

## Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

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



#### NEW QUESTION 1

- (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 2

- (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 3

- (Exam Topic 2)

Which one of the following affects the classification of data?

- A. Assigned security label
- B. Multilevel Security (MLS) architecture
- C. Minimum query size
- D. Passage of time

**Answer:** D

#### NEW QUESTION 4

- (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 5

- (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 6

- (Exam Topic 3)

Which of the following mobile code security models relies only on trust?

- A. Code signing
- B. Class authentication
- C. Sandboxing
- D. Type safety

**Answer:** A

#### NEW QUESTION 7

- (Exam Topic 3)

Which security service is served by the process of encryption plaintext with the sender's private key and decrypting cipher text with the sender's public key?

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

**Answer:** A

#### NEW QUESTION 8

- (Exam Topic 4)

Which of the following operates at the Network Layer of the Open System Interconnection (OSI) model?

- A. Packet filtering
- B. Port services filtering
- C. Content filtering
- D. Application access control

**Answer:** A

#### NEW QUESTION 9

- (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 10

- (Exam Topic 4)

What is the purpose of an Internet Protocol (IP) spoofing attack?

- A. To send excessive amounts of data to a process, making it unpredictable
- B. To intercept network traffic without authorization
- C. To disguise the destination address from a target's IP filtering devices
- D. To convince a system that it is communicating with a known entity

**Answer:** D

#### NEW QUESTION 10

- (Exam Topic 4)

In a Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which layer is responsible for negotiating and establishing a connection with another node?

- A. Transport layer
- B. Application layer
- C. Network layer
- D. Session layer

**Answer:** A

#### NEW QUESTION 13

- (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 14

- (Exam Topic 6)

Which of the following is of GREATEST assistance to auditors when reviewing system configurations?

- A. Change management processes
- B. User administration procedures
- C. Operating System (OS) baselines
- D. System backup documentation

**Answer:** A

#### NEW QUESTION 18

- (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 19

- (Exam Topic 7)

A continuous information security monitoring program can BEST reduce risk through which of the following?

- A. Collecting security events and correlating them to identify anomalies
- B. Facilitating system-wide visibility into the activities of critical user accounts
- C. Encompassing people, process, and technology
- D. Logging both scheduled and unscheduled system changes

**Answer:** B

#### NEW QUESTION 20

- (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 24

- (Exam Topic 7)

What is the PRIMARY reason for implementing change management?

- A. Certify and approve releases to the environment
- B. Provide version rollbacks for system changes
- C. Ensure that all applications are approved
- D. Ensure accountability for changes to the environment

**Answer:** D

#### NEW QUESTION 25

- (Exam Topic 7)

What should be the FIRST action to protect the chain of evidence when a desktop computer is involved?

- A. Take the computer to a forensic lab
- B. Make a copy of the hard drive
- C. Start documenting
- D. Turn off the computer

**Answer:** C

#### NEW QUESTION 29

- (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 32

- (Exam Topic 9)

Which of the following is ensured when hashing files during chain of custody handling?

- A. Availability
- B. Accountability
- C. Integrity
- D. Non-repudiation

**Answer:** C

#### NEW QUESTION 34

- (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 38

- (Exam Topic 9)

Which of the following is a limitation of the Common Vulnerability Scoring System (CVSS) as it relates to conducting code review?

- A. It has normalized severity ratings.
- B. It has many worksheets and practices to implement.
- C. It aims to calculate the risk of published vulnerabilities.
- D. It requires a robust risk management framework to be put in place.

**Answer:** C

#### NEW QUESTION 42

- (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 45

- (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 47

- (Exam Topic 9)

In the area of disaster planning and recovery, what strategy entails the presentation of information about the plan?

- A. Communication
- B. Planning
- C. Recovery
- D. Escalation

**Answer:** A

#### NEW QUESTION 52

- (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 56

- (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 57

- (Exam Topic 9)

Which one of the following transmission media is MOST effective in preventing data interception?

- A. Microwave
- B. Twisted-pair
- C. Fiber optic
- D. Coaxial cable

**Answer:** C

#### NEW QUESTION 58

- (Exam Topic 9)

During an audit of system management, auditors find that the system administrator has not been trained. What actions need to be taken at once to ensure the integrity of systems?

- A. A review of hiring policies and methods of verification of new employees
- B. A review of all departmental procedures
- C. A review of all training procedures to be undertaken
- D. A review of all systems by an experienced administrator

**Answer:** D

#### NEW QUESTION 63

- (Exam Topic 9)

The stringency of an Information Technology (IT) security assessment will be determined by the

- A. system's past security record.
- B. size of the system's database.
- C. sensitivity of the system's data.
- D. age of the system.

**Answer:** C

#### NEW QUESTION 68

- (Exam Topic 9)

Which of the following is considered best practice for preventing e-mail spoofing?

- A. Spam filtering
- B. Cryptographic signature
- C. Uniform Resource Locator (URL) filtering
- D. Reverse Domain Name Service (DNS) lookup

**Answer:** B

#### NEW QUESTION 73

- (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 76

- (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 81

- (Exam Topic 9)

When building a data center, site location and construction factors that increase the level of vulnerability to physical threats include

- A. hardened building construction with consideration of seismic factors.
- B. adequate distance from and lack of access to adjacent buildings.
- C. curved roads approaching the data center.
- D. proximity to high crime areas of the city.

**Answer:** D

### NEW QUESTION 83

- (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 84

- (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 86

- (Exam Topic 9)

Which of the following is an essential element of a privileged identity lifecycle management?

- A. Regularly perform account re-validation and approval
- B. Account provisioning based on multi-factor authentication
- C. Frequently review performed activities and request justification
- D. Account information to be provided by supervisor or line manager

**Answer:** A

### NEW QUESTION 90

- (Exam Topic 9)

An organization is selecting a service provider to assist in the consolidation of multiple computing sites including development, implementation and ongoing support of various computer systems. Which of the following MUST be verified by the Information Security Department?

- A. The service provider's policies are consistent with ISO/IEC27001 and there is evidence that the service provider is following those policies.
- B. The service provider will segregate the data within its systems and ensure that each region's policies are met.
- C. The service provider will impose controls and protections that meet or exceed the current systems controls and produce audit logs as verification.
- D. The service provider's policies can meet the requirements imposed by the new environment even if they differ from the organization's current policies.

**Answer:** D

### NEW QUESTION 93

- (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 94

- (Exam Topic 9)

Which of the following assessment metrics is BEST used to understand a system's vulnerability to potential exploits?

- A. Determining the probability that the system functions safely during any time period
- B. Quantifying the system's available services
- C. Identifying the number of security flaws within the system
- D. Measuring the system's integrity in the presence of failure

**Answer:** C

### NEW QUESTION 98

- (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 102

- (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 104

- (Exam Topic 9)

Which of the following statements is TRUE for point-to-point microwave transmissions?

- A. They are not subject to interception due to encryption.
- B. Interception only depends on signal strength.
- C. They are too highly multiplexed for meaningful interception.
- D. They are subject to interception by an antenna within proximity.

**Answer: D**

#### NEW QUESTION 109

- (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 111

- (Exam Topic 9)

The FIRST step in building a firewall is to

- A. assign the roles and responsibilities of the firewall administrators.
- B. define the intended audience who will read the firewall policy.
- C. identify mechanisms to encourage compliance with the policy.
- D. perform a risk analysis to identify issues to be addressed.

**Answer: D**

#### NEW QUESTION 113

- (Exam Topic 9)

Which of the following is TRUE about Disaster Recovery Plan (DRP) testing?

- A. Operational networks are usually shut down during testing.
- B. Testing should continue even if components of the test fail.
- C. The company is fully prepared for a disaster if all tests pass.
- D. Testing should not be done until the entire disaster plan can be tested.

**Answer: B**

#### NEW QUESTION 116

- (Exam Topic 9)

The Hardware Abstraction Layer (HAL) is implemented in the

- A. system software.
- B. system hardware.
- C. application software.
- D. network hardware.

**Answer: A**

#### NEW QUESTION 121

- (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 126

- (Exam Topic 9)

Which one of the following is a fundamental objective in handling an incident?

- A. To restore control of the affected systems
- B. To confiscate the suspect's computers
- C. To prosecute the attacker
- D. To perform full backups of the system

**Answer:** A

#### NEW QUESTION 127

- (Exam Topic 9)

Which type of control recognizes that a transaction amount is excessive in accordance with corporate policy?

- A. Detection
- B. Prevention
- C. Investigation
- D. Correction

**Answer:** A

#### NEW QUESTION 129

- (Exam Topic 9)

Alternate encoding such as hexadecimal representations is MOST often observed in which of the following forms of attack?

- A. Smurf
- B. Rootkit exploit
- C. Denial of Service (DoS)
- D. Cross site scripting (XSS)

**Answer:** D

#### NEW QUESTION 134

- (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 136

- (Exam Topic 9)

Which of the following would be the FIRST step to take when implementing a patch management program?

- A. Perform automatic deployment of patches.
- B. Monitor for vulnerabilities and threats.
- C. Prioritize vulnerability remediation.
- D. Create a system inventory.

**Answer:** D

#### NEW QUESTION 140

- (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 142

- (Exam Topic 9)

What is the ultimate objective of information classification?

- A. To assign responsibility for mitigating the risk to vulnerable systems
- B. To ensure that information assets receive an appropriate level of protection
- C. To recognize that the value of any item of information may change over time
- D. To recognize the optimal number of classification categories and the benefits to be gained from their use

**Answer:** B

#### NEW QUESTION 143

- (Exam Topic 9)

Which of the following is an effective method for avoiding magnetic media data remanence?

- A. Degaussing
- B. Encryption
- C. Data Loss Prevention (DLP)
- D. Authentication

**Answer:** A

#### NEW QUESTION 145

- (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 147

- (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 148

- (Exam Topic 9)

Which one of the following affects the classification of data?

- A. Passage of time
- B. Assigned security label
- C. Multilevel Security (MLS) architecture
- D. Minimum query size

**Answer:** A

#### NEW QUESTION 153

- (Exam Topic 9)

What should be the INITIAL response to Intrusion Detection System/Intrusion Prevention System (IDS/IPS) alerts?

- A. Ensure that the Incident Response Plan is available and current.
- B. Determine the traffic's initial source and block the appropriate port.
- C. Disable or disconnect suspected target and source systems.
- D. Verify the threat and determine the scope of the attack.

**Answer:** D

#### NEW QUESTION 156

- (Exam Topic 10)

What is the MAIN feature that onion routing networks offer?

- A. Non-repudiation
- B. Traceability
- C. Anonymity
- D. Resilience

**Answer:** C

#### NEW QUESTION 159

- (Exam Topic 10)

Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?

- A. Requirements Analysis
- B. Development and Deployment
- C. Production Operations
- D. Utilization Support

**Answer:** A

#### NEW QUESTION 163

- (Exam Topic 10)

What do Capability Maturity Models (CMM) serve as a benchmark for in an organization?

- A. Experience in the industry
- B. Definition of security profiles
- C. Human resource planning efforts
- D. Procedures in systems development

**Answer:** D

#### NEW QUESTION 167

- (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 168

- (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 organization should ensure that the third party's physical security controls are in place so that they

- A. are more rigorous than the original controls.
- B. are able to limit access to sensitive information.
- C. allow access by the organization staff at any time.
- D. cannot be accessed by subcontractors of the third party.

**Answer:** B

#### NEW QUESTION 171

- (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 176

- (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 178

- (Exam Topic 10)

Which of the following MOST influences the design of the organization's electronic monitoring policies?

- A. Workplace privacy laws
- B. Level of organizational trust
- C. Results of background checks
- D. Business ethical considerations

**Answer:** A

**NEW QUESTION 180**

- (Exam Topic 10)

According to best practice, which of the following groups is the MOST effective in performing an information security compliance audit?

- A. In-house security administrators
- B. In-house Network Team
- C. Disaster Recovery (DR) Team
- D. External consultants

**Answer:** D

**NEW QUESTION 182**

- (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 187**

- (Exam Topic 10)

Which of the following are required components for implementing software configuration management systems?

- A. Audit control and signoff
- B. User training and acceptance
- C. Rollback and recovery processes
- D. Regression testing and evaluation

**Answer:** C

**NEW QUESTION 192**

- (Exam Topic 10)

What component of a web application that stores the session state in a cookie can be bypassed by an attacker?

- A. An initialization check
- B. An identification check
- C. An authentication check
- D. An authorization check

**Answer:** C

**NEW QUESTION 194**

- (Exam Topic 10)

A business has implemented Payment Card Industry Data Security Standard (PCI-DSS) compliant handheld credit card processing on their Wireless Local Area Network (WLAN) topology. The network team partitioned the WLAN to create a private segment for credit card processing using a firewall to control device access and route traffic to the card processor on the Internet. What components are in the scope of PCI-DSS?

- A. The entire enterprise network infrastructure.
- B. The handheld devices, wireless access points and border gateway.
- C. The end devices, wireless access points, WLAN, switches, management console, and firewall.
- D. The end devices, wireless access points, WLAN, switches, management console, and Internet

**Answer:** C

**NEW QUESTION 199**

- (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 the intrusion causes the system processes to hang, which of the following has been affected?

- A. System integrity
- B. System availability
- C. System confidentiality
- D. System auditability

**Answer:** B

**NEW QUESTION 204**

- (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 208

- (Exam Topic 10)

Which of the following is a detective access control mechanism?

- A. Log review
- B. Least privilege
- C. Password complexity
- D. Non-disclosure agreement

**Answer: A**

#### NEW QUESTION 209

- (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 211

- (Exam Topic 10)

Which of the following is the MOST effective attack against cryptographic hardware modules?

- A. Plaintext
- B. Brute force
- C. Power analysis
- D. Man-in-the-middle (MITM)

**Answer: C**

#### NEW QUESTION 213

- (Exam Topic 10)

When is security personnel involvement in the Systems Development Life Cycle (SDLC) process MOST beneficial?

- A. Testing phase
- B. Development phase
- C. Requirements definition phase
- D. Operations and maintenance phase

**Answer: C**

#### NEW QUESTION 216

- (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 220

- (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 MOST likely allow the organization to keep risk at an acceptable level?

- A. Increasing the amount of audits performed by third parties
- B. Removing privileged accounts from operational staff
- C. Assigning privileged functions to appropriate staff
- D. Separating the security function into distinct roles

**Answer: C**

#### NEW QUESTION 224

- (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 225

- (Exam Topic 10)

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

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

**Answer: C**

#### NEW QUESTION 227

- (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 232

- (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 235

- (Exam Topic 10)

Which of the following is the MAIN goal of a data retention policy?

- A. Ensure that data is destroyed properly.
- B. Ensure that data recovery can be done on the data.
- C. Ensure the integrity and availability of data for a predetermined amount of time.
- D. Ensure the integrity and confidentiality of data for a predetermined amount of time.

**Answer: C**

#### NEW QUESTION 238

- (Exam Topic 10)

Refer to the information below to answer the question.

Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.

After magnetic drives were degaussed twice according to the product manufacturer's directions, what is the MOST LIKELY security issue with degaussing?

- A. Commercial products often have serious weaknesses of the magnetic force available in the degausser product.
- B. Degausser products may not be properly maintained and operated.
- C. The inability to turn the drive around in the chamber for the second pass due to human error.
- D. Inadequate record keeping when sanitizing media.

**Answer:** B

#### NEW QUESTION 242

- (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 247

- (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.

When determining appropriate resource allocation, which of the following is MOST important to monitor?

- A. Number of system compromises
- B. Number of audit findings
- C. Number of staff reductions
- D. Number of additional assets

**Answer:** B

#### NEW QUESTION 250

- (Exam Topic 10)

A risk assessment report recommends upgrading all perimeter firewalls to mitigate a particular finding. Which of the following BEST supports this recommendation?

- A. The inherent risk is greater than the residual risk.
- B. The Annualized Loss Expectancy (ALE) approaches zero.
- C. The expected loss from the risk exceeds mitigation costs.
- D. The infrastructure budget can easily cover the upgrade costs.

**Answer:** C

#### NEW QUESTION 254

- (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 257

- (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 259

- (Exam Topic 11)

A security professional has been asked to evaluate the options for the location of a new data center within a multifloor building. Concerns for the data center include emanations and physical access controls.

Which of the following is the BEST location?

- A. On the top floor
- B. In the basement
- C. In the core of the building

D. In an exterior room with windows

**Answer:** C

**NEW QUESTION 262**

- (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 264**

- (Exam Topic 11)

Which of the following BEST describes a Protection Profile (PP)?

- A. A document that expresses an implementation independent set of security requirements for an IT product that meets specific consumer needs.
- B. A document that is used to develop an IT security product from its security requirements definition.
- C. A document that expresses an implementation dependent set of security requirements which contains only the security functional requirements.
- D. A document that represents evaluated products where there is a one-to-one correspondence between a PP and a Security Target (ST).

**Answer:** A

**NEW QUESTION 265**

- (Exam Topic 11)

Which of the following is the BEST approach to take in order to effectively incorporate the concepts of business continuity into the organization?

- A. Ensure end users are aware of the planning activities
- B. Validate all regulatory requirements are known and fully documented
- C. Develop training and awareness programs that involve all stakeholders
- D. Ensure plans do not violate the organization's cultural objectives and goals

**Answer:** C

**NEW QUESTION 270**

- (Exam Topic 11)

Which of the following is the MOST important element of change management documentation?

- A. List of components involved
- B. Number of changes being made
- C. Business case justification
- D. A stakeholder communication

**Answer:** C

**NEW QUESTION 272**

- (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 274**

- (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 276**

- (Exam Topic 11)

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

What is the best approach for the CISO?

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

#### NEW QUESTION 279

- (Exam Topic 11)

Disaster Recovery Plan (DRP) training material should be

- A. consistent so that all audiences receive the same training.
- B. stored in a fire proof safe to ensure availability when needed.
- C. only delivered in paper format.
- D. presented in a professional looking manner.

**Answer:** A

#### NEW QUESTION 280

- (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 284

- (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 286

- (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 287

- (Exam Topic 11)

Which security approach will BEST minimize Personally Identifiable Information (PII) loss from a data breach?

- A. A strong breach notification process
- B. Limited collection of individuals' confidential data
- C. End-to-end data encryption for data in transit
- D. Continuous monitoring of potential vulnerabilities

**Answer:** B

#### NEW QUESTION 290

- (Exam Topic 11)

An organization lacks a data retention policy. Of the following, who is the BEST person to consult for such requirement?

- A. Application Manager
- B. Database Administrator
- C. Privacy Officer
- D. Finance Manager

**Answer:** C

#### NEW QUESTION 294

- (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 298

- (Exam Topic 11)

Which of the following describes the BEST configuration management practice?

- A. After installing a new system, the configuration files are copied to a separate back-up system and hashed to detect tampering.
- B. After installing a new system, the configuration files are copied to an air-gapped system and hashed to detect tampering.
- C. The firewall rules are backed up to an air-gapped system.
- D. A baseline configuration is created and maintained for all relevant systems.

**Answer:** D

#### NEW QUESTION 303

- (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 305**

- (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 310**

- (Exam Topic 11)

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**NEW QUESTION 313**

- (Exam Topic 11)

The PRIMARY security concern for handheld devices is the

- A. strength of the encryption algorithm.
- B. spread of malware during synchronization.
- C. ability to bypass the authentication mechanism.
- D. strength of the Personal Identification Number (PIN).

**Answer:** C

**NEW QUESTION 317**

- (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 318**

- (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 323**

- (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 326**

- (Exam Topic 11)

What does an organization FIRST review to assure compliance with privacy requirements?

- A. Best practices
- B. Business objectives
- C. Legal and regulatory mandates
- D. Employee's compliance to policies and standards

**Answer:** C

**NEW QUESTION 331**

- (Exam Topic 11)

Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic media.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**NEW QUESTION 336**

- (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 337**

- (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 340

- (Exam Topic 11)

Who is ultimately responsible to ensure that information assets are categorized and adequate measures are taken to protect them?

- A. Data Custodian
- B. Executive Management
- C. Chief Information Security Officer
- D. Data/Information/Business Owners

**Answer:** B

#### NEW QUESTION 341

- (Exam Topic 11)

In the Open System Interconnection (OSI) model, which layer is responsible for the transmission of binary data over a communications network?

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

**Answer:** B

#### NEW QUESTION 346

- (Exam Topic 11)

In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

LAN 4

#### NEW QUESTION 349

- (Exam Topic 11)

Which of the following is the MOST important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?

- A. Application interface entry and endpoints
- B. The likelihood and impact of a vulnerability
- C. Countermeasures and mitigations for vulnerabilities
- D. A data flow diagram for the application and attack surface analysis

**Answer:** D

#### NEW QUESTION 352

- (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 355

- (Exam Topic 11)

Which of the following provides the minimum set of privileges required to perform a job function and restricts the user to a domain with the required privileges?

- A. Access based on rules
- B. Access based on user's role
- C. Access determined by the system
- D. Access based on data sensitivity

**Answer: B**

#### NEW QUESTION 357

- (Exam Topic 12)

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

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

**Answer: B**

#### NEW QUESTION 359

- (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 360

- (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 361

- (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 364

- (Exam Topic 12)

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

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

**Answer: B**

#### NEW QUESTION 366

- (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 368

- (Exam Topic 12)

Between which pair of Open System Interconnection (OSI) Reference Model layers are routers used as a communications device?

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

**Answer:** B

#### NEW QUESTION 369

- (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 373

- (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 376

- (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 381

- (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 383

- (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 386

- (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 388**

- (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 389**

- (Exam Topic 12)

Which of the following is the PRIMARY reason for employing physical security personnel at entry points in facilities where card access is in operation?

- A. To verify that only employees have access to the facility.
- B. To identify present hazards requiring remediation.
- C. To monitor staff movement throughout the facility.
- D. To provide a safe environment for employees.

Answer: D

**NEW QUESTION 393**

- (Exam Topic 12)

What is an advantage of Elliptic Curve Cryptography (ECC)?

- A. Cryptographic approach that does not require a fixed-length key
- B. Military-strength security that does not depend upon secrecy of the algorithm
- C. Opportunity to use shorter keys for the same level of security
- D. Ability to use much longer keys for greater security

Answer: C

**NEW QUESTION 398**

- (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 402**

- (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 406**

- (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 407**

- (Exam Topic 12)

When building a data classification scheme, which of the following is the PRIMARY concern?

- A. Purpose
- B. Cost effectiveness
- C. Availability

D. Authenticity

**Answer:** D

**NEW QUESTION 411**

- (Exam Topic 12)

Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?

- A. Notification tool
- B. Message queuing tool
- C. Security token tool
- D. Synchronization tool

**Answer:** C

**NEW QUESTION 415**

- (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 419**

- (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 423**

- (Exam Topic 13)

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

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

**Answer:** B

**NEW QUESTION 428**

- (Exam Topic 13)

Which of the following is the MOST important security goal when performing application interface testing?

- A. Confirm that all platforms are supported and function properly
- B. Evaluate whether systems or components pass data and control correctly to one another
- C. Verify compatibility of software, hardware, and network connections
- D. Examine error conditions related to external interfaces to prevent application details leakage

**Answer:** B

**NEW QUESTION 431**

- (Exam Topic 13)

Which of the following MUST be in place to recognize a system attack?

- A. Stateful firewall
- B. Distributed antivirus
- C. Log analysis
- D. Passive honeypot

**Answer:** A

**NEW QUESTION 435**

- (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 440

- (Exam Topic 13)

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

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

**Answer:** B

#### NEW QUESTION 443

- (Exam Topic 13)

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

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

**Answer:** A

#### NEW QUESTION 446

- (Exam Topic 13)

Which of the following is the MOST common method of memory protection?

- A. Compartmentalization
- B. Segmentation
- C. Error correction
- D. Virtual Local Area Network (VLAN) tagging

**Answer:** B

#### NEW QUESTION 449

- (Exam Topic 13)

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

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

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

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

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

#### NEW QUESTION 452

- (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 457**

- (Exam Topic 13)

What is the process of removing sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique?

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

**Answer:** A

**NEW QUESTION 459**

- (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 460**

- (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 463**

- (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 464**

- (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 468**

- (Exam Topic 13)

When developing solutions for mobile devices, in which phase of the Software Development Life Cycle (SDLC) should technical limitations related to devices be specified?

- A. Implementation
- B. Initiation
- C. Review
- D. Development

**Answer:** A

**NEW QUESTION 472**

- (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 473

- (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 478

- (Exam Topic 13)

Proven application security principles include which of the following?

- A. Minimizing attack surface area
- B. Hardening the network perimeter
- C. Accepting infrastructure security controls
- D. Developing independent modules

**Answer:** A

#### NEW QUESTION 480

- (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 483

- (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:

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

#### NEW QUESTION 488

- (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 489

- (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 493

- (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 495

- (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 496

- (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 499

- (Exam Topic 13)

Which of the following would MINIMIZE the ability of an attacker to exploit a buffer overflow?

- A. Memory review
- B. Code review
- C. Message division
- D. Buffer division

**Answer:** B

#### NEW QUESTION 502

- (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 505

- (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 510

- (Exam Topic 13)

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

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

**Answer:** C

#### NEW QUESTION 511

- (Exam Topic 13)

Who is accountable for the information within an Information System (IS)?

- A. Security manager
- B. System owner
- C. Data owner
- D. Data processor

**Answer:** B

#### Explanation:

Section: Security Operations

#### NEW QUESTION 513

- (Exam Topic 13)

A security professional determines that a number of outsourcing contracts inherited from a previous merger do not adhere to the current security requirements. Which of the following BEST minimizes the risk of this happening again?

- A. Define additional security controls directly after the merger
- B. Include a procurement officer in the merger team
- C. Verify all contracts before a merger occurs
- D. Assign a compliancy officer to review the merger conditions

**Answer:** D

#### NEW QUESTION 517

- (Exam Topic 13)

Which of the BEST internationally recognized standard for evaluating security products and systems?

- A. Payment Card Industry Data Security Standards (PCI-DSS)
- B. Common Criteria (CC)
- C. Health Insurance Portability and Accountability Act (HIPAA)
- D. Sarbanes-Oxley (SOX)

**Answer:** B

#### NEW QUESTION 522

- (Exam Topic 13)

Which of the following is the GREATEST benefit of implementing a Role Based Access Control (RBAC) system?

- A. Integration using Lightweight Directory Access Protocol (LDAP)
- B. Form-based user registration process
- C. Integration with the organizations Human Resources (HR) system
- D. A considerably simpler provisioning process

**Answer:** D

#### NEW QUESTION 523

- (Exam Topic 13)

What is the correct order of steps in an information security assessment?

Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

#### NEW QUESTION 526

- (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 529

- (Exam Topic 13)

A company receives an email threat informing of an Imminent Distributed Denial of Service (DDoS) attack targeting its web application, unless ransom is paid. Which of the following techniques BEST addresses that threat?

- A. Deploying load balancers to distribute inbound traffic across multiple data centers
- B. Set Up Web Application Firewalls (WAFs) to filter out malicious traffic
- C. Implementing reverse web-proxies to validate each new inbound connection
- D. Coordinate with and utilize capabilities within Internet Service Provider (ISP)

**Answer:** D

#### NEW QUESTION 531

- (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 536

- (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 537

- (Exam Topic 13)

Which of the following techniques is known to be effective in spotting resource exhaustion problems, especially with resources such as processes, memory, and connections?

- A. Automated dynamic analysis
- B. Automated static analysis
- C. Manual code review
- D. Fuzzing

**Answer:** A

#### NEW QUESTION 539

- (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 542

- (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 545

- (Exam Topic 13)

“Stateful” differs from “Static” packet filtering firewalls by being aware of which of the following?

- A. Difference between a new and an established connection
- B. Originating network location
- C. Difference between a malicious and a benign packet payload
- D. Originating application session

**Answer:** A

#### NEW QUESTION 549

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

## Money Back Guarantee

### CISSP Practice Exam Features:

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