

## CISSP Dumps

# Certified Information Systems Security Professional (CISSP)

<https://www.certleader.com/CISSP-dumps.html>



#### 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)

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 3

- (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 4

- (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 5

- (Exam Topic 2)

Which of the following BEST describes the responsibilities of a data owner?

- A. Ensuring quality and validation through periodic audits for ongoing data integrity
- B. Maintaining fundamental data availability, including data storage and archiving
- C. Ensuring accessibility to appropriate users, maintaining appropriate levels of data security
- D. Determining the impact the information has on the mission of the organization

**Answer: C**

#### 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 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 9**

- (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 10**

- (Exam Topic 6)

Which of the following is a PRIMARY benefit of using a formalized security testing report format and structure?

- A. Executive audiences will understand the outcomes of testing and most appropriate next steps for corrective actions to be taken
- B. Technical teams will understand the testing objectives, testing strategies applied, and business risk associated with each vulnerability
- C. Management teams will understand the testing objectives and reputational risk to the organization
- D. Technical and management teams will better understand the testing objectives, results of each test phase, and potential impact levels

**Answer:** D

**NEW QUESTION 10**

- (Exam Topic 7)

Which of the following types of business continuity tests includes assessment of resilience to internal and external risks without endangering live operations?

- A. Walkthrough
- B. Simulation
- C. Parallel
- D. White box

**Answer:** B

**NEW QUESTION 11**

- (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 16**

- (Exam Topic 9)

Internet Protocol (IP) source address spoofing is used to defeat

- A. address-based authentication.
- B. Address Resolution Protocol (ARP).
- C. Reverse Address Resolution Protocol (RARP).
- D. Transmission Control Protocol (TCP) hijacking.

**Answer:** A

**NEW QUESTION 19**

- (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 23**

- (Exam Topic 9)

Logical access control programs are MOST effective when they are

- A. approved by external auditors.
- B. combined with security token technology.
- C. maintained by computer security officers.
- D. made part of the operating system.

**Answer:** D

**NEW QUESTION 27**

- (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 28**

- (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 30**

- (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 33**

- (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 37**

- (Exam Topic 9)

The Structured Query Language (SQL) implements Discretionary Access Controls (DAC) using

- A. INSERT and DELETE.
- B. GRANT and REVOKE.
- C. PUBLIC and PRIVATE.
- D. ROLLBACK and TERMINATE.

**Answer:** B

**NEW QUESTION 41**

- (Exam Topic 9)

Which one of the following considerations has the LEAST impact when considering transmission security?

- A. Network availability
- B. Data integrity
- C. Network bandwidth
- D. Node locations

**Answer:** C

**NEW QUESTION 42**

- (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 46**

- (Exam Topic 9)

Which of the following is an attacker MOST likely to target to gain privileged access to a system?

- A. Programs that write to system resources
- B. Programs that write to user directories
- C. Log files containing sensitive information
- D. Log files containing system calls

**Answer:** A

**NEW QUESTION 50**

- (Exam Topic 9)

The process of mutual authentication involves a computer system authenticating a user and authenticating the

- A. user to the audit process.
- B. computer system to the user.
- C. user's access to all authorized objects.
- D. computer system to the audit process.

**Answer:** B

**NEW QUESTION 53**

- (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 57**

- (Exam Topic 9)

In a financial institution, who has the responsibility for assigning the classification to a piece of information?

- A. Chief Financial Officer (CFO)
- B. Chief Information Security Officer (CISO)
- C. Originator or nominated owner of the information
- D. Department head responsible for ensuring the protection of the information

**Answer:** C

**NEW QUESTION 61**

- (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 63**

- (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 65**

- (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 69**

- (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 72**

- (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 74**

- (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 79**

- (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 81**

- (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 82**

- (Exam Topic 9)

Which of the following is the FIRST step of a penetration test plan?

- A. Analyzing a network diagram of the target network
- B. Notifying the company's customers
- C. Obtaining the approval of the company's management
- D. Scheduling the penetration test during a period of least impact

**Answer:** C

**NEW QUESTION 84**

- (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 85**

- (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 88**

- (Exam Topic 9)

When constructing an Information Protection Policy (IPP), it is important that the stated rules are necessary, adequate, and

- A. flexible.
- B. confidential.
- C. focused.
- D. achievable.

**Answer:** D

**NEW QUESTION 91**

- (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 96**

- (Exam Topic 9)

A system has been scanned for vulnerabilities and has been found to contain a number of communication ports that have been opened without authority. To which of the following might this system have been subjected?

- A. Trojan horse
- B. Denial of Service (DoS)
- C. Spoofing
- D. Man-in-the-Middle (MITM)

**Answer:** A

**NEW QUESTION 100**

- (Exam Topic 9)

By allowing storage communications to run on top of Transmission Control Protocol/Internet Protocol (TCP/IP) with a Storage Area Network (SAN), the

- A. confidentiality of the traffic is protected.
- B. opportunity to sniff network traffic exists.
- C. opportunity for device identity spoofing is eliminated.
- D. storage devices are protected against availability attacks.

**Answer:**

B

**NEW QUESTION 102**

- (Exam Topic 9)

The goal of software assurance in application development is to

- A. enable the development of High Availability (HA) systems.
- B. facilitate the creation of Trusted Computing Base (TCB) systems.
- C. prevent the creation of vulnerable applications.
- D. encourage the development of open source applications.

**Answer: C**

**NEW QUESTION 107**

- (Exam Topic 9)

Which of the following wraps the decryption key of a full disk encryption implementation and ties the hard disk drive to a particular device?

- A. Trusted Platform Module (TPM)
- B. Preboot eXecution Environment (PXE)
- C. Key Distribution Center (KDC)
- D. Simple Key-Management for Internet Protocol (SKIP)

**Answer: A**

**NEW QUESTION 108**

- (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 113**

- (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 116**

- (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 121**

- (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 125**

- (Exam Topic 10)

Which of the following is the MOST beneficial to review when performing an IT audit?

- A. Audit policy
- B. Security log
- C. Security policies
- D. Configuration settings



**Answer:** C

**NEW QUESTION 127**

- (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 addition to web browsers, what PRIMARY areas need to be addressed concerning mobile code used for malicious purposes?

- A. Text editors, database, and Internet phone applications
- B. Email, presentation, and database applications
- C. Image libraries, presentation and spreadsheet applications
- D. Email, media players, and instant messaging applications

**Answer:** D

**NEW QUESTION 129**

- (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 134**

- (Exam Topic 10)

Which of the following is the MOST difficult to enforce when using cloud computing?

- A. Data access
- B. Data backup
- C. Data recovery
- D. Data disposal

**Answer:** D

**NEW QUESTION 139**

- (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 MUST the plan include in order to reduce client-side exploitation?

- A. Approved web browsers
- B. Network firewall procedures
- C. Proxy configuration
- D. Employee education

**Answer:** D

**NEW QUESTION 143**

- (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
Systems	Systems	Authenticatio

#### NEW QUESTION 144

- (Exam Topic 10)

What is the BEST first step for determining if the appropriate security controls are in place for protecting data at rest?

- A. Identify regulatory requirements
- B. Conduct a risk assessment
- C. Determine business drivers
- D. Review the security baseline configuration

**Answer: B**

#### NEW QUESTION 147

- (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 151

- (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 155

- (Exam Topic 10)

Which of the following methods provides the MOST protection for user credentials?

- A. Forms-based authentication
- B. Digest authentication
- C. Basic authentication
- D. Self-registration

**Answer: B**

#### NEW QUESTION 160

- (Exam Topic 10)

Which of the following is a critical factor for implementing a successful data classification program?

- A. Executive sponsorship
- B. Information security sponsorship
- C. End-user acceptance
- D. Internal audit acceptance

**Answer: A**

#### NEW QUESTION 162

- (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 164

- (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 166

- (Exam Topic 10)

Which of the following MUST system and database administrators be aware of and apply when configuring systems used for storing personal employee data?

- A. Secondary use of the data by business users
- B. The organization's security policies and standards
- C. The business purpose for which the data is to be used
- D. The overall protection of corporate resources and data

**Answer:** B

#### NEW QUESTION 170

- (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. Which of the following BEST describes the access control methodology used?

- A. Least privilege
- B. Lattice Based Access Control (LBAC)
- C. Role Based Access Control (RBAC)
- D. Lightweight Directory Access Control (LDAP)

**Answer:** C

#### NEW QUESTION 175

- (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 180

- (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 181

- (Exam Topic 10)

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

**Answer: C**

#### **NEW QUESTION 186**

- (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.

What additional considerations are there if the third party is located in a different country?

- A. The organizational structure of the third party and how it may impact timelines within the organization
- B. The ability of the third party to respond to the organization in a timely manner and with accurate information
- C. The effects of transborder data flows and customer expectations regarding the storage or processing of their data
- D. The quantity of data that must be provided to the third party and how it is to be used

**Answer: C**

#### **NEW QUESTION 189**

- (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 190**

- (Exam Topic 11)

What is the MOST effective method of testing custom application code?

- A. Negative testing
- B. White box testing
- C. Penetration testing
- D. Black box testing

**Answer: B**

#### **NEW QUESTION 195**

- (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 196**

- (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 201**

- (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 203**

- (Exam Topic 11)

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

Step

Order

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Step

Order

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

**NEW QUESTION 205**

- (Exam Topic 11)

What should happen when an emergency change to a system must be performed?

- A. The change must be given priority at the next meeting of the change control board.
- B. Testing and approvals must be performed quickly.
- C. The change must be performed immediately and then submitted to the change board.
- D. The change is performed and a notation is made in the system log.

**Answer:** B

**NEW QUESTION 208**

- (Exam Topic 11)

After a thorough analysis, it was discovered that a perpetrator compromised a network by gaining access to the network through a Secure Socket Layer (SSL) Virtual Private Network (VPN) gateway. The perpetrator guessed a username and brute forced the password to gain access. Which of the following BEST mitigates this issue?

- A. Implement strong passwords authentication for VPN
- B. Integrate the VPN with centralized credential stores
- C. Implement an Internet Protocol Security (IPSec) client
- D. Use two-factor authentication mechanisms

**Answer:** D



**NEW QUESTION 209**

- (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 214**

- (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 218**

- (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 222**

- (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 226**

- (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 227**

- (Exam Topic 11)

Which of the following standards/guidelines requires an Information Security Management System (ISMS) to be defined?

- A. International Organization for Standardization (ISO) 27000 family
- B. Information Technology Infrastructure Library (ITIL)
- C. Payment Card Industry Data Security Standard (PCIDSS)
- D. ISO/IEC 20000

**Answer:** A

**NEW QUESTION 231**

- (Exam Topic 11)

Which of the following roles has the obligation to ensure that a third party provider is capable of processing and handling data in a secure manner and meeting the standards set by the organization?

- A. Data Custodian
- B. Data Owner
- C. Data Creator
- D. Data User



**Answer:** B

**NEW QUESTION 236**

- (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 238**

- (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 243**

- (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 244**

- (Exam Topic 11)

For privacy protected data, which of the following roles has the highest authority for establishing dissemination rules for the data?

- A. Information Systems Security Officer
- B. Data Owner
- C. System Security Architect
- D. Security Requirements Analyst

**Answer:** B

**NEW QUESTION 246**

- (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 249**

- (Exam Topic 11)

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

## Security Engineering

## Definition

Security Risk Treatment

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

Threat Assessment

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

Protection Needs

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

Risk

The method used to identify feasible security risk mitigation options and plans.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

## Security Engineering

## Definition

Security Risk Treatment

Protection Needs

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

Threat Assessment

Risk

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

Protection Needs

Threat Assessment

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

Risk

Security Risk Treatment

The method used to identify feasible security risk mitigation options and plans.

### NEW QUESTION 254

- (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 259

- (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 263

- (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 265**

- (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.

<u>Sequence</u>		<u>Method</u>
1		Overwriting
2		Degaussing
3		Destruction
4		Deleting

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

<u>Sequence</u>		<u>Method</u>
1	3	Overwriting
2	2	Degaussing
3	1	Destruction
4	4	Deleting

**NEW QUESTION 269**

- (Exam Topic 11)

Discretionary Access Control (DAC) is based on which of the following?

- A. Information source and destination
- B. Identification of subjects and objects
- C. Security labels and privileges
- D. Standards and guidelines

**Answer:** B

**NEW QUESTION 272**

- (Exam Topic 11)

For an organization considering two-factor authentication for secure network access, which of the following is MOST secure?

- A. Challenge response and private key
- B. Digital certificates and Single Sign-On (SSO)
- C. Tokens and passphrase
- D. Smart card and biometrics

**Answer:** D

**NEW QUESTION 275**

- (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 278**

- (Exam Topic 11)

Which of the following BEST avoids data remanence disclosure for cloud hosted resources?

- A. Strong encryption and deletion of the keys after data is deleted.
- B. Strong encryption and deletion of the virtual host after data is deleted.
- C. Software based encryption with two factor authentication.
- D. Hardware based encryption on dedicated physical servers.

**Answer:** A

**NEW QUESTION 281**

- (Exam Topic 11)

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

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

**Answer:** C

**NEW QUESTION 282**

- (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 283**

- (Exam Topic 11)

A Simple Power Analysis (SPA) attack against a device directly observes which of the following?

- A. Static discharge
- B. Consumption
- C. Generation
- D. Magnetism

**Answer:** B

**NEW QUESTION 284**

- (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 287**

- (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 291**

- (Exam Topic 11)

The 802.1x standard provides a framework for what?

- A. Network authentication for only wireless networks
- B. Network authentication for wired and wireless networks
- C. Wireless encryption using the Advanced Encryption Standard (AES)
- D. Wireless network encryption using Secure Sockets Layer (SSL)

**Answer:** B

**NEW QUESTION 295**

- (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 300**

- (Exam Topic 11)

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

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

**Answer:** B

**NEW QUESTION 303**

- (Exam Topic 11)

An organization is found lacking the ability to properly establish performance indicators for its Web hosting solution during an audit. What would be the MOST probable cause?

- A. Improper deployment of the Service-Oriented Architecture (SOA)
- B. Absence of a Business Intelligence (BI) solution
- C. Inadequate cost modeling
- D. Insufficient Service Level Agreement (SLA)

**Answer:** D

**NEW QUESTION 306**

- (Exam Topic 11)

The MAIN reason an organization conducts a security authorization process is to

- A. force the organization to make conscious risk decisions.
- B. assure the effectiveness of security controls.
- C. assure the correct security organization exists.
- D. force the organization to enlist management support.

**Answer:** A

**NEW QUESTION 307**

- (Exam Topic 11)

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

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

**Answer:** B

**NEW QUESTION 311**

- (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 316**

- (Exam Topic 12)

Match the name of access control model with its associated restriction.

Drag each access control model to its appropriate restriction access on the right.



<u>Access Control Model</u>		<u>Restrictions</u>
Mandatory Access Control		End user cannot set controls
Discretionary Access Control (DAC)		Subject has total control over objects
Role Based Access Control (RBAC)		Dynamically assigns permissions to particular duties based on job function
Rule based access control		Dynamically assigns roles to subjects based on criteria assigned by a custodian

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Mandatory Access Control – End user cannot set controls

Discretionary Access Control (DAC) – Subject has total control over objects

Role Based Access Control (RBAC) – Dynamically assigns roles permissions to particular duties based on job function

Rule Based access control – Dynamically assigns roles to subjects based on criteria assigned by a custodian.

**NEW QUESTION 318**

- (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 321**

- (Exam Topic 12)

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

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

**Answer:** A

**NEW QUESTION 322**

- (Exam Topic 12)

An Intrusion Detection System (IDS) has recently been deployed in a Demilitarized Zone (DMZ). The IDS detects a flood of malformed packets. Which of the following BEST describes what has occurred?

- A. Denial of Service (DoS) attack
- B. Address Resolution Protocol (ARP) spoof
- C. Buffer overflow
- D. Ping flood attack

**Answer:** A

**NEW QUESTION 326**

- (Exam Topic 12)

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

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

**Answer:** D

**NEW QUESTION 331**

- (Exam Topic 12)

Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item?

- A. Property book
- B. Chain of custody form
- C. Search warrant return
- D. Evidence tag

**Answer:** D

#### **NEW QUESTION 332**

- (Exam Topic 12)

What does the Maximum Tolerable Downtime (MTD) determine?

- A. The estimated period of time a business critical database can remain down before customers are affected.
- B. The fixed length of time a company can endure a disaster without any Disaster Recovery (DR) planning
- C. The estimated period of time a business can remain interrupted beyond which it risks never recovering
- D. The fixed length of time in a DR process before redundant systems are engaged

**Answer:** C

#### **NEW QUESTION 337**

- (Exam Topic 12)

What operations role is responsible for protecting the enterprise from corrupt or contaminated media?

- A. Information security practitioner
- B. Information librarian
- C. Computer operator
- D. Network administrator

**Answer:** B

#### **NEW QUESTION 341**

- (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 342**

- (Exam Topic 12)

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

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

**Answer:** A

#### **NEW QUESTION 347**

- (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 349**

- (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 351**

- (Exam Topic 12)

Which one of the following activities would present a significant security risk to organizations when employing a Virtual Private Network (VPN) solution?

- A. VPN bandwidth
- B. Simultaneous connection to other networks
- C. Users with Internet Protocol (IP) addressing conflicts
- D. Remote users with administrative rights

**Answer: B**

**NEW QUESTION 352**

- (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 355**

- (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 360**

- (Exam Topic 12)

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

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

**Answer: D**

**NEW QUESTION 365**

- (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 366**

- (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 369**

- (Exam Topic 12)

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

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

**Answer: D**

**NEW QUESTION 370**

- (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 372**

- (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 375**

- (Exam Topic 12)

Which of the following is the PRIMARY reason to perform regular vulnerability scanning of an organization network?

- A. Provide vulnerability reports to management.
- B. Validate vulnerability remediation activities.
- C. Prevent attackers from discovering vulnerabilities.
- D. Remediate known vulnerabilities.

**Answer:** B

**NEW QUESTION 377**

- (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 381**

- (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 383**

- (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 385**

- (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 389**

- (Exam Topic 13)

A company seizes a mobile device suspected of being used in committing fraud. What would be the BEST method used by a forensic examiner to isolate the powered-on device from the network and preserve the evidence?

- A. Put the device in airplane mode
- B. Suspend the account with the telecommunication provider
- C. Remove the SIM card
- D. Turn the device off

**Answer:** A

#### **NEW QUESTION 390**

- (Exam Topic 13)

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

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

**Answer:** C

#### **NEW QUESTION 391**

- (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 395**

- (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 399**

- (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 400**

- (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 404**

- (Exam Topic 13)

The organization would like to deploy an authorization mechanism for an Information Technology (IT) infrastructure project with high employee turnover. Which access control mechanism would be preferred?

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

**Answer:** D

**NEW QUESTION 405**

- (Exam Topic 13)

Within the company, desktop clients receive Internet Protocol (IP) address over Dynamic Host Configuration Protocol (DHCP). Which of the following represents a valid measure to help protect the network against unauthorized access?

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

**Answer:** B

**NEW QUESTION 407**

- (Exam Topic 13)

What is the second step in the identity and access provisioning lifecycle?

- A. Provisioning
- B. Review
- C. Approval
- D. Revocation

**Answer:** B

**NEW QUESTION 412**

- (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 413**

- (Exam Topic 13)

Transport Layer Security (TLS) provides which of the following capabilities for a remote access server?

- A. Transport layer handshake compression
- B. Application layer negotiation
- C. Peer identity authentication
- D. Digital certificate revocation

**Answer:** C

**NEW QUESTION 418**

- (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 419**

- (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 420**

- (Exam Topic 13)

A chemical plant wants to upgrade the Industrial Control System (ICS) to transmit data using Ethernet instead of RS422. The project manager wants to simplify administration and maintenance by utilizing the office network infrastructure and staff to implement this upgrade. Which of the following is the GREATEST impact on security for the network?

- A. The network administrators have no knowledge of ICS
- B. The ICS is now accessible from the office network
- C. The ICS does not support the office password policy
- D. RS422 is more reliable than Ethernet

**Answer:** B

**NEW QUESTION 424**

- (Exam Topic 13)

What does a Synchronous (SYN) flood attack do?

- A. Forces Transmission Control Protocol /Internet Protocol (TCP/IP) connections into a reset state
- B. Establishes many new Transmission Control Protocol / Internet Protocol (TCP/IP) connections
- C. Empties the queue of pending Transmission Control Protocol /Internet Protocol (TCP/IP) requests
- D. Exceeds the limits for new Transmission Control Protocol /Internet Protocol (TCP/IP) connections

**Answer:** B

**NEW QUESTION 425**

- (Exam Topic 13)

Who has the PRIMARY responsibility to ensure that security objectives are aligned with organization goals?

- A. Senior management
- B. Information security department
- C. Audit committee
- D. All users

**Answer:** C

**NEW QUESTION 429**

- (Exam Topic 13)

An organization has discovered that users are visiting unauthorized websites using anonymous proxies. Which of the following is the BEST way to prevent future occurrences?

- A. Remove the anonymity from the proxy
- B. Analyze Internet Protocol (IP) traffic for proxy requests
- C. Disable the proxy server on the firewall
- D. Block the Internet Protocol (IP) address of known anonymous proxies

**Answer:** C

**NEW QUESTION 434**

- (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 437**

- (Exam Topic 13)

During examination of Internet history records, the following string occurs within a Unique Resource Locator (URL):

`http://www.companysite.com/products/products.asp?productid=123`

or `1=1`

What type of attack does this indicate?

- A. Directory traversal
- B. Structured Query Language (SQL) injection
- C. Cross-Site Scripting (XSS)
- D. Shellcode injection

**Answer:** C

#### **NEW QUESTION 439**

- (Exam Topic 13)

Attack trees are MOST useful for which of the following?

- A. Determining system security scopes
- B. Generating attack libraries
- C. Enumerating threats
- D. Evaluating Denial of Service (DoS) attacks

**Answer:** A

#### **NEW QUESTION 444**

- (Exam Topic 13)

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

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

**Answer:** A

#### **NEW QUESTION 446**

- (Exam Topic 13)

Which of the following is BEST achieved through the use of eXtensible Access Markup Language (XACML)?

- A. Minimize malicious attacks from third parties
- B. Manage resource privileges
- C. Share digital identities in hybrid cloud
- D. Defined a standard protocol

**Answer:** D

#### **NEW QUESTION 451**

- (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 453**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your CISSP Exam with Our Prep Materials Via below:**

<https://www.certleader.com/CISSP-dumps.html>