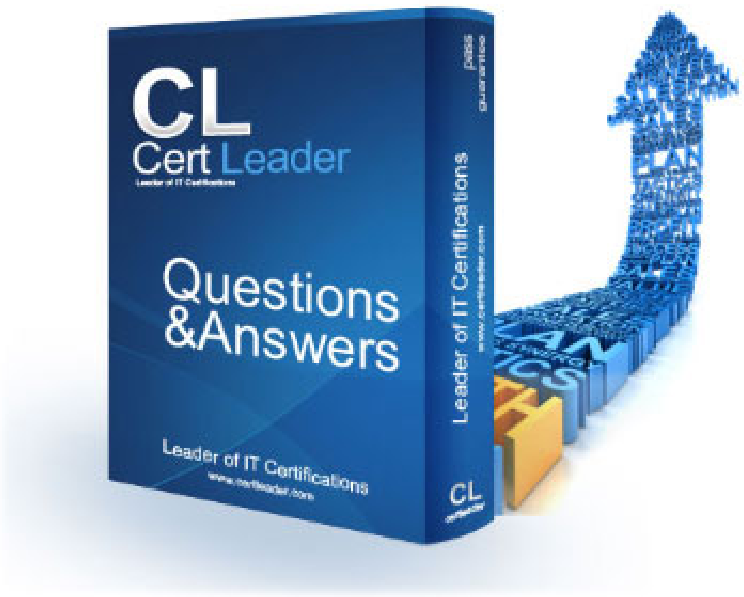
# CISSP Dumps

# Certified Information Systems Security Professional (CISSP)

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



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

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

**Answer:** C

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

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

**Answer:** B

**NEW QUESTION 3**
- (Exam Topic 1)
Which of the following 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 4**
- (Exam Topic 2)
Which of the following is an effective control in preventing electronic cloning of Radio Frequency Identification (RFID) based access cards?

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

**Answer:** C

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

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

**Answer:** A

**NEW QUESTION 7**
- (Exam Topic 3)
The use of private and public encryption keys is fundamental in the implementation of which of the following?

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

**Answer:** A

**NEW QUESTION 8**
- (Exam Topic 3)
Who in the organization is accountable for classification of data information assets?

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

**Answer:** A

**NEW QUESTION 9**
- (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 10**
- (Exam Topic 4)
In a Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which layer is responsible for negotiating and establishing a connection with another node?

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

**Answer:** A

**NEW QUESTION 10**
- (Exam Topic 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 13**
- (Exam Topic 5)
Which of the following BEST describes an access control method utilizing cryptographic keys derived from a smart card private key that is embedded within mobile devices?

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

**Answer:** A

**NEW QUESTION 18**
- (Exam Topic 6)
Which of the following is of GREATEST assistance to auditors when reviewing system configurations?

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

**Answer:** A

**NEW QUESTION 22**
- (Exam Topic 6)
In which of the following programs is it MOST important to include the collection of security process data?

A. Quarterly access reviews
B. Security continuous monitoring

C. Business continuity testing
D. Annual security training

**Answer:** A

**NEW QUESTION 23**
- (Exam Topic 7)
Which of the following types of business continuity tests includes assessment of resilience to internal and external risks without endangering live operations?

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

**Answer:** B

**NEW QUESTION 28**
- (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 33**
- (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 35**
- (Exam Topic 7)
Which of the following is the FIRST step in the incident response process?

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

**Answer:** D

**NEW QUESTION 36**
- (Exam Topic 8)
A Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. The program is not working as expected. What is the MOST probable security feature of Java preventing the program from operating as intended?

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

**Answer:** A

**NEW QUESTION 38**
- (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 41**
- (Exam Topic 8)
The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle

(SDLC)?

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

**Answer:** A

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

**NEW QUESTION 43**
- (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 47**
- (Exam Topic 9)
Which of the following MUST be part of a contract to support electronic discovery of data stored in a cloud environment?

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

**Answer:** D

**NEW QUESTION 51**
- (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 55**
- (Exam Topic 9)
Which layer of the Open Systems Interconnections (OSI) model implementation adds information concerning the logical connection between the sender and receiver?

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

**Answer:** C

**NEW QUESTION 58**
- (Exam Topic 9)
Which one of the following considerations has the LEAST impact when considering transmission security?

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

**Answer:** C

**NEW QUESTION 59**
- (Exam Topic 9)
Which of the following is considered best practice for preventing e-mail spoofing?

A. Spam filtering
B. Cryptographic signature
C. Uniform Resource Locator (URL) filtering
D. Reverse Domain Name Service (DNS) lookup

**Answer:** B

**NEW QUESTION 62**
- (Exam Topic 9)
The process of mutual authentication involves a computer system authenticating a user and authenticating the

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

**Answer:** B

**NEW QUESTION 67**
- (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 69**
- (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 74**
- (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 79**
- (Exam Topic 9)
The BEST method of demonstrating a company's security level to potential customers is

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

**Answer:** A

**NEW QUESTION 82**
- (Exam Topic 9)
An external attacker has compromised an organization's network security perimeter and installed a sniffer onto an inside computer. Which of the following is the MOST effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information?

A. Implement packet filtering on the network firewalls
B. Require strong authentication for administrators
C. Install Host Based Intrusion Detection Systems (HIDS)
D. Implement logical network segmentation at the switches

**Answer:** D

**NEW QUESTION 86**
- (Exam Topic 9)
In Business Continuity Planning (BCP), what is the importance of documenting business processes?

A. Provides senior management with decision-making tools
B. Establishes and adopts ongoing testing and maintenance strategies

C. Defines who will perform which functions during a disaster or emergency
D. Provides an understanding of the organization's interdependencies

**Answer:** D

**NEW QUESTION 91**
- (Exam Topic 9)
Which of the following can BEST prevent security flaws occurring in outsourced software development?

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

**Answer:** C

**NEW QUESTION 96**
- (Exam Topic 9)
The Hardware Abstraction Layer (HAL) is implemented in the

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

**Answer:** A

**NEW QUESTION 99**
- (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 100**
- (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 104**
- (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 109**
- (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 113**
- (Exam Topic 9)
When implementing controls in a heterogeneous end-point network for an organization, it is critical that

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

**Answer:** C

**NEW QUESTION 116**
- (Exam Topic 9)
What maintenance activity is responsible for defining, implementing, and testing updates to application systems?

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

**Answer:** A

**NEW QUESTION 117**
- (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 122**
- (Exam Topic 9)
Who must approve modifications to an organization's production infrastructure configuration?

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

**Answer:** B

**NEW QUESTION 123**
- (Exam Topic 9)
Which of the following is an effective method for avoiding magnetic media data remanence?

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

**Answer:** A

**NEW QUESTION 124**
- (Exam Topic 9)
What is the MOST important purpose of testing the Disaster Recovery Plan (DRP)?

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

**Answer:** C

**NEW QUESTION 127**
- (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 130**
- (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 133**
- (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 135**
- (Exam Topic 9)
At a MINIMUM, a formal review of any Disaster Recovery Plan (DRP) should be conducted

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

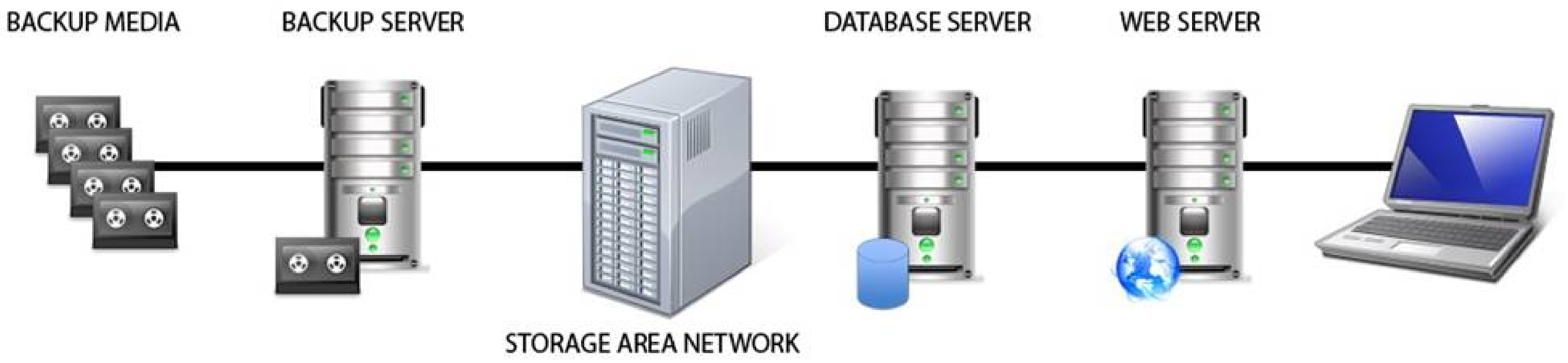
**Answer:** C

**NEW QUESTION 140**
- (Exam Topic 10)
Which of the following violates identity and access management best practices?

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

**Answer:** C

**NEW QUESTION 141**
- (Exam Topic 10)
Identify the component that MOST likely lacks digital accountability related to information access. Click on the correct device in the image below.



A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 144**
- (Exam Topic 10)
Which of the following describes the concept of a Single Sign-On (SSO) system?

A. Users are authenticated to one system at a time.

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

**Answer:** C

**NEW QUESTION 148**
- (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 150**
- (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 152**
- (Exam Topic 10)
Which of the following assures that rules are followed in an identity management architecture?

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

**Answer:** D

**NEW QUESTION 156**
- (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 159**
- (Exam Topic 10)
Which of the following is required to determine classification and ownership?

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

**Answer:** A

**NEW QUESTION 163**
- (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 164**
- (Exam Topic 10)
A business has implemented Payment Card Industry Data Security Standard (PCI-DSS) compliant handheld credit card processing on their Wireless Local Area

Network (WLAN) topology. The network team partitioned the WLAN to create a private segment for credit card processing using a firewall to control device access and route traffic to the card processor on the Internet. What components are in the scope of PCI-DSS?

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

**Answer:** C

**NEW QUESTION 166**
- (Exam Topic 10)
Which of the following is the BEST solution to provide redundancy for telecommunications links?

A. Provide multiple links from the same telecommunications vendor.
B. Ensure that the telecommunications links connect to the network in one location.
C. Ensure that the telecommunications links connect to the network in multiple locations.
D. Provide multiple links from multiple telecommunications vendors.

**Answer:** D

**NEW QUESTION 167**
- (Exam Topic 10)
During the procurement of a new information system, it was determined that some of the security requirements were not addressed in the system specification. Which of the following is the MOST likely reason for this?

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

**Answer:** D

**NEW QUESTION 171**
- (Exam Topic 10)
When implementing a secure wireless network, which of the following supports authentication and authorization for individual client endpoints?

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

**Answer:** C

**NEW QUESTION 176**
- (Exam Topic 10)
When is security personnel involvement in the Systems Development Life Cycle (SDLC) process MOST beneficial?

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

**Answer:** C

**NEW QUESTION 177**
- (Exam Topic 10)
Which of the following is a BEST practice when traveling internationally with laptops containing Personally Identifiable Information (PII)?

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

**Answer:** B

**NEW QUESTION 181**
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
Which of the following will MOST likely allow the organization to keep risk at an acceptable level?

A. Increasing the amount of audits performed by third parties
B. Removing privileged accounts from operational staff
C. Assigning privileged functions to appropriate staff

D. Separating the security function into distinct roles

**Answer:** C

**NEW QUESTION 184**
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Which of the following is considered the MOST important priority for the information security officer?

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

**Answer:** A

**NEW QUESTION 185**
- (Exam Topic 10)
Which of the following BEST describes Recovery Time Objective (RTO)?

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

**Answer:** C

**NEW QUESTION 188**
- (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 191**
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
Following best practice, where should the permitted access for each department and job classification combination be specified?

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

**Answer:** B

**NEW QUESTION 192**
- (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 194**
- (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

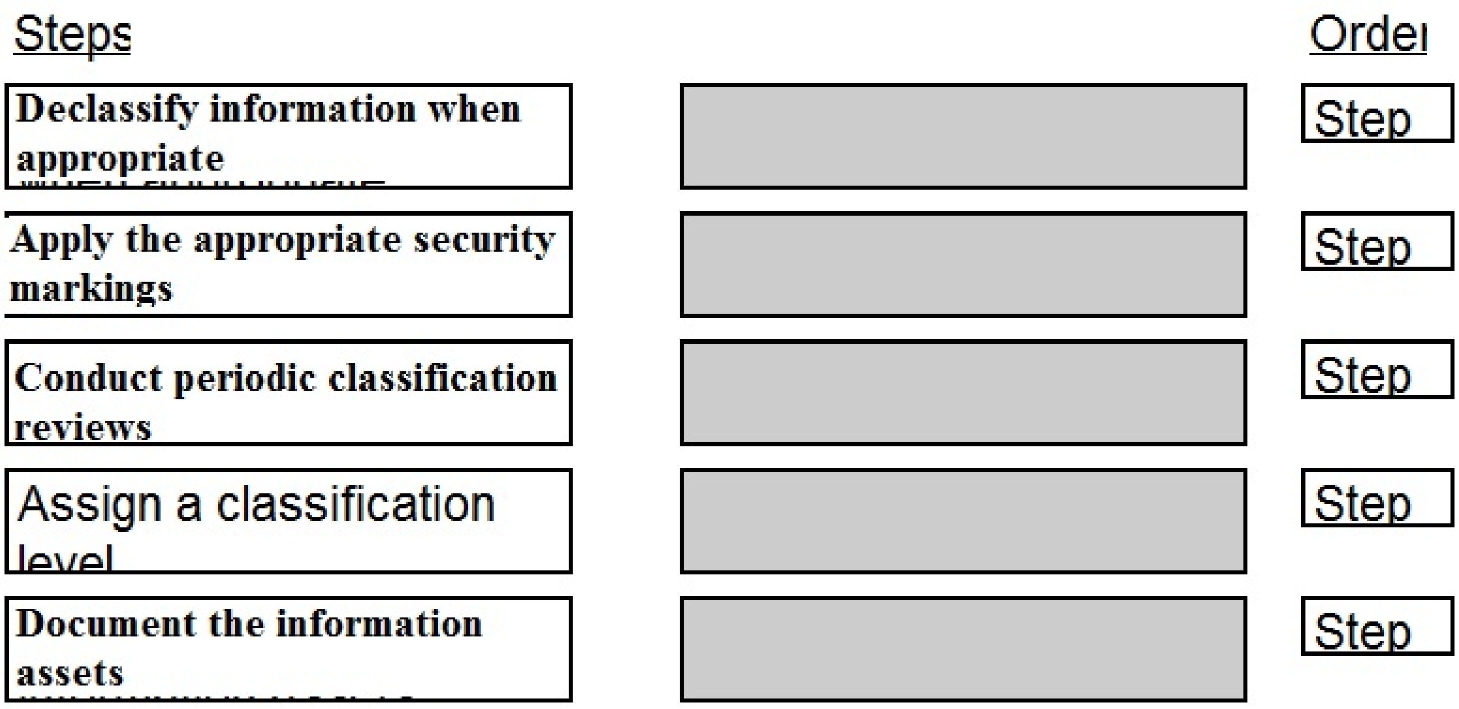
**Answer:** D

**NEW QUESTION 199**
- (Exam Topic 10)
A Business Continuity Plan (BCP) is based on

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

**Answer:** C

**NEW QUESTION 201**
- (Exam Topic 10)
Place the following information classification steps in sequential order.

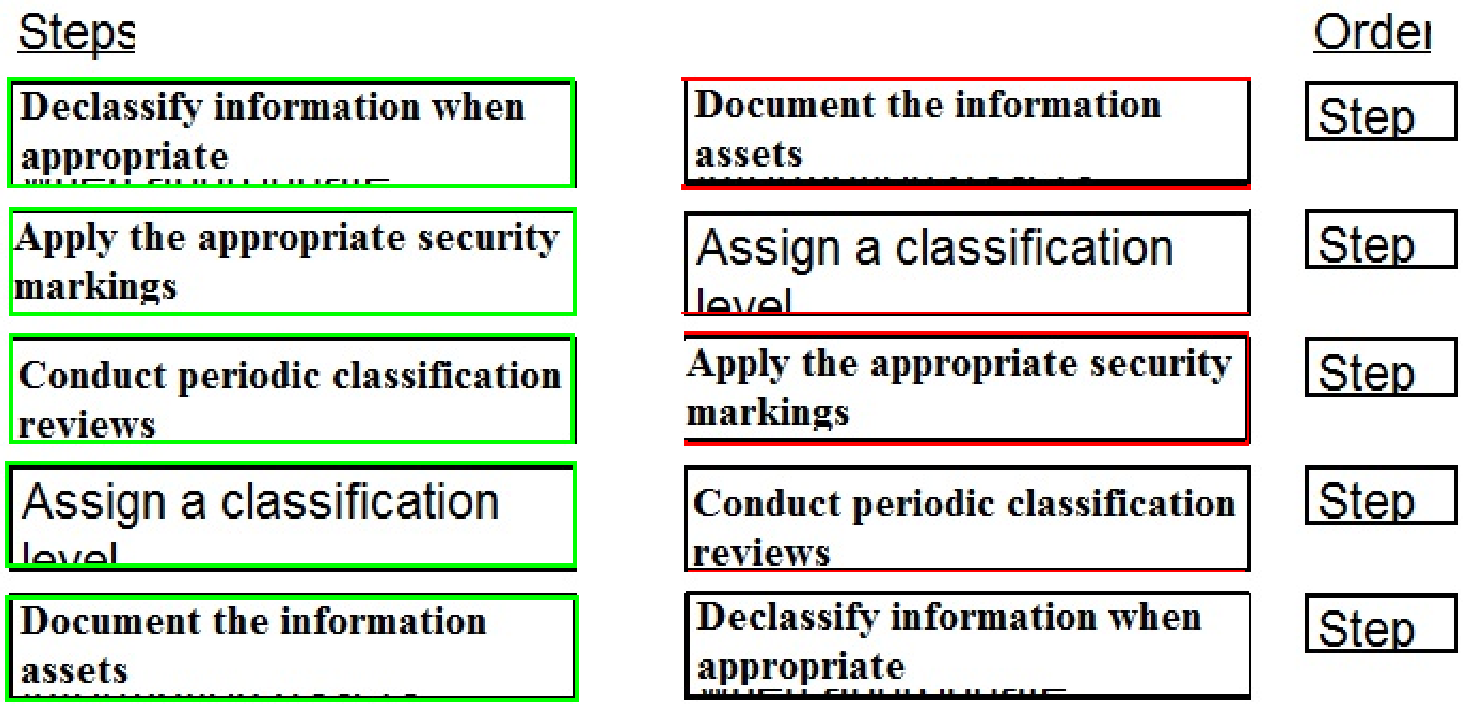


| Steps | | Order |
|---|---|---|
| Declassify information when appropriate | | Step |
| Apply the appropriate security markings | | Step |
| Conduct periodic classification reviews | | Step |
| Assign a classification level | | Step |
| Document the information assets | | Step |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**



| Steps | | 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 206**
- (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 208**
- (Exam Topic 10)
The amount of data that will be collected during an audit is PRIMARILY determined by the

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

**Answer:** A

**NEW QUESTION 209**
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
The security program can be considered effective when

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

**Answer:** D

**NEW QUESTION 210**
- (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 212**
- (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 215**
- (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 218**
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
When determining appropriate resource allocation, which of the following is MOST important to monitor?

A. Number of system compromises
B. Number of audit findings
C. Number of staff reductions
D. Number of additional assets

**Answer:** B

**NEW QUESTION 223**
- (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 226**
- (Exam Topic 10)
A risk assessment report recommends upgrading all perimeter firewalls to mitigate a particular finding. Which of the following BEST supports this recommendation?

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

**Answer:** C

**NEW QUESTION 229**
- (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 232**
- (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 233**
- (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 237**
- (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 238**
- (Exam Topic 10)
Which of the following is critical for establishing an initial baseline for software components in the operation and maintenance of applications?

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

**Answer:** B

**NEW QUESTION 239**
- (Exam Topic 10)
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
Aside from the potential records which may have been viewed, which of the following should be the PRIMARY concern regarding the database information?

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

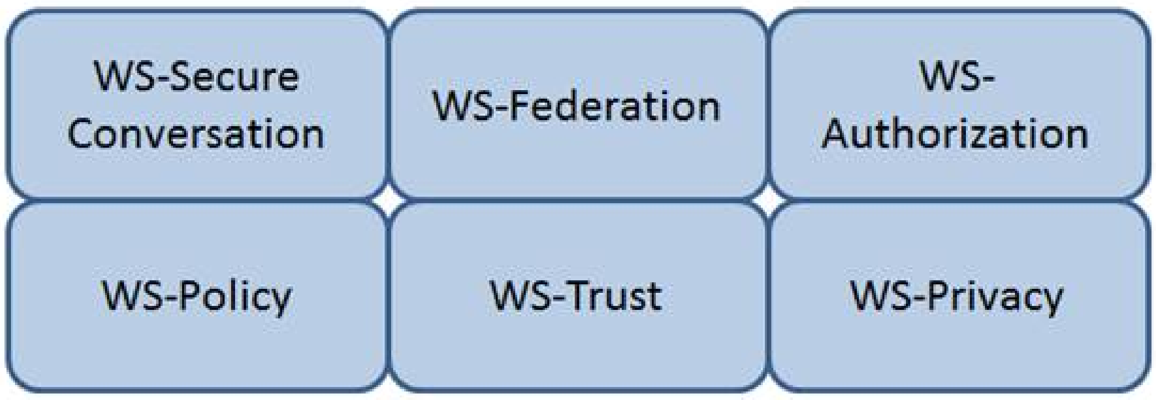
**Answer:** A

**NEW QUESTION 243**
- (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 246**
- (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 249**
- (Exam Topic 11)
What is the GREATEST challenge to identifying data leaks?

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

**Answer:** B

**NEW QUESTION 253**
- (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 254**
- (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 259**
- (Exam Topic 11)
Data remanence refers to which of the following?

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

**Answer:** D

**NEW QUESTION 262**
- (Exam Topic 11)
Which of the following PRIMARILY contributes to security incidents in web-based applications?

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

**Answer:** C

**NEW QUESTION 263**
- (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 265**
- (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 269**
- (Exam Topic 11)

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

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

**Answer:** A

**NEW QUESTION 274**
- (Exam Topic 11)
Single Sign-On (SSO) is PRIMARILY designed to address which of the following?

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

**Answer:** D

**NEW QUESTION 277**
- (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 279**
- (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 283**
- (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 285**
- (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

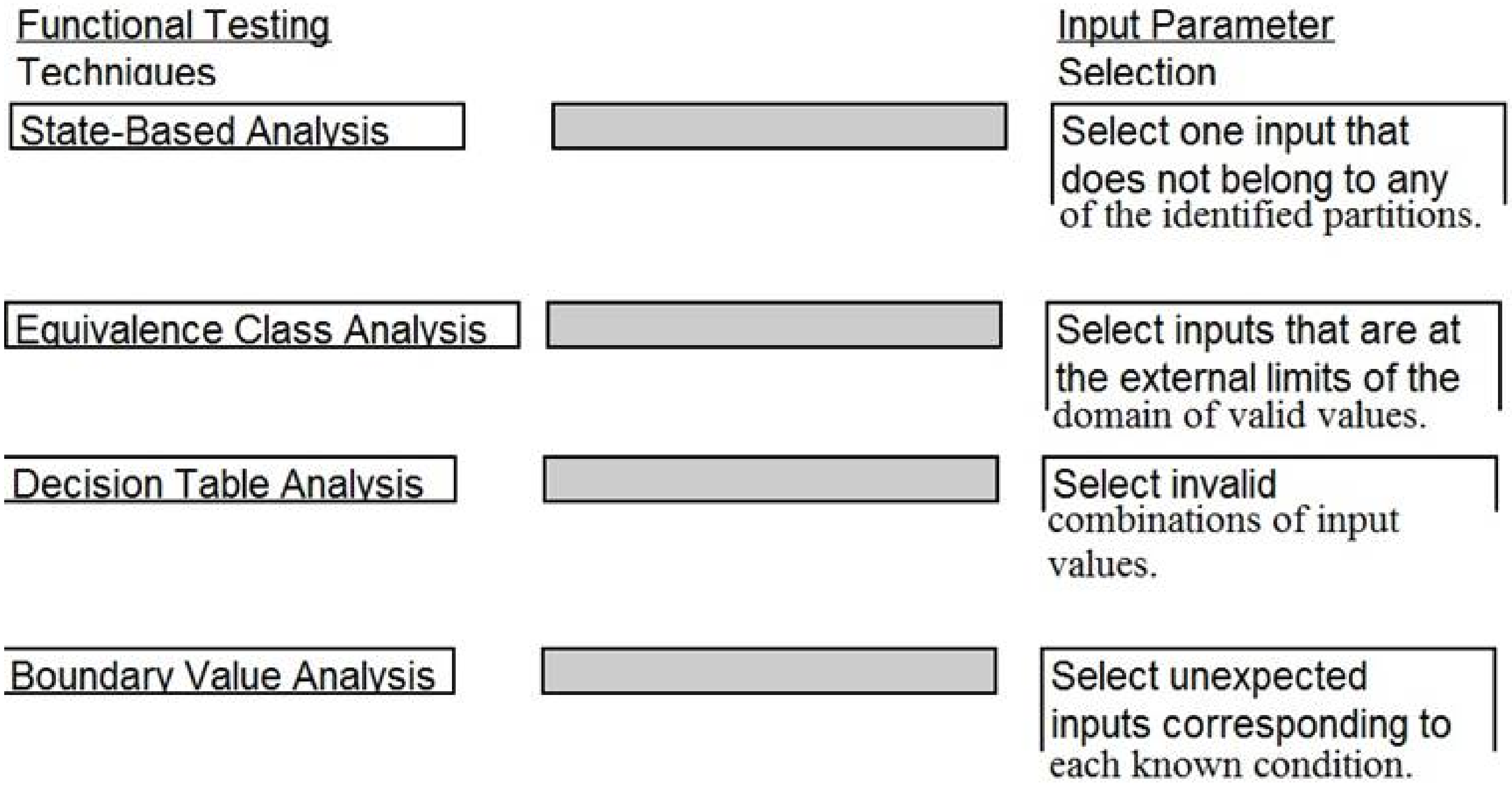
**NEW QUESTION 289**
- (Exam Topic 11)
Which of the following is the PRIMARY security concern associated with the implementation of smart cards?

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 294**

- (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.

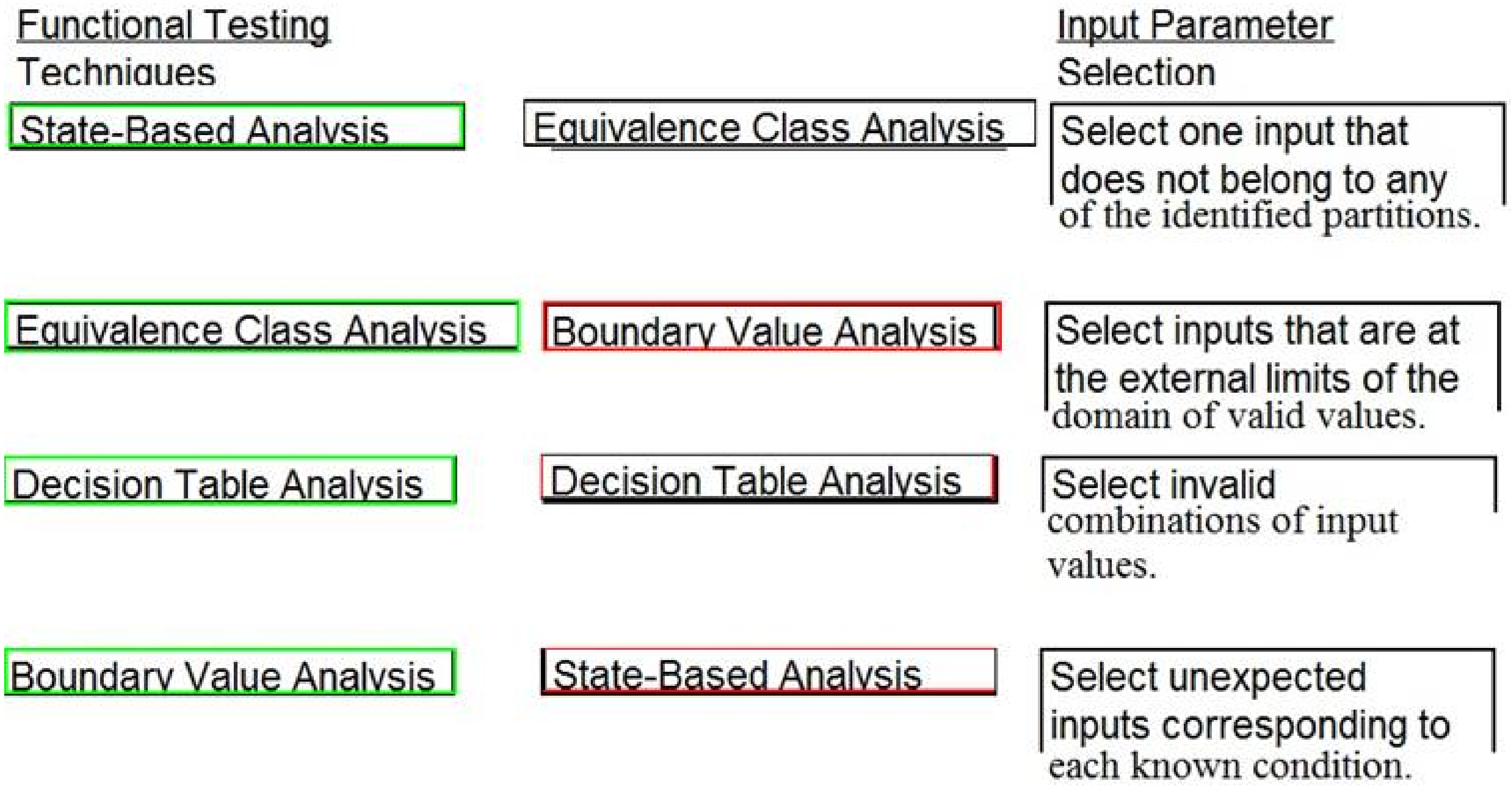


| Functional Testing Techniques | | Input Parameter Selection |
|---|---|---|
| State-Based Analysis | | Select one input that does not belong to any of the identified partitions. |
| Equivalence Class Analysis | | Select inputs that are at the external limits of the domain of valid values. |
| Decision 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 298**
- (Exam Topic 11)
To protect auditable information, which of the following MUST be configured to only allow read access?

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

**Answer:** B

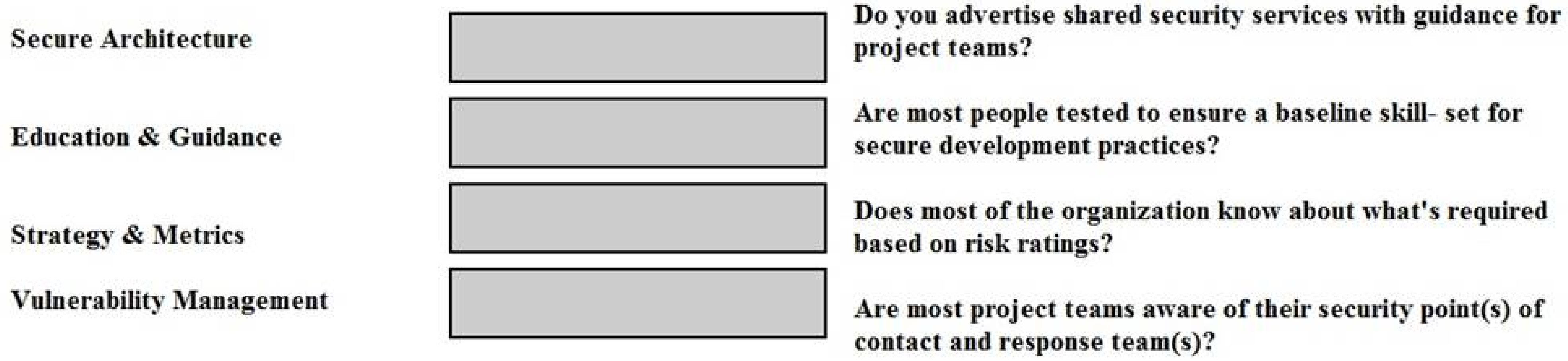
**NEW QUESTION 303**
- (Exam Topic 11)
What type of encryption is used to protect sensitive data in transit over a network?

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 304**
- (Exam Topic 11)
Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).



Secure Architecture

Education & Guidance

Strategy & Metrics

Vulnerability Management

Do you advertise shared security services with guidance for project teams?

Are most people tested to ensure a baseline skill- set for secure development practices?

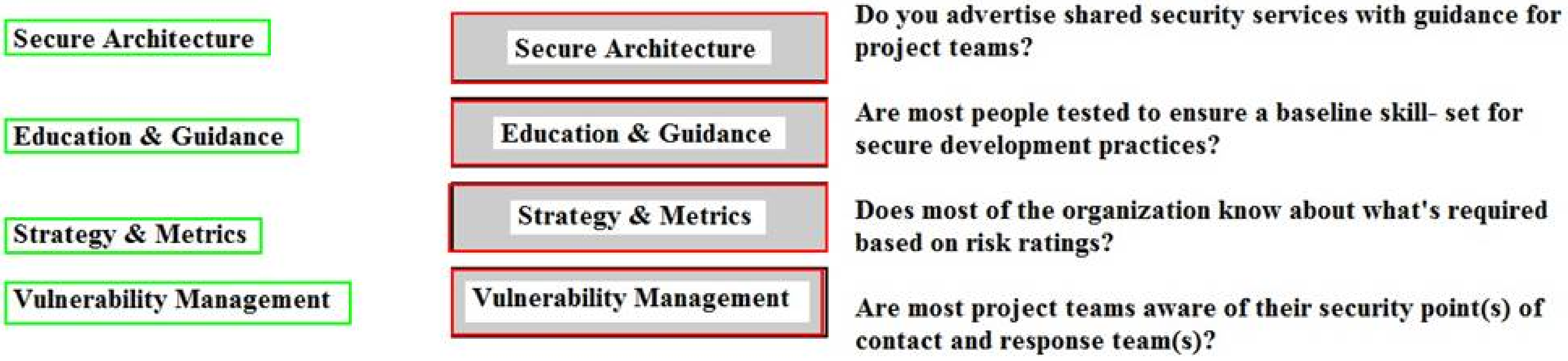
Does most of the organization know about what's required based on risk ratings?

Are most project teams aware of their security point(s) of contact and response team(s)?

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**



Secure Architecture

Education & Guidance

Strategy & Metrics

Vulnerability Management

Secure Architecture — Do you advertise shared security services with guidance for project teams?

Education & Guidance — Are most people tested to ensure a baseline skill- set for secure development practices?

Strategy & Metrics — Does most of the organization know about what's required based on risk ratings?

Vulnerability Management — Are most project teams aware of their security point(s) of contact and response team(s)?

**NEW QUESTION 307**
- (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

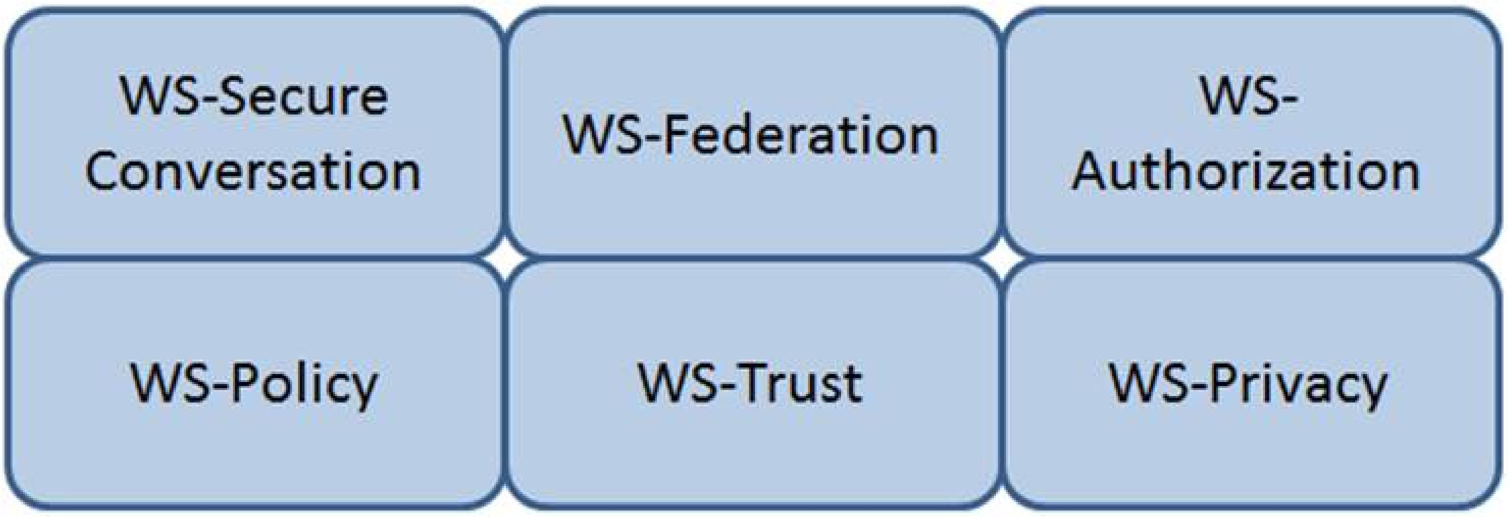
**Answer:** A

**NEW QUESTION 310**
- (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 314**
- (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 319**
- (Exam Topic 11)
Sensitive customer data is going to be added to a database. What is the MOST effective implementation for ensuring data privacy?

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

**Answer:** B

**NEW QUESTION 324**
- (Exam Topic 11)
Data leakage of sensitive information is MOST often concealed by which of the following?

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

**Answer:** A

**NEW QUESTION 328**
- (Exam Topic 11)
What does an organization FIRST review to assure compliance with privacy requirements?

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

**Answer:** C

**NEW QUESTION 331**

- (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 334**
- (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 338**
- (Exam Topic 11)
Which of the following questions can be answered using user and group entitlement reporting?

A. When a particular file was last accessed by a user
B. Change control activities for a particular group of users
C. The number of failed login attempts for a particular user
D. Where does a particular user have access within the network

**Answer:** D

**NEW QUESTION 340**
- (Exam Topic 11)
For an organization considering two-factor authentication for secure network access, which of the following is MOST secure?

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

**Answer:** D

**NEW QUESTION 343**
- (Exam Topic 11)
What is the GREATEST challenge of an agent-based patch management solution?

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

**Answer:** B

**NEW QUESTION 344**
- (Exam Topic 11)
Which of the following protocols would allow an organization to maintain a centralized list of users that can read a protected webpage?

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

**Answer:** A

**NEW QUESTION 347**
- (Exam Topic 11)
Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?

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

**Answer:** C

**NEW QUESTION 349**
- (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 354**
- (Exam Topic 11)
Which of the following is the MOST important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?

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

**Answer:** D

**NEW QUESTION 359**
- (Exam Topic 11)
By carefully aligning the pins in the lock, which of the following defines the opening of a mechanical lock without the proper key?

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

**Answer:** B

**NEW QUESTION 361**
- (Exam Topic 12)
The restoration priorities of a Disaster Recovery Plan (DRP) are based on which of the following documents?

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

**Answer:** B

**NEW QUESTION 363**
- (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 367**
- (Exam Topic 12)
A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

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

**Answer:** A

**NEW QUESTION 372**
- (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 375**
- (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 379**
- (Exam Topic 12)
What type of wireless network attack BEST describes an Electromagnetic Pulse (EMP) attack?

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

**Answer:** B

**NEW QUESTION 381**
- (Exam Topic 12)
Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item?

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

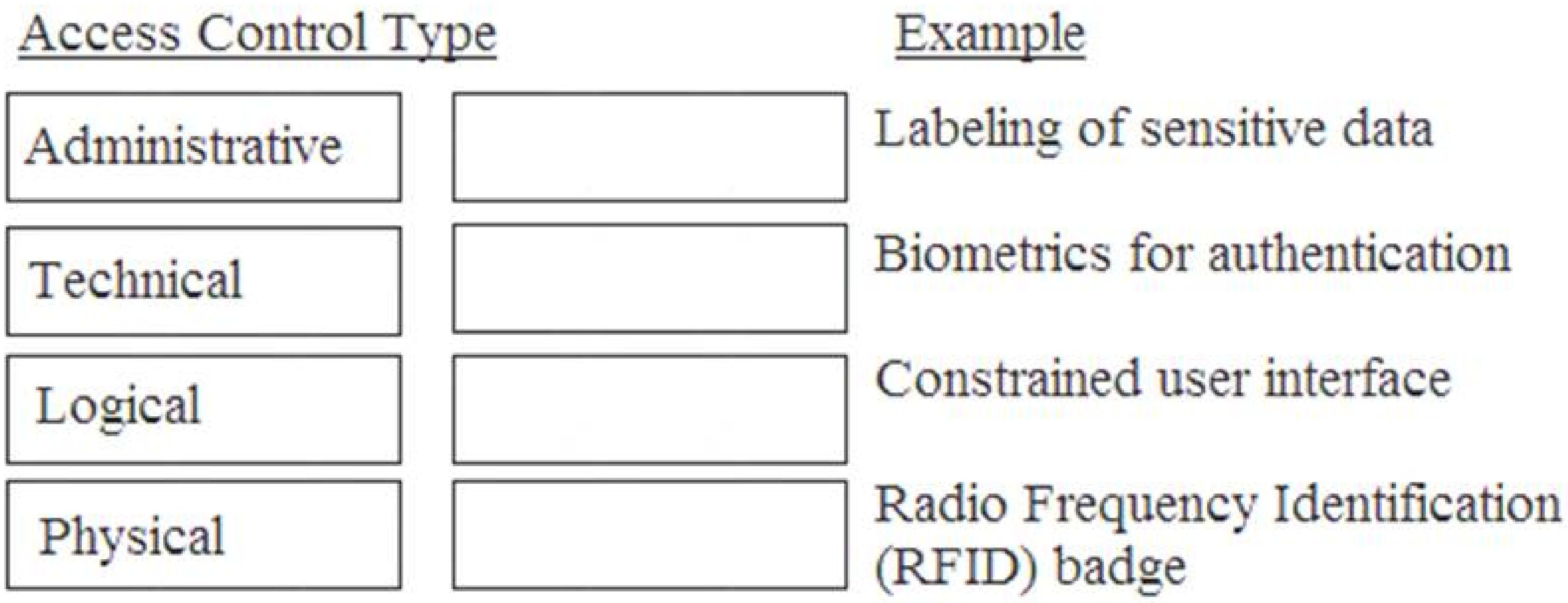
**Answer:** D

**NEW QUESTION 386**
- (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 388**
- (Exam Topic 12)
Match the access control type to the example of the control type. Drag each access control type net to its corresponding example.



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

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 391**
- (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 396**
- (Exam Topic 12)
Although code using a specific program language may not be susceptible to a buffer overflow attack,

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

**Answer:** C

**NEW QUESTION 399**
- (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 404**
- (Exam Topic 12)
Which of the following is needed to securely distribute symmetric cryptographic keys?

A. Officially approved Public-Key Infrastructure (PKI) Class 3 or Class 4 certificates
B. Officially approved and compliant key management technology and processes
C. An organizationally approved communication protection policy and key management plan
D. Hardware tokens that protect the user's private key.

**Answer:** C

**NEW QUESTION 407**
- (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 408**
- (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 413**
- (Exam Topic 12)

An organization's information security strategic plan MUST be reviewed

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

**Answer:** C

**NEW QUESTION 414**
- (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 419**
- (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 424**
- (Exam Topic 12)
A security architect plans to reference a Mandatory Access Control (MAC) model for implementation. This indicates that which of the following properties are being prioritized?

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

**Answer:** C

**NEW QUESTION 428**
- (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 432**
- (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 437**
- (Exam Topic 12)
Reciprocal backup site agreements are considered to be

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

**Answer:** B

**NEW QUESTION 440**
- (Exam Topic 12)
What balance MUST be considered when web application developers determine how informative application error messages should be constructed?

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

**Answer:** A

**NEW QUESTION 443**
- (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 444**
- (Exam Topic 13)
Which of the following is the MOST important security goal when performing application interface testing?

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

**Answer:** B

**NEW QUESTION 446**
- (Exam Topic 13)
Due to system constraints, a group of system administrators must share a high-level access set of credentials. Which of the following would be MOST appropriate to implement?

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

**Answer:** C

**Explanation:**
Section: Security Operations

**NEW QUESTION 449**
- (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 453**
- (Exam Topic 13)
What protocol is often used between gateway hosts on the Internet?

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

**Answer:** B

**NEW QUESTION 457**
- (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 458**
- (Exam Topic 13)
An organization plan on purchasing a custom software product developed by a small vendor to support its
business model. Which unique consideration should be made part of the contractual agreement potential long-term risks associated with creating this dependency?

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

**Answer:** B

**NEW QUESTION 459**
- (Exam Topic 13)
What capability would typically be included in a commercially available software package designed for access control?

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

**Answer:** A

**NEW QUESTION 463**
- (Exam Topic 13)
Which of the following combinations would MOST negatively affect availability?

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

**Answer:** A

**NEW QUESTION 466**
- (Exam Topic 13)
Which of the following mechanisms will BEST prevent a Cross-Site Request Forgery (CSRF) attack?

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

**Answer:** C

**NEW QUESTION 471**
- (Exam Topic 13)
Which factors MUST be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?

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

**Answer:** A

**NEW QUESTION 473**
- (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 478**
- (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 480**
- (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 484**
- (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 487**
- (Exam Topic 13)
When developing solutions for mobile devices, in which phase of the Software Development Life Cycle (SDLC) should technical limitations related to devices be specified?

A. Implementation
B. Initiation
C. Review
D. Development

**Answer:** A

**NEW QUESTION 491**
- (Exam Topic 13)
Mandatory Access Controls (MAC) are based on:

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

**Answer:** A

**NEW QUESTION 494**
- (Exam Topic 13)
What does electronic vaulting accomplish?

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

**Answer:** A

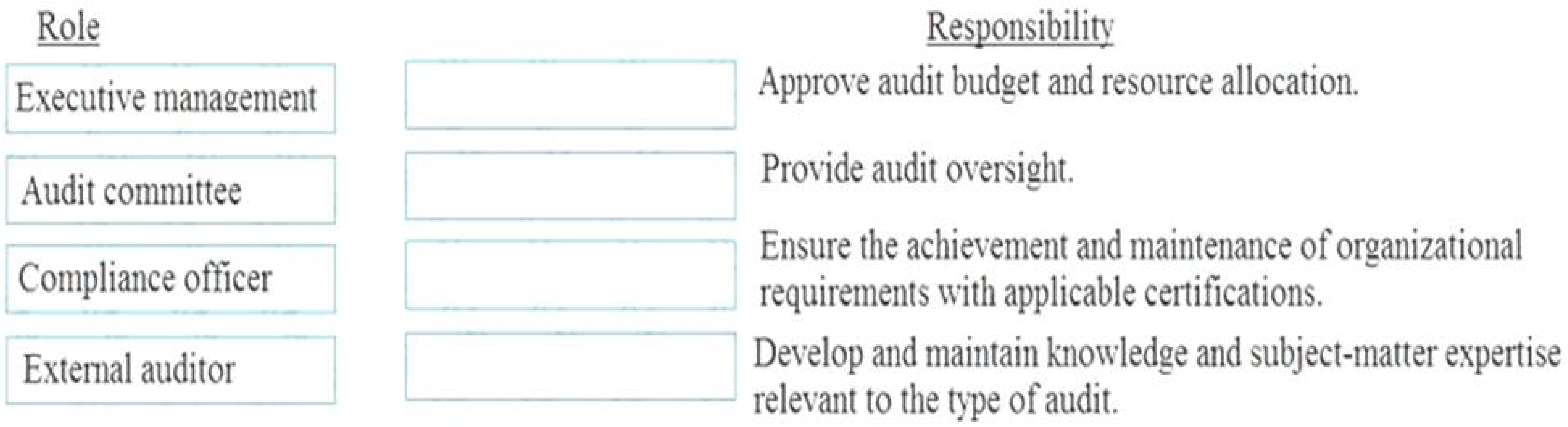
**Explanation:**
Section: Security Operations

**NEW QUESTION 496**
- (Exam Topic 13)
Which of the following is considered a secure coding practice?

A. Use concurrent access for shared variables and resources
B. Use checksums to verify the integrity of libraries
C. Use new code for common tasks
D. Use dynamic execution functions to pass user supplied data

**Answer:** B

**NEW QUESTION 498**
- (Exam Topic 13)
Match the functional roles in an external audit to their responsibilities. Drag each role on the left to its corresponding responsibility on the right. Select and Place:

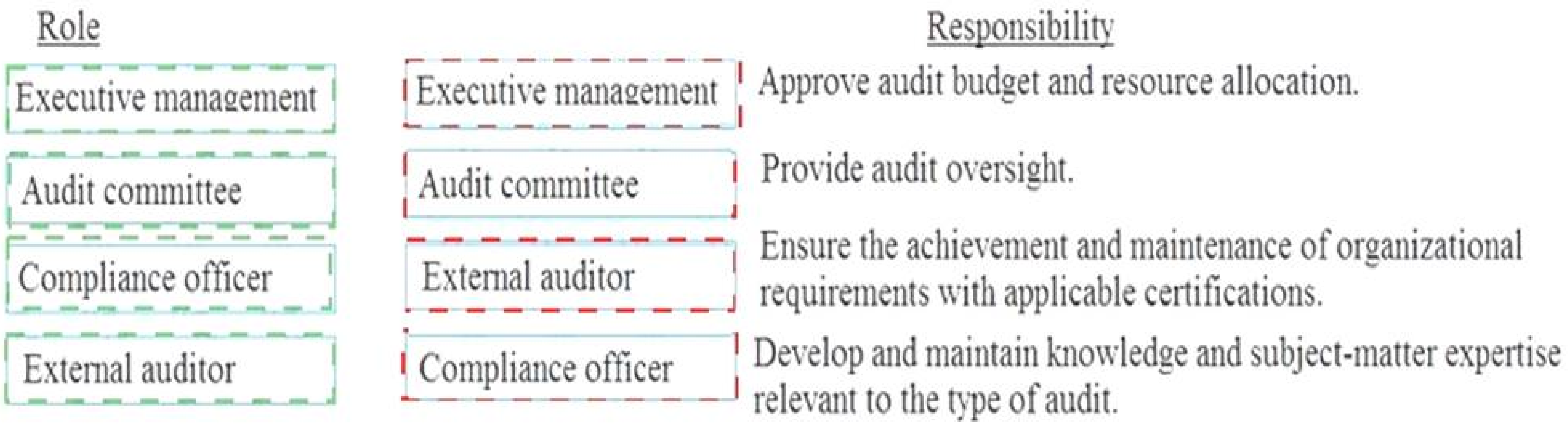


| Role | | Responsibility |
|---|---|---|
| Executive management | | Approve audit budget and resource allocation. |
| Audit committee | | Provide audit oversight. |
| Compliance officer | | Ensure the achievement and maintenance of organizational requirements with applicable certifications. |
| External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

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**



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

**NEW QUESTION 500**
- (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 503**
- (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 507**
- (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 508**
- (Exam Topic 13)
What MUST each information owner do when a system contains data from multiple information owners?

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

**Answer:** C

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

**NEW QUESTION 513**
- (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 514**
- (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 519**
- (Exam Topic 13)
Who has the PRIMARY responsibility to ensure that security objectives are aligned with organization goals?

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

**Answer:** C

**NEW QUESTION 524**
- (Exam Topic 13)
Which of the following is the MOST appropriate action when reusing media that contains sensitive data?

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

**Answer:** B

**NEW QUESTION 529**
- (Exam Topic 13)
Which of the following alarm systems is recommended to detect intrusions through windows in a high-noise, occupied environment?

A. Acoustic sensor
B. Motion sensor
C. Shock sensor

D. Photoelectric sensor

**Answer:** C

**NEW QUESTION 530**
- (Exam Topic 13)
The MAIN use of Layer 2 Tunneling Protocol (L2TP) is to tunnel data

A. through a firewall at the Session layer
B. through a firewall at the Transport layer
C. in the Point-to-Point Protocol (PPP)
D. in the Payload Compression Protocol (PCP)

**Answer:** C

**NEW QUESTION 531**
- (Exam Topic 13)
Which of the following is BEST achieved through the use of eXtensible Access Markup Language (XACML)?

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

**Answer:** D

**NEW QUESTION 532**
......