

ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)



NEW QUESTION 1

- (Exam Topic 1)

A company whose Information Technology (IT) services are being delivered from a Tier 4 data center, is preparing a companywide Business Continuity Planning (BCP). Which of the following failures should the IT manager be concerned with?

- A. Application
- B. Storage
- C. Power
- D. Network

Answer: C

NEW QUESTION 2

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 3

- (Exam Topic 2)

Which one of the following affects the classification of data?

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

Answer: D

NEW QUESTION 4

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 5

- (Exam Topic 2)

An organization has doubled in size due to a rapid market share increase. The size of the Information Technology (IT) staff has maintained pace with this growth. The organization hires several contractors whose onsite time is limited. The IT department has pushed its limits building servers and rolling out workstations and has a backlog of account management requests.

Which contract is BEST in offloading the task from the IT staff?

- A. Platform as a Service (PaaS)
- B. Identity as a Service (IDaaS)
- C. Desktop as a Service (DaaS)
- D. Software as a Service (SaaS)

Answer: B

NEW QUESTION 6

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 7

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 8

- (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 9

- (Exam Topic 4)

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

- A. Layer 2 Tunneling Protocol (L2TP)
- B. Link Control Protocol (LCP)
- C. Challenge Handshake Authentication Protocol (CHAP)
- D. Packet Transfer Protocol (PTP)

Answer: B

NEW QUESTION 10

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 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 13

- (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 5)

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

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

Answer: B

NEW QUESTION 19

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 22

- (Exam Topic 6)

Which of the following could cause a Denial of Service (DoS) against an authentication system?

- A. Encryption of audit logs
- B. No archiving of audit logs
- C. Hashing of audit logs
- D. Remote access audit logs

Answer: D

NEW QUESTION 23

- (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 26

- (Exam Topic 6)

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

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

Answer: D

NEW QUESTION 28

- (Exam Topic 6)

In which of the following programs is it MOST important to include the collection of security process data?

- A. Quarterly access reviews
- B. Security continuous monitoring
- C. Business continuity testing
- D. Annual security training

Answer: A

NEW QUESTION 30

- (Exam Topic 7)

A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?

- A. Guaranteed recovery of all business functions
- B. Minimization of the need decision making during a crisis
- C. Insurance against litigation following a disaster
- D. Protection from loss of organization resources

Answer: D

NEW QUESTION 34

- (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 37

- (Exam Topic 8)

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

Answer: C

NEW QUESTION 40

- (Exam Topic 8)

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

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

Answer: D

NEW QUESTION 41

- (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 46

- (Exam Topic 8)

Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

- A. Lack of software documentation
- B. License agreements requiring release of modified code
- C. Expiration of the license agreement
- D. Costs associated with support of the software

Answer: D

NEW QUESTION 47

- (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 50

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 55

- (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 60

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 61

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 65

- (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 68

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 72

- (Exam Topic 9)

A vulnerability test on an Information System (IS) is conducted to

- A. exploit security weaknesses in the IS.
- B. measure system performance on systems with weak security controls.
- C. evaluate the effectiveness of security controls.
- D. prepare for Disaster Recovery (DR) planning.

Answer: C

NEW QUESTION 76

- (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 78

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 82

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 86

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 89

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 93

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 97

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 98

- (Exam Topic 9)

Which layer of the Open Systems Interconnections (OSI) model implementation adds information concerning the logical connection between the sender and receiver?

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

Answer: C

NEW QUESTION 99

- (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 101

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 106

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 110

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 113

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 116

- (Exam Topic 9)

How can a forensic specialist exclude from examination a large percentage of operating system files residing on a copy of the target system?

- A. Take another backup of the media in question then delete all irrelevant operating system files.
- B. Create a comparison database of cryptographic hashes of the files from a system with the same operating system and patch level.
- C. Generate a message digest (MD) or secure hash on the drive image to detect tampering of the media being examined.
- D. Discard harmless files for the operating system, and known installed programs.

Answer: B

NEW QUESTION 117

- (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 120

- (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 123

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 128

- (Exam Topic 9)

What security management control is MOST often broken by collusion?

- A. Job rotation
- B. Separation of duties
- C. Least privilege model
- D. Increased monitoring

Answer: B

NEW QUESTION 129

- (Exam Topic 9)

The PRIMARY purpose of a security awareness program is to

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

Answer: A

NEW QUESTION 130

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 135

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 137

- (Exam Topic 9)

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

- A. Mandatory Access Control (MAC).
- B. owner-administered control.

- C. owner-dependent access control.
- D. Discretionary Access Control (DAC).

Answer: D

NEW QUESTION 142

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 145

- (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 148

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 150

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 152

- (Exam Topic 9)

Which of the following is the BEST way to verify the integrity of a software patch?

- A. Cryptographic checksums
- B. Version numbering
- C. Automatic updates
- D. Vendor assurance

Answer: A

NEW QUESTION 156

- (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 159

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 164

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 169

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 174

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 175

- (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 180

- (Exam Topic 9)

The Hardware Abstraction Layer (HAL) is implemented in the

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

Answer: A

NEW QUESTION 184

- (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 185

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 187

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 188

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 193

- (Exam Topic 9)

What is the ultimate objective of information classification?

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

Answer: B

NEW QUESTION 194

- (Exam Topic 9)

Following the completion of a network security assessment, which of the following can BEST be demonstrated?

- A. The effectiveness of controls can be accurately measured
- B. A penetration test of the network will fail
- C. The network is compliant to industry standards
- D. All unpatched vulnerabilities have been identified

Answer: A

NEW QUESTION 198

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 201

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 205

- (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 206

- (Exam Topic 9)

A software scanner identifies a region within a binary image having high entropy. What does this MOST likely indicate?

- A. Encryption routines
- B. Random number generator
- C. Obfuscated code
- D. Botnet command and control

Answer: C

NEW QUESTION 209

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 213

- (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 217

- (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 221

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 223

- (Exam Topic 9)

Which of the following is the BEST mitigation from phishing attacks?

- A. Network activity monitoring
- B. Security awareness training
- C. Corporate policy and procedures
- D. Strong file and directory permissions

Answer:

B

NEW QUESTION 228

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 231

- (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 233

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 236

- (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 241

- (Exam Topic 9)

The goal of software assurance in application development is to

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

Answer: C

NEW QUESTION 242

- (Exam Topic 9)

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

- A. To provide access to system privileges
- B. To provide access to the operating system
- C. To ensure that unauthorized persons cannot access the computers
- D. To ensure that management knows what users are currently logged on

Answer: C

NEW QUESTION 245

- (Exam Topic 9)

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

- A. The behavior is ethical because the tool will be used to create a better virus scanner.

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

Answer: A

NEW QUESTION 247

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 252

- (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 254

- (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 258

- (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 263

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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

Answer: B

NEW QUESTION 266

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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

Answer: B

NEW QUESTION 268

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 273

- (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 275

- (Exam Topic 10)

Refer to the information below to answer the question.

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

Table A

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

Table B

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

Which of the following is true according to the star property (*property)?

- A. User D can write to File 1
- B. User B can write to File 1
- C. User A can write to File 1
- D. User C can write to File 1

Answer: C

NEW QUESTION 280

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 282

- (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 287

- (Exam Topic 10)

What physical characteristic does a retinal scan biometric device measure?

- A. The amount of light reflected by the retina

- B. The size, curvature, and shape of the retina
- C. The pattern of blood vessels at the back of the eye
- D. The pattern of light receptors at the back of the eye

Answer: C

NEW QUESTION 292

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 295

- (Exam Topic 10)

An online retail company has formulated a record retention schedule for customer transactions. Which of the following is a valid reason a customer transaction is kept beyond the retention schedule?

- A. Pending legal hold
- B. Long term data mining needs
- C. Customer makes request to retain
- D. Useful for future business initiatives

Answer: A

NEW QUESTION 300

- (Exam Topic 10)

Which of the following assures that rules are followed in an identity management architecture?

- A. Policy database
- B. Digital signature
- C. Policy decision point
- D. Policy enforcement point

Answer: D

NEW QUESTION 303

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 306

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 308

- (Exam Topic 10)

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

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

Answer: A

NEW QUESTION 311

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

Answer: D

NEW QUESTION 313

- (Exam Topic 10)

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

Area		Technolog
Facilities		Encryption
Devices		Window
Information		Firewall
Systems		Authenticatio

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Area		Technolog
Facilities	Information	Encryption
Devices	Facilities	Window
Information	Devices	Firewall
Systems	Systems	Authenticatio

NEW QUESTION 318

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

Answer: A

NEW QUESTION 319

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 322

- (Exam Topic 10)

A security manager has noticed an inconsistent application of server security controls resulting in vulnerabilities on critical systems. What is the MOST likely cause of this issue?

- A. A lack of baseline standards
- B. Improper documentation of security guidelines
- C. A poorly designed security policy communication program
- D. Host-based Intrusion Prevention System (HIPS) policies are ineffective

Answer: A

NEW QUESTION 324

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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

Answer: B

NEW QUESTION 328

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 331

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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

Answer: B

NEW QUESTION 335

- (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 337

- (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 340

- (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 345

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 346

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 350

- (Exam Topic 10)

Which of the following is the MOST crucial for a successful audit plan?

- A. Defining the scope of the audit to be performed
- B. Identifying the security controls to be implemented
- C. Working with the system owner on new controls
- D. Acquiring evidence of systems that are not compliant

Answer: A

NEW QUESTION 354

- (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 355

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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

Answer: A

NEW QUESTION 360

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 363

- (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 367

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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

Answer: A

NEW QUESTION 372

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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

Answer: A

NEW QUESTION 375

- (Exam Topic 10)

Refer to the information below to answer the question.

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

Which of the following BEST describes the access control methodology used?

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

Answer: C

NEW QUESTION 378

- (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 382

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 383

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

Answer: D

NEW QUESTION 386

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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

Answer: B

NEW QUESTION 390

- (Exam Topic 10)

An organization decides to implement a partial Public Key Infrastructure (PKI) with only the servers having digital certificates. What is the security benefit of this implementation?

- A. Clients can authenticate themselves to the servers.
- B. Mutual authentication is available between the clients and servers.
- C. Servers are able to issue digital certificates to the client.
- D. Servers can authenticate themselves to the client.

Answer: D

NEW QUESTION 394

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 399

- (Exam Topic 10)

From a security perspective, which of the following is a best practice to configure a Domain Name Service (DNS) system?

- A. Configure secondary servers to use the primary server as a zone forwarder.
- B. Block all Transmission Control Protocol (TCP) connections.
- C. Disable all recursive queries on the name servers.
- D. Limit zone transfers to authorized devices.

Answer: D

NEW QUESTION 400

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 404

- (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 407

- (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 411

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 414

- (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 417

- (Exam Topic 10)

Refer to the information below to answer the question.

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

The effectiveness of the security program can PRIMARILY be measured through

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

Answer: A

NEW QUESTION 418

- (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 423

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 428

- (Exam Topic 11)

Which of the following BEST describes the purpose of performing security certification?

- A. To identify system threats, vulnerabilities, and acceptable level of risk
- B. To formalize the confirmation of compliance to security policies and standards
- C. To formalize the confirmation of completed risk mitigation and risk analysis
- D. To verify that system architecture and interconnections with other systems are effectively implemented

Answer: B

NEW QUESTION 430

- (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 432

- (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 435

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 437

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 438

- (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 439

- (Exam Topic 11)

What is the GREATEST challenge to identifying data leaks?

- A. Available technical tools that enable user activity monitoring.
- B. Documented asset classification policy and clear labeling of assets.
- C. Senior management cooperation in investigating suspicious behavior.
- D. Law enforcement participation to apprehend and interrogate suspects.

Answer: B

NEW QUESTION 440

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 443

- (Exam Topic 11)

Data remanence refers to which of the following?

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

Answer: D

NEW QUESTION 447

- (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 450

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 455

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 457

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 458

- (Exam Topic 11)

If compromised, which of the following would lead to the exploitation of multiple virtual machines?

- A. Virtual device drivers
- B. Virtual machine monitor
- C. Virtual machine instance
- D. Virtual machine file system

Answer: B

NEW QUESTION 463

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 467

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 470

- (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 472

- (Exam Topic 11)

Which of the following PRIMARILY contributes to security incidents in web-based applications?

- A. Systems administration and operating systems
- B. System incompatibility and patch management
- C. Third-party applications and change controls
- D. Improper stress testing and application interfaces

Answer: C

NEW QUESTION 473

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 476

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 478

- (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 482

- (Exam Topic 11)

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

- A. Application Manager
- B. Database Administrator

- C. Privacy Officer
- D. Finance Manager

Answer: C

NEW QUESTION 484

- (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 487

- (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 491

- (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 493

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 494

- (Exam Topic 11)

Which of the following describes the BEST configuration management practice?

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

Answer: D

NEW QUESTION 497

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 501

- (Exam Topic 11)

After acquiring the latest security updates, what must be done before deploying to production systems?

- A. Use tools to detect missing system patches
- B. Install the patches on a test system
- C. Subscribe to notifications for vulnerabilities
- D. Assess the severity of the situation

Answer: B

NEW QUESTION 506

- (Exam Topic 11)

A software security engineer is developing a black box-based test plan that will measure the system's reaction to incorrect or illegal inputs or unexpected operational errors and situations. Match the functional testing techniques on the left with the correct input parameters on the right.

Functional Testing Techniques		Input Parameter Selection
State-Based Analysis		Select one input that does not belong to any of the identified partitions.
Equivalence Class Analysis		Select inputs that are at the external limits of the domain of valid values.
Decision Table Analysis		Select invalid combinations of input values.
Boundary Value Analysis		Select unexpected inputs corresponding to each known condition.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Functional Testing Techniques		Input Parameter Selection
State-Based Analysis	Equivalence Class Analysis	Select one input that does not belong to any of the identified partitions.
Equivalence Class Analysis	Boundary Value Analysis	Select inputs that are at the external limits of the domain of valid values.
Decision Table Analysis	Decision Table Analysis	Select invalid combinations of input values.
Boundary Value Analysis	State-Based Analysis	Select unexpected inputs corresponding to each known condition.

NEW QUESTION 509

- (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 512

- (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?

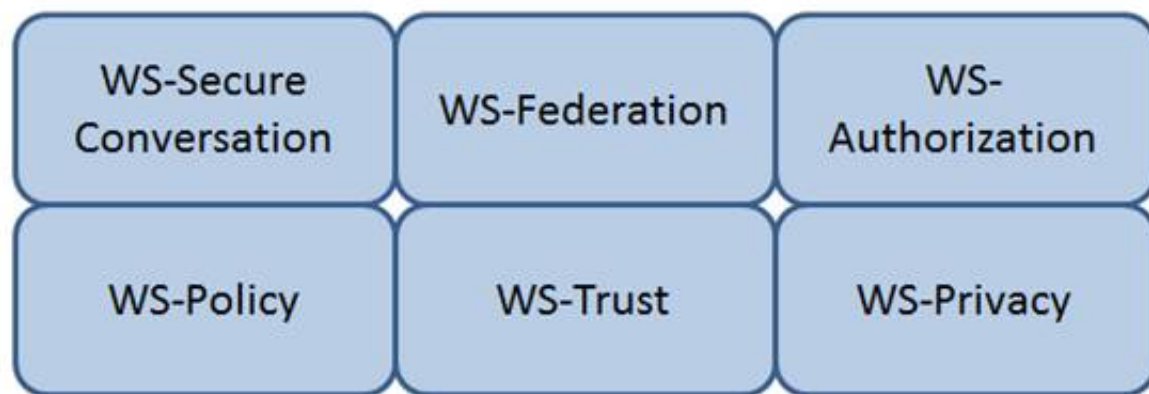
- A. Acceptance of risk by the authorizing official
- B. Remediation of vulnerabilities
- C. Adoption of standardized policies and procedures
- D. Approval of the System Security Plan (SSP)

Answer: A

NEW QUESTION 514

- (Exam Topic 11)

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

WS-Federation

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

NEW QUESTION 516

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 520

- (Exam Topic 11)

Secure Sockets Layer (SSL) encryption protects

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

Answer: C

NEW QUESTION 525

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 527

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 528

- (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 530

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 535

- (Exam Topic 11)

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

Security Engineering

Definition

Security Risk Treatment

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

Threat Assessment

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

Protection Needs

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

Risk

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Security Engineering

Definition

Security Risk Treatment

Protection Needs

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

Threat Assessment

Risk

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

Protection Needs

Threat Assessment

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

Risk

Security Risk Treatment

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

NEW QUESTION 539

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 544

- (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 549

- (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 550

- (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 553

- (Exam Topic 11)

Which one of the following is a common risk with network configuration management?

- A. Patches on the network are difficult to keep current.
- B. It is the responsibility of the systems administrator.
- C. User ID and passwords are never set to expire.
- D. Network diagrams are not up to date.

Answer: D

NEW QUESTION 555

- (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 557

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 562

- (Exam Topic 11)

Which one of the following operates at the session, transport, or network layer of the Open System Interconnection (OSI) model?

- A. Data at rest encryption
- B. Configuration Management
- C. Integrity checking software
- D. Cyclic redundancy check (CRC)

Answer: D

NEW QUESTION 565

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 570

- (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 573

- (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 577

- (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 578

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 583

- (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 588

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 592

- (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?

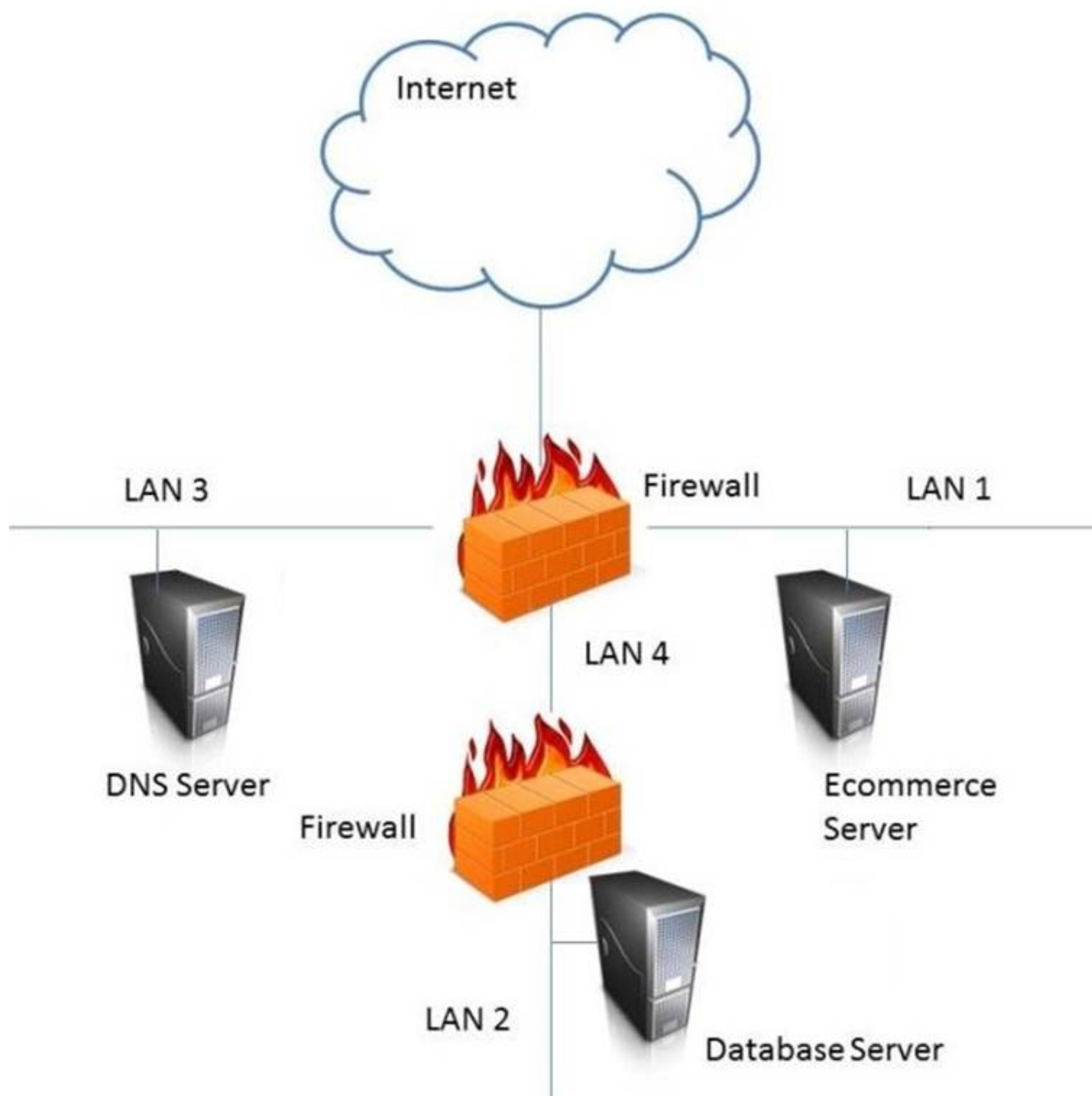
- A. Retention
- B. Reporting
- C. Recovery
- D. Remediation

Answer: A

NEW QUESTION 597

- (Exam Topic 11)

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

LAN 4

NEW QUESTION 600

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 601

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 605

- (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 607

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 608

- (Exam Topic 11)

The BEST method to mitigate the risk of a dictionary attack on a system is to

- A. use a hardware token.
- B. use complex passphrases.
- C. implement password history.
- D. encrypt the access control list (ACL).

Answer: A

NEW QUESTION 611

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 614

- (Exam Topic 12)

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

- A. Transport

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

Answer: D

NEW QUESTION 616

- (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 620

- (Exam Topic 12)

What is the difference between media marking and media labeling?

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

Answer: D

NEW QUESTION 623

- (Exam Topic 12)

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

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

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:

Mandatory Access Control – End user cannot set controls

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

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

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

NEW QUESTION 628

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 632

- (Exam Topic 12)

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

following BEST describes what has occurred?

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

Answer: A

NEW QUESTION 636

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 639

- (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 643

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 648

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 649

- (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 650

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 655

- (Exam Topic 12)

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

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

Answer: C

NEW QUESTION 657

- (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 662

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 664

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 667

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 670

- (Exam Topic 12)

Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

- A. Reversal
- B. Gray box
- C. Blind
- D. White box

Answer: B

NEW QUESTION 671

- (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 674

- (Exam Topic 12)

What does the Maximum Tolerable Downtime (MTD) determine?

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

Answer: C

NEW QUESTION 679

- (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 682

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 683

- (Exam Topic 12)

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

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

Answer: C

NEW QUESTION 684

- (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 687

- (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 691

- (Exam Topic 12)

A company was ranked as high in the following National Institute of Standards and Technology (NIST) functions: Protect, Detect, Respond and Recover. However, a low maturity grade was attributed to the Identify function. In which of the following the controls categories does this company need to improve when analyzing its processes individually?

- A. Asset Management, Business Environment, Governance and Risk Assessment
- B. Access Control, Awareness and Training, Data Security and Maintenance
- C. Anomalies and Events, Security Continuous Monitoring and Detection Processes
- D. Recovery Planning, Improvements and Communications

Answer: A

NEW QUESTION 694

- (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 699

- (Exam Topic 12)

How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

- A. Examines log messages or other indications on the system.
- B. Monitors alarms sent to the system administrator
- C. Matches traffic patterns to virus signature files
- D. Examines the Access Control List (ACL)

Answer: C

NEW QUESTION 702

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 705

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 707

- (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 711

- (Exam Topic 12)

An organization's information security strategic plan MUST be reviewed

- A. whenever there are significant changes to a major application.
- B. quarterly, when the organization's strategic plan is updated.
- C. whenever there are major changes to the business.
- D. every three years, when the organization's strategic plan is updated.

Answer: C

NEW QUESTION 714

- (Exam Topic 12)

Which of the following is BEST suited for exchanging authentication and authorization messages in a multi-party decentralized environment?

- A. Lightweight Directory Access Protocol (LDAP)
- B. Security Assertion Markup Language (SAML)
- C. Internet Mail Access Protocol
- D. Transport Layer Security (TLS)

Answer: B

NEW QUESTION 716

- (Exam Topic 12)

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

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

Answer: C

NEW QUESTION 721

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 724

- (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 727

- (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 728

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 732

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 736

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 740

- (Exam Topic 12)

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

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

Answer: C

NEW QUESTION 745

- (Exam Topic 12)

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

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

Answer: C

NEW QUESTION 750

- (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 752

- (Exam Topic 12)

Which of the following countermeasures is the MOST effective in defending against a social engineering attack?

- A. Mandating security policy acceptance
- B. Changing individual behavior
- C. Evaluating security awareness training
- D. Filtering malicious e-mail content

Answer: C

NEW QUESTION 757

- (Exam Topic 12)

What is a characteristic of Secure Socket Layer (SSL) and Transport Layer Security (TLS)?

- A. SSL and TLS provide a generic channel security mechanism on top of Transmission Control Protocol (TCP).
- B. SSL and TLS provide nonrepudiation by default.
- C. SSL and TLS do not provide security for most routed protocols.
- D. SSL and TLS provide header encapsulation over HyperText Transfer Protocol (HTTP).

Answer: A

NEW QUESTION 758

- (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 762

- (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 763

- (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 767

- (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 770

- (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 772

- (Exam Topic 13)

Which one of the following is an advantage of an effective release control strategy from a configuration control standpoint?

- A. Ensures that a trace for all deliverables is maintained and auditable
- B. Enforces backward compatibility between releases
- C. Ensures that there is no loss of functionality between releases
- D. Allows for future enhancements to existing features

Answer: C

NEW QUESTION 775

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 776

- (Exam Topic 13)

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

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

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 781

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 783

- (Exam Topic 13)

As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

- A. Use a web scanner to scan for vulnerabilities within the website.
- B. Perform a code review to ensure that the database references are properly addressed.
- C. Establish a secure connection to the web server to validate that only the approved ports are open.
- D. Enter only numbers in the web form and verify that the website prompts the user to enter a valid input.

Answer: D

NEW QUESTION 785

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 788

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 793

- (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 797

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 799

- (Exam Topic 13)

A Denial of Service (DoS) attack on a syslog server exploits weakness in which of the following protocols?

- A. Point-to-Point Protocol (PPP) and Internet Control Message Protocol (ICMP)
- B. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
- C. Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)
- D. Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

Answer: B

NEW QUESTION 800

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 801

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 806

- (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 810

- (Exam Topic 13)

Which of the following is the BEST reason for the use of security metrics?

- A. They ensure that the organization meets its security objectives.
- B. They provide an appropriate framework for Information Technology (IT) governance.
- C. They speed up the process of quantitative risk assessment.
- D. They quantify the effectiveness of security processes.

Answer: B

NEW QUESTION 814

- (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 816

- (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 818

- (Exam Topic 13)

Mandatory Access Controls (MAC) are based on:

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

Answer: A

NEW QUESTION 819

- (Exam Topic 13)

Which of the following is a common characteristic of privacy?

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

Answer: A

NEW QUESTION 821

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 824

- (Exam Topic 13)

Proven application security principles include which of the following?

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

Answer: A

NEW QUESTION 828

- (Exam Topic 13)

Which type of test would an organization perform in order to locate and target exploitable defects?

- A. Penetration
- B. System
- C. Performance
- D. Vulnerability

Answer: A

NEW QUESTION 830

- (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 835

- (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 838

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 841

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 843

- (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 846

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 847

- (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 training
- D. The purpose of awareness presentations is to broaden attention of security.
- E. Awareness is not training
- F. The purpose of awareness presentation is simply to focus attention on security.

Answer: C

NEW QUESTION 851

- (Exam Topic 13)

Which of the following **MUST** be scalable to address security concerns raised by the integration of third-party identity services?

- A. Mandatory Access Controls (MAC)
- B. Enterprise security architecture
- C. Enterprise security procedures
- D. Role Based Access Controls (RBAC)

Answer: D

NEW QUESTION 852

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CISSP Practice Exam Features:

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

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