



ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 2

- (Exam Topic 3)

The use of private and public encryption keys is fundamental in the implementation of which of the following?

- A. Diffie-Hellman algorithm
- B. Secure Sockets Layer (SSL)
- C. Advanced Encryption Standard (AES)
- D. Message Digest 5 (MD5)

Answer: A

NEW QUESTION 3

- (Exam Topic 3)

What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?

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

Answer: D

NEW QUESTION 4

- (Exam Topic 4)

Which of the following is the BEST network defense against unknown types of attacks or stealth attacks in progress?

- A. Intrusion Prevention Systems (IPS)
- B. Intrusion Detection Systems (IDS)
- C. Stateful firewalls
- D. Network Behavior Analysis (NBA) tools

Answer: D

NEW QUESTION 5

- (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 6

- (Exam Topic 5)

What is the BEST approach for controlling access to highly sensitive information when employees have the same level of security clearance?

- A. Audit logs
- B. Role-Based Access Control (RBAC)
- C. Two-factor authentication
- D. Application of least privilege

Answer: B

NEW QUESTION 7

- (Exam Topic 6)

A Virtual Machine (VM) environment has five guest Operating Systems (OS) and provides strong isolation. What MUST an administrator review to audit a user's access to data files?

- A. Host VM monitor audit logs
- B. Guest OS access controls
- C. Host VM access controls
- D. Guest OS audit logs

Answer: A

NEW QUESTION 8

- (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 9

- (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 10

- (Exam Topic 8)

A Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. The program is not working as expected. What is the MOST probable security feature of Java preventing the program from operating as intended?

- A. Least privilege
- B. Privilege escalation
- C. Defense in depth
- D. Privilege bracketing

Answer: A

NEW QUESTION 10

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 11

- (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 12

- (Exam Topic 9)

Copyright provides protection for which of the following?

- A. Ideas expressed in literary works
- B. A particular expression of an idea
- C. New and non-obvious inventions
- D. Discoveries of natural phenomena

Answer: B

NEW QUESTION 13

- (Exam Topic 9)

Why is a system's criticality classification important in large organizations?

- A. It provides for proper prioritization and scheduling of security and maintenance tasks.

- B. It reduces critical system support workload and reduces the time required to apply patches.
- C. It allows for clear systems status communications to executive management.
- D. It provides for easier determination of ownership, reducing confusion as to the status of the asset.

Answer: A

NEW QUESTION 17

- (Exam Topic 9)

Checking routing information on e-mail to determine it is in a valid format and contains valid information is an example of which of the following anti-spam approaches?

- A. Simple Mail Transfer Protocol (SMTP) blacklist
- B. Reverse Domain Name System (DNS) lookup
- C. Hashing algorithm
- D. Header analysis

Answer: D

NEW QUESTION 19

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 20

- (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 25

- (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 29

- (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 34

- (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 35

- (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 36

- (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 39

- (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 43

- (Exam Topic 9)

Which one of the following security mechanisms provides the BEST way to restrict the execution of privileged procedures?

- A. Role Based Access Control (RBAC)
- B. Biometric access control
- C. Federated Identity Management (IdM)
- D. Application hardening

Answer: A

NEW QUESTION 45

- (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 47

- (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 49

- (Exam Topic 9)

Which one of the following describes granularity?

- A. Maximum number of entries available in an Access Control List (ACL)
- B. Fineness to which a trusted system can authenticate users
- C. Number of violations divided by the number of total accesses
- D. Fineness to which an access control system can be adjusted

Answer: D

NEW QUESTION 52

- (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 54

- (Exam Topic 9)

The BEST way to check for good security programming practices, as well as auditing for possible backdoors, is to conduct

- A. log auditing.
- B. code reviews.
- C. impact assessments.
- D. static analysis.

Answer: B

NEW QUESTION 59

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 61

- (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 62

- (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 64

- (Exam Topic 9)

Which of the following defines the key exchange for Internet Protocol Security (IPSec)?

- A. Secure Sockets Layer (SSL) key exchange
- B. Internet Key Exchange (IKE)
- C. Security Key Exchange (SKE)
- D. Internet Control Message Protocol (ICMP)

Answer: B

NEW QUESTION 69

- (Exam Topic 9)

Why MUST a Kerberos server be well protected from unauthorized access?

- A. It contains the keys of all clients.
- B. It always operates at root privilege.
- C. It contains all the tickets for services.
- D. It contains the Internet Protocol (IP) address of all network entities.

Answer:

A

NEW QUESTION 74

- (Exam Topic 9)

When designing a networked Information System (IS) where there will be several different types of individual access, what is the FIRST step that should be taken to ensure all access control requirements are addressed?

- A. Create a user profile.
- B. Create a user access matrix.
- C. Develop an Access Control List (ACL).
- D. Develop a Role Based Access Control (RBAC) list.

Answer: B

NEW QUESTION 77

- (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 78

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 80

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 85

- (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 88

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 92

- (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 97

- (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 101

- (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 103

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 104

- (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 109

- (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 112

- (Exam Topic 10)

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

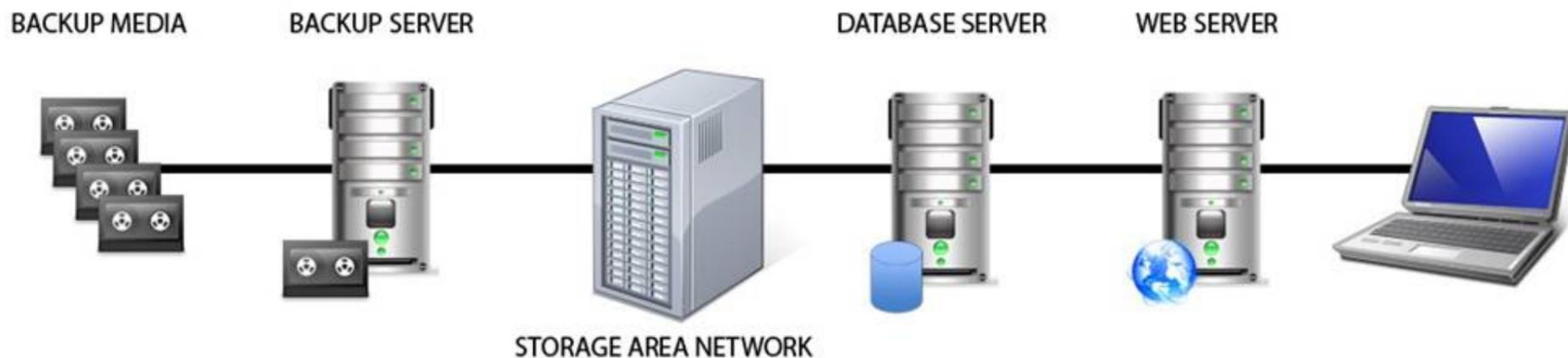
- A. Experience in the industry
- B. Definition of security profiles
- C. Human resource planning efforts
- D. Procedures in systems development

Answer: D

NEW QUESTION 115

- (Exam Topic 10)

Identify the component that MOST likely lacks digital accountability related to information access. Click on the correct device in the image below.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Backup Media

Reference: Official (ISC)2 Guide to the CISSP CBK, Third Edition page 1029

NEW QUESTION 120

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 125

- (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 126

- (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 131

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 132

- (Exam Topic 10)

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

- A. Masquerading, salami, malware, polymorphism
- B. Brute force, dictionary, phishing, keylogger

- C. Zeus, netbus, rabbit, turtle
- D. Token, biometrics, IDS, DLP

Answer: B

NEW QUESTION 137

- (Exam Topic 10)

Which of the following is required to determine classification and ownership?

- A. System and data resources are properly identified
- B. Access violations are logged and audited
- C. Data file references are identified and linked
- D. System security controls are fully integrated

Answer: A

NEW QUESTION 140

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

Answer: D

NEW QUESTION 141

- (Exam Topic 10)

What is the PRIMARY advantage of using automated application security testing tools?

- A. The application can be protected in the production environment.
- B. Large amounts of code can be tested using fewer resources.
- C. The application will fail less when tested using these tools.
- D. Detailed testing of code functions can be performed.

Answer: B

NEW QUESTION 145

- (Exam Topic 10)

What is a common challenge when implementing Security Assertion Markup Language (SAML) for identity integration between on-premise environment and an external identity provider service?

- A. Some users are not provisioned into the service.
- B. SAML tokens are provided by the on-premise identity provider.
- C. Single users cannot be revoked from the service.
- D. SAML tokens contain user information.

Answer: A

NEW QUESTION 146

- (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 148

- (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 150

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 154

- (Exam Topic 10)

Which of the following actions MUST be taken if a vulnerability is discovered during the maintenance stage in a System Development Life Cycle (SDLC)?

- A. Make changes following principle and design guidelines.
- B. Stop the application until the vulnerability is fixed.
- C. Report the vulnerability to product owner.
- D. Monitor the application and review code.

Answer: C

NEW QUESTION 157

- (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 159

- (Exam Topic 10)

During the procurement of a new information system, it was determined that some of the security requirements were not addressed in the system specification. Which of the following is the MOST likely reason for this?

- A. The procurement officer lacks technical knowledge.
- B. The security requirements have changed during the procurement process.
- C. There were no security professionals in the vendor's bidding team.
- D. The description of the security requirements was insufficient.

Answer: D

NEW QUESTION 164

- (Exam Topic 10)

Refer to the information below to answer the question.

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

Table A

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

Table B

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

In a Bell-LaPadula system, which user cannot write to File 3?

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

Answer: D

NEW QUESTION 166

- (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.

Following best practice, where should the permitted access for each department and job classification combination be specified?

- A. Security procedures
- B. Security standards
- C. Human resource policy
- D. Human resource standards

Answer: B

NEW QUESTION 170

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement. Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?

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

Answer: A

NEW QUESTION 173

- (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 could have MOST likely prevented the Peer-to-Peer (P2P) program from being installed on the computer?

- A. Removing employee's full access to the computer
- B. Supervising their child's use of the computer
- C. Limiting computer's access to only the employee
- D. Ensuring employee understands their business conduct guidelines

Answer: A

NEW QUESTION 175

- (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 180

- (Exam Topic 10)

Refer to the information below to answer the question.

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

The security program can be considered effective when

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

Answer: D

NEW QUESTION 183

- (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 188

- (Exam Topic 10)

An organization's data policy MUST include a data retention period which is based on

- A. application dismissal.
- B. business procedures.
- C. digital certificates expiration.
- D. regulatory compliance.

Answer: D

NEW QUESTION 190

- (Exam Topic 10)

Without proper signal protection, embedded systems may be prone to which type of attack?

- A. Brute force
- B. Tampering
- C. Information disclosure
- D. Denial of Service (DoS)

Answer: C

NEW QUESTION 193

- (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 197

- (Exam Topic 10)

During an audit, the auditor finds evidence of potentially illegal activity. Which of the following is the MOST appropriate action to take?

- A. Immediately call the police
- B. Work with the client to resolve the issue internally
- C. Advise the person performing the illegal activity to cease and desist
- D. Work with the client to report the activity to the appropriate authority

Answer: D

NEW QUESTION 198

- (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 200

- (Exam Topic 10)

When using third-party software developers, which of the following is the MOST effective method of providing software development Quality Assurance (QA)?

- A. Retain intellectual property rights through contractual wording.
- B. Perform overlapping code reviews by both parties.
- C. Verify that the contractors attend development planning meetings.
- D. Create a separate contractor development environment.

Answer: B

NEW QUESTION 205

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 207

- (Exam Topic 10)

What is the MOST important reason to configure unique user IDs?

- A. Supporting accountability
- B. Reducing authentication errors
- C. Preventing password compromise
- D. Supporting Single Sign On (SSO)

Answer: A

NEW QUESTION 212

- (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.

Aside from the potential records which may have been viewed, which of the following should be the PRIMARY concern regarding the database information?

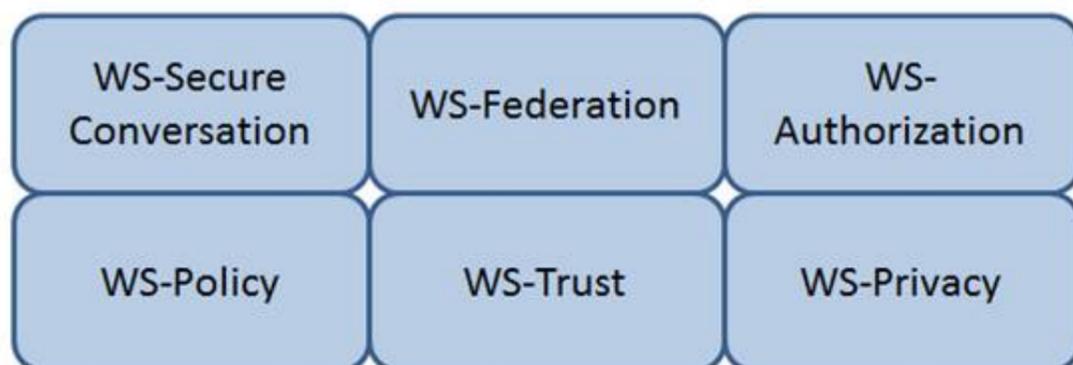
- A. Unauthorized database changes
- B. Integrity of security logs
- C. Availability of the database
- D. Confidentiality of the incident

Answer: A

NEW QUESTION 216

- (Exam Topic 11)

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

WS-Authorization

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

NEW QUESTION 219

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 224

- (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 228

- (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 229

- (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 233

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 235

- (Exam Topic 11)

Data remanence refers to which of the following?

- A. The remaining photons left in a fiber optic cable after a secure transmission.
- B. The retention period required by law or regulation.
- C. The magnetic flux created when removing the network connection from a server or personal computer.
- D. The residual information left on magnetic storage media after a deletion or erasure.

Answer: D

NEW QUESTION 236

- (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 238

- (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 243

- (Exam Topic 11)

A mobile device application that restricts the storage of user information to just that which is needed to accomplish lawful business goals adheres to what privacy principle?

- A. Onward transfer
- B. Collection Limitation
- C. Collector Accountability
- D. Individual Participation

Answer: B

NEW QUESTION 246

- (Exam Topic 11)

How can lessons learned from business continuity training and actual recovery incidents BEST be used?

- A. As a means for improvement
- B. As alternative options for awareness and training
- C. As indicators of a need for policy
- D. As business function gap indicators

Answer: A

NEW QUESTION 247

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 252

- (Exam Topic 11)

Regarding asset security and appropriate retention, which of the following INITIAL top three areas are important to focus on?

- A. Security control baselines, access controls, employee awareness and training
- B. Human resources, asset management, production management
- C. Supply chain lead time, inventory control, encryption
- D. Polygraphs, crime statistics, forensics

Answer: A

NEW QUESTION 256

- (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 260

- (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 265

- (Exam Topic 11)

During a fingerprint verification process, which of the following is used to verify identity and authentication?

- A. A pressure value is compared with a stored template
- B. Sets of digits are matched with stored values
- C. A hash table is matched to a database of stored value
- D. A template of minutiae is compared with a stored template

Answer: D

NEW QUESTION 269

- (Exam Topic 11)

How does Encapsulating Security Payload (ESP) in transport mode affect the Internet Protocol (IP)?

- A. Encrypts and optionally authenticates the IP header, but not the IP payload
- B. Encrypts and optionally authenticates the IP payload, but not the IP header
- C. Authenticates the IP payload and selected portions of the IP header
- D. Encrypts and optionally authenticates the complete IP packet

Answer: B

NEW QUESTION 273

- (Exam Topic 11)

A security professional is asked to provide a solution that restricts a bank teller to only perform a savings deposit transaction but allows a supervisor to perform corrections after the transaction. Which of the following is the MOST effective solution?

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

Answer: C

NEW QUESTION 274

- (Exam Topic 11)

Secure Sockets Layer (SSL) encryption protects

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

Answer: C

NEW QUESTION 276

- (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 279

- (Exam Topic 11)

The PRIMARY security concern for handheld devices is the

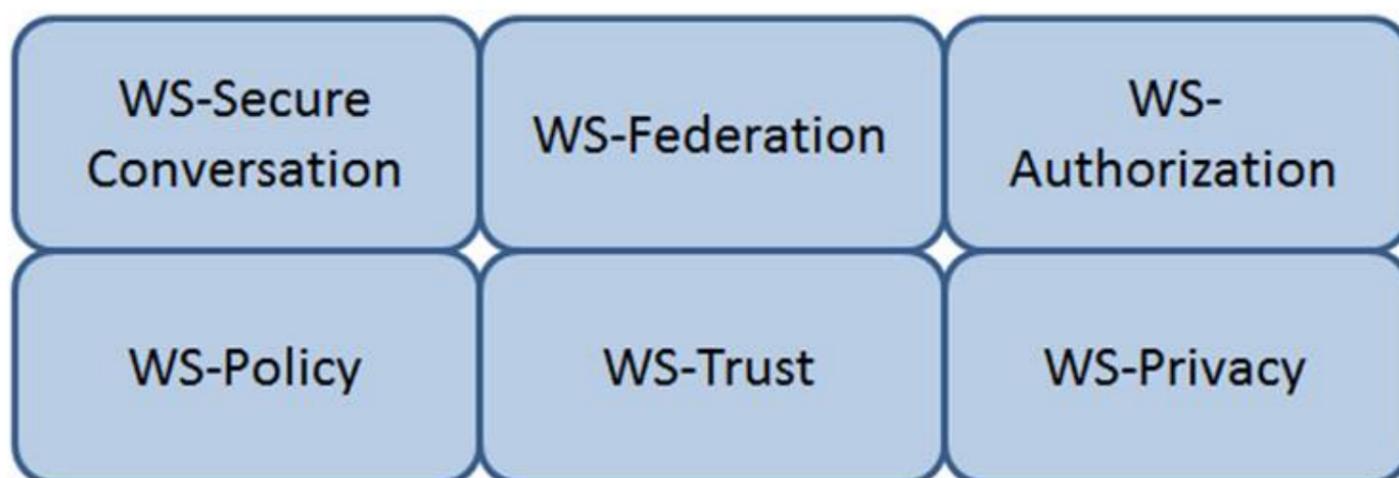
- A. strength of the encryption algorithm.
- B. spread of malware during synchronization.
- C. ability to bypass the authentication mechanism.
- D. strength of the Personal Identification Number (PIN).

Answer: C

NEW QUESTION 284

- (Exam Topic 11)

Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated? Click on the correct specification in the image below.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

WS-Trust

The protocol used for issuing security tokens is based on WS-Trust. WS-Trust is a Web service specification that builds on WS-Security. It describes a protocol used for issuance, exchange, and validation of security tokens. WS-Trust provides a solution for interoperability by defining a protocol for issuing and exchanging security tokens, based on token format, namespace, or trust boundaries.

Reference: <https://msdn.microsoft.com/en-us/library/ff650503.aspx>

NEW QUESTION 287

- (Exam Topic 11)

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

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

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

Answer: A

NEW QUESTION 292

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 294

- (Exam Topic 11)

What is the PRIMARY goal for using Domain Name System Security Extensions (DNSSEC) to sign records?

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

Answer: A

NEW QUESTION 299

- (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 300

- (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 301

- (Exam Topic 11)

The 802.1x standard provides a framework for what?

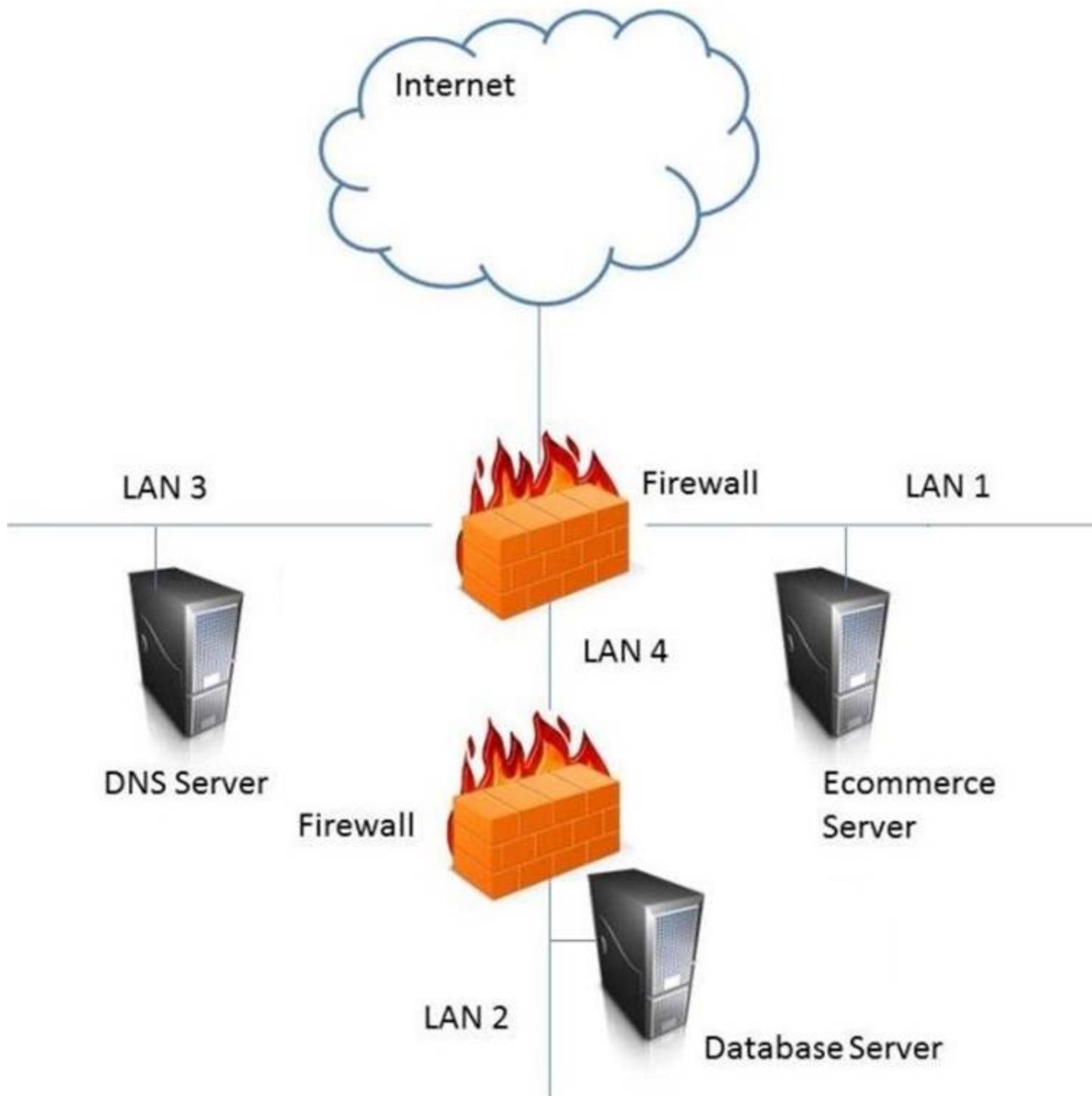
- A. Network authentication for only wireless networks
- B. Network authentication for wired and wireless networks
- C. Wireless encryption using the Advanced Encryption Standard (AES)
- D. Wireless network encryption using Secure Sockets Layer (SSL)

Answer: B

NEW QUESTION 306

- (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 308

- (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 311

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 314

- (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 316

- (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 318

- (Exam Topic 12)

As a best practice, the Security Assessment Report (SAR) should include which of the following sections?

- A. Data classification policy
- B. Software and hardware inventory
- C. Remediation recommendations
- D. Names of participants

Answer: B

NEW QUESTION 323

- (Exam Topic 12)

What is the difference between media marking and media labeling?

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

Answer: D

NEW QUESTION 325

- (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 330

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 333

- (Exam Topic 12)

How should an organization determine the priority of its remediation efforts after a vulnerability assessment has been conducted?

- A. Use an impact-based approach.
- B. Use a risk-based approach.
- C. Use a criticality-based approach.
- D. Use a threat-based approach.

Answer: B

NEW QUESTION 334

- (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 336

- (Exam Topic 12)

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

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

Answer: C

NEW QUESTION 341

- (Exam Topic 12)

Match the types of e-authentication tokens to their description.

Drag each e-authentication token on the left to its corresponding description on the right.

E-Authentication Token

Memorized Secret Token

Out-of-Band Token

Look-up Secret Token

Pre-registered Knowledge Token

Description

A physical or electronic token that stores a set of secrets between the claimant and the credential service provider

A physical token that is uniquely addressable and can receive a verifier-selected secret for one-time use

A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process

A secret shared between the subscriber and credential service provider that is typically character strings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Look-up secret token - A physical or electronic token that stores a set of secrets between the claimant and the credential service provider

Out-of-Band Token - A physical token that is uniquely addressable and can receive a verifier-selected secret for one-time use

Pre-registered Knowledge Token - A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process

Memorized Secret Token - A secret shared between the subscriber and credential service provider that is typically character strings

NEW QUESTION 346

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 347

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 352

- (Exam Topic 12)

Which of the following BEST describes a chosen plaintext attack?

- A. The cryptanalyst can generate ciphertext from arbitrary text.
- B. The cryptanalyst examines the communication being sent back and forth.
- C. The cryptanalyst can choose the key and algorithm to mount the attack.
- D. The cryptanalyst is presented with the ciphertext from which the original message is determined.

Answer: A

NEW QUESTION 354

- (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 356

- (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 360

- (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 362

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 366

- (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 371

- (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 375

- (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 377

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 382

- (Exam Topic 12)

Which of the following is a characteristic of the initialization vector when using Data Encryption Standard (DES)?

- A. It must be known to both sender and receiver.
- B. It can be transmitted in the clear as a random number.
- C. It must be retained until the last block is transmitted.
- D. It can be used to encrypt and decrypt information.

Answer: B

NEW QUESTION 383

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 384

- (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 389

- (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 391

- (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 393

- (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 398

- (Exam Topic 13)

A security compliance manager of a large enterprise wants to reduce the time it takes to perform network, system, and application security compliance audits while increasing quality and effectiveness of the results. What should be implemented to BEST achieve the desired results?

- A. Configuration Management Database (CMDB)
- B. Source code repository
- C. Configuration Management Plan (CMP)
- D. System performance monitoring application

Answer: C

NEW QUESTION 399

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 403

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 405

- (Exam Topic 13)

Why is planning in Disaster Recovery (DR) an interactive process?

- A. It details off-site storage plans
- B. It identifies omissions in the plan
- C. It defines the objectives of the plan
- D. It forms part of the awareness process

Answer: B

NEW QUESTION 410

- (Exam Topic 13)

An organization's security policy delegates to the data owner the ability to assign which user roles have access to a particular resource. What type of authorization mechanism is being used?

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

Answer: A

NEW QUESTION 412

- (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 415

- (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 418

- (Exam Topic 13)

Which of the following are important criteria when designing procedures and acceptance criteria for acquired software?

- A. Code quality, security, and origin
- B. Architecture, hardware, and firmware
- C. Data quality, provenance, and scaling
- D. Distributed, agile, and bench testing

Answer: A

NEW QUESTION 419

- (Exam Topic 13)

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

Security Engineering Term

Definition

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

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.

Protection Needs Assessment

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

Threat Assessment

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

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

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

NEW QUESTION 420

- (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 424

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 427

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 431

- (Exam Topic 13)

Which of the following is the MOST efficient mechanism to account for all staff during a speedy nonemergency evacuation from a large security facility?

- A. Large mantrap where groups of individuals leaving are identified using facial recognition technology
- B. Radio Frequency Identification (RFID) sensors worn by each employee scanned by sensors at each exitdoor
- C. Emergency exits with push bars with coordinates at each exit checking off the individual against a predefined list
- D. Card-activated turnstile where individuals are validated upon exit

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 434

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 437

- (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 438

- (Exam Topic 13)

What is the MOST significant benefit of an application upgrade that replaces randomly generated session keys with certificate based encryption for communications with backend servers?

- A. Non-repudiation
- B. Efficiency
- C. Confidentially
- D. Privacy

Answer: A

NEW QUESTION 441

- (Exam Topic 13)

What does electronic vaulting accomplish?

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

Answer: A

Explanation:

Section: Security Operations

NEW QUESTION 442

- (Exam Topic 13)

Which of the following is a responsibility of the information owner?

- A. Ensure that users and personnel complete the required security training to access the Information System (IS)
- B. Defining proper access to the Information System (IS), including privileges or access rights
- C. Managing identification, implementation, and assessment of common security controls
- D. Ensuring the Information System (IS) is operated according to agreed upon security requirements

Answer: C

NEW QUESTION 444

- (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 445

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 447

- (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 449

- (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 451

- (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 454

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 456

- (Exam Topic 13)

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

- A. A non-volatile tamper-resistant storage for storing both data and signing keys in a secure fashion
- B. A protected Pre-Basic Input/Output System (BIOS) which specifies a method or a metric for "measuring"the state of a computing platform

- C. A secure processor targeted at managing digital keys and accelerating digital signing
- D. A platform-independent software interface for accessing computer functions

Answer: A

NEW QUESTION 458

- (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 461

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 465

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 467

- (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 472

- (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 474

- (Exam Topic 13)

Who would be the BEST person to approve an organizations information security policy?

- A. Chief Information Officer (CIO)
- B. Chief Information Security Officer (CISO)
- C. Chief internal auditor
- D. Chief Executive Officer (CEO)

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 479

- (Exam Topic 13)

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

- A. Application proxy
- B. Port filter
- C. Network boundary router
- D. Access layer switch

Answer: A

NEW QUESTION 484

- (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 487

- (Exam Topic 13)

The security accreditation task of the System Development Life Cycle (SDLC) process is completed at the end of which phase?

- A. System acquisition and development
- B. System operations and maintenance
- C. System initiation
- D. System implementation

Answer: B

NEW QUESTION 492

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CISSP Practice Exam Features:

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

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