



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)

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

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

Answer: C

NEW QUESTION 3

- (Exam Topic 1)

Which of the following actions will reduce risk to a laptop before traveling to a high risk area?

- A. Examine the device for physical tampering
- B. Implement more stringent baseline configurations
- C. Purge or re-image the hard disk drive
- D. Change access codes

Answer: D

NEW QUESTION 4

- (Exam Topic 1)

Intellectual property rights are PRIMARY concerned with which of the following?

- A. Owner's ability to realize financial gain
- B. Owner's ability to maintain copyright
- C. Right of the owner to enjoy their creation
- D. Right of the owner to control delivery method

Answer: D

NEW QUESTION 5

- (Exam Topic 1)

Which of the following types of technologies would be the MOST cost-effective method to provide a reactive control for protecting personnel in public areas?

- A. Install mantraps at the building entrances
- B. Enclose the personnel entry area with polycarbonate plastic
- C. Supply a duress alarm for personnel exposed to the public
- D. Hire a guard to protect the public area

Answer: D

NEW QUESTION 6

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 7

- (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 8

- (Exam Topic 2)

Which of the following is an effective control in preventing electronic cloning of Radio Frequency Identification (RFID) based access cards?

- A. Personal Identity Verification (PIV)
- B. Cardholder Unique Identifier (CHUID) authentication
- C. Physical Access Control System (PACS) repeated attempt detection
- D. Asymmetric Card Authentication Key (CAK) challenge-response

Answer: C

NEW QUESTION 9

- (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 10

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 10

- (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 12

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 14

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 18

- (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 22

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 24

- (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 25

- (Exam Topic 4)

At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

- A. Link layer
- B. Physical layer
- C. Session layer
- D. Application layer

Answer: D

NEW QUESTION 28

- (Exam Topic 6)

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

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

Answer: A

NEW QUESTION 29

- (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)

Recovery strategies of a Disaster Recovery planning (DRIP) MUST be aligned with which of the following?

- A. Hardware and software compatibility issues
- B. Applications' critically and downtime tolerance
- C. Budget constraints and requirements
- D. Cost/benefit analysis and business objectives

Answer: D

NEW QUESTION 32

- (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 33

- (Exam Topic 7)

What is the PRIMARY reason for implementing change management?

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

Answer: D

NEW QUESTION 38

- (Exam Topic 8)

Which of the following is a web application control that should be put into place to prevent exploitation of Operating System (OS) bugs?

- A. Check arguments in function calls
- B. Test for the security patch level of the environment
- C. Include logging functions
- D. Digitally sign each application module

Answer: B

NEW QUESTION 43

- (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 46

- (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 47

- (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 52

- (Exam Topic 9)

Logical access control programs are MOST effective when they are

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

Answer: D

NEW QUESTION 54

- (Exam Topic 9)

The key benefits of a signed and encrypted e-mail include

- A. confidentiality, authentication, and authorization.
- B. confidentiality, non-repudiation, and authentication.
- C. non-repudiation, authorization, and authentication.
- D. non-repudiation, confidentiality, and authorization.

Answer: B

NEW QUESTION 56

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 61

- (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 65

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 67

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 71

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 76

- (Exam Topic 9)

Multi-threaded applications are more at risk than single-threaded applications to

- A. race conditions.
- B. virus infection.
- C. packet sniffing.
- D. database injection.

Answer: A

NEW QUESTION 78

- (Exam Topic 9)

Which of the following is an authentication protocol in which a new random number is generated uniquely for each login session?

- A. Challenge Handshake Authentication Protocol (CHAP)
- B. Point-to-Point Protocol (PPP)
- C. Extensible Authentication Protocol (EAP)
- D. Password Authentication Protocol (PAP)

Answer: A

NEW QUESTION 81

- (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 83

- (Exam Topic 9)

Which of the following is the best practice for testing a Business Continuity Plan (BCP)?

- A. Test before the IT Audit
- B. Test when environment changes
- C. Test after installation of security patches
- D. Test after implementation of system patches

Answer: B

NEW QUESTION 85

- (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 88

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 92

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 96

- (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 97

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 101

- (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 106

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 111

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 114

- (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 116

- (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 121

- (Exam Topic 9)

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

Answer: D

NEW QUESTION 123

- (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 128

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 131

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 134

- (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 137

- (Exam Topic 9)

The birthday attack is MOST effective against which one of the following cipher technologies?

- A. Chaining block encryption
- B. Asymmetric cryptography
- C. Cryptographic hash
- D. Streaming cryptography

Answer: C

NEW QUESTION 139

- (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 141

- (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 143

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 145

- (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 147

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 150

- (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 152

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 157

- (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 161

- (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 165

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 169

- (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 173

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 175

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 176

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 179

- (Exam Topic 9)

Which of the following MUST be done when promoting a security awareness program to senior management?

- A. Show the need for security; identify the message and the audience
- B. Ensure that the security presentation is designed to be all-inclusive
- C. Notify them that their compliance is mandatory
- D. Explain how hackers have enhanced information security

Answer: A

NEW QUESTION 183

- (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 185

- (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 186

- (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 189

- (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 190

- (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 195

- (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 199

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 204

- (Exam Topic 10)

What is the MAIN feature that onion routing networks offer?

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

Answer: C

NEW QUESTION 205

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 210

- (Exam Topic 10)

Which of the following describes the concept of a Single Sign-On (SSO) system?

- A. Users are authenticated to one system at a time.
- B. Users are identified to multiple systems with several credentials.
- C. Users are authenticated to multiple systems with one login.
- D. Only one user is using the system at a time.

Answer: C

NEW QUESTION 214

- (Exam Topic 10)

Which of the following is an example of two-factor authentication?

- A. Retina scan and a palm print
- B. Fingerprint and a smart card
- C. Magnetic stripe card and an ID badge
- D. Password and Completely Automated Public Turing test to tell Computers and Humans Apart(CAPTCHA)

Answer: B

NEW QUESTION 218

- (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 219

- (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 223

- (Exam Topic 10)

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

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

Answer: A

NEW QUESTION 224

- (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 225

- (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 it is discovered that large quantities of information have been copied by the unauthorized individual, what attribute of the data has been compromised?

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

Answer: D

NEW QUESTION 228

- (Exam Topic 10)

According to best practice, which of the following is required when implementing third party software in a production environment?

- A. Scan the application for vulnerabilities
- B. Contract the vendor for patching
- C. Negotiate end user application training
- D. Escrow a copy of the software

Answer: A

NEW QUESTION 231

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 236

- (Exam Topic 10)

Which of the following BEST mitigates a replay attack against a system using identity federation and Security Assertion Markup Language (SAML) implementation?

- A. Two-factor authentication
- B. Digital certificates and hardware tokens
- C. Timed sessions and Secure Socket Layer (SSL)
- D. Passwords with alpha-numeric and special characters

Answer: C

NEW QUESTION 241

- (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 244

- (Exam Topic 10)

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

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

Answer: A

NEW QUESTION 246

- (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 247

- (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 248

- (Exam Topic 10)

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

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

Answer: A

NEW QUESTION 249

- (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 251

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 255

- (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 260

- (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 263

- (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 267

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 270

- (Exam Topic 10)

Refer to the information below to answer the question.

A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes. Following best practice, where should the permitted access for each department and job classification combination be specified?

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

Answer: B

NEW QUESTION 272

- (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 276

- (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 280

- (Exam Topic 10)

A Business Continuity Plan (BCP) is based on

- A. the policy and procedures manual.
- B. an existing BCP from a similar organization.
- C. a review of the business processes and procedures.
- D. a standard checklist of required items and objectives.

Answer: C

NEW QUESTION 281

- (Exam Topic 10)

Refer to the information below to answer the question.

A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.

What is the BEST reason for the organization to pursue a plan to mitigate client-based attacks?

- A. Client privilege administration is inherently weaker than server privilege administration.
- B. Client hardening and management is easier on clients than on servers.
- C. Client-based attacks are more common and easier to exploit than server and network based attacks.
- D. Client-based attacks have higher financial impact.

Answer: C

NEW QUESTION 286

- (Exam Topic 10)

Refer to the information below to answer the question.

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

The security program can be considered effective when

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

Answer: D

NEW QUESTION 289

- (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 292

- (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 295

- (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 298

- (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 299

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 303

- (Exam Topic 10)

A thorough review of an organization's audit logs finds that a disgruntled network administrator has intercepted emails meant for the Chief Executive Officer (CEO) and changed them before forwarding them to their intended recipient. What type of attack has MOST likely occurred?

- A. Spoofing
- B. Eavesdropping
- C. Man-in-the-middle
- D. Denial of service

Answer: C

NEW QUESTION 308

- (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 310

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 315

- (Exam Topic 10)

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

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

Answer: A

NEW QUESTION 316

- (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.

Organizational policy requires the deletion of user data from Personal Digital Assistant (PDA) devices before disposal. It may not be possible to delete the user data if the device is malfunctioning. Which destruction method below provides the BEST assurance that the data has been removed?

- A. Knurling
- B. Grinding
- C. Shredding
- D. Degaussing

Answer: C

NEW QUESTION 319

- (Exam Topic 11)

What is the process called when impact values are assigned to the security objectives for information types?

- A. Qualitative analysis
- B. Quantitative analysis
- C. Remediation
- D. System security categorization

Answer: D

NEW QUESTION 323

- (Exam Topic 11)

Which of the following prevents improper aggregation of privileges in Role Based Access Control (RBAC)?

- A. Hierarchical inheritance
- B. Dynamic separation of duties
- C. The Clark-Wilson security model
- D. The Bell-LaPadula security model

Answer: B

NEW QUESTION 327

- (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 328

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 331

- (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 335

- (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 336

- (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 339

- (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 342

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 345

- (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 348

- (Exam Topic 11)

Which of the following is the BEST method to assess the effectiveness of an organization's vulnerability management program?

- A. Review automated patch deployment reports
- B. Periodic third party vulnerability assessment
- C. Automated vulnerability scanning
- D. Perform vulnerability scan by security team

Answer: B

NEW QUESTION 351

- (Exam Topic 11)

Which of the following is most helpful in applying the principle of LEAST privilege?

- A. Establishing a sandboxing environment
- B. Setting up a Virtual Private Network (VPN) tunnel
- C. Monitoring and reviewing privileged sessions
- D. Introducing a job rotation program

Answer: A

NEW QUESTION 352

- (Exam Topic 11)

Which of the following disaster recovery test plans will be MOST effective while providing minimal risk?

- A. Read-through
- B. Parallel
- C. Full interruption
- D. Simulation

Answer: B

NEW QUESTION 354

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 357

- (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 361

- (Exam Topic 11)

The World Trade Organization's (WTO) agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires authors of computer software to be given the

- A. right to refuse or permit commercial rentals.
- B. right to disguise the software's geographic origin.
- C. ability to tailor security parameters based on location.
- D. ability to confirm license authenticity of their works.

Answer: A

NEW QUESTION 362

- (Exam Topic 11)

An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?

- A. Limits and scope of the testing.
- B. Physical location of server room and wiring closet.
- C. Logical location of filters and concentrators.
- D. Employee directory and organizational chart.

Answer: A

NEW QUESTION 366

- (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 369

- (Exam Topic 11)

When planning a penetration test, the tester will be MOST interested in which information?

- A. Places to install back doors
- B. The main network access points
- C. Job application handouts and tours
- D. Exploits that can attack weaknesses

Answer: B

NEW QUESTION 373

- (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 377

- (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 378

- (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.

<u>Functional Testing Techniques</u>		<u>Input Parameter Selection</u>
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

State-Based Analysis

Equivalence Class Analysis

Input Parameter Selection

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 380

- (Exam Topic 11)

Retaining system logs for six months or longer can be valuable for what activities?

- A. Disaster recovery and business continuity
- B. Forensics and incident response
- C. Identity and authorization management
- D. Physical and logical access control

Answer: B

NEW QUESTION 385

- (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 386

- (Exam Topic 11)

What type of encryption is used to protect sensitive data in transit over a network?

- A. Payload encryption and transport encryption
- B. Authentication Headers (AH)
- C. Keyed-Hashing for Message Authentication
- D. Point-to-Point Encryption (P2PE)

Answer: A

NEW QUESTION 387

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 391

- (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 395

- (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 399

- (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

[Empty box]

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

[Empty box]

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

[Empty box]

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

Risk

[Empty box]

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 400

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 402

- (Exam Topic 11)

Sensitive customer data is going to be added to a database. What is the MOST effective implementation for ensuring data privacy?

- A. Discretionary Access Control (DAC) procedures
- B. Mandatory Access Control (MAC) procedures
- C. Data link encryption
- D. Segregation of duties

Answer: B

NEW QUESTION 404

- (Exam Topic 11)

Which of the following controls is the FIRST step in protecting privacy in an information system?

- A. Data Redaction
- B. Data Minimization
- C. Data Encryption
- D. Data Storage

Answer: B

NEW QUESTION 407

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 409

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 411

- (Exam Topic 11)

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

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

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

Answer: A

NEW QUESTION 416

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 417

- (Exam Topic 11)

Which of the following methods can be used to achieve confidentiality and integrity for data in transit?

- A. Multiprotocol Label Switching (MPLS)
- B. Internet Protocol Security (IPSec)
- C. Federated identity management
- D. Multi-factor authentication

Answer: B

NEW QUESTION 421

- (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 426

- (Exam Topic 11)

What type of test assesses a Disaster Recovery (DR) plan using realistic disaster scenarios while maintaining minimal impact to business operations?

- A. Parallel
- B. Walkthrough
- C. Simulation
- D. Tabletop

Answer: C

NEW QUESTION 427

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 429

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 431

- (Exam Topic 11)

Which of the following BEST describes the purpose of the security functional requirements of Common Criteria?

- A. Level of assurance of the Target of Evaluation (TOE) in intended operational environment
- B. Selection to meet the security objectives stated in test documents
- C. Security behavior expected of a TOE
- D. Definition of the roles and responsibilities

Answer: C

NEW QUESTION 435

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 439

- (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 442

- (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

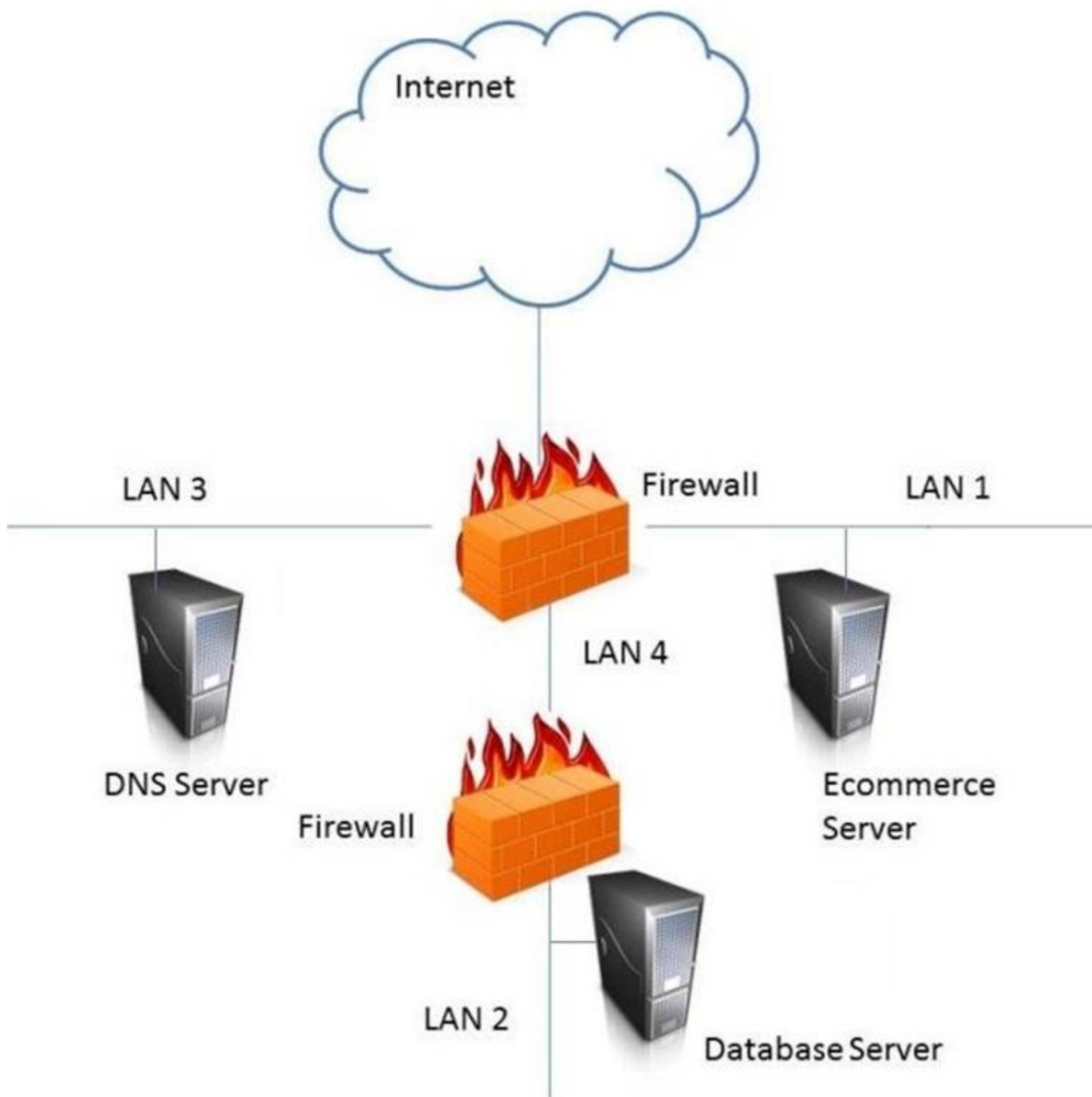
D. Remediation

Answer: A

NEW QUESTION 445

- (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 449

- (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 454

- (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 457

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 459

- (Exam Topic 11)

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

What is the best approach for the CISO?

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

What is the best approach for the CISO?

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

Answer: B

NEW QUESTION 462

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 467

- (Exam Topic 11)

A global organization wants to implement hardware tokens as part of a multifactor authentication solution for remote access. The PRIMARY advantage of this implementation is

- A. the scalability of token enrollment.
- B. increased accountability of end users.
- C. it protects against unauthorized access.
- D. it simplifies user access administration.

Answer: C

NEW QUESTION 468

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 469

- (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 471

- (Exam Topic 12)

Which of the following information **MUST** be provided for user account provisioning?

- A. Full name
- B. Unique identifier
- C. Security question
- D. Date of birth

Answer: B

NEW QUESTION 474

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 477

- (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 482

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 487

- (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 491

- (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 492

- (Exam Topic 12)

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

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

E-Authentication Token	Description
Memorized Secret Token	
Out-of-Band Token	
Look-up Secret Token	
Pre-registered Knowledge Token	

A physical or electronic token that stores a set of secrets between the claimant and the credential service provider
A physical token that is uniquely addressable and can receive a verifier-selected secret for one-time use
A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process
A secret shared between the subscriber and credential service provider that is typically character strings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

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

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

NEW QUESTION 493

- (Exam Topic 12)

Which of the following is MOST important when deploying digital certificates?

- A. Validate compliance with X.509 digital certificate standards
- B. Establish a certificate life cycle management framework
- C. Use a third-party Certificate Authority (CA)
- D. Use no less than 256-bit strength encryption when creating a certificate

Answer: B

NEW QUESTION 498

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 501

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 504

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 508

- (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 512

- (Exam Topic 12)

What is the BEST way to encrypt web application communications?

- A. Secure Hash Algorithm 1 (SHA-1)
- B. Secure Sockets Layer (SSL)
- C. Cipher Block Chaining Message Authentication Code (CBC-MAC)
- D. Transport Layer Security (TLS)

Answer: D

NEW QUESTION 517

- (Exam Topic 12)

At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

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

Answer: C

NEW QUESTION 520

- (Exam Topic 12)

When writing security assessment procedures, what is the MAIN purpose of the test outputs and reports?

- A. To force the software to fail and document the process
- B. To find areas of compromise in confidentiality and integrity
- C. To allow for objective pass or fail decisions
- D. To identify malware or hidden code within the test results

Answer: C

NEW QUESTION 522

- (Exam Topic 12)

Which of the following is the PRIMARY benefit of a formalized information classification program?

- A. It minimized system logging requirements.
- B. It supports risk assessment.
- C. It reduces asset vulnerabilities.
- D. It drives audit processes.

Answer: B

NEW QUESTION 527

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 528

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 533

- (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 535

- (Exam Topic 12)

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

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

Answer: C

NEW QUESTION 538

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 540

- (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 542

- (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 544

- (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 546

- (Exam Topic 12)

During the Security Assessment and Authorization process, what is the PRIMARY purpose for conducting a hardware and software inventory?

- A. Calculate the value of assets being accredited.
- B. Create a list to include in the Security Assessment and Authorization package.
- C. Identify obsolete hardware and software.
- D. Define the boundaries of the information system.

Answer: A

NEW QUESTION 548

- (Exam Topic 12)

What balance MUST be considered when web application developers determine how informative application error messages should be constructed?

- A. Risk versus benefit
- B. Availability versus auditability
- C. Confidentiality versus integrity
- D. Performance versus user satisfaction

Answer: A

NEW QUESTION 550

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 554

- (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 559

- (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 564

- (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 568

- (Exam Topic 13)

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

- A. undergo a security assessment as part of authorization process
- B. establish a risk management strategy

- C. harden the hosting server, and perform hosting and application vulnerability scans
- D. establish policies and procedures on system and services acquisition

Answer: D

NEW QUESTION 571

- (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 572

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 577

- (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 578

- (Exam Topic 13)

What protocol is often used between gateway hosts on the Internet?

- A. Exterior Gateway Protocol (EGP)
- B. Border Gateway Protocol (BGP)
- C. Open Shortest Path First (OSPF)
- D. Internet Control Message Protocol (ICMP)

Answer: B

NEW QUESTION 583

- (Exam Topic 13)

In an organization where Network Access Control (NAC) has been deployed, a device trying to connect to the network is being placed into an isolated domain. What could be done on this device in order to obtain proper connectivity?

- A. Connect the device to another network jack
- B. Apply remediation's according to security requirements
- C. Apply Operating System (OS) patches
- D. Change the Message Authentication Code (MAC) address of the network interface

Answer: B

NEW QUESTION 584

- (Exam Topic 13)

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

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

Answer:

A

NEW QUESTION 585

- (Exam Topic 13)

Which of the following is a direct monetary cost of a security incident?

- A. Morale
- B. Reputation
- C. Equipment
- D. Information

Answer: C

NEW QUESTION 588

- (Exam Topic 13)

Which security access policy contains fixed security attributes that are used by the system to determine a user's access to a file or object?

- A. Mandatory Access Control (MAC)
- B. Access Control List (ACL)
- C. Discretionary Access Control (DAC)
- D. Authorized user control

Answer: A

NEW QUESTION 590

- (Exam Topic 13)

Even though a particular digital watermark is difficult to detect, which of the following represents a way it might still be inadvertently removed?

- A. Truncating parts of the data
- B. Applying Access Control Lists (ACL) to the data
- C. Appending non-watermarked data to watermarked data
- D. Storing the data in a database

Answer: A

NEW QUESTION 592

- (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 596

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 599

- (Exam Topic 13)

The design review for an application has been completed and is ready for release. What technique should an organization use to assure application integrity?

- A. Application authentication
- B. Input validation
- C. Digital signing
- D. Device encryption

Answer: C

NEW QUESTION 601

- (Exam Topic 13)

It is MOST important to perform which of the following to minimize potential impact when implementing a new vulnerability scanning tool in a production environment?

- A. Negotiate schedule with the Information Technology (IT) operation's team
- B. Log vulnerability summary reports to a secured server

- C. Enable scanning during off-peak hours
- D. Establish access for Information Technology (IT) management

Answer: A

Explanation:

Section: Security Operations

NEW QUESTION 603

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 606

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 609

- (Exam Topic 13)

When determining who can accept the risk associated with a vulnerability, which of the following is MOST important?

- A. Countermeasure effectiveness
- B. Type of potential loss
- C. Incident likelihood
- D. Information ownership

Answer: C

NEW QUESTION 610

- (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 612

- (Exam Topic 13)

A security practitioner is tasked with securing the organization's Wireless Access Points (WAP). Which of these is the MOST effective way of restricting this environment to authorized users?

- A. Enable Wi-Fi Protected Access 2 (WPA2) encryption on the wireless access point
- B. Disable the broadcast of the Service Set Identifier (SSID) name
- C. Change the name of the Service Set Identifier (SSID) to a random value not associated with the organization
- D. Create Access Control Lists (ACL) based on Media Access Control (MAC) addresses

Answer: D

NEW QUESTION 617

- (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 618

- (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 620

- (Exam Topic 13)

What are the steps of a risk assessment?

- A. identification, analysis, evaluation
- B. analysis, evaluation, mitigation
- C. classification, identification, risk management
- D. identification, evaluation, mitigation

Answer: A

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 623

- (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 625

- (Exam Topic 13)

What does electronic vaulting accomplish?

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

Answer: A

Explanation:

Section: Security Operations

NEW QUESTION 628

- (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 632

- (Exam Topic 13)

What is the PRIMARY goal of fault tolerance?

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

Answer: A

NEW QUESTION 635

- (Exam Topic 13)

An organization recently conducted a review of the security of its network applications. One of the vulnerabilities found was that the session key used in encrypting sensitive information to a third party server had been hard-coded in the client and server applications. Which of the following would be MOST effective in mitigating this vulnerability?

- A. Diffie-Hellman (DH) algorithm
- B. Elliptic Curve Cryptography (ECC) algorithm
- C. Digital Signature algorithm (DSA)
- D. Rivest-Shamir-Adleman (RSA) algorithm

Answer: A

NEW QUESTION 640

- (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 644

- (Exam Topic 13)

An Information Technology (IT) professional attends a cybersecurity seminar on current incident response methodologies. What code of ethics canon is being observed?

- A. Provide diligent and competent service to principals
- B. Protect society, the commonwealth, and the infrastructure
- C. Advance and protect the profession
- D. Act honorable, honesty, justly, responsibly, and legally

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 649

- (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 652

- (Exam Topic 13)

Which of the following entails identification of data and links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

- A. Security governance
- B. Risk management
- C. Security portfolio management
- D. Risk assessment

Answer: B

NEW QUESTION 657

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 662

- (Exam Topic 13)

When developing a business case for updating a security program, the security program owner MUST do which of the following?

- A. Identify relevant metrics
- B. Prepare performance test reports
- C. Obtain resources for the security program
- D. Interview executive management

Answer: A

NEW QUESTION 666

- (Exam Topic 13)

What is the foundation of cryptographic functions?

- A. Encryption
- B. Cipher
- C. Hash
- D. Entropy

Answer: A

NEW QUESTION 668

- (Exam Topic 13)

When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

- A. Log all activities associated with sensitive systems
- B. Provide links to security policies
- C. Confirm that confidentiality agreements are signed
- D. Employ strong access controls

Answer: D

NEW QUESTION 673

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 676

- (Exam Topic 13)

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

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

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 678

- (Exam Topic 13)

Which Identity and Access Management (IAM) process can be used to maintain the principle of least privilege?

- A. identity provisioning
- B. access recovery
- C. multi-factor authentication (MFA)
- D. user access review

Answer: A

NEW QUESTION 679

- (Exam Topic 13)

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

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

Answer:

B

NEW QUESTION 681

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 682

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 686

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 687

- (Exam Topic 13)

Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) only provides which of the following?

- A. Mutual authentication
- B. Server authentication
- C. User authentication
- D. Streaming ciphertext data

Answer: C

NEW QUESTION 690

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 691

- (Exam Topic 13)

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

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

Answer: D

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 693

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 696

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 697

- (Exam Topic 13)

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

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

or `1=1`

What type of attack does this indicate?

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

Answer: C

NEW QUESTION 702

- (Exam Topic 13)

Attack trees are MOST useful for which of the following?

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

Answer: A

NEW QUESTION 703

- (Exam Topic 13)

Which of the following is the BEST metric to obtain when gaining support for an Identify and Access Management (IAM) solution?

- A. Application connection successes resulting in data leakage
- B. Administrative costs for restoring systems after connection failure
- C. Employee system timeouts from implementing wrong limits
- D. Help desk costs required to support password reset requests

Answer: D

NEW QUESTION 707

- (Exam Topic 13)

Which of the following would BEST support effective testing of patch compatibility when patches are applied to an organization's systems?

- A. Standardized configurations for devices
- B. Standardized patch testing equipment
- C. Automated system patching
- D. Management support for patching

Answer: A

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 711

- (Exam Topic 13)

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

- A. a functional evacuation of personnel
- B. a specific test by response teams of individual emergency response functions
- C. an activation of the backup site

D. a full-scale simulation of an emergency and the subsequent response functions.

Answer: D

NEW QUESTION 715

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 716

- (Exam Topic 13)

Access to which of the following is required to validate web session management?

- A. Log timestamp
- B. Live session traffic
- C. Session state variables
- D. Test scripts

Answer: C

NEW QUESTION 718

- (Exam Topic 13)

Which of the following is a common feature of an Identity as a Service (IDaaS) solution?

- A. Single Sign-On (SSO) authentication support
- B. Privileged user authentication support
- C. Password reset service support
- D. Terminal Access Controller Access Control System (TACACS) authentication support

Answer: A

NEW QUESTION 719

.....

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](#)