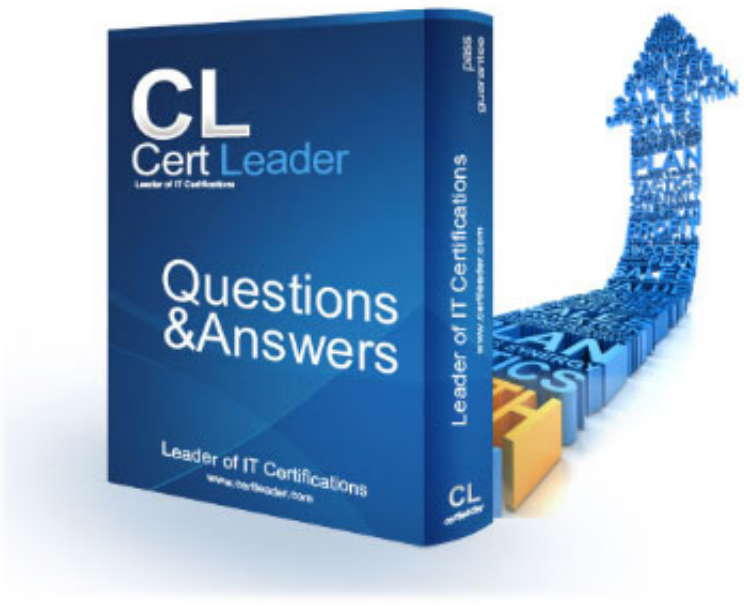
CISSP Dumps

Certified Information Systems Security Professional (CISSP)

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



NEW QUESTION 1
- (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 2
- (Exam Topic 1)
All of the following items should be included in a Business Impact Analysis (BIA) questionnaire EXCEPT questions that

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

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
Which of the following actions will reduce risk to a laptop before traveling to a high risk area?

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

Answer: D

NEW QUESTION 4
- (Exam Topic 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 5
- (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 6
- (Exam Topic 3)
Which security service is served by the process of encryption plaintext with the sender’s private key and decrypting cipher text with the sender’s public key?

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

Answer: A

NEW QUESTION 7
- (Exam Topic 3)
Which component of the Security Content Automation Protocol (SCAP) specification contains the data required to estimate the severity of vulnerabilities identified automated vulnerability assessments?

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

Answer: B

NEW QUESTION 8
- (Exam Topic 3)
The use of private and public encryption keys is fundamental in the implementation of which of the following?

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

Answer: A

NEW QUESTION 9
- (Exam Topic 3)
Who in the organization is accountable for classification of data information assets?

A. Data owner
B. Data architect
C. Chief Information Security Officer (CISO)
D. Chief Information Officer (CIO)

Answer: A

NEW QUESTION 10
- (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 10
- (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 11
- (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 16
- (Exam Topic 4)
Which of the following is the BEST network defense against unknown types of attacks or stealth attacks in progress?

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

Answer: D

NEW QUESTION 21
- (Exam Topic 4)
Which of the following factors contributes to the weakness of Wired Equivalent Privacy (WEP) protocol?

A. WEP uses a small range Initialization Vector (IV)

B. WEP uses Message Digest 5 (MD5)
C. WEP uses Diffie-Hellman
D. WEP does not use any Initialization Vector (IV)

Answer: A

NEW QUESTION 23
- (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 26
- (Exam Topic 5)
Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee's salary?

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

Answer: C

NEW QUESTION 27
- (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 28
- (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 33
- (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 34
- (Exam Topic 6)
In which of the following programs is it MOST important to include the collection of security process data?

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

Answer: A

NEW QUESTION 37

- (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 38
- (Exam Topic 7)
A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?

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

Answer: D

NEW QUESTION 39
- (Exam Topic 7)
Which of the following types of business continuity tests includes assessment of resilience to internal and external risks without endangering live operations?

A. Walkthrough
B. Simulation
C. Parallel
D. White box

Answer: B

NEW QUESTION 43
- (Exam Topic 7)
When is a Business Continuity Plan (BCP) considered to be valid?

A. When it has been validated by the Business Continuity (BC) manager
B. When it has been validated by the board of directors
C. When it has been validated by all threat scenarios
D. When it has been validated by realistic exercises

Answer: D

NEW QUESTION 45
- (Exam Topic 7)
What should be the FIRST action to protect the chain of evidence when a desktop computer is involved?

A. Take the computer to a forensic lab
B. Make a copy of the hard drive
C. Start documenting
D. Turn off the computer

Answer: C

NEW QUESTION 49
- (Exam Topic 7)
Which of the following is the FIRST step in the incident response process?

A. Determine the cause of the incident
B. Disconnect the system involved from the network
C. Isolate and contain the system involved
D. Investigate all symptoms to confirm the incident

Answer: D

NEW QUESTION 51
- (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 55
- (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 58
- (Exam Topic 8)
Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

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

Answer: D

NEW QUESTION 61
- (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 64
- (Exam Topic 9)
What is the FIRST step in developing a security test and its evaluation?

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

Answer: C

NEW QUESTION 68
- (Exam Topic 9)
Which of the following is a method used to prevent Structured Query Language (SQL) injection attacks?

A. Data compression
B. Data classification
C. Data warehousing
D. Data validation

Answer: D

NEW QUESTION 69
- (Exam Topic 9)
Logical access control programs are MOST effective when they are

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

Answer: D

NEW QUESTION 73
- (Exam Topic 9)
Which of the following is a limitation of the Common Vulnerability Scoring System (CVSS) as it relates to conducting code review?

A. It has normalized severity ratings.
B. It has many worksheets and practices to implement.

C. It aims to calculate the risk of published vulnerabilities.
D. It requires a robust risk management framework to be put in place.

Answer: C

NEW QUESTION 78
- (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 83
- (Exam Topic 9)
Contingency plan exercises are intended to do which of the following?

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

Answer: A

NEW QUESTION 85
- (Exam Topic 9)
In the area of disaster planning and recovery, what strategy entails the presentation of information about the plan?

A. Communication
B. Planning
C. Recovery
D. Escalation

Answer: A

NEW QUESTION 87
- (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 89
- (Exam Topic 9)
The key benefits of a signed and encrypted e-mail include

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

Answer: B

NEW QUESTION 93
- (Exam Topic 9)
Which one of the following transmission media is MOST effective in preventing data interception?

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

Answer: C

NEW QUESTION 98
- (Exam Topic 9)
Which layer of the Open Systems Interconnections (OSI) model implementation adds information concerning the logical connection between the sender and

receiver?

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

Answer: C

NEW QUESTION 103
- (Exam Topic 9)
The overall goal of a penetration test is to determine a system's

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

Answer: A

NEW QUESTION 108
- (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 110
- (Exam Topic 9)
The Structured Query Language (SQL) implements Discretionary Access Controls (DAC) using

A. INSERT and DELETE.
B. GRANT and REVOKE.
C. PUBLIC and PRIVATE.
D. ROLLBACK and TERMINATE.

Answer: B

NEW QUESTION 112
- (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 116
- (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 119
- (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 124

- (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 128
- (Exam Topic 9)
Which of the following is an attacker MOST likely to target to gain privileged access to a system?

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

Answer: A

NEW QUESTION 131
- (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 136
- (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 137
- (Exam Topic 9)
How can a forensic specialist exclude from examination a large percentage of operating system files residing on a copy of the target system?

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

Answer: B

NEW QUESTION 141
- (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 143
- (Exam Topic 9)
In a financial institution, who has the responsibility for assigning the classification to a piece of information?

A. Chief Financial Officer (CFO)
B. Chief Information Security Officer (CISO)
C. Originator or nominated owner of the information
D. Department head responsible for ensuring the protection of the information

Answer: C

NEW QUESTION 146
- (Exam Topic 9)
Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

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

Answer: C

NEW QUESTION 149
- (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 150
- (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 151
- (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 152
- (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 153
- (Exam Topic 9)
Which of the following is the MAIN reason that system re-certification and re-accreditation are needed?

A. To assist data owners in making future sensitivity and criticality determinations
B. To assure the software development team that all security issues have been addressed
C. To verify that security protection remains acceptable to the organizational security policy
D. To help the security team accept or reject new systems for implementation and production

Answer: C

NEW QUESTION 155
- (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 160
- (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 162
- (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 165
- (Exam Topic 9)
In Business Continuity Planning (BCP), what is the importance of documenting business processes?

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

Answer: D

NEW QUESTION 169
- (Exam Topic 9)
Which of the following can BEST prevent security flaws occurring in outsourced software development?

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

Answer: C

NEW QUESTION 170
- (Exam Topic 9)
The Hardware Abstraction Layer (HAL) is implemented in the

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

Answer: A

NEW QUESTION 174
- (Exam Topic 9)
The birthday attack is MOST effective against which one of the following cipher technologies?

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

Answer: C

NEW QUESTION 177
- (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 182
- (Exam Topic 9)
Which of the following elements MUST a compliant EU-US Safe Harbor Privacy Policy contain?

A. An Explanation: of how long the data subject's collected information will be retained for and how it will be eventually disposed.
B. An Explanation: of who can be contacted at the organization collecting the information if corrections are required by the data subject.
C. An Explanation: of the regulatory frameworks and compliance standards the information collecting organization adheres to.
D. An Explanation: of all the technologies employed by the collecting organization in gathering information on the data subject.

Answer: B

NEW QUESTION 186
- (Exam Topic 9)
In a basic SYN flood attack, what is the attacker attempting to achieve?

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

Answer: A

NEW QUESTION 190
- (Exam Topic 9)
Which of the following is a network intrusion detection technique?

A. Statistical anomaly
B. Perimeter intrusion
C. Port scanning
D. Network spoofing

Answer: A

NEW QUESTION 193
- (Exam Topic 9)
What is the ultimate objective of information classification?

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

Answer: B

NEW QUESTION 195
- (Exam Topic 9)
Following the completion of a network security assessment, which of the following can BEST be demonstrated?

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

Answer: A

NEW QUESTION 198
- (Exam Topic 9)
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 203
- (Exam Topic 9)
Which of the following defines the key exchange for Internet Protocol Security (IPSec)?

A. Secure Sockets Layer (SSL) key exchange

B. Internet Key Exchange (IKE)
C. Security Key Exchange (SKE)
D. Internet Control Message Protocol (ICMP)

Answer: B

NEW QUESTION 208
- (Exam Topic 9)
Why MUST a Kerberos server be well protected from unauthorized access?

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

Answer: A

NEW QUESTION 211
- (Exam Topic 9)
What maintenance activity is responsible for defining, implementing, and testing updates to application systems?

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

Answer: A

NEW QUESTION 213
- (Exam Topic 9)
A software scanner identifies a region within a binary image having high entropy. What does this MOST likely indicate?

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

Answer: C

NEW QUESTION 218
- (Exam Topic 9)
Which of the following actions should be performed when implementing a change to a database schema in a production system?

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

Answer: D

NEW QUESTION 223
- (Exam Topic 9)
Who must approve modifications to an organization's production infrastructure configuration?

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

Answer: B

NEW QUESTION 227
- (Exam Topic 9)
What is the MOST important purpose of testing the Disaster Recovery Plan (DRP)?

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

Answer: C

NEW QUESTION 230
- (Exam Topic 9)
Which of the following is a potential risk when a program runs in privileged mode?

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

Answer: D

NEW QUESTION 233
- (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 234
- (Exam Topic 9)
What is the MOST effective countermeasure to a malicious code attack against a mobile system?

A. Sandbox
B. Change control
C. Memory management
D. Public-Key Infrastructure (PKI)

Answer: A

NEW QUESTION 237
- (Exam Topic 9)
Which one of the following affects the classification of data?

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

Answer: A

NEW QUESTION 238
- (Exam Topic 9)
A system has been scanned for vulnerabilities and has been found to contain a number of communication ports that have been opened without authority. To which of the following might this system have been subjected?

A. Trojan horse
B. Denial of Service (DoS)
C. Spoofing
D. Man-in-the-Middle (MITM)

Answer: A

NEW QUESTION 243
- (Exam Topic 9)
The goal of software assurance in application development is to

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

Answer: C

NEW QUESTION 248
- (Exam Topic 9)
An engineer in a software company has created a virus creation tool. The tool can generate thousands of polymorphic viruses. The engineer is planning to use the tool in a controlled environment to test the company's next generation virus scanning software. Which would BEST describe the behavior of the engineer and why?

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

Answer: A

NEW QUESTION 252

- (Exam Topic 9)
Which of the following Disaster Recovery (DR) sites is the MOST difficult to test?

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

Answer: B

NEW QUESTION 253
- (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 257
- (Exam Topic 9)
What should be the INITIAL response to Intrusion Detection System/Intrusion Prevention System (IDS/IPS) alerts?

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

Answer: D

NEW QUESTION 258
- (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 261
- (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 264
- (Exam Topic 10)
What is the MAIN feature that onion routing networks offer?

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

Answer: C

NEW QUESTION 266
- (Exam Topic 10)
Which of the following violates identity and access management best practices?

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

Answer: C

NEW QUESTION 269
- (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 272
- (Exam Topic 10)
Which of the following is the BEST reason to review audit logs periodically?

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

Answer: C

NEW QUESTION 276
- (Exam Topic 10)
Which of the following provides effective management assurance for a Wireless Local Area Network (WLAN)?

A. Maintaining an inventory of authorized Access Points (AP) and connecting devices
B. Setting the radio frequency to the minimum range required
C. Establishing a Virtual Private Network (VPN) tunnel between the WLAN client device and a VPN concentrator
D. Verifying that all default passwords have been changed

Answer: A

NEW QUESTION 280
- (Exam Topic 10)
According to best practice, which of the following groups is the MOST effective in performing an information security compliance audit?

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

Answer: D

NEW QUESTION 285
- (Exam Topic 10)
During an investigation of database theft from an organization's web site, it was determined that the Structured Query Language (SQL) injection technique was used despite input validation with client-side scripting. Which of the following provides the GREATEST protection against the same attack occurring again?

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

Answer: C

NEW QUESTION 288
- (Exam Topic 10)
What physical characteristic does a retinal scan biometric device measure?

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

Answer: C

NEW QUESTION 292
- (Exam Topic 10)
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 293
- (Exam Topic 10)
If an attacker in a SYN flood attack uses someone else's valid host address as the source address, the system under attack will send a large number of Synchronize/Acknowledge (SYN/ACK) packets to the

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

Answer: D

NEW QUESTION 298
- (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 303
- (Exam Topic 10)
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
If it is discovered that large quantities of information have been copied by the unauthorized individual, what attribute of the data has been compromised?

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

Answer: D

NEW QUESTION 307
- (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.
In addition to web browsers, what PRIMARY areas need to be addressed concerning mobile code used for malicious purposes?

A. Text editors, database, and Internet phone applications
B. Email, presentation, and database applications
C. Image libraries, presentation and spreadsheet applications
D. Email, media players, and instant messaging applications

Answer: D

NEW QUESTION 312
- (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 314
- (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 319
- (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 MUST the plan include in order to reduce client-side exploitation?

A. Approved web browsers
B. Network firewall procedures
C. Proxy configuration
D. Employee education

Answer: D

NEW QUESTION 324
- (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 327
- (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 329
- (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 331
- (Exam Topic 10)
What is the BEST first step for determining if the appropriate security controls are in place for protecting data at rest?

A. Identify regulatory requirements
B. Conduct a risk assessment
C. Determine business drivers
D. Review the security baseline configuration

Answer: B

NEW QUESTION 336
- (Exam Topic 10)
A business has implemented Payment Card Industry Data Security Standard (PCI-DSS) compliant handheld credit card processing on their Wireless Local Area Network (WLAN) topology. The network team partitioned the WLAN to create a private segment for credit card processing using a firewall to control device access and route traffic to the card processor on the Internet. What components are in the scope of PCI-DSS?

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

Answer: C

NEW QUESTION 338
- (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 341
- (Exam Topic 10)
Which of the following is a detective access control mechanism?

A. Log review
B. Least privilege
C. Password complexity
D. Non-disclosure agreement

Answer: A

NEW QUESTION 344
- (Exam Topic 10)
Which of the following is the MOST effective attack against cryptographic hardware modules?

A. Plaintext
B. Brute force
C. Power analysis
D. Man-in-the-middle (MITM)

Answer: C

NEW QUESTION 345
- (Exam Topic 10)
Which of the following is a BEST practice when traveling internationally with laptops containing Personally Identifiable Information (PII)?

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

Answer: B

NEW QUESTION 346
- (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 350

- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Which of the following is considered the MOST important priority for the information security officer?

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

Answer: A

NEW QUESTION 355
- (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 357
- (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 359
- (Exam Topic 10)
Which of the following problems is not addressed by using OAuth (Open Standard to Authorization) 2.0 to integrate a third-party identity provider for a service?

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

Answer: C

NEW QUESTION 362
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
Following best practice, where should the permitted access for each department and job classification combination be specified?

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

Answer: B

NEW QUESTION 366
- (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 368
- (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 370
- (Exam Topic 10)
Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following methods is the MOST effective way of removing the Peer-to-Peer (P2P) program from the computer?

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

Answer: B

NEW QUESTION 375
- (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 378
- (Exam Topic 10)
Place the following information classification steps in sequential order.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 383
- (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 388

- (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 391
- (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.

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 396
- (Exam Topic 10)
Refer to the information below to answer the question.
Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.
After magnetic drives were degaussed twice according to the product manufacturer's directions, what is the MOST LIKELY security issue with degaussing?

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

Answer: B

NEW QUESTION 400
- (Exam Topic 10)
For a service provider, which of the following MOST effectively addresses confidentiality concerns for customers using cloud computing?

A. Hash functions
B. Data segregation
C. File system permissions
D. Non-repudiation controls

Answer: B

NEW QUESTION 403
- (Exam Topic 10)
Which of the following secure startup mechanisms are PRIMARILY designed to thwart attacks?

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

Answer: B

NEW QUESTION 407
- (Exam Topic 10)
From a security perspective, which of the following is a best practice to configure a Domain Name Service (DNS) system?

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

Answer: D

NEW QUESTION 411
- (Exam Topic 10)
Which of the following is the BEST way to determine if a particular system is able to identify malicious software without executing it?

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

Answer: B

NEW QUESTION 416
- (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 419
- (Exam Topic 10)
An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a PRIMARY security concern?

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

Answer: C

NEW QUESTION 423
- (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 424
- (Exam Topic 10)
Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
What additional considerations are there if the third party is located in a different country?

A. The organizational structure of the third party and how it may impact timelines within the organization
B. The ability of the third party to respond to the organization in a timely manner and with accurate information
C. The effects of transborder data flows and customer expectations regarding the storage or processing of their data
D. The quantity of data that must be provided to the third party and how it is to be used

Answer: C

NEW QUESTION 427
- (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 430
- (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 431
- (Exam Topic 11)
Which of the following BEST describes the purpose of performing security certification?

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

Answer: B

NEW QUESTION 433
- (Exam Topic 11)
The application of which of the following standards would BEST reduce the potential for data breaches?

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

Answer: D

NEW QUESTION 435
- (Exam Topic 11)
A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

A. Public Key Infrastructure (PKI) and digital signatures
B. Trusted server certificates and passphrases
C. User ID and password
D. Asymmetric encryption and User ID

Answer: A

NEW QUESTION 436
- (Exam Topic 11)
Which of the following is generally indicative of a replay attack when dealing with biometric authentication?

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

Answer: D

NEW QUESTION 440

- (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 445
- (Exam Topic 11)
What is the GREATEST challenge to identifying data leaks?

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

Answer: B

NEW QUESTION 450
- (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 454
- (Exam Topic 11)
Which of the following is the BEST approach to take in order to effectively incorporate the concepts of business continuity into the organization?

A. Ensure end users are aware of the planning activities
B. Validate all regulatory requirements are known and fully documented
C. Develop training and awareness programs that involve all stakeholders
D. Ensure plans do not violate the organization's cultural objectives and goals

Answer: C

NEW QUESTION 458
- (Exam Topic 11)
Which of the following is the MOST important element of change management documentation?

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

Answer: C

NEW QUESTION 460
- (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 461
- (Exam Topic 11)
A mobile device application that restricts the storage of user information to just that which is needed to accomplish lawful business goals adheres to what privacy principle?

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

Answer: B

NEW QUESTION 465
- (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 467
- (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 470
- (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 472
- (Exam Topic 11)
Which of the following types of security testing is the MOST effective in providing a better indication of the everyday security challenges of an organization when performing a security risk assessment?

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

Answer: D

NEW QUESTION 476
- (Exam Topic 11)
Which of the following 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 481
- (Exam Topic 11)
Which of the following entities is ultimately accountable for data remanence vulnerabilities with data replicated by a cloud service provider?

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

Answer: A

NEW QUESTION 486
- (Exam Topic 11)
What is an important characteristic of Role Based Access Control (RBAC)?

A. Supports Mandatory Access Control (MAC)
B. Simplifies the management of access rights

C. Relies on rotation of duties
D. Requires two factor authentication

Answer: B

NEW QUESTION 490
- (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 493
- (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 497
- (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 501
- (Exam Topic 11)
Which of the following roles has the obligation to ensure that a third party provider is capable of processing and handling data in a secure manner and meeting the standards set by the organization?

A. Data Custodian
B. Data Owner
C. Data Creator
D. Data User

Answer: B

NEW QUESTION 503
- (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 508
- (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 511
- (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 512
- (Exam Topic 11)
Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

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

Answer: B

NEW QUESTION 514
- (Exam Topic 11)
The World Trade Organization's (WTO) agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires authors of computer software to be given the

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

Answer: A

NEW QUESTION 519
- (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 523
- (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 526
- (Exam Topic 11)
To protect auditable information, which of the following MUST be configured to only allow read access?

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

Answer: B

NEW QUESTION 530
- (Exam Topic 11)
Which of the following is the BEST example of weak management commitment to the protection of security assets and resources?

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

Answer: A

NEW QUESTION 534

- (Exam Topic 11)
Which of the following explains why record destruction requirements are included in a data retention policy?

A. To comply with legal and business requirements
B. To save cost for storage and backup
C. To meet destruction guidelines
D. To validate data ownership

Answer: A

NEW QUESTION 539
- (Exam Topic 11)
The BEST example of the concept of "something that a user has" when providing an authorized user access to a computing system is

A. the user's hand geometry.
B. a credential stored in a token.
C. a passphrase.
D. the user's face.

Answer: B

NEW QUESTION 543
- (Exam Topic 11)
Which of the following is an essential step before performing Structured Query Language (SQL) penetration tests on a production system?

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

Answer: C

NEW QUESTION 544
- (Exam Topic 11)
Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 546
- (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 549
- (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 550
- (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 553
- (Exam Topic 11)
The implementation of which features of an identity management system reduces costs and administration overhead while improving audit and accountability?

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

Answer: C

NEW QUESTION 554
- (Exam Topic 11)
Drag the following Security Engineering terms on the left to the BEST definition on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 558
- (Exam Topic 11)
Which of the following is an advantage of on-premise Credential Management Systems?

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

Answer: B

NEW QUESTION 562

- (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 566
- (Exam Topic 11)
What is one way to mitigate the risk of security flaws in custom software?

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

Answer: B

NEW QUESTION 567
- (Exam Topic 11)
What does an organization FIRST review to assure compliance with privacy requirements?

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

Answer: C

NEW QUESTION 568
- (Exam Topic 11)
An organization has decided to contract with a cloud-based service provider to leverage their identity as a service offering. They will use Open Authentication (OAuth) 2.0 to authenticate external users to the organization's services.
As part of the authentication process, which of the following must the end user provide?

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

Answer: A

NEW QUESTION 569
- (Exam Topic 11)
Which of the following is the MOST effective method of mitigating data theft from an active user workstation?

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

Answer: D

NEW QUESTION 571
- (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 572
- (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 574
- (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 577
- (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 578
- (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 583
- (Exam Topic 11)
For an organization considering two-factor authentication for secure network access, which of the following is MOST secure?

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

Answer: D

NEW QUESTION 584
- (Exam Topic 11)
What is the GREATEST challenge of an agent-based patch management solution?

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

Answer: B

NEW QUESTION 589
- (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 594
- (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 597
- (Exam Topic 11)
A Simple Power Analysis (SPA) attack against a device directly observes which of the following?

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

Answer: B

NEW QUESTION 602
- (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 604
- (Exam Topic 11)
Are companies legally required to report all data breaches?

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

Answer: A

NEW QUESTION 608
- (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 613
- (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 615
- (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 619
- (Exam Topic 11)
In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 621
- (Exam Topic 12)
As a best practice, the Security Assessment Report (SAR) should include which of the following sections?

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

Answer: B

NEW QUESTION 622
- (Exam Topic 12)
Match the name of access control model with its associated restriction.
Drag each access control model to its appropriate restriction access on the right.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 623
- (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 625
- (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 630
- (Exam Topic 12)
A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

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

Answer: A

NEW QUESTION 631
- (Exam Topic 12)
Which of the following adds end-to-end security inside a Layer 2 Tunneling Protocol (L2TP) Internet Protocol Security (IPSec) connection?

A. Temporal Key Integrity Protocol (TKIP)
B. Secure Hash Algorithm (SHA)
C. Secure Shell (SSH)
D. Transport Layer Security (TLS)

Answer: B

NEW QUESTION 633
- (Exam Topic 12)
Which of the following is the MAIN reason for using configuration management?

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

Answer: D

NEW QUESTION 635
- (Exam Topic 12)
Which of the following sets of controls should allow an investigation if an attack is not blocked by preventive controls or detected by monitoring?

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

Answer: C

NEW QUESTION 639
- (Exam Topic 12)
Match the types of e-authentication tokens to their description.
Drag each e-authentication token on the left to its corresponding description on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Look-up secret token - A physical or electronic token that stores a set of secrets between the claimant and the credential service provider
Out-of-Band Token - A physical token that is uniquely addressable and can receive a verifier-selected secret for one-time use
Pre-registered Knowledge Token - A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process
Memorized Secret Token - A secret shared between the subscriber and credential service provider that is typically character strings

NEW QUESTION 644
- (Exam Topic 12)
What type of wireless network attack BEST describes an Electromagnetic Pulse (EMP) attack?

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

Answer: B

NEW QUESTION 647
- (Exam Topic 12)
Between which pair of Open System Interconnection (OSI) Reference Model layers are routers used as a communications device?

A. Transport and Session
B. Data-Link and Transport
C. Network and Session

D. Physical and Data-Link

Answer: B

NEW QUESTION 650
- (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.

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 654
- (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 659
- (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 663
- (Exam Topic 12)
Determining outage costs caused by a disaster can BEST be measured by the

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

Answer: C

NEW QUESTION 667
- (Exam Topic 12)
A database administrator is asked by a high-ranking member of management to perform specific changes to the accounting system database. The administrator is specifically instructed to not track or evidence the change in a ticket. Which of the following is the BEST course of action?

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

Answer: D

NEW QUESTION 672
- (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 677
- (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 678
- (Exam Topic 12)
What is the BEST way to encrypt web application communications?

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

Answer: D

NEW QUESTION 679
- (Exam Topic 12)
At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

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

Answer: C

NEW QUESTION 680
- (Exam Topic 12)
Which of the following is the PRIMARY benefit of a formalized information classification program?

A. It minimized system logging requirements.
B. It supports risk assessment.
C. It reduces asset vulnerabilities.

D. It drives audit processes.

Answer: B

NEW QUESTION 681
- (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 685
- (Exam Topic 12)
What is an advantage of Elliptic Curve Cryptography (ECC)?

A. Cryptographic approach that does not require a fixed-length key
B. Military-strength security that does not depend upon secrecy of the algorithm
C. Opportunity to use shorter keys for the same level of security
D. Ability to use much longer keys for greater security

Answer: C

NEW QUESTION 687
- (Exam Topic 12)
Which of the following is BEST suited for exchanging authentication and authorization messages in a multi-party decentralized environment?

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

Answer: B

NEW QUESTION 689
- (Exam Topic 12)
An organization regularly conducts its own penetration tests. Which of the following scenarios MUST be covered for the test to be effective?

A. Third-party vendor with access to the system
B. System administrator access compromised
C. Internal attacker with access to the system
D. Internal user accidentally accessing data

Answer: C

NEW QUESTION 690
- (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 694
- (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 695
- (Exam Topic 12)
An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a PRIMARY security concern?

A. Ownership

B. Confidentiality
C. Availability
D. Integrity

Answer: C

NEW QUESTION 696
- (Exam Topic 12)
In configuration management, what baseline configuration information MUST be maintained for each computer system?

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

Answer: A

NEW QUESTION 699
- (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 703
- (Exam Topic 12)
Which of the following are effective countermeasures against passive network-layer attacks?

A. Federated security and authenticated access controls
B. Trusted software development and run time integrity controls
C. Encryption and security enabled applications
D. Enclave boundary protection and computing environment defense

Answer: C

NEW QUESTION 708
- (Exam Topic 12)
From a cryptographic perspective, the service of non-repudiation includes which of the following features?

A. Validity of digital certificates
B. Validity of the authorization rules
C. Proof of authenticity of the message
D. Proof of integrity of the message

Answer: C

NEW QUESTION 712
- (Exam Topic 12)
When evaluating third-party applications, which of the following is the GREATEST responsibility of Information Security?

A. Accept the risk on behalf of the organization.
B. Report findings to the business to determine security gaps.
C. Quantify the risk to the business for product selection.
D. Approve the application that best meets security requirements.

Answer: C

NEW QUESTION 713
- (Exam Topic 12)
When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?

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

Answer: D

NEW QUESTION 718
- (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 720
- (Exam Topic 12)
During the Security Assessment and Authorization process, what is the PRIMARY purpose for conducting a hardware and software inventory?

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

Answer: A

NEW QUESTION 721
- (Exam Topic 12)
Which of the following countermeasures is the MOST effective in defending against a social engineering attack?

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

Answer: C

NEW QUESTION 725
- (Exam Topic 13)
Which of the following steps should be performed FIRST when purchasing Commercial Off-The-Shelf (COTS) software?

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

Answer: D

NEW QUESTION 727
- (Exam Topic 13)
A control to protect from a Denial-of-Service (DoS) attach has been determined to stop 50% of attacks, and additionally reduces the impact of an attack by 50%. What is the residual risk?

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

Answer: A

NEW QUESTION 732
- (Exam Topic 13)
Which one of the following is an advantage of an effective release control strategy form a configuration control standpoint?

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

Answer: C

NEW QUESTION 736
- (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 738

- (Exam Topic 13)
Due to system constraints, a group of system administrators must share a high-level access set of credentials. Which of the following would be MOST appropriate to implement?

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

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 743
- (Exam Topic 13)
Who is responsible for the protection of information when it is shared with or provided to other organizations?

A. Systems owner
B. Authorizing Official (AO)
C. Information owner
D. Security officer

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 746
- (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 751
- (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 756
- (Exam Topic 13)
What is the MAIN reason for testing a Disaster Recovery Plan (DRP)?

A. To ensure Information Technology (IT) staff knows and performs roles assigned to each of them
B. To validate backup sites' effectiveness
C. To find out what does not work and fix it
D. To create a high level DRP awareness among Information Technology (IT) staff

Answer: B

NEW QUESTION 759
- (Exam Topic 13)
What capability would typically be included in a commercially available software package designed for access control?

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

Answer: A

NEW QUESTION 760
- (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 761
- (Exam Topic 13)
Which security access policy contains fixed security attributes that are used by the system to determine a user's access to a file or object?

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

Answer: A

NEW QUESTION 766
- (Exam Topic 13)
Even though a particular digital watermark is difficult to detect, which of the following represents a way it might still be inadvertently removed?

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

Answer: A

NEW QUESTION 769
- (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 771
- (Exam Topic 13)
It is MOST important to perform which of the following to minimize potential impact when implementing a new vulnerability scanning tool in a production environment?

A. Negotiate schedule with the Information Technology (IT) operation's team
B. Log vulnerability summary reports to a secured server
C. Enable scanning during off-peak hours
D. Establish access for Information Technology (IT) management

Answer: A

Explanation:
Section: Security Operations

NEW QUESTION 775
- (Exam Topic 13)
Which of the following is the MOST efficient mechanism to account for all staff during a speedy nonemergency evacuation from a large security facility?

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

Answer: B

Explanation:
Section: Security Operations

NEW QUESTION 778
- (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 782
- (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 784
- (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 787
- (Exam Topic 13)
What are the steps of a risk assessment?

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

Answer: A

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 790
- (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 793
- (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 796
- (Exam Topic 13)
Match the name of access control model with its associated restriction.
Drag each access control model to its appropriate restriction access on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 801
- (Exam Topic 13)
The core component of Role Based Access Control (RBAC) must be constructed of defined data elements. Which elements are required?

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

Answer: C

NEW QUESTION 806
- (Exam Topic 13)
What is the PRIMARY goal of fault tolerance?

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

Answer: A

NEW QUESTION 808
- (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 810
- (Exam Topic 13)
Assessing a third party's risk by counting bugs in the code may not be the best measure of an attack surface within the supply chain.
Which of the following is LEAST associated with the attack surface?

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

Answer: C

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 811
- (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 815
- (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 816
- (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 821
- (Exam Topic 13)
What is the expected outcome of security awareness in support of a security awareness program?

A. Awareness activities should be used to focus on security concerns and respond to those concerns accordingly
B. Awareness is not an activity or part of the training but rather a state of persistence to support the program
C. Awareness is trainin
D. The purpose of awareness presentations is to broaden attention of security.
E. Awareness is not trainin
F. The purpose of awareness presentation is simply to focus attention on security.

Answer: C

NEW QUESTION 824
- (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 825
- (Exam Topic 13)
Which of the following entails identification of data and links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

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

Answer: B

NEW QUESTION 830
- (Exam Topic 13)
When developing a business case for updating a security program, the security program owner MUST do which of the following?

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

Answer: A

NEW QUESTION 832
- (Exam Topic 13)
What is the foundation of cryptographic functions?

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

Answer: A

NEW QUESTION 834
- (Exam Topic 13)
When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

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

Answer: D

NEW QUESTION 835
- (Exam Topic 13)
Which of the following is part of a Trusted Platform Module (TPM)?

A. A non-volatile tamper-resistant storage for storing both data and signing keys in a secure fashion
B. A protected Pre-Basic Input/Output System (BIOS) which specifies a method or a metric for “measuring”the state of a computing platform
C. A secure processor targeted at managing digital keys and accelerating digital signing
D. A platform-independent software interface for accessing computer functions

Answer: A

NEW QUESTION 837
- (Exam Topic 13)
Which of the following is a responsibility of a data steward?

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

Answer: A

NEW QUESTION 842
- (Exam Topic 13)
What does a Synchronous (SYN) flood attack do?

A. Forces Transmission Control Protocol /Internet Protocol (TCP/IP) connections into a reset state

B. Establishes many new Transmission Control Protocol / Internet Protocol (TCP/IP) connections
C. Empties the queue of pending Transmission Control Protocol /Internet Protocol (TCP/IP) requests
D. Exceeds the limits for new Transmission Control Protocol /Internet Protocol (TCP/IP) connections

Answer: B

NEW QUESTION 845
- (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 847
- (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 852
- (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 855
- (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 858
- (Exam Topic 13)
As part of an application penetration testing process, session hijacking can BEST be achieved by which of the following?

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

Answer: D

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 863
- (Exam Topic 13)
Which of the following is the MOST important part of an awareness and training plan to prepare employees for emergency situations?

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

Answer: C

NEW QUESTION 867
- (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 870
- (Exam Topic 13)
During examination of Internet history records, the following string occurs within a Unique Resource Locator (URL):
http://www.companysite.com/products/products.asp?productid=123
or 1=1
What type of attack does this indicate?

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

Answer: C

NEW QUESTION 873
- (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 874
- (Exam Topic 13)
A Security Operations Center (SOC) receives an incident response notification on a server with an active
intruder who has planted a backdoor. Initial notifications are sent and communications are established. What MUST be considered or evaluated before performing the next step?

A. Notifying law enforcement is crucial before hashing the contents of the server hard drive
B. Identifying who executed the incident is more important than how the incident happened
C. Removing the server from the network may prevent catching the intruder
D. Copying the contents of the hard drive to another storage device may damage the evidence

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 878
.....

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