CISSP Dumps

Certified Information Systems Security Professional (CISSP)

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

NEW QUESTION 1
- (Exam Topic 1)
An important principle of defense in depth is that achieving information security requires a balanced focus on which PRIMARY elements?

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

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
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 3
- (Exam Topic 1)
When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined?

A. Only when assets are clearly defined
B. Only when standards are defined
C. Only when controls are put in place
D. Only procedures are defined

Answer: A

NEW QUESTION 4
- (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 5
- (Exam Topic 1)
All of the following items should be included in a Business Impact Analysis (BIA) questionnaire EXCEPT questions that

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

Answer: B

NEW QUESTION 6
- (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 7
- (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 8
- (Exam Topic 2)
In a data classification scheme, the data is owned by the

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

Answer: B

NEW QUESTION 9
- (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 10
- (Exam Topic 2)
Which of the following is an initial consideration when developing an information security management system?

A. Identify the contractual security obligations that apply to the organizations
B. Understand the value of the information assets
C. Identify the level of residual risk that is tolerable to management
D. Identify relevant legislative and regulatory compliance requirements

Answer: B

NEW QUESTION 10
- (Exam Topic 2)
When implementing a data classification program, why is it important to avoid too much granularity?

A. The process will require too many resources
B. It will be difficult to apply to both hardware and software
C. It will be difficult to assign ownership to the data
D. The process will be perceived as having value

Answer: A

NEW QUESTION 13
- (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 16
- (Exam Topic 3)
Which of the following mobile code security models relies only on trust?

A. Code signing
B. Class authentication
C. Sandboxing
D. Type safety

Answer: A

NEW QUESTION 17
- (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 21
- (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 25
- (Exam Topic 4)
An input validation and exception handling vulnerability has been discovered on a critical web-based system. Which of the following is MOST suited to quickly implement a control?

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

Answer: A

NEW QUESTION 30
- (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 31
- (Exam Topic 4)
Which of the following is used by the Point-to-Point Protocol (PPP) to determine packet formats?

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

Answer: B

NEW QUESTION 36
- (Exam Topic 5)
A manufacturing organization wants to establish a Federated Identity Management (FIM) system with its 20 different supplier companies. Which of the following is the BEST solution for the manufacturing organization?

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

Answer: C

NEW QUESTION 38
- (Exam Topic 5)
What is the BEST approach for controlling access to highly sensitive information when employees have the same level of security clearance?

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

Answer: B

NEW QUESTION 40

- (Exam Topic 6)
Which of the following could cause a Denial of Service (DoS) against an authentication system?

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

Answer: D

NEW QUESTION 42
- (Exam Topic 6)
A Virtual Machine (VM) environment has five guest Operating Systems (OS) and provides strong isolation. What MUST an administrator review to audit a user's access to data files?

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

Answer: A

NEW QUESTION 44
- (Exam Topic 6)
Which of the following is a PRIMARY benefit of using a formalized security testing report format and structure?

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

Answer: D

NEW QUESTION 47
- (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 49
- (Exam Topic 7)
An organization is found lacking the ability to properly establish performance indicators for its Web hosting solution during an audit. What would be the MOST probable cause?

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

Answer: D

NEW QUESTION 53
- (Exam Topic 7)
With what frequency should monitoring of a control occur when implementing Information Security Continuous Monitoring (ISCM) solutions?

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

Answer: B

NEW QUESTION 57
- (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 61
- (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 64
- (Exam Topic 8)
Which of the following is the BEST method to prevent malware from being introduced into a production environment?

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

Answer: D

NEW QUESTION 66
- (Exam Topic 8)
A Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. The program is not working as expected.
What is the MOST probable security feature of Java preventing the program from operating as intended?

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

Answer: A

NEW QUESTION 68
- (Exam Topic 8)
The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle (SDLC)?

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

Answer: A

Explanation:
Reference https://online.concordiA.edu/computer-science/system-development-life-cycle-phases/

NEW QUESTION 72
- (Exam Topic 9)
The three PRIMARY requirements for a penetration test are

A. A defined goal, limited time period, and approval of management
B. A general objective, unlimited time, and approval of the network administrator
C. An objective statement, disclosed methodology, and fixed cost
D. A stated objective, liability waiver, and disclosed methodology

Answer: A

NEW QUESTION 77
- (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 79
- (Exam Topic 9)
Which of the following is ensured when hashing files during chain of custody handling?

A. Availability
B. Accountability
C. Integrity
D. Non-repudiation

Answer: C

NEW QUESTION 83
- (Exam Topic 9)
To prevent inadvertent disclosure of restricted information, which of the following would be the LEAST effective process for eliminating data prior to the media being discarded?

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

Answer: C

NEW QUESTION 88
- (Exam Topic 9)
Which one of the following is a threat related to the use of web-based client side input validation?

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

Answer: A

NEW QUESTION 89
- (Exam Topic 9)
A vulnerability test on an Information System (IS) is conducted to

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

Answer: C

NEW QUESTION 92
- (Exam Topic 9)
Copyright provides protection for which of the following?

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

Answer: B

NEW QUESTION 95
- (Exam Topic 9)
What technique BEST describes antivirus software that detects viruses by watching anomalous behavior?

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

Answer: D

NEW QUESTION 96
- (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 100

- (Exam Topic 9)
Which one of the following transmission media is MOST effective in preventing data interception?

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

Answer: C

NEW QUESTION 103
- (Exam Topic 9)
Checking routing information on e-mail to determine it is in a valid format and contains valid information is an example of which of the following anti-spam approaches?

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

Answer: D

NEW QUESTION 104
- (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 105
- (Exam Topic 9)
Which security action should be taken FIRST when computer personnel are terminated from their jobs?

A. Remove their computer access
B. Require them to turn in their badge
C. Conduct an exit interview
D. Reduce their physical access level to the facility

Answer: A

NEW QUESTION 109
- (Exam Topic 9)
The type of authorized interactions a subject can have with an object is

A. control.
B. permission.
C. procedure.
D. protocol.

Answer: B

NEW QUESTION 114
- (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 117
- (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 120
- (Exam Topic 9)
Including a Trusted Platform Module (TPM) in the design of a computer system is an example of a technique to what?

A. Interface with the Public Key Infrastructure (PKI)
B. Improve the quality of security software
C. Prevent Denial of Service (DoS) attacks
D. Establish a secure initial state

Answer: D

NEW QUESTION 123
- (Exam Topic 9)
Which one of these risk factors would be the LEAST important consideration in choosing a building site for a new computer facility?

A. Vulnerability to crime
B. Adjacent buildings and businesses
C. Proximity to an airline flight path
D. Vulnerability to natural disasters

Answer: C

NEW QUESTION 127
- (Exam Topic 9)
The process of mutual authentication involves a computer system authenticating a user and authenticating the

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

Answer: B

NEW QUESTION 130
- (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 133
- (Exam Topic 9)
A security professional has just completed their organization's Business Impact Analysis (BIA). Following Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) best practices, what would be the professional's NEXT step?

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

Answer: A

NEW QUESTION 135
- (Exam Topic 9)
What security management control is MOST often broken by collusion?

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

Answer: B

NEW QUESTION 137
- (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 139
- (Exam Topic 9)
Which of the following does the Encapsulating Security Payload (ESP) provide?

A. Authorization and integrity
B. Availability and integrity
C. Integrity and confidentiality
D. Authorization and confidentiality

Answer: C

NEW QUESTION 143
- (Exam Topic 9)
Which one of the following is the MOST important in designing a biometric access system if it is essential that no one other than authorized individuals are admitted?

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

Answer: A

NEW QUESTION 146
- (Exam Topic 9)
Which of the following is an essential element of a privileged identity lifecycle management?

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

Answer: A

NEW QUESTION 147
- (Exam Topic 9)
A practice that permits the owner of a data object to grant other users access to that object would usually provide

A. Mandatory Access Control (MAC).
B. owner-administered control.
C. owner-dependent access control.
D. Discretionary Access Control (DAC).

Answer: D

NEW QUESTION 149
- (Exam Topic 9)
Which one of the following security mechanisms provides the BEST way to restrict the execution of privileged procedures?

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

Answer: A

NEW QUESTION 150
- (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 155
- (Exam Topic 9)
Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?

A. Transparent Database Encryption (TDE)
B. Column level database encryption

C. Volume encryption
D. Data tokenization

Answer: D

NEW QUESTION 156
- (Exam Topic 9)
Which of the following statements is TRUE for point-to-point microwave transmissions?

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

Answer: D

NEW QUESTION 160
- (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 165
- (Exam Topic 9)
Which of the following is the BEST way to verify the integrity of a software patch?

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

Answer: A

NEW QUESTION 169
- (Exam Topic 9)
The FIRST step in building a firewall is to

A. assign the roles and responsibilities of the firewall administrators.
B. define the intended audience who will read the firewall policy.
C. identify mechanisms to encourage compliance with the policy.
D. perform a risk analysis to identify issues to be addressed.

Answer: D

NEW QUESTION 171
- (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 176
- (Exam Topic 9)
What would be the PRIMARY concern when designing and coordinating a security assessment for an Automatic Teller Machine (ATM) system?

A. Physical access to the electronic hardware
B. Regularly scheduled maintenance process
C. Availability of the network connection
D. Processing delays

Answer: A

NEW QUESTION 180
- (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 183
- (Exam Topic 9)
Which of the following is a security limitation of File Transfer Protocol (FTP)?

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

Answer: D

NEW QUESTION 184
- (Exam Topic 9)
Which one of the following effectively obscures network addresses from external exposure when implemented on a firewall or router?

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

Answer: A

NEW QUESTION 185
- (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 188
- (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 193
- (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 198
- (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 201
- (Exam Topic 9)
When transmitting information over public networks, the decision to encrypt it should be based on

A. the estimated monetary value of the information.
B. whether there are transient nodes relaying the transmission.
C. the level of confidentiality of the information.
D. the volume of the information.

Answer: C

NEW QUESTION 205
- (Exam Topic 9)
Following the completion of a network security assessment, which of the following can BEST be demonstrated?

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

Answer: A

NEW QUESTION 208
- (Exam Topic 9)
In a data classification scheme, the data is owned by the

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

Answer: B

NEW QUESTION 209
- (Exam Topic 9)
When implementing controls in a heterogeneous end-point network for an organization, it is critical that

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

Answer: C

NEW QUESTION 214
- (Exam Topic 9)
While impersonating an Information Security Officer (ISO), an attacker obtains information from company employees about their User IDs and passwords. Which method of information gathering has the attacker used?

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

Answer: C

NEW QUESTION 218
- (Exam Topic 9)
When constructing an Information Protection Policy (IPP), it is important that the stated rules are necessary, adequate, and

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

Answer: D

NEW QUESTION 219
- (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 220
- (Exam Topic 9)
Which of the following does Temporal Key Integrity Protocol (TKIP) support?

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

Answer: C

NEW QUESTION 221
- (Exam Topic 9)
Which of the following BEST represents the principle of open design?

A. Disassembly, analysis, or reverse engineering will reveal the security functionality of the computer system.
B. Algorithms must be protected to ensure the security and interoperability of the designed system.
C. A knowledgeable user should have limited privileges on the system to prevent their ability to compromise security capabilities.
D. The security of a mechanism should not depend on the secrecy of its design or implementation.

Answer: D

NEW QUESTION 222
- (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 226
- (Exam Topic 9)
Which of the following wraps the decryption key of a full disk encryption implementation and ties the hard disk drive to a particular device?

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

Answer: A

NEW QUESTION 228
- (Exam Topic 9)
Two companies wish to share electronic inventory and purchase orders in a supplier and client relationship. What is the BEST security solution for them?

A. Write a Service Level Agreement (SLA) for the two companies.
B. Set up a Virtual Private Network (VPN) between the two companies.
C. Configure a firewall at the perimeter of each of the two companies.
D. Establish a File Transfer Protocol (FTP) connection between the two companies.

Answer: B

NEW QUESTION 232
- (Exam Topic 9)
At a MINIMUM, a formal review of any Disaster Recovery Plan (DRP) should be conducted

A. monthly.
B. quarterly.
C. annually.
D. bi-annually.

Answer: C

NEW QUESTION 237
- (Exam Topic 9)
In Disaster Recovery (DR) and business continuity training, which BEST describes a functional drill?

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

Answer: B

NEW QUESTION 242
- (Exam Topic 10)
Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?

A. Requirements Analysis
B. Development and Deployment
C. Production Operations
D. Utilization Support

Answer: A

NEW QUESTION 245
- (Exam Topic 10)
Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following solutions would have MOST likely detected the use of peer-to-peer programs when the computer was connected to the office network?
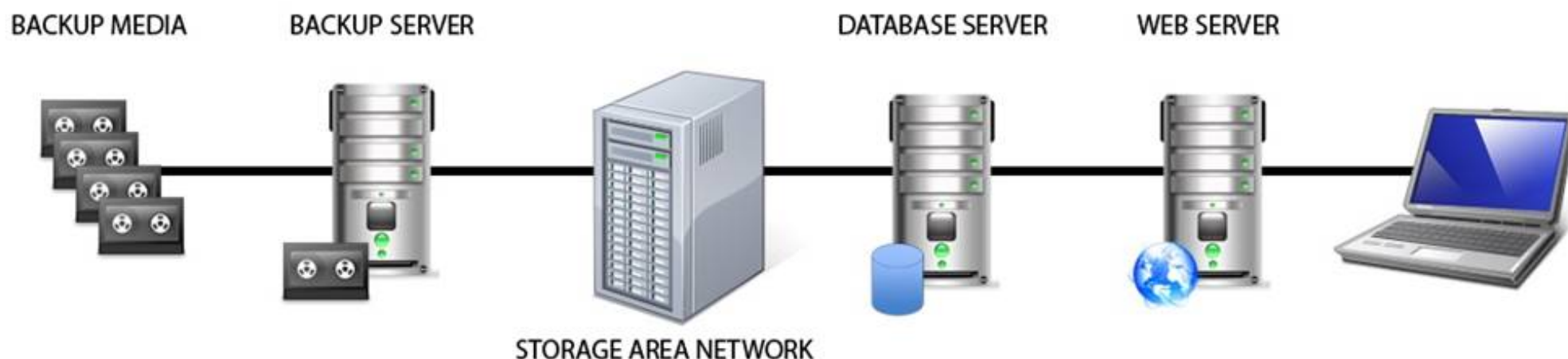
A. Anti-virus software
B. Intrusion Prevention System (IPS)
C. Anti-spyware software
D. Integrity checking software

Answer: B

NEW QUESTION 249
- (Exam Topic 10)
Identify the component that MOST likely lacks digital accountability related to information access. Click on the correct device in the image below.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 251
- (Exam Topic 10)
Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
The organization should ensure that the third party's physical security controls are in place so that they

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

Answer: B

NEW QUESTION 255
- (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 258
- (Exam Topic 10)
When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?

A. Perform a service provider PCI-DSS assessment on a yearly basis.
B. Validate the service provider's PCI-DSS compliance status on a regular basis.
C. Validate that the service providers security policies are in alignment with those of the organization.
D. Ensure that the service provider updates and tests its Disaster Recovery Plan (DRP) on a yearly basis.

Answer: B

NEW QUESTION 263
- (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			Table B	
User	Clearance Level		Files	Security Class
A	Restricted		1	Restricted
B	Confidential		2	Confidential
C	Secret		3	Secret
D	Top 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 265
- (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 267
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration
functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
Which of the following will be the PRIMARY security concern as staff is released from the organization?

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

Answer: B

NEW QUESTION 271
- (Exam Topic 10)
An online retail company has formulated a record retention schedule for customer transactions. Which of the following is a valid reason a customer transaction is kept beyond the retention schedule?

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

Answer: A

NEW QUESTION 276
- (Exam Topic 10)
What does secure authentication with logging provide?

A. Data integrity
B. Access accountability
C. Encryption logging format
D. Segregation of duties

Answer: B

NEW QUESTION 279
- (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 280
- (Exam Topic 10)
Which item below is a federated identity standard?

A. 802.11i
B. Kerberos
C. Lightweight Directory Access Protocol (LDAP)
D. Security Assertion Markup Language (SAML)

Answer: D

NEW QUESTION 281
- (Exam Topic 10)
What is the MOST effective method for gaining unauthorized access to a file protected with a long complex password?

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

Answer: C

NEW QUESTION 284
- (Exam Topic 10)
Multi-Factor Authentication (MFA) is necessary in many systems given common types of password attacks. Which of the following is a correct list of password attacks?

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

Answer: B

NEW QUESTION 287
- (Exam Topic 10)
Which of the following is required to determine classification and ownership?

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

Answer: A

NEW QUESTION 289
- (Exam Topic 10)
Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
The third party needs to have

A. processes that are identical to that of the organization doing the outsourcing.
B. access to the original personnel that were on staff at the organization.

C. the ability to maintain all of the applications in languages they are familiar with.
D. access to the skill sets consistent with the programming languages used by the organization.

Answer: D

NEW QUESTION 291
- (Exam Topic 10)
Given the various means to protect physical and logical assets, match the access management area to the technology.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 293
- (Exam Topic 10)
A security manager has noticed an inconsistent application of server security controls resulting in vulnerabilities on critical systems. What is the MOST likely cause of this issue?

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

Answer: A

NEW QUESTION 297
- (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 302
- (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 304

- (Exam Topic 10)
During the procurement of a new information system, it was determined that some of the security requirements were not addressed in the system specification. Which of the following is the MOST likely reason for this?

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

Answer: D

NEW QUESTION 308
- (Exam Topic 10)
When implementing a secure wireless network, which of the following supports authentication and authorization for individual client endpoints?

A. Temporal Key Integrity Protocol (TKIP)
B. Wi-Fi Protected Access (WPA) Pre-Shared Key (PSK)
C. Wi-Fi Protected Access 2 (WPA2) Enterprise
D. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

Answer: C

NEW QUESTION 311
- (Exam Topic 10)
With data labeling, which of the following MUST be the key decision maker?

A. Information security
B. Departmental management
C. Data custodian
D. Data owner

Answer: D

NEW QUESTION 315
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
Which of the following will MOST likely allow the organization to keep risk at an acceptable level?

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

Answer: C

NEW QUESTION 317
- (Exam Topic 10)
A large bank deploys hardware tokens to all customers that use their online banking system. The token generates and displays a six digit numeric password every 60 seconds. The customers must log into their bank accounts using this numeric password. This is an example of

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

Answer: D

NEW QUESTION 321
- (Exam Topic 10)
What is the BEST method to detect the most common improper initialization problems in programming languages?

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

Answer: B

NEW QUESTION 324
- (Exam Topic 10)
Which of the following MUST system and database administrators be aware of and apply when configuring systems used for storing personal employee data?

A. Secondary use of the data by business users
B. The organization's security policies and standards

C. The business purpose for which the data is to be used
D. The overall protection of corporate resources and data

Answer: B

NEW QUESTION 325
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?

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

Answer: A

NEW QUESTION 329
- (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 333
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
Which of the following BEST describes the access control methodology used?

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

Answer: C

NEW QUESTION 335
- (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 338
- (Exam Topic 10)
Which of the following is the MAIN goal of a data retention policy?

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

Answer: C

NEW QUESTION 341
- (Exam Topic 10)
The use of proximity card to gain access to a building is an example of what type of security control?

A. Legal
B. Logical

C. Physical
D. Procedural

Answer: C

NEW QUESTION 344
- (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 346
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
In addition to authentication at the start of the user session, best practice would require re-authentication

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

Answer: D

NEW QUESTION 350
- (Exam Topic 10)
A large university needs to enable student access to university resources from their homes. Which of the following provides the BEST option for low maintenance and ease of deployment?

A. Provide students with Internet Protocol Security (IPSec) Virtual Private Network (VPN) client software.
B. Use Secure Sockets Layer (SSL) VPN technology.
C. Use Secure Shell (SSH) with public/private keys.
D. Require students to purchase home router capable of VPN.

Answer: B

NEW QUESTION 351
- (Exam Topic 10)
The amount of data that will be collected during an audit is PRIMARILY determined by the

A. audit scope.
B. auditor's experience level.
C. availability of the datA.
D. integrity of the datA.

Answer: A

NEW QUESTION 352
- (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		Table B	
User	Clearance Level	Files	Security Class
A	Restricted	1	Restricted
B	Confidential	2	Confidential
C	Secret	3	Secret
D	Top Secret	4	Top Secret

In a Bell-LaPadula system, which user has the MOST restrictions when writing data to any of the four files?

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

Answer: D

NEW QUESTION 353
- (Exam Topic 10)
An organization decides to implement a partial Public Key Infrastructure (PKI) with only the servers having digital certificates. What is the security benefit of this implementation?

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

Answer: D

NEW QUESTION 355
- (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 358
- (Exam Topic 10)
Which of the following is the PRIMARY benefit of a formalized information classification program?

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

Answer: B

NEW QUESTION 359
- (Exam Topic 10)
A risk assessment report recommends upgrading all perimeter firewalls to mitigate a particular finding. Which of the following BEST supports this recommendation?

A. The inherent risk is greater than the residual risk.
B. The Annualized Loss Expectancy (ALE) approaches zero.
C. The expected loss from the risk exceeds mitigation costs.
D. The infrastructure budget can easily cover the upgrade costs.

Answer: C

NEW QUESTION 362
- (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 363
- (Exam Topic 10)
During an audit, the auditor finds evidence of potentially illegal activity. Which of the following is the MOST appropriate action to take?

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

Answer: D

NEW QUESTION 368
- (Exam Topic 10)
When using third-party software developers, which of the following is the MOST effective method of providing software development Quality Assurance (QA)?

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

Answer: B

NEW QUESTION 371
- (Exam Topic 10)
Which of the following provides the MOST protection against data theft of sensitive information when a laptop is stolen?

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

Answer: D

NEW QUESTION 372
- (Exam Topic 10)
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
Aside from the potential records which may have been viewed, which of the following should be the PRIMARY concern regarding the database information?

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

Answer: A

NEW QUESTION 374
- (Exam Topic 11)
What is the process called when impact values are assigned to the security objectives for information types?
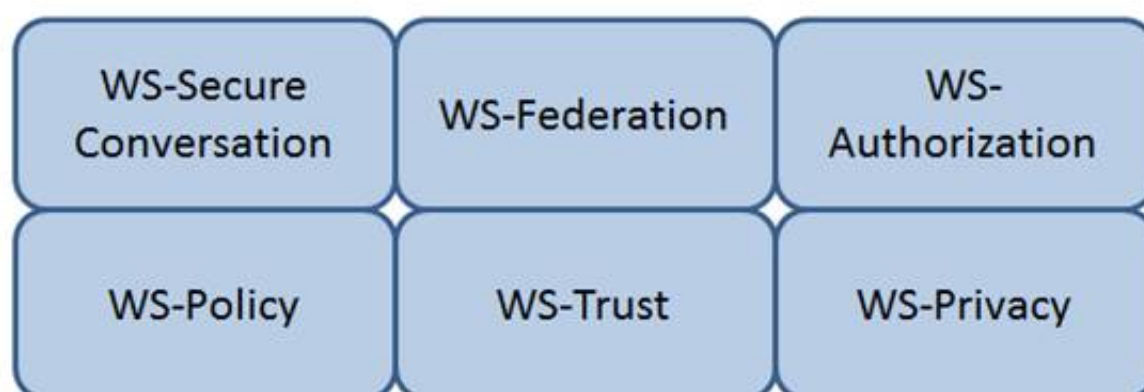
A. Qualitative analysis
B. Quantitative analysis
C. Remediation
D. System security categorization

Answer: D

NEW QUESTION 375
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the correct specification in the image below.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 379
- (Exam Topic 11)
If an identification process using a biometric system detects a 100% match between a presented template and a stored template, what is the interpretation of this result?

A. User error
B. Suspected tampering
C. Accurate identification
D. Unsuccessful identification

Answer: B

NEW QUESTION 383
- (Exam Topic 11)
A security professional has been asked to evaluate the options for the location of a new data center within a multifloor building. Concerns for the data center include emanations and physical access controls.
Which of the following is the BEST location?

A. On the top floor
B. In the basement
C. In the core of the building
D. In an exterior room with windows

Answer: C

NEW QUESTION 386
- (Exam Topic 11)
Which of the following BEST describes a Protection Profile (PP)?

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

Answer: A

NEW QUESTION 389
- (Exam Topic 11)
Changes to a Trusted Computing Base (TCB) system that could impact the security posture of that system and trigger a recertification activity are documented in the

A. security impact analysis.
B. structured code review.
C. routine self assessment.
D. cost benefit analysis.

Answer: A

NEW QUESTION 392
- (Exam Topic 11)
What should happen when an emergency change to a system must be performed?

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

Answer: B

NEW QUESTION 395
- (Exam Topic 11)
Which of the following is a reason to use manual patch installation instead of automated patch management?

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

Answer: C

NEW QUESTION 397
- (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 399
- (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 400
- (Exam Topic 11)
How can lessons learned from business continuity training and actual recovery incidents BEST be used?

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

Answer: A

NEW QUESTION 402
- (Exam Topic 11)
How does an organization verify that an information system's current hardware and software match the standard system configuration?

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

Answer: C

NEW QUESTION 406
- (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 408
- (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 409
- (Exam Topic 11)
Disaster Recovery Plan (DRP) training material should be

A. consistent so that all audiences receive the same training.
B. stored in a fire proof safe to ensure availability when needed.
C. only delivered in paper format.
D. presented in a professional looking manner.

Answer: A

NEW QUESTION 412

- (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 416
- (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 419
- (Exam Topic 11)
Which of the following analyses is performed to protect information assets?

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

Answer: A

NEW QUESTION 424
- (Exam Topic 11)
Single Sign-On (SSO) is PRIMARILY designed to address which of the following?

A. Confidentiality and Integrity
B. Availability and Accountability
C. Integrity and Availability
D. Accountability and Assurance

Answer: D

NEW QUESTION 429
- (Exam Topic 11)
Discretionary Access Control (DAC) restricts access according to

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

Answer: C

NEW QUESTION 432
- (Exam Topic 11)
Which of the following standards/guidelines requires an Information Security Management System (ISMS) to be defined?

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

Answer: A

NEW QUESTION 433
- (Exam Topic 11)
What is the MOST efficient way to secure a production program and its data?

A. Disable default accounts and implement access control lists (ACL)
B. Harden the application and encrypt the data
C. Disable unused services and implement tunneling
D. Harden the servers and backup the data

Answer: B

NEW QUESTION 437
- (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 439
- (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 440
- (Exam Topic 11)
During a fingerprint verification process, which of the following is used to verify identity and authentication?

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

Answer: D

NEW QUESTION 443
- (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 447
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.
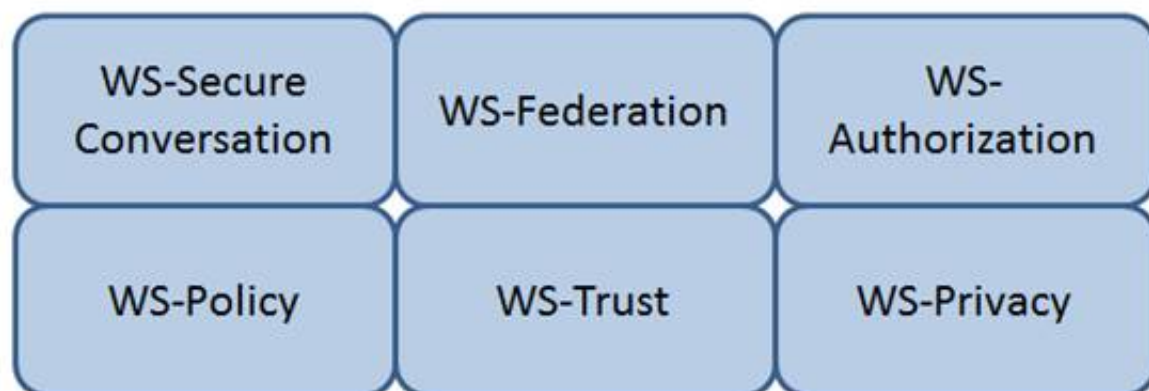
A. Mastered
B. Not Mastered

Answer: A

Explanation:
WS-Federation
Reference: Java Web Services: Up and Running" By Martin Kalin page 228

NEW QUESTION 449
- (Exam Topic 11)
For privacy protected data, which of the following roles has the highest authority for establishing dissemination rules for the data?

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

Answer: B

NEW QUESTION 451
- (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 455
- (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 457
- (Exam Topic 11)
The PRIMARY security concern for handheld devices is the

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

Answer: C

NEW QUESTION 461
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued,
renewed and validated? Click on the correct specification in the image below.
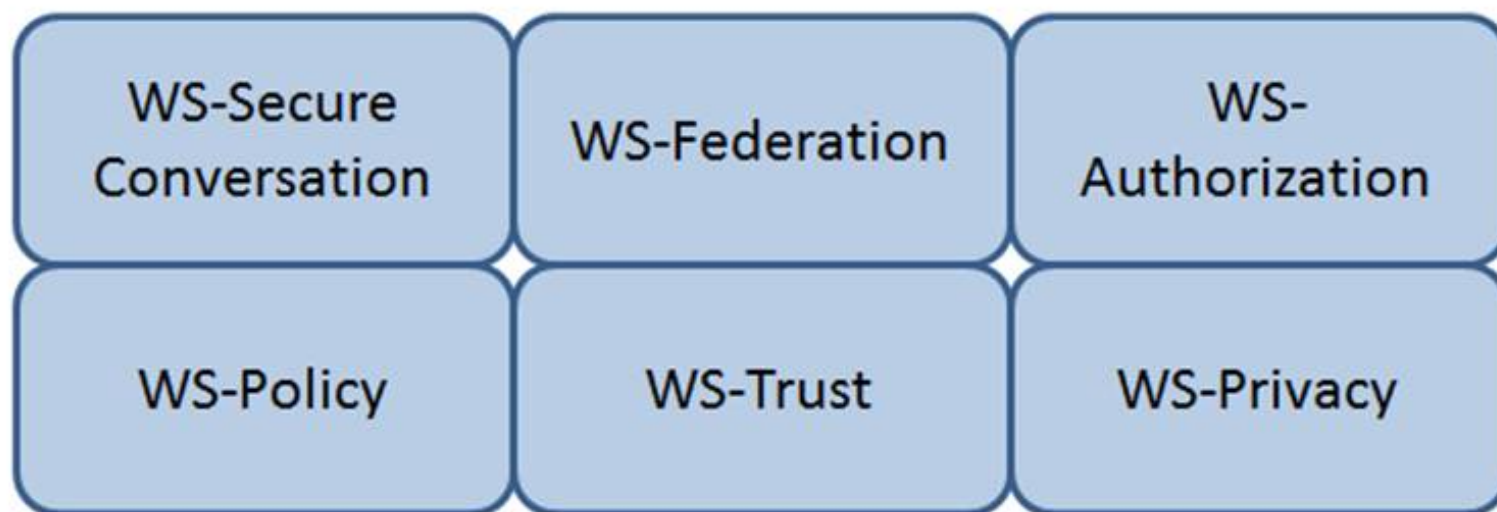
A. Mastered
B. Not Mastered

Answer: A

Explanation:
WS-Trust
The protocol used for issuing security tokens is based on WS-Trust. WS-Trust is a Web service specification that builds on WS-Security. It describes a protocol used for issuance, exchange, and validation of security tokens. WS-Trust provides a solution for interoperability by defining a protocol for issuing and exchanging security tokens, based on token format, namespace, or trust boundaries.
Reference: https://msdn.microsoft.com/en-us/library/ff650503.aspx

NEW QUESTION 464
- (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 467
- (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 469
- (Exam Topic 11)
Software Code signing is used as a method of verifying what security concept?

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

Answer: A

NEW QUESTION 473

- (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 477
- (Exam Topic 11)
The goal of a Business Continuity Plan (BCP) training and awareness program is to

A. enhance the skills required to create, maintain, and execute the plan.
B. provide for a high level of recovery in case of disaster.
C. describe the recovery organization to new employees.
D. provide each recovery team with checklists and procedures.

Answer: A

NEW QUESTION 482
- (Exam Topic 11)
The PRIMARY outcome of a certification process is that it provides documented

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

Answer: D

NEW QUESTION 486
- (Exam Topic 11)
What security risk does the role-based access approach mitigate MOST effectively?

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

Answer: A

NEW QUESTION 488
- (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 491
- (Exam Topic 11)
Which one of the following operates at the session, transport, or network layer of the Open System Interconnection (OSI) model?

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

Answer: D

NEW QUESTION 493
- (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 494
- (Exam Topic 11)
Discretionary Access Control (DAC) is based on which of the following?

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

Answer: B

NEW QUESTION 497
- (Exam Topic 11)
A network scan found 50% of the systems with one or more critical vulnerabilities. Which of the following represents the BEST action?

A. Assess vulnerability risk and program effectiveness.
B. Assess vulnerability risk and business impact.
C. Disconnect all systems with critical vulnerabilities.
D. Disconnect systems with the most number of vulnerabilities.

Answer: B

NEW QUESTION 499
- (Exam Topic 11)
When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?

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

Answer: B

NEW QUESTION 501
- (Exam Topic 11)
Which of the following BEST avoids data remanence disclosure for cloud hosted resources?

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

Answer: A

NEW QUESTION 502
- (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 506
- (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 511
- (Exam Topic 11)
Which of the following protocols would allow an organization to maintain a centralized list of users that can read a protected webpage?

A. Lightweight Directory Access Control (LDAP)
B. Security Assertion Markup Language (SAML)
C. Hypertext Transfer Protocol (HTTP)
D. Kerberos

Answer: A

NEW QUESTION 516
- (Exam Topic 11)
Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?

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

Answer: C

NEW QUESTION 520
- (Exam Topic 11)
While inventorying storage equipment, it is found that there are unlabeled, disconnected, and powered off devices. Which of the following is the correct procedure for handling such equipment?

A. They should be recycled to save energy.
B. They should be recycled according to NIST SP 800-88.
C. They should be inspected and sanitized following the organizational policy.
D. They should be inspected and categorized properly to sell them for reuse.

Answer: C

NEW QUESTION 525
- (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 529
- (Exam Topic 11)
Which of the following secures web transactions at the Transport Layer?

A. Secure HyperText Transfer Protocol (S-HTTP)
B. Secure Sockets Layer (SSL)
C. Socket Security (SOCKS)
D. Secure Shell (SSH)

Answer: B

NEW QUESTION 533
- (Exam Topic 11)
The 802.1x standard provides a framework for what?

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

Answer: B

NEW QUESTION 535
- (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
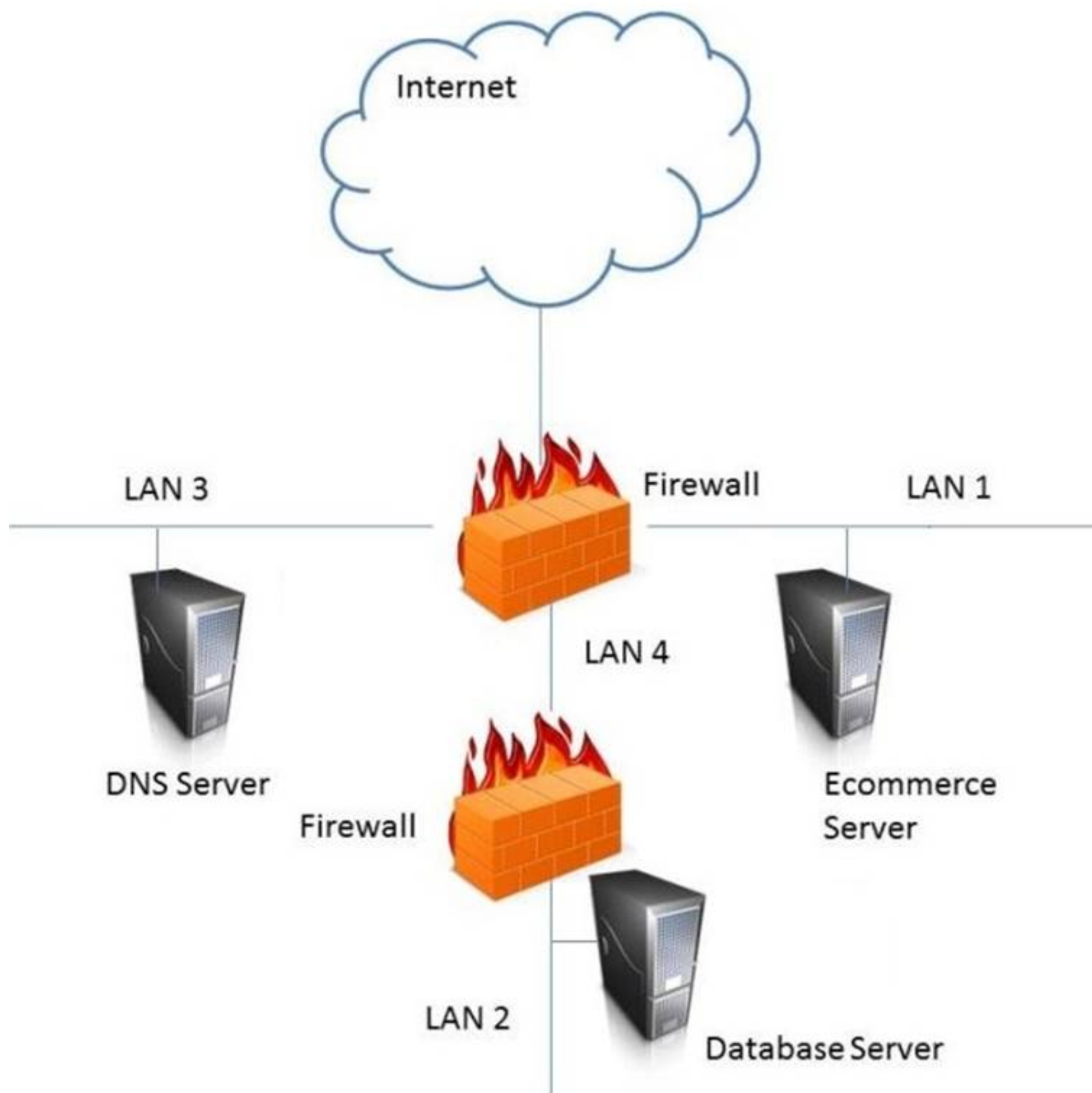B. Reporting
C. Recovery
D. Remediation

Answer: A

NEW QUESTION 540
- (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 545
- (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 547
- (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 548
- (Exam Topic 11)
Which of the following is the PRIMARY benefit of implementing data-in-use controls?

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

Answer: C

NEW QUESTION 549
- (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 553
- (Exam Topic 11)
In order for a security policy to be effective within an organization, it MUST include

A. strong statements that clearly define the problem.
B. a list of all standards that apply to the policy.
C. owner information and date of last revision.
D. disciplinary measures for non compliance.

Answer: D

NEW QUESTION 557
- (Exam Topic 11)
The BEST method to mitigate the risk of a dictionary attack on a system is to

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

Answer: A

NEW QUESTION 561
- (Exam Topic 11)
The MAIN reason an organization conducts a security authorization process is to

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

Answer: A

NEW QUESTION 563
- (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 566
- (Exam Topic 12)
Which of the following is the BEST method to reduce the effectiveness of phishing attacks?

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

Answer: A

NEW QUESTION 571
- (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 574
- (Exam Topic 12)
Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

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

Answer: A

NEW QUESTION 577
- (Exam Topic 12)
Which Radio Frequency Interference (RFI) phenomenon associated with bundled cable runs can create information leakage?

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

Answer: D

NEW QUESTION 582
- (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 583
- (Exam Topic 12)
Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

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

Answer: B

NEW QUESTION 584
- (Exam Topic 12)
The PRIMARY outcome of a certification process is that it provides documented

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

Answer: D

NEW QUESTION 586

- (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 587
- (Exam Topic 12)
Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item?

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

Answer: D

NEW QUESTION 589
- (Exam Topic 12)
Which of the following is an advantage of on-premise Credential Management Systems?

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

Answer: B

NEW QUESTION 591
- (Exam Topic 12)
What does the Maximum Tolerable Downtime (MTD) determine?

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

Answer: C

NEW QUESTION 593
- (Exam Topic 12)
Which of the following media sanitization techniques is MOST likely to be effective for an organization using public cloud services?

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

Answer: B

NEW QUESTION 594
- (Exam Topic 12)
Match the access control type to the example of the control type. Drag each access control type net to its corresponding example.

Access Control Type		Example
Administrative		Labeling of sensitive data
Technical		Biometrics for authentication
Logical		Constrained user interface
Physical		Radio Frequency Identification (RFID) badge

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Administrative – labeling of sensitive data Technical – Constrained user interface Logical – Biometrics for authentication Physical – Radio Frequency Identification 9RFID) badge

NEW QUESTION 599
- (Exam Topic 12)
Which of the following BEST describes a chosen plaintext attack?

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

Answer: A

NEW QUESTION 604
- (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 607
- (Exam Topic 12)
In general, servers that are facing the Internet should be placed in a demilitarized zone (DMZ). What is MAIN purpose of the DMZ?

A. Reduced risk to internal systems.
B. Prepare the server for potential attacks.
C. Mitigate the risk associated with the exposed server.
D. Bypass the need for a firewall.

Answer: A

NEW QUESTION 612
- (Exam Topic 12)
Although code using a specific program language may not be susceptible to a buffer overflow attack,

A. most calls to plug-in programs are susceptible.
B. most supporting application code is susceptible.
C. the graphical images used by the application could be susceptible.
D. the supporting virtual machine could be susceptible.

Answer: C

NEW QUESTION 616
- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 617
- (Exam Topic 12)
An employee of a retail company has been granted an extended leave of absence by Human Resources (HR). This information has been formally communicated to the access provisioning team. Which of the following is the BEST action to take?

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

Answer: D

NEW QUESTION 622
- (Exam Topic 12)
Which of the following BEST represents the concept of least privilege?

A. Access to an object is denied unless access is specifically allowed.
B. Access to an object is only available to the owner.
C. Access to an object is allowed unless it is protected by the information security policy.
D. Access to an object is only allowed to authenticated users via an Access Control List (ACL).

Answer: A

NEW QUESTION 624
- (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 629
- (Exam Topic 12)
Which one of the following activities would present a significant security risk to organizations when employing a Virtual Private Network (VPN) solution?

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

Answer: B

NEW QUESTION 632
- (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 637
- (Exam Topic 12)
An organization's information security strategic plan MUST be reviewed

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

Answer: C

NEW QUESTION 639
- (Exam Topic 12)
Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

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

Answer: A

NEW QUESTION 641
- (Exam Topic 12)
A security architect plans to reference a Mandatory Access Control (MAC) model for implementation. This indicates that which of the following properties are being prioritized?

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

Answer: C

NEW QUESTION 646
- (Exam Topic 12)
In order to assure authenticity, which of the following are required?

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

Answer: D

NEW QUESTION 647
- (Exam Topic 12)
The goal of a Business Impact Analysis (BIA) is to determine which of the following?

A. Cost effectiveness of business recovery
B. Cost effectiveness of installing software security patches
C. Resource priorities for recovery and Maximum Tolerable Downtime (MTD)
D. Which security measures should be implemented

Answer: C

NEW QUESTION 648
- (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 653
- (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 655
- (Exam Topic 12)
A user sends an e-mail request asking for read-only access to files that are not considered sensitive. A Discretionary Access Control (DAC) methodology is in place. Which is the MOST suitable approach that the administrator should take?

A. Administrator should request data owner approval to the user access
B. Administrator should request manager approval for the user access
C. Administrator should directly grant the access to the non-sensitive files
D. Administrator should assess the user access need and either grant or deny the access

Answer: A

NEW QUESTION 656
- (Exam Topic 12)
Reciprocal backup site agreements are considered to be

A. a better alternative than the use of warm sites.
B. difficult to test for complex systems.
C. easy to implement for similar types of organizations.
D. easy to test and implement for complex systems.

Answer: B

NEW QUESTION 659
- (Exam Topic 12)
Backup information that is critical to the organization is identified through a

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

Answer: D

NEW QUESTION 660
- (Exam Topic 12)
What is the MOST important element when considering the effectiveness of a training program for Business Continuity (BC) and Disaster Recovery (DR)?

A. Management support
B. Consideration of organizational need
C. Technology used for delivery
D. Target audience

Answer: B

NEW QUESTION 664
- (Exam Topic 12)
In which identity management process is the subject's identity established?

A. Trust
B. Provisioning
C. Authorization
D. Enrollment

Answer: D

NEW QUESTION 665
- (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 670
- (Exam Topic 13)
Which one of the following data integrity models assumes a lattice of integrity levels?

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

Answer: B

NEW QUESTION 675
- (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 676
- (Exam Topic 13)
Which of the following is the MOST effective practice in managing user accounts when an employee is terminated?

A. Implement processes for automated removal of access for terminated employees.
B. Delete employee network and system IDs upon termination.
C. Manually remove terminated employee user-access to all systems and applications.
D. Disable terminated employee network ID to remove all access.

Answer: B

NEW QUESTION 678
- (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 680
- (Exam Topic 13)
Why is planning in Disaster Recovery (DR) an interactive process?

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

Answer: B

NEW QUESTION 683
- (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 688
- (Exam Topic 13)
From a security perspective, which of the following assumptions MUST be made about input to an
application?

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

Answer: D

NEW QUESTION 690
- (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 692
- (Exam Topic 13)
As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

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

Answer: D

NEW QUESTION 695
- (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 700
- (Exam Topic 13)
An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject's data?

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

Answer: C

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 704
- (Exam Topic 13)
Which of the following are important criteria when designing procedures and acceptance criteria for acquired software?

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

Answer: A

NEW QUESTION 705
- (Exam Topic 13)
Which of the following is the MOST common method of memory protection?

A. Compartmentalization
B. Segmentation
C. Error correction
D. Virtual Local Area Network (VLAN) tagging

Answer: B

NEW QUESTION 706
- (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 709
- (Exam Topic 13)

Which of the following combinations would MOST negatively affect availability?

A. Denial of Service (DoS) attacks and outdated hardware
B. Unauthorized transactions and outdated hardware
C. Fire and accidental changes to data
D. Unauthorized transactions and denial of service attacks

Answer: A

NEW QUESTION 711
- (Exam Topic 13)
A Denial of Service (DoS) attack on a syslog server exploits weakness in which of the following protocols?

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

Answer: B

NEW QUESTION 716
- (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 721
- (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 726
- (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 728
- (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 731
- (Exam Topic 13)
Which of the following is a characteristic of an internal audit?

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

Answer: D

NEW QUESTION 735
- (Exam Topic 13)
An organization has outsourced its financial transaction processing to a Cloud Service Provider (CSP) who will provide them with Software as a Service (SaaS). If there was a data breach who is responsible for monetary losses?

A. The Data Protection Authority (DPA)
B. The Cloud Service Provider (CSP)
C. The application developers
D. The data owner

Answer: B

NEW QUESTION 740
- (Exam Topic 13)
What is the MAIN purpose of a change management policy?

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

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 742
- (Exam Topic 13)
What can happen when an Intrusion Detection System (IDS) is installed inside a firewall-protected internal network?

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

Answer: A

NEW QUESTION 747
- (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 751
- (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 756
- (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 757
- (Exam Topic 13)
Match the functional roles in an external audit to their responsibilities. Drag each role on the left to its corresponding responsibility on the right. Select and Place:

Role		Responsibility
Executive management		Approve audit budget and resource allocation.
Audit committee		Provide audit oversight.
Compliance officer		Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor		Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Role		Responsibility
Executive management	Executive management	Approve audit budget and resource allocation.
Audit committee	Audit committee	Provide audit oversight.
Compliance officer	External auditor	Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor	Compliance officer	Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

NEW QUESTION 762
- (Exam Topic 13)
Which of the following would an attacker BEST be able to accomplish through the use of Remote Access
Tools (RAT)?

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

Answer: D

NEW QUESTION 765
- (Exam Topic 13)
In a change-controlled environment, which of the following is MOST likely to lead to unauthorized changes to production programs?

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

Answer: B

NEW QUESTION 766
- (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. Diffle-Hellman (DH) algorithm
B. Elliptic Curve Cryptography (ECC) algorithm
C. Digital Signature algorithm (DSA)
D. Rivest-Shamir-Adleman (RSA) algorithm

Answer: A

NEW QUESTION 767
- (Exam Topic 13)
Within the company, desktop clients receive Internet Protocol (IP) address over Dynamic Host Configuration Protocol (DHCP).
Which of the following represents a valid measure to help protect the network against unauthorized access?

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

Answer: B

NEW QUESTION 768
- (Exam Topic 13)
What is the second step in the identity and access provisioning lifecycle?

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

Answer: B

NEW QUESTION 772
- (Exam Topic 13)
Which of the following is MOST appropriate for protecting confidentially 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 773
- (Exam Topic 13)
Transport Layer Security (TLS) provides which of the following capabilities for a remote access server?

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

Answer: C

NEW QUESTION 774
- (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 776
- (Exam Topic 13)
What MUST each information owner do when a system contains data from multiple information owners?

A. Provide input to the Information System (IS) owner regarding the security requirements of the data
B. Review the Security Assessment report (SAR) for the Information System (IS) and authorize the IS to operate.
C. Develop and maintain the System Security Plan (SSP) for the Information System (IS) containing the data
D. Move the data to an Information System (IS) that does not contain data owned by other information owners

Answer: C

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 779
- (Exam Topic 13)
A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report.

In which phase of the assessment was this error MOST likely made?

A. Enumeration
B. Reporting
C. Detection
D. Discovery

Answer: A

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 782
- (Exam Topic 13)
After following the processes defined within the change management plan, a super user has upgraded a device within an Information system.
What step would be taken to ensure that the upgrade did NOT affect the network security posture?

A. Conduct an Assessment and Authorization (A&A)
B. Conduct a security impact analysis
C. Review the results of the most recent vulnerability scan
D. Conduct a gap analysis with the baseline configuration

Answer: B

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 783
- (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 784
- (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 785
- (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 787
- (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 791

- (Exam Topic 13)
Which of the following is the MOST appropriate action when reusing media that contains sensitive data?

A. Erase
B. Sanitize
C. Encrypt
D. Degauss

Answer: B

NEW QUESTION 794
- (Exam Topic 13)
A user has infected a computer with malware by connecting a Universal Serial Bus (USB) storage device. Which of the following is MOST effective to mitigate future infections?

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

Answer: C

NEW QUESTION 795
- (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 799
- (Exam Topic 13)
Which of the following is the GREATEST benefit of implementing a Role Based Access Control (RBAC)
system?

A. Integration using Lightweight Directory Access Protocol (LDAP)
B. Form-based user registration process
C. Integration with the organizations Human Resources (HR) system
D. A considerably simpler provisioning process

Answer: D

NEW QUESTION 802
- (Exam Topic 13)
What is the correct order of steps in an information security assessment?
Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.

Actions

| Define the perimeter. |
| Identify the vulnerability. |
| Assess the risk. |
| Determine the actions. |

Steps

	Step 1
	Step 2
	Step 3
	Step 4

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

| Define the perimeter. |
| Identify the vulnerability. |
| Assess the risk. |
| Determine the actions. |

Steps

Identify the vulnerability.	Step 1
Define the perimeter.	Step 2
Assess the risk.	Step 3
Determine the actions.	Step 4

NEW QUESTION 806
- (Exam Topic 13)
In a High Availability (HA) environment, what is the PRIMARY goal of working with a virtual router address as the gateway to a network?

A. The second of two routers can periodically check in to make sure that the first router is operational.
B. The second of two routers can better absorb a Denial of Service (DoS) attack knowing the first router is present.
C. The first of two routers fails and is reinstalled, while the second handles the traffic flawlessly.
D. The first of two routers can better handle specific traffic, while the second handles the rest of the traffic seamlessly.

Answer: C

NEW QUESTION 811
- (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 814
- (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 818
- (Exam Topic 13)
Which of the following is BEST achieved through the use of eXtensible Access Markup Language (XACML)?

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

Answer: D

NEW QUESTION 823
......

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

    All transactions are protected by VeriSign!

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

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