



ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 2

- (Exam Topic 1)

Which of the following represents the GREATEST risk to data confidentiality?

- A. Network redundancies are not implemented
- B. Security awareness training is not completed
- C. Backup tapes are generated unencrypted
- D. Users have administrative privileges

Answer: C

NEW QUESTION 3

- (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 4

- (Exam Topic 2)

Which one of the following affects the classification of data?

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

Answer: D

NEW QUESTION 5

- (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 6

- (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 7

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 8

- (Exam Topic 4)

An input validation and exception handling vulnerability has been discovered on a critical web-based system. Which of the following is MOST suited to quickly implement a control?

- A. Add a new rule to the application layer firewall
- B. Block access to the service
- C. Install an Intrusion Detection System (IDS)
- D. Patch the application source code

Answer: A

NEW QUESTION 9

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 10

- (Exam Topic 4)

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 10

- (Exam Topic 5)

A manufacturing organization wants to establish a Federated Identity Management (FIM) system with its 20 different supplier companies. Which of the following is the BEST solution for the manufacturing organization?

- A. Trusted third-party certification
- B. Lightweight Directory Access Protocol (LDAP)
- C. Security Assertion Markup language (SAML)
- D. Cross-certification

Answer: C

NEW QUESTION 11

- (Exam Topic 5)

Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee's salary?

- A. Limit access to predefined queries
- B. Segregate the database into a small number of partitions each with a separate security level
- C. Implement Role Based Access Control (RBAC)
- D. Reduce the number of people who have access to the system for statistical purposes

Answer: C

NEW QUESTION 14

- (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 16

- (Exam Topic 7)

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

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

Answer: A

NEW QUESTION 18

- (Exam Topic 7)

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

Answer: D

NEW QUESTION 22

- (Exam Topic 7)

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

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

Answer: B

NEW QUESTION 25

- (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 26

- (Exam Topic 8)

Which of the following is the BEST method to prevent malware from being introduced into a production environment?

- A. Purchase software from a limited list of retailers
- B. Verify the hash key or certificate key of all updates
- C. Do not permit programs, patches, or updates from the Internet
- D. Test all new software in a segregated environment

Answer: D

NEW QUESTION 31

- (Exam Topic 8)

The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle (SDLC)?

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

Answer: A

Explanation:

Reference <https://online.concordia.edu/computer-science/system-development-life-cycle-phases/>

NEW QUESTION 32

- (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 34

- (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 38

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 42

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 43

- (Exam Topic 9)

An organization allows ping traffic into and out of their network. An attacker has installed a program on the network that uses the payload portion of the ping packet to move data into and out of the network. What type of attack has the organization experienced?

- A. Data leakage
- B. Unfiltered channel
- C. Data emanation
- D. Covert channel

Answer: D

NEW QUESTION 45

- (Exam Topic 9)

What is the term commonly used to refer to a technique of authenticating one machine to another by forging packets from a trusted source?

- A. Man-in-the-Middle (MITM) attack
- B. Smurfing
- C. Session redirect
- D. Spoofing

Answer: D

NEW QUESTION 50

- (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 55

- (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 58

- (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 61

- (Exam Topic 9)

A security professional has just completed their organization's Business Impact Analysis (BIA). Following Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) best practices, what would be the professional's NEXT step?

- A. Identify and select recovery strategies.
- B. Present the findings to management for funding.
- C. Select members for the organization's recovery teams.
- D. Prepare a plan to test the organization's ability to recover its operations.

Answer: A

NEW QUESTION 65

- (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 68

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 69

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 74

- (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 77

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 81

- (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 82

- (Exam Topic 9)

Which of the following can BEST prevent security flaws occurring in outsourced software development?

- A. Contractual requirements for code quality
- B. Licensing, code ownership and intellectual property rights
- C. Certification of the quality and accuracy of the work done
- D. Delivery dates, change management control and budgetary control

Answer: C

NEW QUESTION 84

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 88

- (Exam Topic 9)

A security consultant has been asked to research an organization's legal obligations to protect privacy-related information. What kind of reading material is MOST relevant to this project?

- A. The organization's current security policies concerning privacy issues
- B. Privacy-related regulations enforced by governing bodies applicable to the organization
- C. Privacy best practices published by recognized security standards organizations
- D. Organizational procedures designed to protect privacy information

Answer: B

NEW QUESTION 91

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 95

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 98

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 102

- (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 104

- (Exam Topic 9)

Which of the following is an appropriate source for test data?

- A. Production data that is secured and maintained only in the production environment.
- B. Test data that has no similarities to production data.
- C. Test data that is mirrored and kept up-to-date with production data.
- D. Production data that has been sanitized before loading into a test environment.

Answer: D

NEW QUESTION 107

- (Exam Topic 9)

When implementing controls in a heterogeneous end-point network for an organization, it is critical that

- A. hosts are able to establish network communications.
- B. users can make modifications to their security software configurations.
- C. common software security components be implemented across all hosts.
- D. firewalls running on each host are fully customizable by the user.

Answer: C

NEW QUESTION 108

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 109

- (Exam Topic 9)

What maintenance activity is responsible for defining, implementing, and testing updates to application systems?

- A. Program change control
- B. Regression testing
- C. Export exception control
- D. User acceptance testing

Answer: A

NEW QUESTION 112

- (Exam Topic 9)

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

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

Answer:

B

NEW QUESTION 115

- (Exam Topic 9)

An Intrusion Detection System (IDS) is generating alarms that a user account has over 100 failed login attempts per minute. A sniffer is placed on the network, and a variety of passwords for that user are noted. Which of the following is MOST likely occurring?

- A. A dictionary attack
- B. A Denial of Service (DoS) attack
- C. A spoofing attack
- D. A backdoor installation

Answer: A

NEW QUESTION 118

- (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 121

- (Exam Topic 9)

Which one of the following affects the classification of data?

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

Answer: A

NEW QUESTION 123

- (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 128

- (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 132

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 134

- (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 139

- (Exam Topic 9)

Which Hyper Text Markup Language 5 (HTML5) option presents a security challenge for network data leakage prevention and/or monitoring?

- A. Cross Origin Resource Sharing (CORS)
- B. WebSockets
- C. Document Object Model (DOM) trees
- D. Web Interface Definition Language (IDL)

Answer: B

NEW QUESTION 143

- (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 146

- (Exam Topic 10)

What is the MAIN feature that onion routing networks offer?

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

Answer: C

NEW QUESTION 149

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 153

- (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 158

- (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 162

- (Exam Topic 10)

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

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

Answer: A

NEW QUESTION 166

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 168

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration

functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.

Which of the following will be the PRIMARY security concern as staff is released from the organization?

- A. Inadequate IT support
- B. Loss of data and separation of duties
- C. Undocumented security controls
- D. Additional responsibilities for remaining staff

Answer: B

NEW QUESTION 169

- (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 170

- (Exam Topic 10)

What is the MOST critical factor to achieve the goals of a security program?

- A. Capabilities of security resources
- B. Executive management support
- C. Effectiveness of security management
- D. Budget approved for security resources

Answer: B

NEW QUESTION 175

- (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 178

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 182

- (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 184

- (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 189

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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

Answer: C

NEW QUESTION 193

- (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 197

- (Exam Topic 10)

Refer to the information below to answer the question.

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

Which of the following will MOST likely allow the organization to keep risk at an acceptable level?

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

Answer: C

NEW QUESTION 201

- (Exam Topic 10)

A system is developed so that its business users can perform business functions but not user administration functions. Application administrators can perform administration functions but not user business functions. These capabilities are BEST described as

- A. least privilege.
- B. rule based access controls.
- C. Mandatory Access Control (MAC).
- D. separation of duties.

Answer: D

NEW QUESTION 202

- (Exam Topic 10)

What is the BEST method to detect the most common improper initialization problems in programming languages?

- A. Use and specify a strong character encoding.
- B. Use automated static analysis tools that target this type of weakness.
- C. Perform input validation on any numeric inputs by assuring that they are within the expected range.
- D. Use data flow analysis to minimize the number of false positives.

Answer: B

NEW QUESTION 207

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 210

- (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 214

- (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 219

- (Exam Topic 10)

Host-Based Intrusion Protection (HIPS) systems are often deployed in monitoring or learning mode during their initial implementation. What is the objective of starting in this mode?

- A. Automatically create exceptions for specific actions or files
- B. Determine which files are unsafe to access and blacklist them
- C. Automatically whitelist actions or files known to the system
- D. Build a baseline of normal or safe system events for review

Answer: D

NEW QUESTION 221

- (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 methods is the MOST effective way of removing the Peer-to-Peer (P2P) program from the computer?

- A. Run software uninstall
- B. Re-image the computer
- C. Find and remove all installation files
- D. Delete all cookies stored in the web browser cache

Answer: B

NEW QUESTION 222

- (Exam Topic 10)

Place the following information classification steps in sequential order.

Steps		Order
Declassify information when appropriate		Step
Apply the appropriate security markings		Step
Conduct periodic classification reviews		Step
Assign a classification level		Step
Document the information assets		Step

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Steps		Order
Declassify information when appropriate	Document the information assets	Step
Apply the appropriate security markings	Assign a classification level	Step
Conduct periodic classification reviews	Apply the appropriate security markings	Step
Assign a classification level	Conduct periodic classification reviews	Step
Document the information assets	Declassify information when appropriate	Step

NEW QUESTION 227

- (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 229

- (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 232

- (Exam Topic 10)

Which of the following is the BEST way to determine if a particular system is able to identify malicious software without executing it?

- A. Testing with a Botnet
- B. Testing with an EICAR file
- C. Executing a binary shellcode
- D. Run multiple antivirus programs

Answer: B

NEW QUESTION 235

- (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 238

- (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 241

- (Exam Topic 10)

Which of the following is the BEST countermeasure to brute force login attacks?

- A. Changing all canonical passwords
- B. Decreasing the number of concurrent user sessions
- C. Restricting initial password delivery only in person
- D. Introducing a delay after failed system access attempts

Answer: D

NEW QUESTION 244

- (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 245

- (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 249

- (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 251

- (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 255

- (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 260

- (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 265

- (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 269

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 273

- (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 274

- (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 275

- (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 276

- (Exam Topic 11)

Discretionary Access Control (DAC) restricts access according to

- A. data classification labeling.
- B. page views within an application.
- C. authorizations granted to the user.
- D. management accreditation.

Answer: C

NEW QUESTION 281

- (Exam Topic 11)

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

- A. A strong breach notification process
- B. Limited collection of individuals' confidential data

- C. End-to-end data encryption for data in transit
- D. Continuous monitoring of potential vulnerabilities

Answer: B

NEW QUESTION 284

- (Exam Topic 11)

Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

- A. Concept, Development, Production, Utilization, Support, Retirement
- B. Stakeholder Requirements Definition, Architectural Design, Implementation, Verification, Operation
- C. Acquisition, Measurement, Configuration Management, Production, Operation, Support
- D. Concept, Requirements, Design, Implementation, Production, Maintenance, Support, Disposal

Answer: B

NEW QUESTION 286

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 290

- (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 293

- (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 296

- (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 297

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 298

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 301

- (Exam Topic 11)

Which of the following is an essential step before performing Structured Query Language (SQL) penetration tests on a production system?

- A. Verify countermeasures have been deactivated.
- B. Ensure firewall logging has been activated.
- C. Validate target systems have been backed up.
- D. Confirm warm site is ready to accept connections.

Answer: C

NEW QUESTION 304

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 309

- (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 311

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 313

- (Exam Topic 11)

The PRIMARY security concern for handheld devices is the

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

Answer: C

NEW QUESTION 316

- (Exam Topic 11)

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

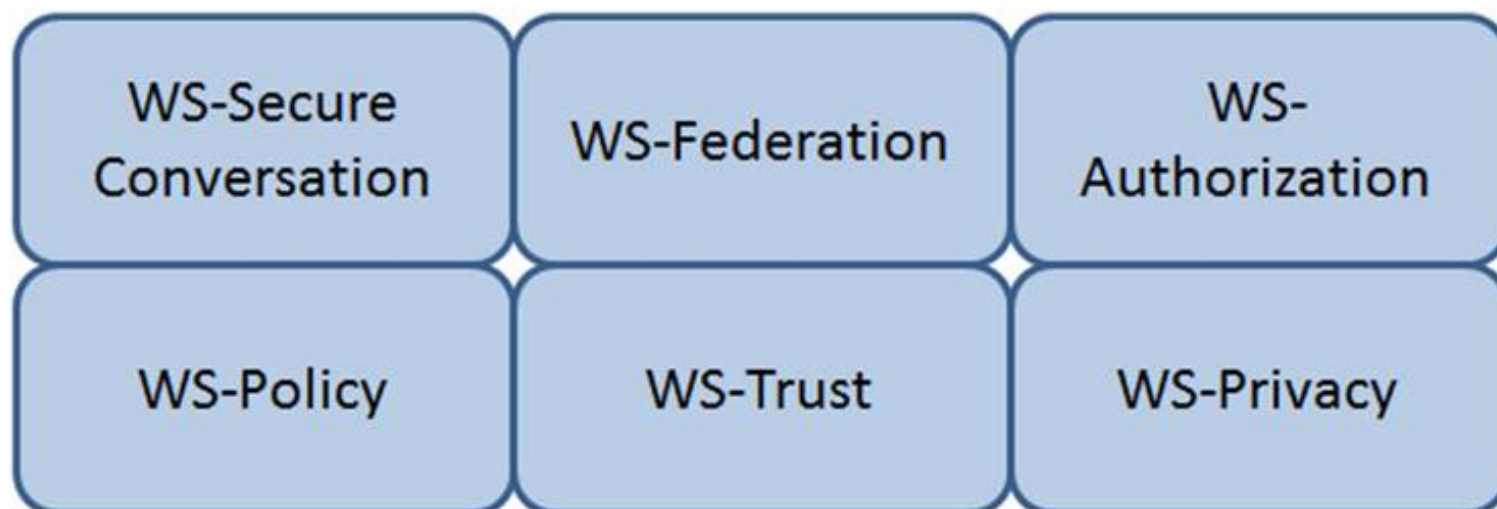
- A. It is useful for testing communications protocols and graphical user interfaces.
- B. It is characterized by the stateless behavior of a process implemented in a function.
- C. Test inputs are obtained from the derived threshold of the given functional specifications.
- D. An entire partition can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

Answer: C

NEW QUESTION 321

- (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 322

- (Exam Topic 11)

Software Code signing is used as a method of verifying what security concept?

- A. Integrity
- B. Confidentiality
- C. Availability
- D. Access Control

Answer: A

NEW QUESTION 323

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 325

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 327

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 330

- (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 332

- (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.

Sequence		Method
1		Overwriting
2		Degaussing
3		Destruction
4		Deleting

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Sequence		Method
1	3	Overwriting
2	2	Degaussing
3	1	Destruction
4	4	Deleting

NEW QUESTION 335

- (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 338

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 339

- (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 344

- (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 349

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 351

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 355

- (Exam Topic 11)

Are companies legally required to report all data breaches?

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

Answer: A

NEW QUESTION 360

- (Exam Topic 11)

While investigating a malicious event, only six days of audit logs from the last month were available. What policy should be updated to address this problem?

- A. Retention
- B. Reporting
- C. Recovery
- D. Remediation

Answer: A

NEW QUESTION 361

- (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 363

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 366

- (Exam Topic 11)

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

What is the best approach for the CISO?

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

What is the best approach for the CISO?

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

Answer: B

NEW QUESTION 370

- (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 375

- (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 380

- (Exam Topic 12)

The restoration priorities of a Disaster Recovery Plan (DRP) are based on which of the following documents?

- A. Service Level Agreement (SLA)
- B. Business Continuity Plan (BCP)
- C. Business Impact Analysis (BIA)
- D. Crisis management plan

Answer: B

NEW QUESTION 384

- (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 387

- (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 391

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 392

- (Exam Topic 12)

Which of the following restricts the ability of an individual to carry out all the steps of a particular process?

- A. Job rotation
- B. Separation of duties
- C. Least privilege
- D. Mandatory vacations

Answer: B

NEW QUESTION 396

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 399

- (Exam Topic 12)

The PRIMARY purpose of accreditation is to:

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

Answer: B

NEW QUESTION 400

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 405

- (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 407

- (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 412

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 416

- (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 420

- (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 423

- (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 424

- (Exam Topic 12)

Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

- A. Length of Initialization Vector (IV)
- B. Protection against message replay
- C. Detection of message tampering
- D. Built-in provision to rotate keys

Answer: A

NEW QUESTION 425

- (Exam Topic 12)

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

- A. Third-party vendor with access to the system
- B. System administrator access compromised
- C. Internal attacker with access to the system

D. Internal user accidentally accessing data

Answer: C

NEW QUESTION 427

- (Exam Topic 12)

A security architect plans to reference a Mandatory Access Control (MAC) model for implementation. This indicates that which of the following properties are being prioritized?

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

Answer: C

NEW QUESTION 429

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 434

- (Exam Topic 12)

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

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

Answer: C

NEW QUESTION 438

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 440

- (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 442

- (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 445

- (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 449

- (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 452

- (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 453

- (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 458

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 460

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 461

- (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 466

- (Exam Topic 13)

A control to protect from a Denial-of-Service (DoS) attack has been determined to stop 50% of attacks, and additionally reduces the impact of an attack by 50%. What is the residual risk?

- A. 25%
- B. 50%
- C. 75%
- D. 100%

Answer: A

NEW QUESTION 471

- (Exam Topic 13)

An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject's data?

- A. Aggregate it into one database in the US
- B. Process it in the US, but store the information in France
- C. Share it with a third party
- D. Anonymize it and process it in the US

Answer: C

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 472

- (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 474

- (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 476

- (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 479

- (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 480

- (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 485

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 486

- (Exam Topic 13)

What is the MAIN purpose of a change management policy?

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

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 488

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 492

- (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 496

- (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 499

- (Exam Topic 13)

Match the name of access control model with its associated restriction.
Drag each access control model to its appropriate restriction access on the right.

Access Control Model	Restrictions
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:

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

NEW QUESTION 500

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 502

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 506

- (Exam Topic 13)

What is the PRIMARY goal of fault tolerance?

- A. Elimination of single point of failure
- B. Isolation using a sandbox
- C. Single point of repair
- D. Containment to prevent propagation

Answer: A

NEW QUESTION 509

- (Exam Topic 13)

Assessing a third party's risk by counting bugs in the code may not be the best measure of an attack surface within the supply chain. Which of the following is LEAST associated with the attack surface?

- A. Input protocols
- B. Target processes
- C. Error messages
- D. Access rights

Answer: C

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 513

- (Exam Topic 13)

Which of the following is MOST appropriate for protecting confidentiality of data stored on a hard drive?

- A. Triple Data Encryption Standard (3DES)
- B. Advanced Encryption Standard (AES)
- C. Message Digest 5 (MD5)
- D. Secure Hash Algorithm 2(SHA-2)

Answer: B

NEW QUESTION 518

- (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 523

- (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 526

- (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 531

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 533

- (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 537

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 538

- (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 543

- (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 546

- (Exam Topic 13)

Which of the following is a responsibility of a data steward?

- A. Ensure alignment of the data governance effort to the organization.
- B. Conduct data governance interviews with the organization.
- C. Document data governance requirements.
- D. Ensure that data decisions and impacts are communicated to the organization.

Answer: A

NEW QUESTION 550

- (Exam Topic 13)

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

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

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 555

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 558

- (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 563

- (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 565

- (Exam Topic 13)

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

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

Answer: D

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 567

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 571

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 574

- (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 579

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 582

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 584

- (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 587

- (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 590

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 594

- (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 599

- (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 601

.....

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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 represents the GREATEST risk to data confidentiality?

- A. Network redundancies are not implemented
- B. Security awareness training is not completed
- C. Backup tapes are generated unencrypted
- D. Users have administrative privileges

Answer: C

NEW QUESTION 3

- (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 4

- (Exam Topic 2)

Which one of the following affects the classification of data?

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

Answer: D

NEW QUESTION 5

- (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 6

- (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 7

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 8

- (Exam Topic 4)

An input validation and exception handling vulnerability has been discovered on a critical web-based system. Which of the following is MOST suited to quickly implement a control?

- A. Add a new rule to the application layer firewall
- B. Block access to the service
- C. Install an Intrusion Detection System (IDS)
- D. Patch the application source code

Answer: A

NEW QUESTION 9

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 10

- (Exam Topic 4)

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 10

- (Exam Topic 5)

A manufacturing organization wants to establish a Federated Identity Management (FIM) system with its 20 different supplier companies. Which of the following is the BEST solution for the manufacturing organization?

- A. Trusted third-party certification
- B. Lightweight Directory Access Protocol (LDAP)
- C. Security Assertion Markup language (SAML)
- D. Cross-certification

Answer: C

NEW QUESTION 11

- (Exam Topic 5)

Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee's salary?

- A. Limit access to predefined queries
- B. Segregate the database into a small number of partitions each with a separate security level
- C. Implement Role Based Access Control (RBAC)
- D. Reduce the number of people who have access to the system for statistical purposes

Answer: C

NEW QUESTION 14

- (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 16

- (Exam Topic 7)

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

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

Answer: A

NEW QUESTION 18

- (Exam Topic 7)

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

Answer: D

NEW QUESTION 22

- (Exam Topic 7)

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

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

Answer: B

NEW QUESTION 25

- (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 26

- (Exam Topic 8)

Which of the following is the BEST method to prevent malware from being introduced into a production environment?

- A. Purchase software from a limited list of retailers
- B. Verify the hash key or certificate key of all updates
- C. Do not permit programs, patches, or updates from the Internet
- D. Test all new software in a segregated environment

Answer: D

NEW QUESTION 31

- (Exam Topic 8)

The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle (SDLC)?

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

Answer: A

Explanation:

Reference <https://online.concordia.edu/computer-science/system-development-life-cycle-phases/>

NEW QUESTION 32

- (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 34

- (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 38

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 42

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 43

- (Exam Topic 9)

An organization allows ping traffic into and out of their network. An attacker has installed a program on the network that uses the payload portion of the ping packet to move data into and out of the network. What type of attack has the organization experienced?

- A. Data leakage
- B. Unfiltered channel
- C. Data emanation
- D. Covert channel

Answer: D

NEW QUESTION 45

- (Exam Topic 9)

What is the term commonly used to refer to a technique of authenticating one machine to another by forging packets from a trusted source?

- A. Man-in-the-Middle (MITM) attack
- B. Smurfing
- C. Session redirect
- D. Spoofing

Answer: D

NEW QUESTION 50

- (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 55

- (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 58

- (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 61

- (Exam Topic 9)

A security professional has just completed their organization's Business Impact Analysis (BIA). Following Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) best practices, what would be the professional's NEXT step?

- A. Identify and select recovery strategies.
- B. Present the findings to management for funding.
- C. Select members for the organization's recovery teams.
- D. Prepare a plan to test the organization's ability to recover its operations.

Answer: A

NEW QUESTION 65

- (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 68

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 69

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 74

- (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 77

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 81

- (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 82

- (Exam Topic 9)

Which of the following can BEST prevent security flaws occurring in outsourced software development?

- A. Contractual requirements for code quality
- B. Licensing, code ownership and intellectual property rights
- C. Certification of the quality and accuracy of the work done
- D. Delivery dates, change management control and budgetary control

Answer: C

NEW QUESTION 84

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 88

- (Exam Topic 9)

A security consultant has been asked to research an organization's legal obligations to protect privacy-related information. What kind of reading material is MOST relevant to this project?

- A. The organization's current security policies concerning privacy issues
- B. Privacy-related regulations enforced by governing bodies applicable to the organization
- C. Privacy best practices published by recognized security standards organizations
- D. Organizational procedures designed to protect privacy information

Answer: B

NEW QUESTION 91

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 95

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 98

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 102

- (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 104

- (Exam Topic 9)

Which of the following is an appropriate source for test data?

- A. Production data that is secured and maintained only in the production environment.
- B. Test data that has no similarities to production data.
- C. Test data that is mirrored and kept up-to-date with production data.
- D. Production data that has been sanitized before loading into a test environment.

Answer: D

NEW QUESTION 107

- (Exam Topic 9)

When implementing controls in a heterogeneous end-point network for an organization, it is critical that

- A. hosts are able to establish network communications.
- B. users can make modifications to their security software configurations.
- C. common software security components be implemented across all hosts.
- D. firewalls running on each host are fully customizable by the user.

Answer: C

NEW QUESTION 108

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 109

- (Exam Topic 9)

What maintenance activity is responsible for defining, implementing, and testing updates to application systems?

- A. Program change control
- B. Regression testing
- C. Export exception control
- D. User acceptance testing

Answer: A

NEW QUESTION 112

- (Exam Topic 9)

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

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

Answer:

B

NEW QUESTION 115

- (Exam Topic 9)

An Intrusion Detection System (IDS) is generating alarms that a user account has over 100 failed login attempts per minute. A sniffer is placed on the network, and a variety of passwords for that user are noted. Which of the following is MOST likely occurring?

- A. A dictionary attack
- B. A Denial of Service (DoS) attack
- C. A spoofing attack
- D. A backdoor installation

Answer: A

NEW QUESTION 118

- (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 121

- (Exam Topic 9)

Which one of the following affects the classification of data?

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

Answer: A

NEW QUESTION 123

- (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 128

- (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 132

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 134

- (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 139

- (Exam Topic 9)

Which Hyper Text Markup Language 5 (HTML5) option presents a security challenge for network data leakage prevention and/or monitoring?

- A. Cross Origin Resource Sharing (CORS)
- B. WebSockets
- C. Document Object Model (DOM) trees
- D. Web Interface Definition Language (IDL)

Answer: B

NEW QUESTION 143

- (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 146

- (Exam Topic 10)

What is the MAIN feature that onion routing networks offer?

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

Answer: C

NEW QUESTION 149

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 153

- (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 158

- (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 162

- (Exam Topic 10)

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

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

Answer: A

NEW QUESTION 166

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 168

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration

functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.

Which of the following will be the PRIMARY security concern as staff is released from the organization?

- A. Inadequate IT support
- B. Loss of data and separation of duties
- C. Undocumented security controls
- D. Additional responsibilities for remaining staff

Answer: B

NEW QUESTION 169

- (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 170

- (Exam Topic 10)

What is the MOST critical factor to achieve the goals of a security program?

- A. Capabilities of security resources
- B. Executive management support
- C. Effectiveness of security management
- D. Budget approved for security resources

Answer: B

NEW QUESTION 175

- (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 178

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 182

- (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 184

- (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 189

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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

Answer: C

NEW QUESTION 193

- (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 197

- (Exam Topic 10)

Refer to the information below to answer the question.

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

Which of the following will MOST likely allow the organization to keep risk at an acceptable level?

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

Answer: C

NEW QUESTION 201

- (Exam Topic 10)

A system is developed so that its business users can perform business functions but not user administration functions. Application administrators can perform administration functions but not user business functions. These capabilities are BEST described as

- A. least privilege.
- B. rule based access controls.
- C. Mandatory Access Control (MAC).
- D. separation of duties.

Answer: D

NEW QUESTION 202

- (Exam Topic 10)

What is the BEST method to detect the most common improper initialization problems in programming languages?

- A. Use and specify a strong character encoding.
- B. Use automated static analysis tools that target this type of weakness.
- C. Perform input validation on any numeric inputs by assuring that they are within the expected range.
- D. Use data flow analysis to minimize the number of false positives.

Answer: B

NEW QUESTION 207

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 210

- (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 214

- (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 219

- (Exam Topic 10)

Host-Based Intrusion Protection (HIPS) systems are often deployed in monitoring or learning mode during their initial implementation. What is the objective of starting in this mode?

- A. Automatically create exceptions for specific actions or files
- B. Determine which files are unsafe to access and blacklist them
- C. Automatically whitelist actions or files known to the system
- D. Build a baseline of normal or safe system events for review

Answer: D

NEW QUESTION 221

- (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 methods is the MOST effective way of removing the Peer-to-Peer (P2P) program from the computer?

- A. Run software uninstall
- B. Re-image the computer
- C. Find and remove all installation files
- D. Delete all cookies stored in the web browser cache

Answer: B

NEW QUESTION 222

- (Exam Topic 10)

Place the following information classification steps in sequential order.

Steps		Order
Declassify information when appropriate		Step
Apply the appropriate security markings		Step
Conduct periodic classification reviews		Step
Assign a classification level		Step
Document the information assets		Step

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Steps		Order
Declassify information when appropriate	Document the information assets	Step
Apply the appropriate security markings	Assign a classification level	Step
Conduct periodic classification reviews	Apply the appropriate security markings	Step
Assign a classification level	Conduct periodic classification reviews	Step
Document the information assets	Declassify information when appropriate	Step

NEW QUESTION 227

- (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 229

- (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 232

- (Exam Topic 10)

Which of the following is the BEST way to determine if a particular system is able to identify malicious software without executing it?

- A. Testing with a Botnet
- B. Testing with an EICAR file
- C. Executing a binary shellcode
- D. Run multiple antivirus programs

Answer: B

NEW QUESTION 235

- (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 238

- (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 241

- (Exam Topic 10)

Which of the following is the BEST countermeasure to brute force login attacks?

- A. Changing all canonical passwords
- B. Decreasing the number of concurrent user sessions
- C. Restricting initial password delivery only in person
- D. Introducing a delay after failed system access attempts

Answer: D

NEW QUESTION 244

- (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 245

- (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 249

- (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 251

- (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 255

- (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 260

- (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 265

- (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 269

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 273

- (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 274

- (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 275

- (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 276

- (Exam Topic 11)

Discretionary Access Control (DAC) restricts access according to

- A. data classification labeling.
- B. page views within an application.
- C. authorizations granted to the user.
- D. management accreditation.

Answer: C

NEW QUESTION 281

- (Exam Topic 11)

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

- A. A strong breach notification process
- B. Limited collection of individuals' confidential data

- C. End-to-end data encryption for data in transit
- D. Continuous monitoring of potential vulnerabilities

Answer: B

NEW QUESTION 284

- (Exam Topic 11)

Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

- A. Concept, Development, Production, Utilization, Support, Retirement
- B. Stakeholder Requirements Definition, Architectural Design, Implementation, Verification, Operation
- C. Acquisition, Measurement, Configuration Management, Production, Operation, Support
- D. Concept, Requirements, Design, Implementation, Production, Maintenance, Support, Disposal

Answer: B

NEW QUESTION 286

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 290

- (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 293

- (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 296

- (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 297

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 298

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 301

- (Exam Topic 11)

Which of the following is an essential step before performing Structured Query Language (SQL) penetration tests on a production system?

- A. Verify countermeasures have been deactivated.
- B. Ensure firewall logging has been activated.
- C. Validate target systems have been backed up.
- D. Confirm warm site is ready to accept connections.

Answer: C

NEW QUESTION 304

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 309

- (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 311

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 313

- (Exam Topic 11)

The PRIMARY security concern for handheld devices is the

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

Answer: C

NEW QUESTION 316

- (Exam Topic 11)

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

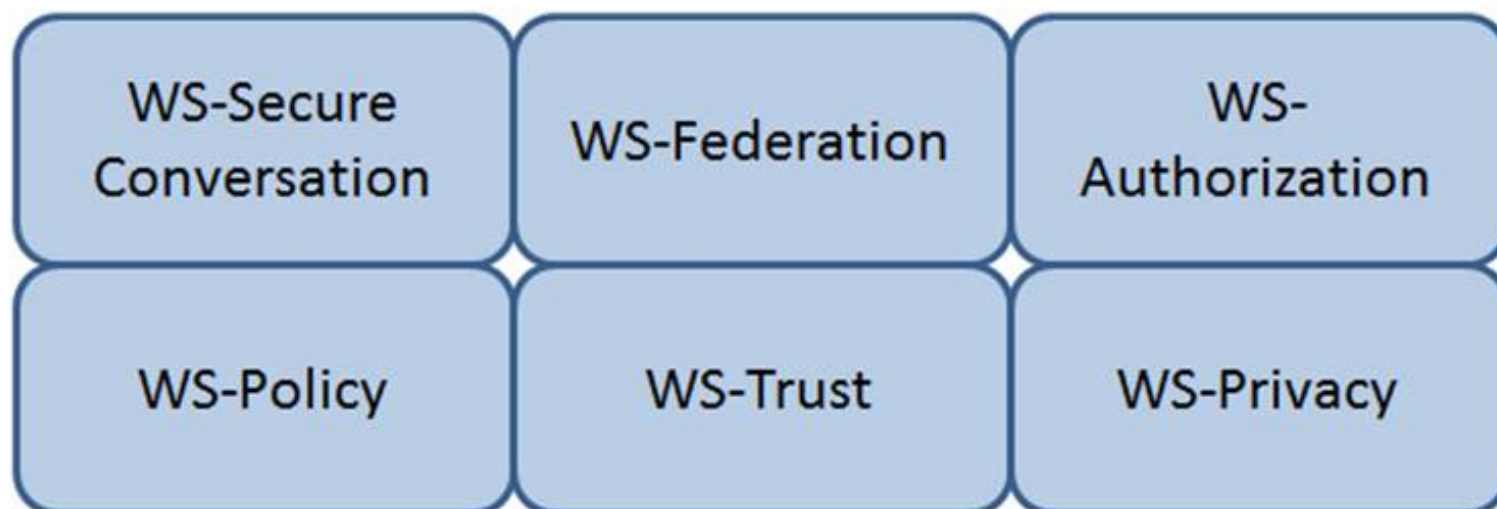
- A. It is useful for testing communications protocols and graphical user interfaces.
- B. It is characterized by the stateless behavior of a process implemented in a function.
- C. Test inputs are obtained from the derived threshold of the given functional specifications.
- D. An entire partition can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

Answer: C

NEW QUESTION 321

- (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 322

- (Exam Topic 11)

Software Code signing is used as a method of verifying what security concept?

- A. Integrity
- B. Confidentiality
- C. Availability
- D. Access Control

Answer: A

NEW QUESTION 323

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 325

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 327

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 330

- (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 332

- (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.

Sequence		Method
1		Overwriting
2		Degaussing
3		Destruction
4		Deleting

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Sequence		Method
1	3	Overwriting
2	2	Degaussing
3	1	Destruction
4	4	Deleting

NEW QUESTION 335

- (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 338

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 339

- (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 344

- (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 349

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 351

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 355

- (Exam Topic 11)

Are companies legally required to report all data breaches?

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

Answer: A

NEW QUESTION 360

- (Exam Topic 11)

While investigating a malicious event, only six days of audit logs from the last month were available. What policy should be updated to address this problem?

- A. Retention
- B. Reporting
- C. Recovery
- D. Remediation

Answer: A

NEW QUESTION 361

- (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 363

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 366

- (Exam Topic 11)

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

What is the best approach for the CISO?

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

What is the best approach for the CISO?

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

Answer: B

NEW QUESTION 370

- (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 375

- (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 380

- (Exam Topic 12)

The restoration priorities of a Disaster Recovery Plan (DRP) are based on which of the following documents?

- A. Service Level Agreement (SLA)
- B. Business Continuity Plan (BCP)
- C. Business Impact Analysis (BIA)
- D. Crisis management plan

Answer: B

NEW QUESTION 384

- (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 387

- (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 391

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 392

- (Exam Topic 12)

Which of the following restricts the ability of an individual to carry out all the steps of a particular process?

- A. Job rotation
- B. Separation of duties
- C. Least privilege
- D. Mandatory vacations

Answer: B

NEW QUESTION 396

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 399

- (Exam Topic 12)

The PRIMARY purpose of accreditation is to:

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

Answer: B

NEW QUESTION 400

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 405

- (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 407

- (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 412

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 416

- (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 420

- (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 423

- (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 424

- (Exam Topic 12)

Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

- A. Length of Initialization Vector (IV)
- B. Protection against message replay
- C. Detection of message tampering
- D. Built-in provision to rotate keys

Answer: A

NEW QUESTION 425

- (Exam Topic 12)

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

- A. Third-party vendor with access to the system
- B. System administrator access compromised
- C. Internal attacker with access to the system

D. Internal user accidentally accessing data

Answer: C

NEW QUESTION 427

- (Exam Topic 12)

A security architect plans to reference a Mandatory Access Control (MAC) model for implementation. This indicates that which of the following properties are being prioritized?

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

Answer: C

NEW QUESTION 429

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 434

- (Exam Topic 12)

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

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

Answer: C

NEW QUESTION 438

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 440

- (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 442

- (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 445

- (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 449

- (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 452

- (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 453

- (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 458

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 460

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 461

- (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 466

- (Exam Topic 13)

A control to protect from a Denial-of-Service (DoS) attack has been determined to stop 50% of attacks, and additionally reduces the impact of an attack by 50%. What is the residual risk?

- A. 25%
- B. 50%
- C. 75%
- D. 100%

Answer: A

NEW QUESTION 471

- (Exam Topic 13)

An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject's data?

- A. Aggregate it into one database in the US
- B. Process it in the US, but store the information in France
- C. Share it with a third party
- D. Anonymize it and process it in the US

Answer: C

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 472

- (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 474

- (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 476

- (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 479

- (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 480

- (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 485

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 486

- (Exam Topic 13)

What is the MAIN purpose of a change management policy?

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

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 488

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 492

- (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 496

- (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 499

- (Exam Topic 13)

Match the name of access control model with its associated restriction.
Drag each access control model to its appropriate restriction access on the right.

Access Control Model	Restrictions
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:

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

NEW QUESTION 500

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 502

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 506

- (Exam Topic 13)

What is the PRIMARY goal of fault tolerance?

- A. Elimination of single point of failure
- B. Isolation using a sandbox
- C. Single point of repair
- D. Containment to prevent propagation

Answer: A

NEW QUESTION 509

- (Exam Topic 13)

Assessing a third party's risk by counting bugs in the code may not be the best measure of an attack surface within the supply chain. Which of the following is LEAST associated with the attack surface?

- A. Input protocols
- B. Target processes
- C. Error messages
- D. Access rights

Answer: C

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 513

- (Exam Topic 13)

Which of the following is MOST appropriate for protecting confidentiality of data stored on a hard drive?

- A. Triple Data Encryption Standard (3DES)
- B. Advanced Encryption Standard (AES)
- C. Message Digest 5 (MD5)
- D. Secure Hash Algorithm 2(SHA-2)

Answer: B

NEW QUESTION 518

- (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 523

- (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 526

- (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 531

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 533

- (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 537

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 538

- (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 543

- (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 546

- (Exam Topic 13)

Which of the following is a responsibility of a data steward?

- A. Ensure alignment of the data governance effort to the organization.
- B. Conduct data governance interviews with the organization.
- C. Document data governance requirements.
- D. Ensure that data decisions and impacts are communicated to the organization.

Answer: A

NEW QUESTION 550

- (Exam Topic 13)

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

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

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 555

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 558

- (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 563

- (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 565

- (Exam Topic 13)

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

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

Answer: D

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 567

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 571

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 574

- (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 579

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 582

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 584

- (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 587

- (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 590

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 594

- (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 599

- (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 601

.....

Relate Links

100% Pass Your CISSP Exam with Exambible Prep Materials

<https://www.exambible.com/CISSP-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>