# ISC2

## Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

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

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

**Answer:** A

**NEW QUESTION 2**
- (Exam Topic 1)
Which of the following represents the GREATEST risk to data confidentiality?

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

**Answer:** C

**NEW QUESTION 3**
- (Exam Topic 1)
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 4**
- (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 5**
- (Exam Topic 1)
Which of the following types of technologies would be the MOST cost-effective method to provide a reactive control for protecting personnel in public areas?

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

**Answer:** D

**NEW QUESTION 6**
- (Exam Topic 1)
What is the MOST important consideration from a data security perspective when an organization plans to relocate?

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

**Answer:** C

**NEW QUESTION 7**
- (Exam Topic 2)
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 8**
- (Exam Topic 2)
Which one of the following affects the classification of data?

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

**Answer:** D

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

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

**Answer:** B

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

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

**Answer:** A

**NEW QUESTION 10**
- (Exam Topic 2)
An organization has doubled in size due to a rapid market share increase. The size of the Information Technology (IT) staff has maintained pace with this growth. The organization hires several contractors whose onsite time is limited. The IT department has pushed its limits building servers and rolling out workstations and has a backlog of account management requests.
Which contract is BEST in offloading the task from the IT staff?

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

**Answer:** B

**NEW QUESTION 15**
- (Exam Topic 3)
Which of the following mobile code security models relies only on trust?

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

**Answer:** A

**NEW QUESTION 16**
- (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 20**
- (Exam Topic 4)
Which of the following operates at the Network Layer of the Open System Interconnection (OSI) model?

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

**Answer:** A


**NEW QUESTION 25**
- (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 30**
- (Exam Topic 4)
What is the purpose of an Internet Protocol (IP) spoofing attack?

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

**Answer:** D


**NEW QUESTION 32**
- (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 37**
- (Exam Topic 4)
At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

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

**Answer:** D


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

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

**Answer:** B


**NEW QUESTION 41**
- (Exam Topic 6)
Which of the following is a PRIMARY benefit of using a formalized security testing report format and structure?

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

**Answer:** D


**NEW QUESTION 42**

- (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 47**
- (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 50**
- (Exam Topic 7)
What would be the MOST cost effective solution for a Disaster Recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours?

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

**Answer:** A


**NEW QUESTION 54**
- (Exam Topic 7)
Which of the following is a PRIMARY advantage of using a third-party identity service?

A. Consolidation of multiple providers
B. Directory synchronization
C. Web based logon
D. Automated account management

**Answer:** D


**NEW QUESTION 58**
- (Exam Topic 7)
What is the MOST important step during forensic analysis when trying to learn the purpose of an unknown application?

A. Disable all unnecessary services
B. Ensure chain of custody
C. Prepare another backup of the system
D. Isolate the system from the network

**Answer:** D


**NEW QUESTION 62**
- (Exam Topic 7)
A continuous information security monitoring program can BEST reduce risk through which of the following?

A. Collecting security events and correlating them to identify anomalies
B. Facilitating system-wide visibility into the activities of critical user accounts
C. Encompassing people, process, and technology
D. Logging both scheduled and unscheduled system changes

**Answer:** B


**NEW QUESTION 63**
- (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 66**
- (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 71**
- (Exam Topic 8)
Which of the following is a web application control that should be put into place to prevent exploitation of Operating System (OS) bugs?

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

**Answer:** B


**NEW QUESTION 75**
- (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 79**
- (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 81**
- (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 86**
- (Exam Topic 9)
The three PRIMARY requirements for a penetration test are

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

**Answer:** A


**NEW QUESTION 87**
- (Exam Topic 9)
Which of the following is the FIRST action that a system administrator should take when it is revealed during a penetration test that everyone in an organization has unauthorized access to a server holding sensitive data?

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

**Answer:**

A

**NEW QUESTION 92**
- (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 97**
- (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 98**
- (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 102**
- (Exam Topic 9)
A vulnerability test on an Information System (IS) is conducted to

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

**Answer:** C

**NEW QUESTION 106**
- (Exam Topic 9)
An organization allows ping traffic into and out of their network. An attacker has installed a program on the network that uses the payload portion of the ping packet to move data into and out of the network. What type of attack has the organization experienced?

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

**Answer:** D

**NEW QUESTION 109**
- (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 113**
- (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 116**
- (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 121**
- (Exam Topic 9)
An internal Service Level Agreement (SLA) covering security is signed by senior managers and is in place. When should compliance to the SLA be reviewed to ensure that a good security posture is being delivered?

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

**Answer:** D

**NEW QUESTION 122**
- (Exam Topic 9)
Why is a system's criticality classification important in large organizations?

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

**Answer:** A

**NEW QUESTION 124**
- (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 127**
- (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 128**
- (Exam Topic 9)
Multi-threaded applications are more at risk than single-threaded applications to

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

**Answer:** A

**NEW QUESTION 132**
- (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 134
- (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 135
- (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 139
- (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 142
- (Exam Topic 9)
As one component of a physical security system, an Electronic Access Control (EAC) token is BEST known for its ability to

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

**Answer:** A


## NEW QUESTION 147
- (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)
The PRIMARY purpose of a security awareness program is to

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

**Answer:** A


## NEW QUESTION 154

- (Exam Topic 9)

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

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

**Answer:** D


## NEW QUESTION 156

- (Exam Topic 9)
Which of the following is a security feature of Global Systems for Mobile Communications (GSM)?

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

**Answer:** A


## NEW QUESTION 161

- (Exam Topic 9)
Which of the following assessment metrics is BEST used to understand a system's vulnerability to potential exploits?

A. Determining the probability that the system functions safely during any time period
B. Quantifying the system's available services
C. Identifying the number of security flaws within the system
D. Measuring the system's integrity in the presence of failure

**Answer:** C


## NEW QUESTION 165

- (Exam Topic 9)
An auditor carrying out a compliance audit requests passwords that are encrypted in the system to verify that the passwords are compliant with policy. Which of the following is the BEST response to the auditor?

A. Provide the encrypted passwords and analysis tools to the auditor for analysis.
B. Analyze the encrypted passwords for the auditor and show them the results.
C. Demonstrate that non-compliant passwords cannot be created in the system.
D. Demonstrate that non-compliant passwords cannot be encrypted in the system.

**Answer:** C


## NEW QUESTION 168

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

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

**Answer:** D


## NEW QUESTION 173

- (Exam Topic 9)
Which of the following is TRUE about Disaster Recovery Plan (DRP) testing?

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

**Answer:** B


## NEW QUESTION 174

- (Exam Topic 9)
The BEST way to check for good security programming practices, as well as auditing for possible backdoors, is to conduct

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

**Answer:** B

**NEW QUESTION 179**
- (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 180**
- (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 185**
- (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 188**
- (Exam Topic 9)
Which of the following is the FIRST step of a penetration test plan?

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

**Answer:** C


**NEW QUESTION 191**
- (Exam Topic 9)
Which type of control recognizes that a transaction amount is excessive in accordance with corporate policy?

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

**Answer:** A


**NEW QUESTION 194**
- (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 198**
- (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 199**
- (Exam Topic 9)
Which of the following is an appropriate source for test data?

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

**Answer:** D


**NEW QUESTION 203**
- (Exam Topic 9)
While impersonating an Information Security Officer (ISO), an attacker obtains information from company employees about their User IDs and passwords. Which method of information gathering has the attacker used?

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

**Answer:** C


**NEW QUESTION 204**
- (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 208**
- (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 210**
- (Exam Topic 9)
An Intrusion Detection System (IDS) is generating alarms that a user account has over 100 failed login attempts per minute. A sniffer is placed on the network, and a variety of passwords for that user are noted. Which of the following is MOST likely occurring?

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

**Answer:** A


**NEW QUESTION 212**
- (Exam Topic 9)
When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?

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

**Answer:** B


**NEW QUESTION 216**
- (Exam Topic 9)
Which of the following is the BEST mitigation from phishing attacks?

A. Network activity monitoring
B. Security awareness training

C. Corporate policy and procedures
D. Strong file and directory permissions

**Answer:** B

**NEW QUESTION 220**
- (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 222**
- (Exam Topic 9)
Which of the following does Temporal Key Integrity Protocol (TKIP) support?

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

**Answer:** C

**NEW QUESTION 223**
- (Exam Topic 9)
By allowing storage communications to run on top of Transmission Control Protocol/Internet Protocol (TCP/IP) with a Storage Area Network (SAN), the

A. confidentiality of the traffic is protected.
B. opportunity to sniff network traffic exists.
C. opportunity for device identity spoofing is eliminated.
D. storage devices are protected against availability attacks.

**Answer:** B

**NEW QUESTION 228**
- (Exam Topic 9)
Which of the following BEST represents the principle of open design?

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

**Answer:** D

**NEW QUESTION 230**
- (Exam Topic 9)
Why must all users be positively identified prior to using multi-user computers?

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

**Answer:** C

**NEW QUESTION 235**
- (Exam Topic 9)
Which of the following wraps the decryption key of a full disk encryption implementation and ties the hard disk drive to a particular device?

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

**Answer:** A

**NEW QUESTION 236**
- (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 241
- (Exam Topic 9)
Which Hyper Text Markup Language 5 (HTML5) option presents a security challenge for network data leakage prevention and/or monitoring?

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

**Answer:** B


## NEW QUESTION 242
- (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 243
- (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 247
- (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 250
- (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 255
- (Exam Topic 10)
Which of the following is the MOST beneficial to review when performing an IT audit?

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

**Answer:** C

**NEW QUESTION 257**
- (Exam Topic 10)
When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?

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

**Answer:** B


**NEW QUESTION 261**
- (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 265**
- (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 266**
- (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 270**
- (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 272**
- (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 275**
- (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 280**
- (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 283**
- (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 284**
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
What MUST the access control logs contain in addition to the identifier?

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

**Answer:** A

**NEW QUESTION 288**
- (Exam Topic 10)
What is the MOST critical factor to achieve the goals of a security program?

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

**Answer:** B

**NEW QUESTION 292**
- (Exam Topic 10)
What is the PRIMARY advantage of using automated application security testing tools?

A. The application can be protected in the production environment.
B. Large amounts of code can be tested using fewer resources.
C. The application will fail less when tested using these tools.
D. Detailed testing of code functions can be performed.

**Answer:** B

**NEW QUESTION 297**
- (Exam Topic 10)
What component of a web application that stores the session state in a cookie can be bypassed by an attacker?

A. An initialization check
B. An identification check

C. An authentication check
D. An authorization check

**Answer:** C


**NEW QUESTION 299**
- (Exam Topic 10)
A security manager has noticed an inconsistent application of server security controls resulting in vulnerabilities on critical systems. What is the MOST likely cause of this issue?

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

**Answer:** A


**NEW QUESTION 300**
- (Exam Topic 10)
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
If the intrusion causes the system processes to hang, which of the following has been affected?

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

**Answer:** B


**NEW QUESTION 304**
- (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 308**
- (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 309**
- (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 the plan, what is the BEST approach to mitigate future internal client-based attacks?

A. Block all client side web exploits at the perimeter.
B. Remove all non-essential client-side web services from the network.
C. Screen for harmful exploits of client-side services before implementation.
D. Harden the client image before deployment.

**Answer:** D


**NEW QUESTION 313**
- (Exam Topic 10)
Refer to the information below to answer the question.
In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

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

In a Bell-LaPadula system, which user cannot write to File 3?

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

**Answer:** D


## NEW QUESTION 318
- (Exam Topic 10)
With data labeling, which of the following MUST be the key decision maker?

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

**Answer:** D


## NEW QUESTION 323
- (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 324
- (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 325
- (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 330
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?

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

**Answer:** A

**NEW QUESTION 334**
- (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 338**
- (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 340**
- (Exam Topic 10)
Host-Based Intrusion Protection (HIPS) systems are often deployed in monitoring or learning mode during their initial implementation. What is the objective of starting in this mode?

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

**Answer:** D

**NEW QUESTION 341**
- (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 343**
- (Exam Topic 10)
Place the following information classification steps in sequential order.

**Steps**

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

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Steps**

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

**NEW QUESTION 344**
- (Exam Topic 10)
Which of the following is the MAIN goal of a data retention policy?

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

**Answer:** C

**NEW QUESTION 347**
- (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 350**
- (Exam Topic 10)
A large university needs to enable student access to university resources from their homes. Which of the following provides the BEST option for low maintenance

and ease of deployment?

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

**Answer:** B

**NEW QUESTION 351**
- (Exam Topic 10)
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 353**
- (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 358**
- (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 363**
- (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 367**
- (Exam Topic 10)
An organization's data policy MUST include a data retention period which is based on

A. application dismissal.
B. business procedures.
C. digital certificates expiration.
D. regulatory compliance.

**Answer:** D

**NEW QUESTION 369**
- (Exam Topic 10)
What is the PRIMARY reason for ethics awareness and related policy implementation?

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

**Answer:** B

**NEW QUESTION 373**
- (Exam Topic 10)
Without proper signal protection, embedded systems may be prone to which type of attack?

A. Brute force
B. Tampering
C. Information disclosure
D. Denial of Service (DoS)

**Answer:** C


**NEW QUESTION 378**
- (Exam Topic 10)
Which of the following is the PRIMARY benefit of a formalized information classification program?

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

**Answer:** B


**NEW QUESTION 382**
- (Exam Topic 10)
A thorough review of an organization's audit logs finds that a disgruntled network administrator has intercepted emails meant for the Chief Executive Officer (CEO) and changed them before forwarding them to their intended recipient. What type of attack has MOST likely occurred?

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

**Answer:** C


**NEW QUESTION 386**
- (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 387**
- (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 391**
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
The effectiveness of the security program can PRIMARILY be measured through

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

**Answer:** A


**NEW QUESTION 393**
- (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 394**
- (Exam Topic 10)
Refer to the information below to answer the question.
Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.
Organizational policy requires the deletion of user data from Personal Digital Assistant (PDA) devices before disposal. It may not be possible to delete the user data if the device is malfunctioning. Which destruction method below provides the BEST assurance that the data has been removed?

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

**Answer:** C


**NEW QUESTION 397**
- (Exam Topic 11)
What is the process called when impact values are assigned to the security objectives for information types?

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

**Answer:** D


**NEW QUESTION 402**
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the correct specification in the image below.
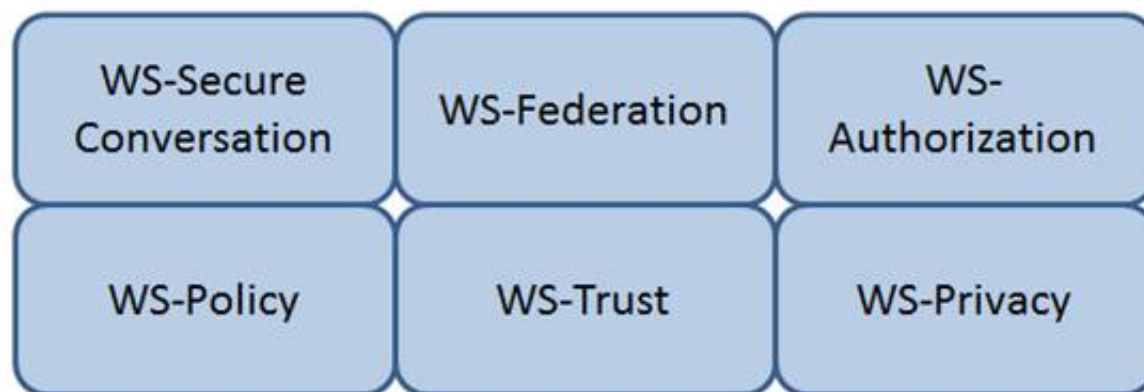


A. Mastered
B. Not Mastered

**Answer:** A

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


**NEW QUESTION 403**
- (Exam Topic 11)
What is the MOST effective method of testing custom application code?

A. Negative testing
B. White box testing
C. Penetration testing

D. Black box testing

**Answer:** B


**NEW QUESTION 407**
- (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 412**
- (Exam Topic 11)
If an identification process using a biometric system detects a 100% match between a presented template and a stored template, what is the interpretation of this result?

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

**Answer:** B


**NEW QUESTION 415**
- (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 417**
- (Exam Topic 11)
Which of the following is a function of Security Assertion Markup Language (SAML)?

A. File allocation
B. Redundancy check
C. Extended validation
D. Policy enforcement

**Answer:** D


**NEW QUESTION 420**
- (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 422**
- (Exam Topic 11)
Changes to a Trusted Computing Base (TCB) system that could impact the security posture of that system and trigger a recertification activity are documented in the

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

**Answer:** A


**NEW QUESTION 423**

- (Exam Topic 11)
Which of the following statements is TRUE regarding state-based analysis as a functional software testing technique?

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

**Answer:** A

## NEW QUESTION 428
- (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 430
- (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 434
- (Exam Topic 11)
What should happen when an emergency change to a system must be performed?

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

**Answer:** B

## NEW QUESTION 439
- (Exam Topic 11)
After a thorough analysis, it was discovered that a perpetrator compromised a network by gaining access to the network through a Secure Socket Layer (SSL) Virtual Private Network (VPN) gateway. The perpetrator guessed a username and brute forced the password to gain access. Which of the following BEST mitigates this issue?

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

**Answer:** D

## NEW QUESTION 444
- (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 447
- (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 452**
- (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 456**
- (Exam Topic 11)
Disaster Recovery Plan (DRP) training material should be

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

**Answer:** A

**NEW QUESTION 457**
- (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 458**
- (Exam Topic 11)
Which of the following is the BEST method to assess the effectiveness of an organization's vulnerability management program?

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

**Answer:** B

**NEW QUESTION 462**
- (Exam Topic 11)
Which of the following is the BIGGEST weakness when using native Lightweight Directory Access Protocol (LDAP) for authentication?

A. Authorizations are not included in the server response
B. Unsalted hashes are passed over the network
C. The authentication session can be replayed
D. Passwords are passed in cleartext

**Answer:** D

**NEW QUESTION 464**
- (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 465**
- (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 470
- (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 475
- (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 479
- (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 482
- (Exam Topic 11)
What is the PRIMARY difference between security policies and security procedures?

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

**Answer:** D

NEW QUESTION 484
- (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 485
- (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 489
- (Exam Topic 11)
Which of the following command line tools can be used in the reconnaisance phase of a network vulnerability assessment?

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

**Answer:** A


**NEW QUESTION 492**
- (Exam Topic 11)
Which of the following describes the BEST configuration management practice?

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

**Answer:** D


**NEW QUESTION 497**
- (Exam Topic 11)
Which of the following is the PRIMARY security concern associated with the implementation of smart cards?

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

**Answer:** C


**NEW QUESTION 499**
- (Exam Topic 11)
A software security engineer is developing a black box-based test plan that will measure the system's reaction to incorrect or illegal inputs or unexpected operational errors and situations. Match the functional testing techniques on the left with the correct input parameters on the right.

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

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 500**
- (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 502**
- (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 504**
- (Exam Topic 11)
What type of encryption is used to protect sensitive data in transit over a network?

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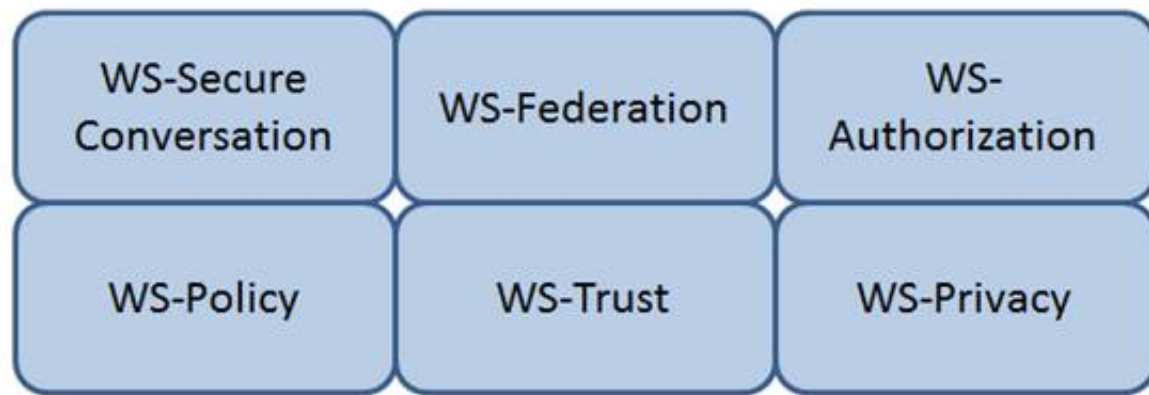C. Keyed-Hashing for Message Authentication
D. Point-to-Point Encryption (P2PE)

**Answer:** A

**NEW QUESTION 506**
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 508**
- (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 510**
- (Exam Topic 11)
Secure Sockets Layer (SSL) encryption protects

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

**Answer:** C

**NEW QUESTION 512**
- (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 514**
- (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 517**
- (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 522**
- (Exam Topic 11)
The PRIMARY security concern for handheld devices is the

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

**Answer:** C


**NEW QUESTION 525**
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued,
renewed and validated? Click on the correct specification in the image below.
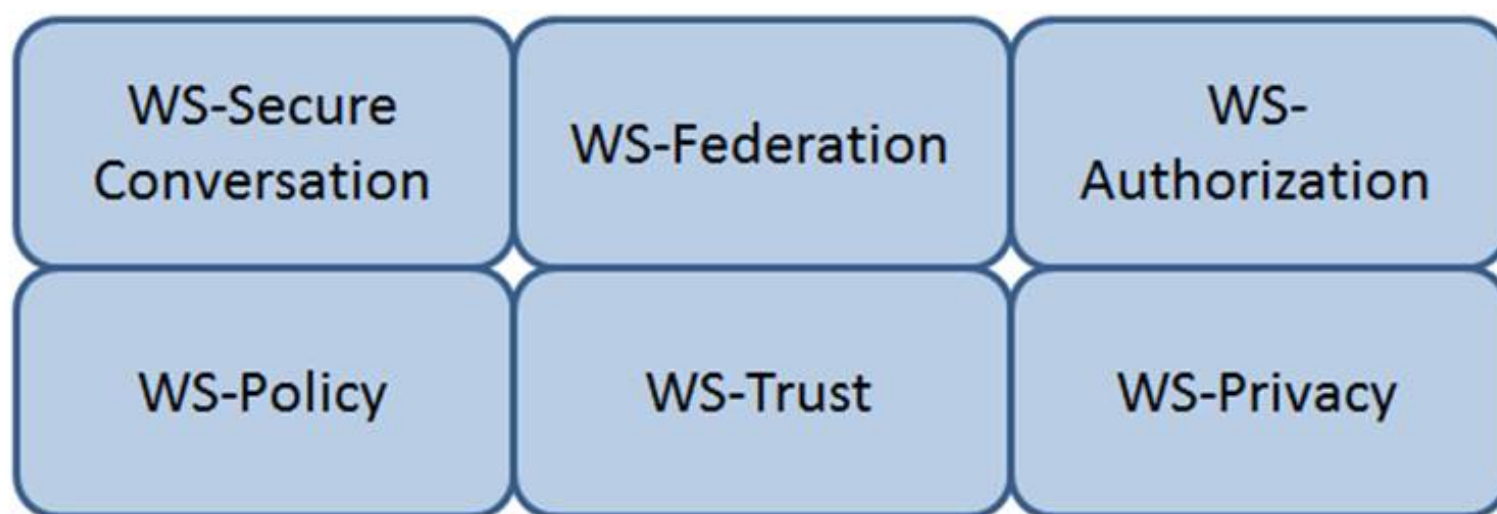


A. Mastered
B. Not Mastered

**Answer:** A

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


**NEW QUESTION 529**
- (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 531**
- (Exam Topic 11)
Which one of the following is a common risk with network configuration management?

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

**Answer:** D


**NEW QUESTION 532**
- (Exam Topic 11)
The goal of a Business Continuity Plan (BCP) training and awareness program is to

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

**Answer:** A


**NEW QUESTION 535**
- (Exam Topic 11)
Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic mediA.



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 539**
- (Exam Topic 11)
What security risk does the role-based access approach mitigate MOST effectively?

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

**Answer:** A


**NEW QUESTION 544**
- (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 545**
- (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 550**
- (Exam Topic 11)
When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?

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

**Answer:** B

**NEW QUESTION 551**
- (Exam Topic 11)
Which of the following BEST avoids data remanence disclosure for cloud hosted resources?

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

**Answer:** A

**NEW QUESTION 555**
- (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 557**
- (Exam Topic 11)
While inventorying storage equipment, it is found that there are unlabeled, disconnected, and powered off devices. Which of the following is the correct procedure for handling such equipment?

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

**Answer:** C

**NEW QUESTION 558**
- (Exam Topic 11)
Which of the following secures web transactions at the Transport Layer?

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

**Answer:** B

**NEW QUESTION 560**
- (Exam Topic 11)

The 802.1x standard provides a framework for what?

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

**Answer:** B

**NEW QUESTION 562**
- (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?
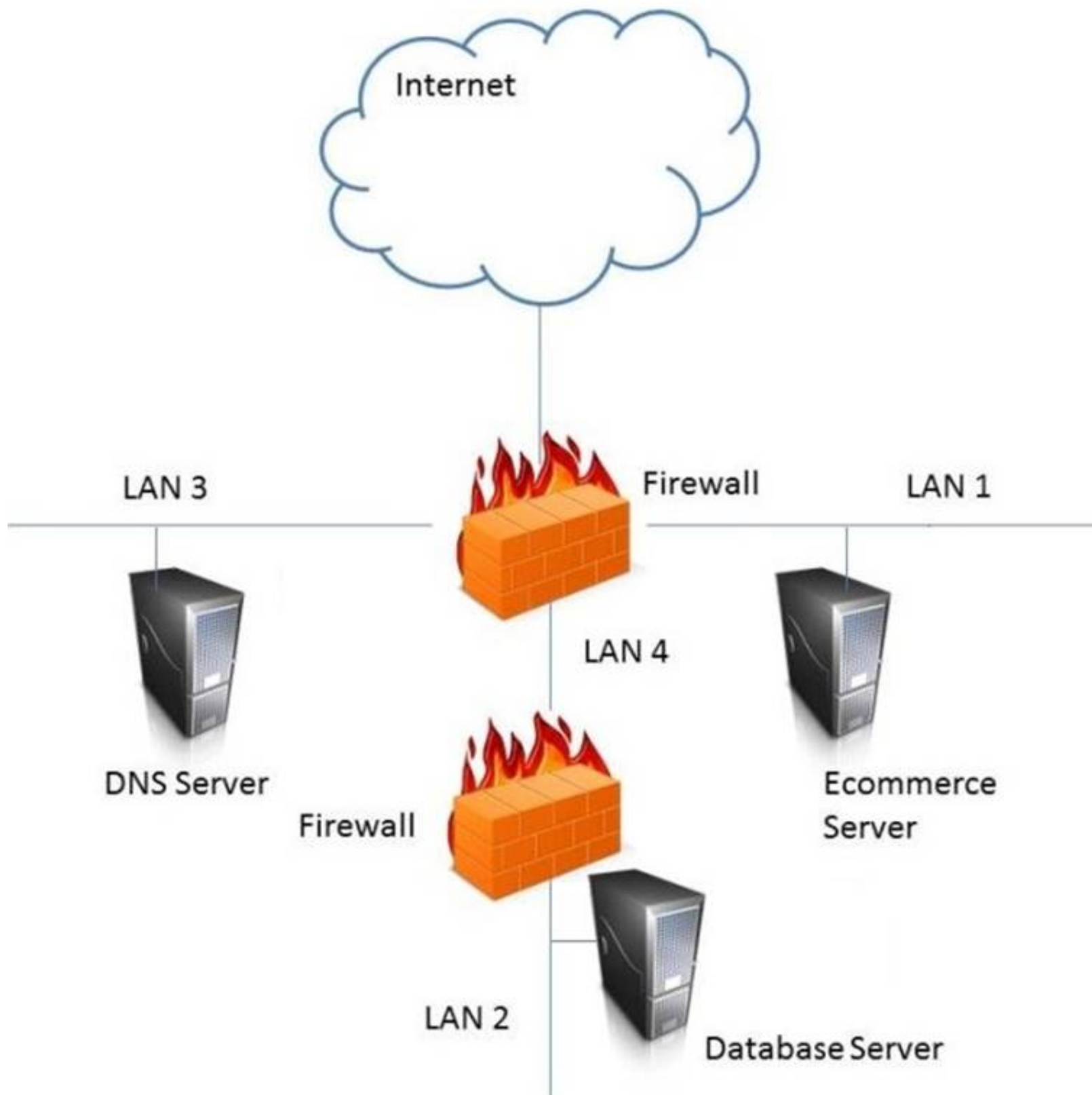
A. Retention
B. Reporting
C. Recovery
D. Remediation

**Answer:** A

**NEW QUESTION 566**
- (Exam Topic 11)
In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
LAN 4

**NEW QUESTION 570**
- (Exam Topic 11)
Which of the following is the PRIMARY issue when collecting detailed log information?

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

**Answer:** B


**NEW QUESTION 572**
- (Exam Topic 11)
The BEST method to mitigate the risk of a dictionary attack on a system is to

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

**Answer:** A


**NEW QUESTION 577**
- (Exam Topic 11)
Which of the following provides the minimum set of privileges required to perform a job function and restricts the user to a domain with the required privileges?

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

**Answer:** B


**NEW QUESTION 580**
- (Exam Topic 12)
What is the difference between media marking and media labeling?

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

**Answer:** D


**NEW QUESTION 581**
- (Exam Topic 12)
A vulnerability in which of the following components would be MOST difficult to detect?

A. Kernel
B. Shared libraries
C. Hardware
D. System application

**Answer:** A


**NEW QUESTION 585**
- (Exam Topic 12)
Which of the following information MUST be provided for user account provisioning?

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

**Answer:** B


**NEW QUESTION 590**
- (Exam Topic 12)
Which of the following is the BEST method to reduce the effectiveness of phishing attacks?

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

**Answer:** A

**NEW QUESTION 593**
- (Exam Topic 12)
Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

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

**Answer:** A

**NEW QUESTION 596**
- (Exam Topic 12)
Which Radio Frequency Interference (RFI) phenomenon associated with bundled cable runs can create information leakage?

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

**Answer:** D

**NEW QUESTION 600**
- (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 602**
- (Exam Topic 12)
Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

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

**Answer:** B

**NEW QUESTION 606**
- (Exam Topic 12)
Which of the following is the MOST important goal of information asset valuation?

A. Developing a consistent and uniform method of controlling access on information assets
B. Developing appropriate access control policies and guidelines
C. Assigning a financial value to an organization's information assets
D. Determining the appropriate level of protection

**Answer:** D

**NEW QUESTION 607**
- (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 610**
- (Exam Topic 12)
The PRIMARY outcome of a certification process is that it provides documented

A. interconnected systems and their implemented security controls.
B. standards for security assessment, testing, and process evaluation.
C. system weakness for remediation.

D. security analyses needed to make a risk-based decision.

**Answer:** D


## NEW QUESTION 614

- (Exam Topic 12)
An application developer is deciding on the amount of idle session time that the application allows before a timeout. The BEST reason for determining the session timeout requirement is

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

**Answer:** A


## NEW QUESTION 617

- (Exam Topic 12)
Which of the following is MOST important when deploying digital certificates?

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

**Answer:** B


## NEW QUESTION 621

- (Exam Topic 12)
During which of the following processes is least privilege implemented for a user account?

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

**Answer:** A


## NEW QUESTION 622

- (Exam Topic 12)
Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

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

**Answer:** B


## NEW QUESTION 626

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

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

**Answer:** B


## NEW QUESTION 630

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

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

**Answer:** C


## NEW QUESTION 632

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

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

**Answer:** B


**NEW QUESTION 636**
- (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 640**
- (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 642**
- (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 644**
- (Exam Topic 12)
Which of the following BEST describes Recovery Time Objective (RTO)?

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

**Answer:** A


**NEW QUESTION 647**
- (Exam Topic 12)
Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

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

**Answer:** A


**NEW QUESTION 651**
- (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 653**

- (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 656**
- (Exam Topic 12)
Which of the following would BEST describe the role directly responsible for data within an organization?

A. Data custodian
B. Information owner
C. Database administrator
D. Quality control

**Answer:** A


**NEW QUESTION 657**
- (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 662**
- (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 665**
- (Exam Topic 12)
When writing security assessment procedures, what is the MAIN purpose of the test outputs and reports?

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

**Answer:** C


**NEW QUESTION 666**
- (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 668**
- (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 672**
- (Exam Topic 12)
Which of the following is the PRIMARY reason for employing physical security personnel at entry points in facilities where card access is in operation?

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

**Answer:** D


**NEW QUESTION 673**
- (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 674**
- (Exam Topic 12)
Which of the following is the MOST important consideration when developing a Disaster Recovery Plan (DRP)?

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

**Answer:** C


**NEW QUESTION 677**
- (Exam Topic 12)
In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of

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

**Answer:** D


**NEW QUESTION 682**
- (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 683**
- (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 686**
- (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 689**
- (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 694**
- (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 696**
- (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 698**
- (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 701**
- (Exam Topic 12)
For network based evidence, which of the following contains traffic details of all network sessions in order to detect anomalies?

A. Alert data
B. User data
C. Content data
D. Statistical data

**Answer:** D


**NEW QUESTION 703**
- (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 708**
- (Exam Topic 12)
Knowing the language in which an encrypted message was originally produced might help a cryptanalyst to perform a

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

**Answer:** C

**NEW QUESTION 710**
- (Exam Topic 12)
Backup information that is critical to the organization is identified through a

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

**Answer:** D

**NEW QUESTION 712**
- (Exam Topic 12)
Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?

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

**Answer:** C

**NEW QUESTION 717**
- (Exam Topic 12)
In which identity management process is the subject's identity established?

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

**Answer:** D

**NEW QUESTION 721**
- (Exam Topic 12)
Which of the following is the PRIMARY reason to perform regular vulnerability scanning of an organization network?

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

**Answer:** B

**NEW QUESTION 722**
- (Exam Topic 12)
What is a characteristic of Secure Socket Layer (SSL) and Transport Layer Security (TLS)?

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

**Answer:** A

**NEW QUESTION 724**
- (Exam Topic 13)
A security compliance manager of a large enterprise wants to reduce the time it takes to perform network, system, and application security compliance audits while increasing quality and effectiveness of the results. What should be implemented to BEST achieve the desired results?

A. Configuration Management Database (CMDB)
B. Source code repository
C. Configuration Management Plan (CMP)
D. System performance monitoring application

**Answer:** C

**NEW QUESTION 727**
- (Exam Topic 13)
Which of the following is the BEST reason for writing an information security policy?

A. To support information security governance
B. To reduce the number of audit findings

C. To deter attackers
D. To implement effective information security controls

**Answer:** A


**NEW QUESTION 732**
- (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 735**
- (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 737**
- (Exam Topic 13)
Which of the following MUST be in place to recognize a system attack?

A. Stateful firewall
B. Distributed antivirus
C. Log analysis
D. Passive honeypot

**Answer:** A


**NEW QUESTION 739**
- (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 743**
- (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 748**
- (Exam Topic 13)
What is the PRIMARY role of a scrum master in agile development?

A. To choose the primary development language
B. To choose the integrated development environment
C. To match the software requirements to the delivery plan
D. To project manage the software delivery

**Answer:** D

**NEW QUESTION 749**
- (Exam Topic 13)
Which of the following is the MOST common method of memory protection?

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

**Answer:** B


**NEW QUESTION 751**
- (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 753**
- (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 757**
- (Exam Topic 13)
Drag the following Security Engineering terms on the left to the BEST definition on the right.

| Security Engineering Term | | Definition |
| --- | --- | --- |
| Risk | | A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of |
| Security Risk Treatment | | The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable. |
| Protection Needs Assessment | | The method used to identify and characterize the dangers anticipated throughout the life cycle of the system. |
| Threat Assessment | | The method used to identify feasible security risk mitigation options and plans. |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Risk - A measure of the extent to which an entity is threatened by a potential circumstance of event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.
Protection Needs Assessment - The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should be asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Threat assessment - The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.

Security Risk Treatment - The method used to identify feasible security risk mitigation options and plans.

**NEW QUESTION 761**
- (Exam Topic 13)
The design review for an application has been completed and is ready for release. What technique should an organization use to assure application integrity?

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

**Answer:** C

**NEW QUESTION 764**
- (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 767**
- (Exam Topic 13)
Which security modes is MOST commonly used in a commercial environment because it protects the integrity
of financial and accounting data?

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

**Answer:** C

**NEW QUESTION 768**
- (Exam Topic 13)
What is the process of removing sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique?

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

**Answer:** A

**NEW QUESTION 772**
- (Exam Topic 13)
Which of the following is a benefit in implementing an enterprise Identity and Access Management (IAM) solution?

A. Password requirements are simplified.
B. Risk associated with orphan accounts is reduced.
C. Segregation of duties is automatically enforced.
D. Data confidentiality is increased.

**Answer:** A

**NEW QUESTION 776**
- (Exam Topic 13)
Which of the following is a characteristic of an internal audit?

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

**Answer:** D

**NEW QUESTION 777**
- (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 780**
- (Exam Topic 13)
Which of the following is the BEST reason for the use of security metrics?

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

**Answer:** B


**NEW QUESTION 782**
- (Exam Topic 13)
A security practitioner is tasked with securing the organization's Wireless Access Points (WAP). Which of these is the MOST effective way of restricting this environment to authorized users?

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

**Answer:** D


**NEW QUESTION 784**
- (Exam Topic 13)
What is the MAIN purpose of a change management policy?

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

**Answer:** C

**Explanation:**
Section: Security Operations


**NEW QUESTION 785**
- (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)
Which of the following is a common characteristic of privacy?

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

**Answer:** A


**NEW QUESTION 794**
- (Exam Topic 13)
Proven application security principles include which of the following?

A. Minimizing attack surface area

B. Hardening the network perimeter
C. Accepting infrastructure security controls
D. Developing independent modules

**Answer:** A

**NEW QUESTION 799**
- (Exam Topic 13)
Which type of test would an organization perform in order to locate and target exploitable defects?

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

**Answer:** A

**NEW QUESTION 803**
- (Exam Topic 13)
Match the functional roles in an external audit to their responsibilities. Drag each role on the left to its corresponding responsibility on the right. Select and Place:



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**



**NEW QUESTION 807**
- (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 812**
- (Exam Topic 13)

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

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

**Answer:** D


**NEW QUESTION 816**
- (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 819**
- (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 822**
- (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 824**
- (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 827**
- (Exam Topic 13)
What is the second step in the identity and access provisioning lifecycle?

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

**Answer:** B


**NEW QUESTION 830**
- (Exam Topic 13)
An Information Technology (IT) professional attends a cybersecurity seminar on current incident response methodologies.
What code of ethics canon is being observed?

A. Provide diligent and competent service to principals

B. Protect society, the commonwealth, and the infrastructure
C. Advance and protect the profession
D. Act honorable, honesty, justly, responsibly, and legally

**Answer:** C

**Explanation:**
Section: Security Operations

**NEW QUESTION 831**
- (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 835**
- (Exam Topic 13)
Which of the following would MINIMIZE the ability of an attacker to exploit a buffer overflow?

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

**Answer:** B

**NEW QUESTION 838**
- (Exam Topic 13)
After following the processes defined within the change management plan, a super user has upgraded a device within an Information system.
What step would be taken to ensure that the upgrade did NOT affect the network security posture?

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

**Answer:** B

**Explanation:**
Section: Security Assessment and Testing

**NEW QUESTION 840**
- (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 841**
- (Exam Topic 13)
Which of the following mandates the amount and complexity of security controls applied to a security risk?

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

**Answer:** C

**NEW QUESTION 843**
- (Exam Topic 13)
At a MINIMUM, audits of permissions to individual or group accounts should be scheduled

A. annually
B. to correspond with staff promotions
C. to correspond with terminations

D. continually

**Answer:** A


**NEW QUESTION 847**
- (Exam Topic 13)
Digital certificates used in Transport Layer Security (TLS) support which of the following?

A. Information input validation
B. Non-repudiation controls and data encryption
C. Multi-Factor Authentication (MFA)
D. Server identity and data confidentially

**Answer:** D


**NEW QUESTION 851**
- (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 854**
......

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons and Answers in PDF Format

## CISSP Practice Exam Features:

* CISSP Questions and Answers Updated Frequently

* CISSP Practice Questions Verified by Expert Senior Certified Staff

* CISSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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