-DSS assessment on a yearly basis.
- B. Validate the service provider's PCI-DSS compliance status on a regular basis.
- C. Validate that the service providers security policies are in alignment with those of the organization.
- D. Ensure that the service provider updates and tests its Disaster Recovery Plan (DRP) on a yearly basis.

**Answer: B**

**NEW QUESTION 244**

- (Exam Topic 10)

Which of the following provides effective management assurance for a Wireless Local Area Network (WLAN)?

- A. Maintaining an inventory of authorized Access Points (AP) and connecting devices
- B. Setting the radio frequency to the minimum range required
- C. Establishing a Virtual Private Network (VPN) tunnel between the WLAN client device and a VPN concentrator
- D. Verifying that all default passwords have been changed

**Answer: A**

**NEW QUESTION 249**

- (Exam Topic 10)

During an investigation of database theft from an organization's web site, it was determined that the Structured Query Language (SQL) injection technique was used despite input validation with client-side scripting. Which of the following provides the GREATEST protection against the same attack occurring again?

- A. Encrypt communications between the servers
- B. Encrypt the web server traffic
- C. Implement server-side filtering
- D. Filter outgoing traffic at the perimeter firewall

**Answer: C**

**NEW QUESTION 253**

- (Exam Topic 10)

If an attacker in a SYN flood attack uses someone else's valid host address as the source address, the system under attack will send a large number of Synchronize/Acknowledge (SYN/ACK) packets to the

- A. default gateway.
- B. attacker's address.
- C. local interface being attacked.
- D. specified source address.

**Answer: D**

**NEW QUESTION 255**

- (Exam Topic 10)

Refer to the information below to answer the question.

During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.

If it is discovered that large quantities of information have been copied by the unauthorized individual, what attribute of the data has been compromised?

- A. Availability
- B. Integrity

- C. Accountability
- D. Confidentiality

**Answer:** D

**NEW QUESTION 260**

- (Exam Topic 10)

According to best practice, which of the following is required when implementing third party software in a production environment?

- A. Scan the application for vulnerabilities
- B. Contract the vendor for patching
- C. Negotiate end user application training
- D. Escrow a copy of the software

**Answer:** A

**NEW QUESTION 262**

- (Exam Topic 10)

Which item below is a federated identity standard?

- A. 802.11i
- B. Kerberos
- C. Lightweight Directory Access Protocol (LDAP)
- D. Security Assertion Markup Language (SAML)

**Answer:** D

**NEW QUESTION 265**

- (Exam Topic 10)

What is the MOST effective method for gaining unauthorized access to a file protected with a long complex password?

- A. Brute force attack
- B. Frequency analysis
- C. Social engineering
- D. Dictionary attack

**Answer:** C

**NEW QUESTION 266**

- (Exam Topic 10)

Multi-Factor Authentication (MFA) is necessary in many systems given common types of password attacks. Which of the following is a correct list of password attacks?

- A. Masquerading, salami, malware, polymorphism
- B. Brute force, dictionary, phishing, keylogger
- C. Zeus, netbus, rabbit, turtle
- D. Token, biometrics, IDS, DLP

**Answer:** B

**NEW QUESTION 270**

- (Exam Topic 10)

Refer to the information below to answer the question.

A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization. The third party needs to have

- A. processes that are identical to that of the organization doing the outsourcing.
- B. access to the original personnel that were on staff at the organization.
- C. the ability to maintain all of the applications in languages they are familiar with.
- D. access to the skill sets consistent with the programming languages used by the organization.

**Answer:** D

**NEW QUESTION 273**

- (Exam Topic 10)

Which of the following BEST mitigates a replay attack against a system using identity federation and Security Assertion Markup Language (SAML) implementation?

- A. Two-factor authentication
- B. Digital certificates and hardware tokens
- C. Timed sessions and Secure Socket Layer (SSL)
- D. Passwords with alpha-numeric and special characters

**Answer:** C

**NEW QUESTION 277**

- (Exam Topic 10)

Given the various means to protect physical and logical assets, match the access management area to the technology.

Area		Technolog
Facilities		Encryption
Devices		Window
Information		Firewall
Systems		Authenticatid

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Area		Technolog
Facilities	Information	Encryption
Devices	Facilities	Window
Information	Devices	Firewall
Svstems	Systems	Authenticatid

**NEW QUESTION 279**

- (Exam Topic 10)

Refer to the information below to answer the question.

A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.

What MUST the access control logs contain in addition to the identifier?

- A. Time of the access
- B. Security classification
- C. Denied access attempts
- D. Associated clearance

Answer: A

**NEW QUESTION 282**

- (Exam Topic 10)

Which of the following is a MAJOR consideration in implementing a Voice over IP (VoIP) network?

- A. Use of a unified messaging.
- B. Use of separation for the voice network.
- C. Use of Network Access Control (NAC) on switches.
- D. Use of Request for Comments (RFC) 1918 addressing.

Answer: B

**NEW QUESTION 283**

- (Exam Topic 10)

Refer to the information below to answer the question.

A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.

Which of the following documents explains the proper use of the organization's assets?

- A. Human resources policy
- B. Acceptable use policy
- C. Code of ethics
- D. Access control policy

Answer: B

#### NEW QUESTION 285

- (Exam Topic 10)

Which of the following is the BEST solution to provide redundancy for telecommunications links?

- A. Provide multiple links from the same telecommunications vendor.
- B. Ensure that the telecommunications links connect to the network in one location.
- C. Ensure that the telecommunications links connect to the network in multiple locations.
- D. Provide multiple links from multiple telecommunications vendors.

**Answer: D**

#### NEW QUESTION 288

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.

Which of the following will indicate where the IT budget is BEST allocated during this time?

- A. Policies
- B. Frameworks
- C. Metrics
- D. Guidelines

**Answer: C**

#### NEW QUESTION 291

- (Exam Topic 10)

Refer to the information below to answer the question.

A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns. In the plan, what is the BEST approach to mitigate future internal client-based attacks?

- A. Block all client side web exploits at the perimeter.
- B. Remove all non-essential client-side web services from the network.
- C. Screen for harmful exploits of client-side services before implementation.
- D. Harden the client image before deployment.

**Answer: D**

#### NEW QUESTION 294

- (Exam Topic 10)

Which of the following is a BEST practice when traveling internationally with laptops containing Personally Identifiable Information (PII)?

- A. Use a thumb drive to transfer information from a foreign computer.
- B. Do not take unnecessary information, including sensitive information.
- C. Connect the laptop only to well-known networks like the hotel or public Internet cafes.
- D. Request international points of contact help scan the laptop on arrival to ensure it is protected.

**Answer: B**

#### NEW QUESTION 298

- (Exam Topic 10)

With data labeling, which of the following MUST be the key decision maker?

- A. Information security
- B. Departmental management
- C. Data custodian
- D. Data owner

**Answer: D**

#### NEW QUESTION 303

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.

Which of the following is considered the MOST important priority for the information security officer?

- A. Formal acceptance of the security strategy
- B. Disciplinary actions taken against unethical behavior
- C. Development of an awareness program for new employees
- D. Audit of all organization system configurations for faults

**Answer: A**

#### NEW QUESTION 308

- (Exam Topic 10)

A large bank deploys hardware tokens to all customers that use their online banking system. The token generates and displays a six digit numeric password every 60 seconds. The customers must log into their bank accounts using this numeric password. This is an example of

- A. asynchronous token.
- B. Single Sign-On (SSO) token.
- C. single factor authentication token.
- D. synchronous token.

**Answer: D**

#### **NEW QUESTION 311**

- (Exam Topic 10)

Which of the following problems is not addressed by using OAuth (Open Standard to Authorization) 2.0 to integrate a third-party identity provider for a service?

- A. Resource Servers are required to use passwords to authenticate end users.
- B. Revocation of access of some users of the third party instead of all the users from the third party.
- C. Compromise of the third party means compromise of all the users in the service.
- D. Guest users need to authenticate with the third party identity provider.

**Answer: C**

#### **NEW QUESTION 314**

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.

Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?

- A. Severity of risk
- B. Complexity of strategy
- C. Frequency of incidents
- D. Ongoing awareness

**Answer: A**

#### **NEW QUESTION 315**

- (Exam Topic 10)

Refer to the information below to answer the question.

A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.

What is the BEST reason for the organization to pursue a plan to mitigate client-based attacks?

- A. Client privilege administration is inherently weaker than server privilege administration.
- B. Client hardening and management is easier on clients than on servers.
- C. Client-based attacks are more common and easier to exploit than server and network based attacks.
- D. Client-based attacks have higher financial impact.

**Answer: C**

#### **NEW QUESTION 316**

- (Exam Topic 10)

Refer to the information below to answer the question.

A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.

In addition to authentication at the start of the user session, best practice would require re-authentication

- A. periodically during a session.
- B. for each business process.
- C. at system sign-off.
- D. after a period of inactivity.

**Answer: D**

#### **NEW QUESTION 321**

- (Exam Topic 10)

The amount of data that will be collected during an audit is PRIMARILY determined by the

- A. audit scope.
- B. auditor's experience level.
- C. availability of the data.
- D. integrity of the data.

**Answer: A**

#### **NEW QUESTION 323**

- (Exam Topic 10)

Refer to the information below to answer the question.

In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

In a Bell-LaPadula system, which user has the MOST restrictions when writing data to any of the four files?

- A. User A
- B. User B
- C. User C
- D. User D

**Answer: D**

**NEW QUESTION 328**

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement. The security program can be considered effective when

- A. vulnerabilities are proactively identified.
- B. audits are regularly performed and reviewed.
- C. backups are regularly performed and validated.
- D. risk is lowered to an acceptable level.

**Answer: D**

**NEW QUESTION 332**

- (Exam Topic 10)

For a service provider, which of the following MOST effectively addresses confidentiality concerns for customers using cloud computing?

- A. Hash functions
- B. Data segregation
- C. File system permissions
- D. Non-repudiation controls

**Answer: B**

**NEW QUESTION 335**

- (Exam Topic 10)

Which of the following secure startup mechanisms are PRIMARILY designed to thwart attacks?

- A. Timing
- B. Cold boot
- C. Side channel
- D. Acoustic cryptanalysis

**Answer: B**

**NEW QUESTION 339**

- (Exam Topic 10)

What is the PRIMARY reason for ethics awareness and related policy implementation?

- A. It affects the workflow of an organization.
- B. It affects the reputation of an organization.
- C. It affects the retention rate of employees.
- D. It affects the morale of the employees.

**Answer: B**

**NEW QUESTION 343**

- (Exam Topic 10)

Which of the following is the PRIMARY benefit of a formalized information classification program?

- A. It drives audit processes.
- B. It supports risk assessment.
- C. It reduces asset vulnerabilities.
- D. It minimizes system logging requirements.

**Answer: B**

**NEW QUESTION 348**

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement. The effectiveness of the security program can PRIMARILY be measured through

- A. audit findings.
- B. risk elimination.
- C. audit requirements.
- D. customer satisfaction.

**Answer: A**

**NEW QUESTION 353**

- (Exam Topic 10)

Which of the following provides the MOST protection against data theft of sensitive information when a laptop is stolen?

- A. Set up a BIOS and operating system password
- B. Encrypt the virtual drive where confidential files can be stored
- C. Implement a mandatory policy in which sensitive data cannot be stored on laptops, but only on the corporate network
- D. Encrypt the entire disk and delete contents after a set number of failed access attempts

**Answer: D**

**NEW QUESTION 354**

- (Exam Topic 10)

Which of the following is critical for establishing an initial baseline for software components in the operation and maintenance of applications?

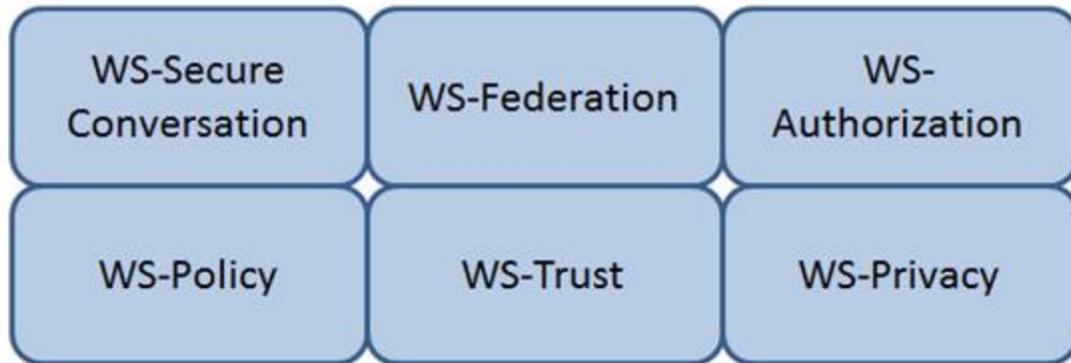
- A. Application monitoring procedures
- B. Configuration control procedures
- C. Security audit procedures
- D. Software patching procedures

**Answer: B**

**NEW QUESTION 355**

- (Exam Topic 11)

Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the correct specification in the image below.



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

WS-Authorization

Reference: Java Web Services: Up and Running" By Martin Kalin page 228

**NEW QUESTION 356**

- (Exam Topic 11)

Which of the following prevents improper aggregation of privileges in Role Based Access Control (RBAC)?

- A. Hierarchical inheritance
- B. Dynamic separation of duties
- C. The Clark-Wilson security model
- D. The Bell-LaPadula security model

**Answer:** B

**NEW QUESTION 360**

- (Exam Topic 11)

The application of which of the following standards would BEST reduce the potential for data breaches?

- A. ISO 9000
- B. ISO 20121
- C. ISO 26000
- D. ISO 27001

**Answer:** D

**NEW QUESTION 362**

- (Exam Topic 11)

A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

- A. Public Key Infrastructure (PKI) and digital signatures
- B. Trusted server certificates and passphrases
- C. User ID and password
- D. Asymmetric encryption and User ID

**Answer:** A

**NEW QUESTION 364**

- (Exam Topic 11)

Which of the following is generally indicative of a replay attack when dealing with biometric authentication?

- A. False Acceptance Rate (FAR) is greater than 1 in 100,000
- B. False Rejection Rate (FRR) is greater than 5 in 100
- C. Inadequately specified templates
- D. Exact match

**Answer:** D

**NEW QUESTION 368**

- (Exam Topic 11)

If an identification process using a biometric system detects a 100% match between a presented template and a stored template, what is the interpretation of this result?

- A. User error
- B. Suspected tampering
- C. Accurate identification
- D. Unsuccessful identification

**Answer:** B

**NEW QUESTION 372**

- (Exam Topic 11)

Which of the following is a function of Security Assertion Markup Language (SAML)?

- A. File allocation
- B. Redundancy check
- C. Extended validation
- D. Policy enforcement

**Answer:** D

**NEW QUESTION 374**

- (Exam Topic 11)

Which of the following statements is TRUE regarding state-based analysis as a functional software testing technique?

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

**Answer:** A

**NEW QUESTION 375**

- (Exam Topic 11)

Which of the following is a reason to use manual patch installation instead of automated patch management?

- A. The cost required to install patches will be reduced.
- B. The time during which systems will remain vulnerable to an exploit will be decreased.
- C. The likelihood of system or application incompatibilities will be decreased.
- D. The ability to cover large geographic areas is increased.

**Answer: C**

**NEW QUESTION 376**

- (Exam Topic 11)

Which of the following has the GREATEST impact on an organization's security posture?

- A. International and country-specific compliance requirements
- B. Security violations by employees and contractors
- C. Resource constraints due to increasing costs of supporting security
- D. Audit findings related to employee access and permissions process

**Answer: A**

**NEW QUESTION 377**

- (Exam Topic 11)

How does an organization verify that an information system's current hardware and software match the standard system configuration?

- A. By reviewing the configuration after the system goes into production
- B. By running vulnerability scanning tools on all devices in the environment
- C. By comparing the actual configuration of the system against the baseline
- D. By verifying all the approved security patches are implemented

**Answer: C**

**NEW QUESTION 382**

- (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**

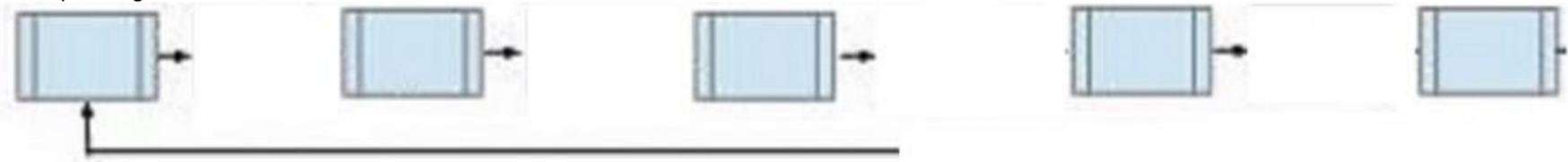
**NEW QUESTION 385**

- (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.

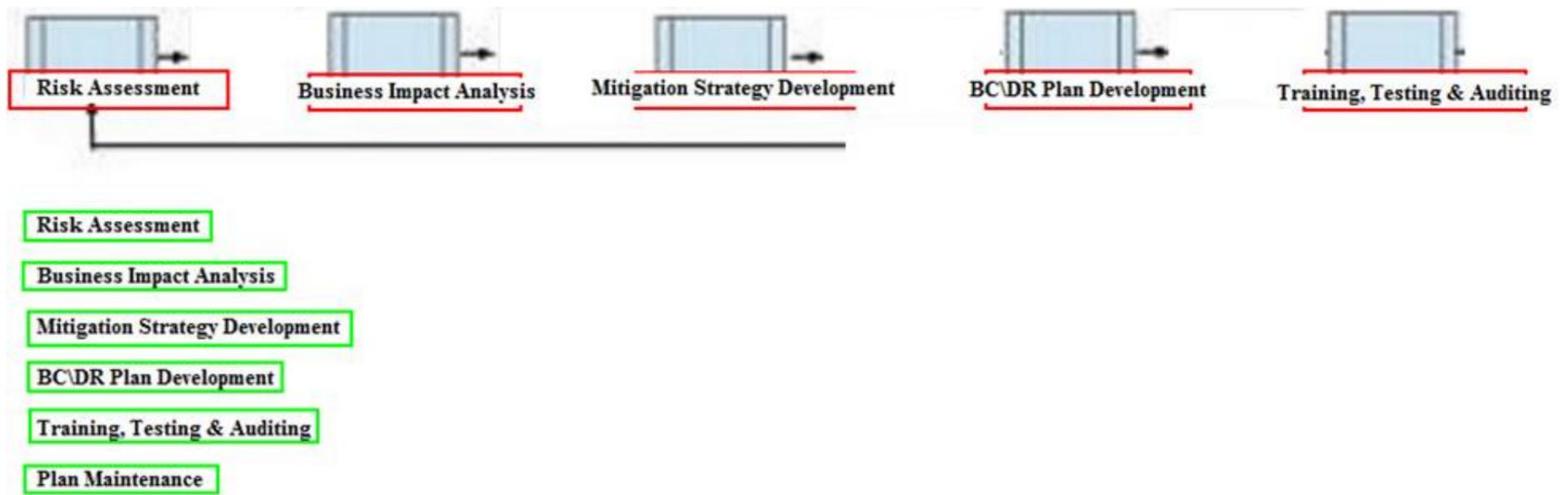


- Risk Assessment**
- Business Impact Analysis**
- Mitigation Strategy Development**
- BC\DR Plan Development**
- Training, Testing & Auditing**
- Plan Maintenance**

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



**NEW QUESTION 387**

- (Exam Topic 11)

Which of the following types of security testing is the MOST effective in providing a better indication of the everyday security challenges of an organization when performing a security risk assessment?

- A. External
- B. Overt
- C. Internal
- D. Covert

**Answer: D**

**NEW QUESTION 388**

- (Exam Topic 11)

Which of the following is the BEST method to assess the effectiveness of an organization's vulnerability management program?

- A. Review automated patch deployment reports
- B. Periodic third party vulnerability assessment
- C. Automated vulnerability scanning
- D. Perform vulnerability scan by security team

**Answer: B**

**NEW QUESTION 390**

- (Exam Topic 11)

Which of the following analyses is performed to protect information assets?

- A. Business impact analysis
- B. Feasibility analysis
- C. Cost benefit analysis
- D. Data analysis

**Answer: A**

**NEW QUESTION 392**

- (Exam Topic 11)

Which of the following is the MOST likely cause of a non-malicious data breach when the source of the data breach was an un-marked file cabinet containing sensitive documents?

- A. Ineffective data classification
- B. Lack of data access controls
- C. Ineffective identity management controls
- D. Lack of Data Loss Prevention (DLP) tools

**Answer: A**

**NEW QUESTION 396**

- (Exam Topic 11)

Which of the following entities is ultimately accountable for data remanence vulnerabilities with data replicated by a cloud service provider?

- A. Data owner
- B. Data steward
- C. Data custodian
- D. Data processor

**Answer: A**

**NEW QUESTION 399**

- (Exam Topic 11)

Which of the following is the BIGGEST weakness when using native Lightweight Directory Access Protocol (LDAP) for authentication?

- A. Authorizations are not included in the server response
- B. Unsalted hashes are passed over the network
- C. The authentication session can be replayed
- D. Passwords are passed in cleartext

**Answer: D**

**NEW QUESTION 400**

- (Exam Topic 11)

Which of the following disaster recovery test plans will be MOST effective while providing minimal risk?

- A. Read-through
- B. Parallel
- C. Full interruption
- D. Simulation

**Answer: B**

**NEW QUESTION 404**

- (Exam Topic 11)

The World Trade Organization's (WTO) agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires authors of computer software to be given the

- A. right to refuse or permit commercial rentals.
- B. right to disguise the software's geographic origin.
- C. ability to tailor security parameters based on location.
- D. ability to confirm license authenticity of their works.

**Answer: A**

**NEW QUESTION 405**

- (Exam Topic 11)

What is the PRIMARY difference between security policies and security procedures?

- A. Policies are used to enforce violations, and procedures create penalties
- B. Policies point to guidelines, and procedures are more contractual in nature
- C. Policies are included in awareness training, and procedures give guidance
- D. Policies are generic in nature, and procedures contain operational details

**Answer: D**

**NEW QUESTION 407**

- (Exam Topic 11)

An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?

- A. Limits and scope of the testing.
- B. Physical location of server room and wiring closet.
- C. Logical location of filters and concentrators.
- D. Employee directory and organizational chart.

**Answer: A**

**NEW QUESTION 408**

- (Exam Topic 11)

When planning a penetration test, the tester will be MOST interested in which information?

- A. Places to install back doors
- B. The main network access points
- C. Job application handouts and tours
- D. Exploits that can attack weaknesses

**Answer: B**

**NEW QUESTION 413**

- (Exam Topic 11)

Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

- A. dig
- B. ifconfig
- C. ipconfig
- D. nbtstat

**Answer:**

A

**NEW QUESTION 417**

- (Exam Topic 11)

Which of the following is the PRIMARY security concern associated with the implementation of smart cards?

- A. The cards have limited memory
- B. Vendor application compatibility
- C. The cards can be misplaced
- D. Mobile code can be embedded in the card

**Answer: C**

**NEW QUESTION 418**

- (Exam Topic 11)

To protect auditable information, which of the following MUST be configured to only allow read access?

- A. Logging configurations
- B. Transaction log files
- C. User account configurations
- D. Access control lists (ACL)

**Answer: B**

**NEW QUESTION 419**

- (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 423**

- (Exam Topic 11)

Which of the following explains why record destruction requirements are included in a data retention policy?

- A. To comply with legal and business requirements
- B. To save cost for storage and backup
- C. To meet destruction guidelines
- D. To validate data ownership

**Answer: A**

**NEW QUESTION 427**

- (Exam Topic 11)

What type of encryption is used to protect sensitive data in transit over a network?

- A. Payload encryption and transport encryption
- B. Authentication Headers (AH)
- C. Keyed-Hashing for Message Authentication
- D. Point-to-Point Encryption (P2PE)

**Answer: A**

**NEW QUESTION 428**

- (Exam Topic 11)

An organization has developed a major application that has undergone accreditation testing. After receiving the results of the evaluation, what is the final step before the application can be accredited?

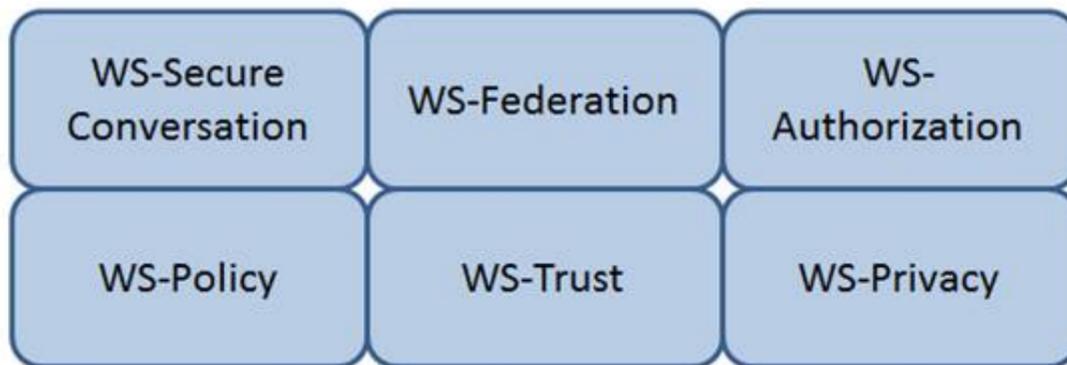
- A. Acceptance of risk by the authorizing official
- B. Remediation of vulnerabilities
- C. Adoption of standardized policies and procedures
- D. Approval of the System Security Plan (SSP)

**Answer: A**

**NEW QUESTION 431**

- (Exam Topic 11)

Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

WS-Federation

Reference: Java Web Services: Up and Running" By Martin Kalin page 228

**NEW QUESTION 436**

- (Exam Topic 11)

Secure Sockets Layer (SSL) encryption protects

- A. data at rest.
- B. the source IP address.
- C. data transmitted.
- D. data availability.

**Answer:** C

**NEW QUESTION 441**

- (Exam Topic 11)

Which methodology is recommended for penetration testing to be effective in the development phase of the life-cycle process?

- A. White-box testing
- B. Software fuzz testing
- C. Black-box testing
- D. Visual testing

**Answer:** A

**NEW QUESTION 446**

- (Exam Topic 11)

The PRIMARY characteristic of a Distributed Denial of Service (DDoS) attack is that it

- A. exploits weak authentication to penetrate networks.
- B. can be detected with signature analysis.
- C. looks like normal network activity.
- D. is commonly confused with viruses or worms.

**Answer:** C

**NEW QUESTION 450**

- (Exam Topic 11)

The implementation of which features of an identity management system reduces costs and administration overhead while improving audit and accountability?

- A. Two-factor authentication
- B. Single Sign-On (SSO)
- C. User self-service
- D. A metadirectory

**Answer:** C

**NEW QUESTION 455**

- (Exam Topic 11)

Application of which of the following Institute of Electrical and Electronics Engineers (IEEE) standards will prevent an unauthorized wireless device from being attached to a network?

- A. IEEE 802.1F
- B. IEEE 802.1H
- C. IEEE 802.1Q
- D. IEEE 802.1X

**Answer: D**

**NEW QUESTION 457**

- (Exam Topic 11)

Which of the following is an advantage of on-premise Credential Management Systems?

- A. Improved credential interoperability
- B. Control over system configuration
- C. Lower infrastructure capital costs
- D. Reduced administrative overhead

**Answer: B**

**NEW QUESTION 459**

- (Exam Topic 11)

Which of the following statements is TRUE regarding value boundary analysis as a functional software testing technique?

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

**Answer: C**

**NEW QUESTION 461**

- (Exam Topic 11)

Sensitive customer data is going to be added to a database. What is the MOST effective implementation for ensuring data privacy?

- A. Discretionary Access Control (DAC) procedures
- B. Mandatory Access Control (MAC) procedures
- C. Data link encryption
- D. Segregation of duties

**Answer: B**

**NEW QUESTION 464**

- (Exam Topic 11)

Which of the following controls is the FIRST step in protecting privacy in an information system?

- A. Data Redaction
- B. Data Minimization
- C. Data Encryption
- D. Data Storage

**Answer: B**

**NEW QUESTION 469**

- (Exam Topic 11)

What is one way to mitigate the risk of security flaws in custom software?

- A. Include security language in the Earned Value Management (EVM) contract
- B. Include security assurance clauses in the Service Level Agreement (SLA)
- C. Purchase only Commercial Off-The-Shelf (COTS) products
- D. Purchase only software with no open source Application Programming Interfaces (APIs)

**Answer: B**

**NEW QUESTION 472**

- (Exam Topic 11)

Which of the following is the MOST effective method of mitigating data theft from an active user workstation?

- A. Implement full-disk encryption
- B. Enable multifactor authentication
- C. Deploy file integrity checkers
- D. Disable use of portable devices

**Answer:**

D

**NEW QUESTION 475**

- (Exam Topic 11)

The PRIMARY outcome of a certification process is that it provides documented

- A. system weaknesses for remediation.
- B. standards for security assessment, testing, and process evaluation.
- C. interconnected systems and their implemented security controls.
- D. security analyses needed to make a risk-based decision.

**Answer: D**

**NEW QUESTION 476**

- (Exam Topic 11)

What security risk does the role-based access approach mitigate MOST effectively?

- A. Excessive access rights to systems and data
- B. Segregation of duties conflicts within business applications
- C. Lack of system administrator activity monitoring
- D. Inappropriate access requests

**Answer: A**

**NEW QUESTION 478**

- (Exam Topic 11)

What type of test assesses a Disaster Recovery (DR) plan using realistic disaster scenarios while maintaining minimal impact to business operations?

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

**Answer: C**

**NEW QUESTION 480**

- (Exam Topic 11)

Which of the following questions can be answered using user and group entitlement reporting?

- A. When a particular file was last accessed by a user
- B. Change control activities for a particular group of users
- C. The number of failed login attempts for a particular user
- D. Where does a particular user have access within the network

**Answer: D**

**NEW QUESTION 483**

- (Exam Topic 11)

When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?

- A. After the system preliminary design has been developed and the data security categorization has been performed
- B. After the business functional analysis and the data security categorization have been performed
- C. After the vulnerability analysis has been performed and before the system detailed design begins
- D. After the system preliminary design has been developed and before the data security categorization begins

**Answer: B**

**NEW QUESTION 484**

- (Exam Topic 11)

What is the GREATEST challenge of an agent-based patch management solution?

- A. Time to gather vulnerability information about the computers in the program
- B. Requires that software be installed, running, and managed on all participating computers
- C. The significant amount of network bandwidth while scanning computers
- D. The consistency of distributing patches to each participating computer

**Answer: B**

**NEW QUESTION 487**

- (Exam Topic 11)

Which of the following protocols would allow an organization to maintain a centralized list of users that can read a protected webpage?

- A. Lightweight Directory Access Control (LDAP)
- B. Security Assertion Markup Language (SAML)
- C. Hypertext Transfer Protocol (HTTP)
- D. Kerberos

Answer: A

**NEW QUESTION 490**

- (Exam Topic 11)

Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?

- A. Policy documentation review
- B. Authentication validation
- C. Periodic log reviews
- D. Interface testing

Answer: C

**NEW QUESTION 493**

- (Exam Topic 11)

Which of the following secures web transactions at the Transport Layer?

- A. Secure HyperText Transfer Protocol (S-HTTP)
- B. Secure Sockets Layer (SSL)
- C. Socket Security (SOCKS)
- D. Secure Shell (SSH)

Answer: B

**NEW QUESTION 495**

- (Exam Topic 11)

Are companies legally required to report all data breaches?

- A. No, different jurisdictions have different rules.
- B. No, not if the data is encrypted.
- C. No, companies' codes of ethics don't require it.
- D. No, only if the breach had a material impact.

Answer: A

**NEW QUESTION 499**

- (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 501**

- (Exam Topic 11)

By carefully aligning the pins in the lock, which of the following defines the opening of a mechanical lock without the proper key?

- A. Lock pinging
- B. Lock picking
- C. Lock bumping
- D. Lock bricking

Answer: B

**NEW QUESTION 502**

- (Exam Topic 11)

A global organization wants to implement hardware tokens as part of a multifactor authentication solution for remote access. The PRIMARY advantage of this implementation is

- A. the scalability of token enrollment.
- B. increased accountability of end users.
- C. it protects against unauthorized access.
- D. it simplifies user access administration.

Answer: C

**NEW QUESTION 504**

- (Exam Topic 12)

A proxy firewall operates at what layer of the Open System Interconnection (OSI) model?

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

**Answer: D**

**NEW QUESTION 508**

- (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 513**

- (Exam Topic 12)

Which of the following is a remote access protocol that uses a static authentication?

- A. Point-to-Point Tunneling Protocol (PPTP)
- B. Routing Information Protocol (RIP)
- C. Password Authentication Protocol (PAP)
- D. Challenge Handshake Authentication Protocol (CHAP)

**Answer: C**

**NEW QUESTION 514**

- (Exam Topic 12)

A vulnerability in which of the following components would be MOST difficult to detect?

- A. Kernel
- B. Shared libraries
- C. Hardware
- D. System application

**Answer: A**

**NEW QUESTION 517**

- (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 521**

- (Exam Topic 12)

Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

- A. Addresses and protocols of network-based logs are analyzed.
- B. Host-based system logging has files stored in multiple locations.
- C. Properly handled network-based logs may be more reliable and valid.
- D. Network-based systems cannot capture users logging into the console.

**Answer: A**

**NEW QUESTION 523**

- (Exam Topic 12)

A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

- A. Enterprise asset management framework
- B. Asset baseline using commercial off the shelf software
- C. Asset ownership database using domain login records
- D. A script to report active user logins on assets

Answer: A

**NEW QUESTION 527**

- (Exam Topic 12)

Which of the following adds end-to-end security inside a Layer 2 Tunneling Protocol (L2TP) Internet Protocol Security (IPSec) connection?

- A. Temporal Key Integrity Protocol (TKIP)
- B. Secure Hash Algorithm (SHA)
- C. Secure Shell (SSH)
- D. Transport Layer Security (TLS)

Answer: B

**NEW QUESTION 532**

- (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 535**

- (Exam Topic 12)

Which of the following is the MAIN reason for using configuration management?

- A. To provide centralized administration
- B. To reduce the number of changes
- C. To reduce errors during upgrades
- D. To provide consistency in security controls

Answer: D

**NEW QUESTION 539**

- (Exam Topic 12)

The PRIMARY outcome of a certification process is that it provides documented

- A. interconnected systems and their implemented security controls.
- B. standards for security assessment, testing, and process evaluation.
- C. system weakness for remediation.
- D. security analyses needed to make a risk-based decision.

Answer: D

**NEW QUESTION 540**

- (Exam Topic 12)

Which of the following sets of controls should allow an investigation if an attack is not blocked by preventive controls or detected by monitoring?

- A. Logging and audit trail controls to enable forensic analysis
- B. Security incident response lessons learned procedures
- C. Security event alert triage done by analysts using a Security Information and Event Management (SIEM) system
- D. Transactional controls focused on fraud prevention

Answer: C

**NEW QUESTION 542**

- (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 547**

- (Exam Topic 12)

Which of the following is MOST important when deploying digital certificates?

- A. Validate compliance with X.509 digital certificate standards
- B. Establish a certificate life cycle management framework

- C. Use a third-party Certificate Authority (CA)
- D. Use no less than 256-bit strength encryption when creating a certificate

**Answer:** B

**NEW QUESTION 552**

- (Exam Topic 12)

During which of the following processes is least privilege implemented for a user account?

- A. Provision
- B. Approve
- C. Request
- D. Review

**Answer:** A

**NEW QUESTION 555**

- (Exam Topic 12)

What type of wireless network attack BEST describes an Electromagnetic Pulse (EMP) attack?

- A. Radio Frequency (RF) attack
- B. Denial of Service (DoS) attack
- C. Data modification attack
- D. Application-layer attack

**Answer:** B

**NEW QUESTION 556**

- (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:** B

**NEW QUESTION 561**

- (Exam Topic 12)

The PRIMARY purpose of accreditation is to:

- A. comply with applicable laws and regulations.
- B. allow senior management to make an informed decision regarding whether to accept the risk of operating the system.
- C. protect an organization's sensitive data.
- D. verify that all security controls have been implemented properly and are operating in the correct manner.

**Answer:** B

**NEW QUESTION 562**

- (Exam Topic 12)

Which of the following media sanitization techniques is MOST likely to be effective for an organization using public cloud services?

- A. Low-level formatting
- B. Secure-grade overwrite erasure
- C. Cryptographic erasure
- D. Drive degaussing

**Answer:** B

**NEW QUESTION 563**

- (Exam Topic 12)

Which of the following BEST describes Recovery Time Objective (RTO)?

- A. Time of application resumption after disaster
- B. Time of application verification after disaster.
- C. Time of data validation after disaster.
- D. Time of data restoration from backup after disaster.

**Answer:** A

**NEW QUESTION 564**

- (Exam Topic 12)

Determining outage costs caused by a disaster can BEST be measured by the

- A. cost of redundant systems and backups.
- B. cost to recover from an outage.
- C. overall long-term impact of the outage.
- D. revenue lost during the outage.

**Answer: C**

**NEW QUESTION 568**

- (Exam Topic 12)

A database administrator is asked by a high-ranking member of management to perform specific changes to the accounting system database. The administrator is specifically instructed to not track or evidence the change in a ticket. Which of the following is the BEST course of action?

- A. Ignore the request and do not perform the change.
- B. Perform the change as requested, and rely on the next audit to detect and report the situation.
- C. Perform the change, but create a change ticket regardless to ensure there is complete traceability.
- D. Inform the audit committee or internal audit directly using the corporate whistleblower process.

**Answer: D**

**NEW QUESTION 572**

- (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 575**

- (Exam Topic 12)

Which of the following would BEST describe the role directly responsible for data within an organization?

- A. Data custodian
- B. Information owner
- C. Database administrator
- D. Quality control

**Answer: A**

**NEW QUESTION 579**

- (Exam Topic 12)

At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

- A. Transport Layer
- B. Data-Link Layer
- C. Network Layer
- D. Application Layer

**Answer: C**

**NEW QUESTION 583**

- (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 585**

- (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 586**

- (Exam Topic 12)

An employee of a retail company has been granted an extended leave of absence by Human Resources (HR). This information has been formally communicated to the access provisioning team. Which of the following is the BEST action to take?

- A. Revoke access temporarily.
- B. Block user access and delete user account after six months.
- C. Block access to the offices immediately.
- D. Monitor account usage temporarily.

**Answer: D**

**NEW QUESTION 591**

- (Exam Topic 12)

Which of the following BEST represents the concept of least privilege?

- A. Access to an object is denied unless access is specifically allowed.
- B. Access to an object is only available to the owner.
- C. Access to an object is allowed unless it is protected by the information security policy.
- D. Access to an object is only allowed to authenticated users via an Access Control List (ACL).

**Answer: A**

**NEW QUESTION 592**

- (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 593**

- (Exam Topic 12)

Which of the following approaches is the MOST effective way to dispose of data on multiple hard drives?

- A. Delete every file on each drive.
- B. Destroy the partition table for each drive using the command line.
- C. Degauss each drive individually.
- D. Perform multiple passes on each drive using approved formatting methods.

**Answer: D**

**NEW QUESTION 595**

- (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 596**

- (Exam Topic 12)

Which of the following is the MOST important consideration when developing a Disaster Recovery Plan (DRP)?

- A. The dynamic reconfiguration of systems
- B. The cost of downtime
- C. A recovery strategy for all business processes
- D. A containment strategy

**Answer: C**

**NEW QUESTION 598**

- (Exam Topic 12)

In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of

- A. systems integration.
- B. risk management.
- C. quality assurance.
- D. change management.

**Answer: D**

**NEW QUESTION 602**

- (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: C**

**NEW QUESTION 606**

- (Exam Topic 12)

In order to assure authenticity, which of the following are required?

- A. Confidentiality and authentication
- B. Confidentiality and integrity
- C. Authentication and non-repudiation
- D. Integrity and non-repudiation

**Answer: D**

**NEW QUESTION 609**

- (Exam Topic 12)

The goal of a Business Impact Analysis (BIA) is to determine which of the following?

- A. Cost effectiveness of business recovery
- B. Cost effectiveness of installing software security patches
- C. Resource priorities for recovery and Maximum Tolerable Downtime (MTD)
- D. Which security measures should be implemented

**Answer: C**

**NEW QUESTION 614**

- (Exam Topic 12)

An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a PRIMARY security concern?

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

**Answer: C**

**NEW QUESTION 617**

- (Exam Topic 12)

In configuration management, what baseline configuration information MUST be maintained for each computer system?

- A. Operating system and version, patch level, applications running, and versions.
- B. List of system changes, test reports, and change approvals
- C. Last vulnerability assessment report and initial risk assessment report
- D. Date of last update, test report, and accreditation certificate

**Answer: A**

**NEW QUESTION 621**

- (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 625**

- (Exam Topic 12)

The application of a security patch to a product previously validate at Common Criteria (CC) Evaluation Assurance Level (EAL) 4 would

- A. require an update of the Protection Profile (PP).
- B. require recertification.
- C. retain its current EAL rating.
- D. reduce the product to EAL 3.

**Answer: B**

**NEW QUESTION 626**

- (Exam Topic 12)

From a cryptographic perspective, the service of non-repudiation includes which of the following features?

- A. Validity of digital certificates
- B. Validity of the authorization rules
- C. Proof of authenticity of the message
- D. Proof of integrity of the message

**Answer: C**

**NEW QUESTION 627**

- (Exam Topic 12)

When evaluating third-party applications, which of the following is the GREATEST responsibility of Information Security?

- A. Accept the risk on behalf of the organization.
- B. Report findings to the business to determine security gaps.
- C. Quantify the risk to the business for product selection.
- D. Approve the application that best meets security requirements.

**Answer: C**

**NEW QUESTION 632**

- (Exam Topic 12)

For network based evidence, which of the following contains traffic details of all network sessions in order to detect anomalies?

- A. Alert data
- B. User data
- C. Content data
- D. Statistical data

**Answer: D**

**NEW QUESTION 637**

- (Exam Topic 12)

Reciprocal backup site agreements are considered to be

- A. a better alternative than the use of warm sites.
- B. difficult to test for complex systems.
- C. easy to implement for similar types of organizations.
- D. easy to test and implement for complex systems.

**Answer: B**

**NEW QUESTION 642**

- (Exam Topic 12)

Knowing the language in which an encrypted message was originally produced might help a cryptanalyst to perform a

- A. clear-text attack.
- B. known cipher attack.
- C. frequency analysis.
- D. stochastic assessment.

**Answer: C**

**NEW QUESTION 644**

- (Exam Topic 12)

What is the MOST important element when considering the effectiveness of a training program for Business Continuity (BC) and Disaster Recovery (DR)?

- A. Management support
- B. Consideration of organizational need
- C. Technology used for delivery
- D. Target audience

**Answer: B**

**NEW QUESTION 646**

- (Exam Topic 12)

In which identity management process is the subject's identity established?

- A. Trust
- B. Provisioning
- C. Authorization
- D. Enrollment

**Answer:**

D

**NEW QUESTION 650**

- (Exam Topic 12)

During the Security Assessment and Authorization process, what is the PRIMARY purpose for conducting a hardware and software inventory?

- A. Calculate the value of assets being accredited.
- B. Create a list to include in the Security Assessment and Authorization package.
- C. Identify obsolete hardware and software.
- D. Define the boundaries of the information system.

**Answer:** A

**NEW QUESTION 651**

- (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 656**

- (Exam Topic 13)

Which of the following is the MOST effective method to mitigate Cross-Site Scripting (XSS) attacks?

- A. Use Software as a Service (SaaS)
- B. Whitelist input validation
- C. Require client certificates
- D. Validate data output

**Answer:** B

**NEW QUESTION 659**

- (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 663**

- (Exam Topic 13)

Which of the following steps should be performed FIRST when purchasing Commercial Off-The-Shelf (COTS) software?

- A. undergo a security assessment as part of authorization process
- B. establish a risk management strategy
- C. harden the hosting server, and perform hosting and application vulnerability scans
- D. establish policies and procedures on system and services acquisition

**Answer:** D

**NEW QUESTION 667**

- (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:** C

**NEW QUESTION 671**

- (Exam Topic 13)

Due to system constraints, a group of system administrators must share a high-level access set of credentials. Which of the following would be MOST appropriate to implement?

- A. Increased console lockout times for failed logon attempts
- B. Reduce the group in size
- C. A credential check-out process for a per-use basis
- D. Full logging on affected systems

**Answer: C**

**Explanation:**

Section: Security Operations

**NEW QUESTION 674**

- (Exam Topic 13)

Who is responsible for the protection of information when it is shared with or provided to other organizations?

- A. Systems owner
- B. Authorizing Official (AO)
- C. Information owner
- D. Security officer

**Answer: C**

**Explanation:**

Section: Security Operations

**NEW QUESTION 676**

- (Exam Topic 13)

What protocol is often used between gateway hosts on the Internet?

- A. Exterior Gateway Protocol (EGP)
- B. Border Gateway Protocol (BGP)
- C. Open Shortest Path First (OSPF)
- D. Internet Control Message Protocol (ICMP)

**Answer: B**

**NEW QUESTION 678**

- (Exam Topic 13)

From a security perspective, which of the following assumptions MUST be made about input to an application?

- A. It is tested
- B. It is logged
- C. It is verified
- D. It is untrusted

**Answer: D**

**NEW QUESTION 680**

- (Exam Topic 13)

In an organization where Network Access Control (NAC) has been deployed, a device trying to connect to the network is being placed into an isolated domain. What could be done on this device in order to obtain proper connectivity?

- A. Connect the device to another network jack
- B. Apply remediation's according to security requirements
- C. Apply Operating System (OS) patches
- D. Change the Message Authentication Code (MAC) address of the network interface

**Answer: B**

**NEW QUESTION 681**

- (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 684**

- (Exam Topic 13)

Unused space in a disk cluster is important in media analysis because it may contain which of the following?

- A. Residual data that has not been overwritten
- B. Hidden viruses and Trojan horses
- C. Information about the File Allocation table (FAT)
- D. Information about patches and upgrades to the system

**Answer:** A

**NEW QUESTION 685**

- (Exam Topic 13)

Which of the following could be considered the MOST significant security challenge when adopting DevOps practices compared to a more traditional control framework?

- A. Achieving Service Level Agreements (SLA) on how quickly patches will be released when a security flaw is found.
- B. Maintaining segregation of duties.
- C. Standardized configurations for logging, alerting, and security metrics.
- D. Availability of security teams at the end of design process to perform last-minute manual audits and reviews.

**Answer:** B

**NEW QUESTION 690**

- (Exam Topic 13)

The design review for an application has been completed and is ready for release. What technique should an organization use to assure application integrity?

- A. Application authentication
- B. Input validation
- C. Digital signing
- D. Device encryption

**Answer:** C

**NEW QUESTION 693**

- (Exam Topic 13)

It is MOST important to perform which of the following to minimize potential impact when implementing a new vulnerability scanning tool in a production environment?

- A. Negotiate schedule with the Information Technology (IT) operation's team
- B. Log vulnerability summary reports to a secured server
- C. Enable scanning during off-peak hours
- D. Establish access for Information Technology (IT) management

**Answer:** A

**Explanation:**

Section: Security Operations

**NEW QUESTION 697**

- (Exam Topic 13)

Which of the following mechanisms will BEST prevent a Cross-Site Request Forgery (CSRF) attack?

- A. parameterized database queries
- B. whitelist input values
- C. synchronized session tokens
- D. use strong ciphers

**Answer:** C

**NEW QUESTION 699**

- (Exam Topic 13)

Which factors MUST be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?

- A. System owner roles and responsibilities, data handling standards, storage and secure development lifecycle requirements
- B. Data stewardship roles, data handling and storage standards, data lifecycle requirements
- C. Compliance office roles and responsibilities, classified material handling standards, storage system lifecycle requirements
- D. System authorization roles and responsibilities, cloud computing standards, lifecycle requirements

**Answer:** A

**NEW QUESTION 701**

- (Exam Topic 13)

Which of the following is a benefit in implementing an enterprise Identity and Access Management (IAM) solution?

- A. Password requirements are simplified.
- B. Risk associated with orphan accounts is reduced.
- C. Segregation of duties is automatically enforced.
- D. Data confidentiality is increased.

**Answer:** A

**NEW QUESTION 702**

- (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 706**

- (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 707**

- (Exam Topic 13)

An organization has outsourced its financial transaction processing to a Cloud Service Provider (CSP) who will provide them with Software as a Service (SaaS). If there was a data breach who is responsible for monetary losses?

- A. The Data Protection Authority (DPA)
- B. The Cloud Service Provider (CSP)
- C. The application developers
- D. The data owner

**Answer:** B

**NEW QUESTION 712**

- (Exam Topic 13)

What is the MAIN purpose of a change management policy?

- A. To assure management that changes to the Information Technology (IT) infrastructure are necessary
- B. To identify the changes that may be made to the Information Technology (IT) infrastructure
- C. To verify that changes to the Information Technology (IT) infrastructure are approved
- D. To determine the necessary for implementing modifications to the Information Technology (IT) infrastructure

**Answer:** C

**Explanation:**

Section: Security Operations

**NEW QUESTION 717**

- (Exam Topic 13)

Mandatory Access Controls (MAC) are based on:

- A. security classification and security clearance
- B. data segmentation and data classification
- C. data labels and user access permissions
- D. user roles and data encryption

**Answer:** A

**NEW QUESTION 718**

- (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:** C

**NEW QUESTION 720**

- (Exam Topic 13)

What are the steps of a risk assessment?

- A. identification, analysis, evaluation
- B. analysis, evaluation, mitigation
- C. classification, identification, risk management
- D. identification, evaluation, mitigation

**Answer:** A

**Explanation:**

Section: Security Assessment and Testing

**NEW QUESTION 721**

- (Exam Topic 13)

Which of the following is a common characteristic of privacy?

- A. Provision for maintaining an audit trail of access to the private data
- B. Notice to the subject of the existence of a database containing relevant credit card data
- C. Process for the subject to inspect and correct personal data on-site
- D. Database requirements for integration of privacy data

**Answer:** A

**NEW QUESTION 726**

- (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 727**

- (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 732**

- (Exam Topic 13)

Match the functional roles in an external audit to their responsibilities. Drag each role on the left to its corresponding responsibility on the right. Select and Place:

<u>Role</u>		<u>Responsibility</u>
Executive management		Approve audit budget and resource allocation.
Audit committee		Provide audit oversight.
Compliance officer		Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor		Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

<u>Role</u>		<u>Responsibility</u>
Executive management	Executive management	Approve audit budget and resource allocation.
Audit committee	Audit committee	Provide audit oversight.
Compliance officer	External auditor	Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor	Compliance officer	Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

**NEW QUESTION 733**

- (Exam Topic 13)

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

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

**Answer: C**

**NEW QUESTION 735**

- (Exam Topic 13)

Which of the following would an attacker BEST be able to accomplish through the use of Remote Access Tools (RAT)?

- A. Reduce the probability of identification
- B. Detect further compromise of the target
- C. Destabilize the operation of the host
- D. Maintain and expand control

**Answer: D**

**NEW QUESTION 738**

- (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: A**

**NEW QUESTION 741**

- (Exam Topic 13)

Which of the following is the MOST challenging issue in apprehending cyber criminals?

- A. They often use sophisticated method to commit a crime.
- B. It is often hard to collect and maintain integrity of digital evidence.
- C. The crime is often committed from a different jurisdiction.
- D. There is often no physical evidence involved.

**Answer: C**

**NEW QUESTION 745**

- (Exam Topic 13)

What is the expected outcome of security awareness in support of a security awareness program?

- A. Awareness activities should be used to focus on security concerns and respond to those concerns accordingly
- B. Awareness is not an activity or part of the training but rather a state of persistence to support the program
- C. Awareness is trainin
- D. The purpose of awareness presentations is to broaden attention of security.
- E. Awareness is not trainin
- F. The purpose of awareness presentation is simply to focus attention on security.

Answer: C

**NEW QUESTION 747**

- (Exam Topic 13)

An Information Technology (IT) professional attends a cybersecurity seminar on current incident response methodologies. What code of ethics canon is being observed?

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

Answer: C

**Explanation:**

Section: Security Operations

**NEW QUESTION 751**

- (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 754**

- (Exam Topic 13)

What MUST each information owner do when a system contains data from multiple information owners?

- A. Provide input to the Information System (IS) owner regarding the security requirements of the data
- B. Review the Security Assessment report (SAR) for the Information System (IS) and authorize the IS to operate.
- C. Develop and maintain the System Security Plan (SSP) for the Information System (IS) containing the data
- D. Move the data to an Information System (IS) that does not contain data owned by other information owners

Answer: C

**Explanation:**

Section: Security Assessment and Testing

**NEW QUESTION 755**

- (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 758**

- (Exam Topic 13)

A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report. In which phase of the assessment was this error MOST likely made?

- A. Enumeration
- B. Reporting
- C. Detection
- D. Discovery

Answer: A

**Explanation:**

Section: Security Assessment and Testing

**NEW QUESTION 762**

- (Exam Topic 13)

After following the processes defined within the change management plan, a super user has upgraded a device within an Information system. What step would be taken to ensure that the upgrade did NOT affect the network security posture?

- A. Conduct an Assessment and Authorization (A&A)

- B. Conduct a security impact analysis
- C. Review the results of the most recent vulnerability scan
- D. Conduct a gap analysis with the baseline configuration

**Answer:** B

**Explanation:**

Section: Security Assessment and Testing

**NEW QUESTION 767**

- (Exam Topic 13)

At a MINIMUM, audits of permissions to individual or group accounts should be scheduled

- A. annually
- B. to correspond with staff promotions
- C. to correspond with terminations
- D. continually

**Answer:** A

**NEW QUESTION 770**

- (Exam Topic 13)

Which of the following is part of a Trusted Platform Module (TPM)?

- A. A non-volatile tamper-resistant storage for storing both data and signing keys in a secure fashion
- B. A protected Pre-Basic Input/Output System (BIOS) which specifies a method or a metric for "measuring" the state of a computing platform
- C. A secure processor targeted at managing digital keys and accelerating digital signing
- D. A platform-independent software interface for accessing computer functions

**Answer:** A

**NEW QUESTION 775**

- (Exam Topic 13)

Which of the following is the MOST appropriate action when reusing media that contains sensitive data?

- A. Erase
- B. Sanitize
- C. Encrypt
- D. Degauss

**Answer:** B

**NEW QUESTION 779**

- (Exam Topic 13)

A user has infected a computer with malware by connecting a Universal Serial Bus (USB) storage device. Which of the following is MOST effective to mitigate future infections?

- A. Develop a written organizational policy prohibiting unauthorized USB devices
- B. Train users on the dangers of transferring data in USB devices
- C. Implement centralized technical control of USB port connections
- D. Encrypt removable USB devices containing data at rest

**Answer:** C

**NEW QUESTION 783**

- (Exam Topic 13)

As part of an application penetration testing process, session hijacking can BEST be achieved by which of the following?

- A. Known-plaintext attack
- B. Denial of Service (DoS)
- C. Cookie manipulation
- D. Structured Query Language (SQL) injection

**Answer:** D

**Explanation:**

Section: Security Assessment and Testing

**NEW QUESTION 784**

- (Exam Topic 13)

Which of the following is the MOST important part of an awareness and training plan to prepare employees for emergency situations?

- A. Having emergency contacts established for the general employee population to get information
- B. Conducting business continuity and disaster recovery training for those who have a direct role in the recovery
- C. Designing business continuity and disaster recovery training programs for different audiences
- D. Publishing a corporate business continuity and disaster recovery plan on the corporate website

Answer: C

**NEW QUESTION 788**

- (Exam Topic 13)

In a High Availability (HA) environment, what is the PRIMARY goal of working with a virtual router address as the gateway to a network?

- A. The second of two routers can periodically check in to make sure that the first router is operational.
- B. The second of two routers can better absorb a Denial of Service (DoS) attack knowing the first router is present.
- C. The first of two routers fails and is reinstalled, while the second handles the traffic flawlessly.
- D. The first of two routers can better handle specific traffic, while the second handles the rest of the traffic seamlessly.

Answer: C

**NEW QUESTION 789**

- (Exam Topic 13)

In Disaster Recovery (DR) and Business Continuity (DC) training, which BEST describes a functional drill?

- A. a functional evacuation of personnel
- B. a specific test by response teams of individual emergency response functions
- C. an activation of the backup site
- D. a full-scale simulation of an emergency and the subsequent response functions.

Answer: D

**NEW QUESTION 793**

- (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 796**

- (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: A

**NEW QUESTION 797**

- (Exam Topic 13)

A post-implementation review has identified that the Voice Over Internet Protocol (VoIP) system was designed to have gratuitous Address Resolution Protocol (ARP) disabled.

Why did the network architect likely design the VoIP system with gratuitous ARP disabled?

- A. Gratuitous ARP requires the use of Virtual Local Area Network (VLAN) 1.
- B. Gratuitous ARP requires the use of insecure layer 3 protocols.
- C. Gratuitous ARP requires the likelihood of a successful brute-force attack on the phone.
- D. Gratuitous ARP requires the risk of a Man-in-the-Middle (MITM) attack.

Answer: D

**NEW QUESTION 800**

- (Exam Topic 13)

Access to which of the following is required to validate web session management?

- A. Log timestamp
- B. Live session traffic
- C. Session state variables
- D. Test scripts

Answer: C

**NEW QUESTION 805**

.....

## **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](#)**