Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

https://www.2passeasy.com/dumps/CISSP/

NEW QUESTION 1
- (Exam Topic 1)
A company whose Information Technology (IT) services are being delivered from a Tier 4 data center, is preparing a companywide Business Continuity Planning (BCP). Which of the following failures should the IT manager be concerned with?

A. Application
B. Storage
C. Power
D. Network

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
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 3
- (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 4
- (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 5
- (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 6
- (Exam Topic 1)
Intellectual property rights are PRIMARY concerned with which of the following?

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

Answer: D

NEW QUESTION 7
- (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 8
- (Exam Topic 2)
Which of the following is MOST important when assigning ownership of an asset to a department?

A. The department should report to the business owner
B. Ownership of the asset should be periodically reviewed
C. Individual accountability should be ensured
D. All members should be trained on their responsibilities

Answer: B

NEW QUESTION 9
- (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 10
- (Exam Topic 3)
Who in the organization is accountable for classification of data information assets?

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

Answer: A

NEW QUESTION 10
- (Exam Topic 3)
What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?

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

Answer: D

NEW QUESTION 11
- (Exam Topic 4)
An input validation and exception handling vulnerability has been discovered on a critical web-based system. Which of the following is MOST suited to quickly implement a control?

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

Answer: A

NEW QUESTION 13
- (Exam Topic 4)
Which of the following is used by the Point-to-Point Protocol (PPP) to determine packet formats?

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

Answer: B

NEW QUESTION 17
- (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 20
- (Exam Topic 5)
Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee's salary?

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

Answer: C

NEW QUESTION 22
- (Exam Topic 6)
A Virtual Machine (VM) environment has five guest Operating Systems (OS) and provides strong isolation. What MUST an administrator review to audit a user's access to data files?

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

Answer: A

NEW QUESTION 23
- (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 27
- (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 28
- (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 29
- (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 32
- (Exam Topic 7)
An organization is found lacking the ability to properly establish performance indicators for its Web hosting solution during an audit. What would be the MOST probable cause?

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

Answer: D

NEW QUESTION 35
- (Exam Topic 7)
With what frequency should monitoring of a control occur when implementing Information Security Continuous Monitoring (ISCM) solutions?

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

Answer: B

NEW QUESTION 38
- (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 42
- (Exam Topic 8)
What is the BEST approach to addressing security issues in legacy web applications?

A. Debug the security issues
B. Migrate to newer, supported applications where possible
C. Conduct a security assessment
D. Protect the legacy application with a web application firewall

Answer: D

NEW QUESTION 44
- (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 49
- (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 54
- (Exam Topic 9)
Internet Protocol (IP) source address spoofing is used to defeat

A. address-based authentication.
B. Address Resolution Protocol (ARP).
C. Reverse Address Resolution Protocol (RARP).
D. Transmission Control Protocol (TCP) hijacking.

Answer: A

NEW QUESTION 59
- (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 60
- (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 65
- (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 66
- (Exam Topic 9)
What technique BEST describes antivirus software that detects viruses by watching anomalous behavior?

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

Answer: D

NEW QUESTION 68
- (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 72
- (Exam Topic 9)
What is the term commonly used to refer to a technique of authenticating one machine to another by forging packets from a trusted source?

A. Man-in-the-Middle (MITM) attack
B. Smurfing
C. Session redirect
D. Spoofing

Answer: D

NEW QUESTION 77
- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 80
- (Exam Topic 9)
The stringency of an Information Technology (IT) security assessment will be determined by the

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

Answer: C

NEW QUESTION 82
- (Exam Topic 9)
Including a Trusted Platform Module (TPM) in the design of a computer system is an example of a technique to what?

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

Answer: D

NEW QUESTION 85
- (Exam Topic 9)
Which one of these risk factors would be the LEAST important consideration in choosing a building site for a new computer facility?

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

Answer: C

NEW QUESTION 90
- (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 94
- (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 96
- (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 98
- (Exam Topic 9)
Which of the following is the best practice for testing a Business Continuity Plan (BCP)?

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

Answer: B

NEW QUESTION 102
- (Exam Topic 9)
In a financial institution, who has the responsibility for assigning the classification to a piece of information?

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

Answer: C

NEW QUESTION 105
- (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 109
- (Exam Topic 9)
What security management control is MOST often broken by collusion?

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

Answer: B

NEW QUESTION 112
- (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 113
- (Exam Topic 9)
Which one of the following is the MOST important in designing a biometric access system if it is essential that no one other than authorized individuals are admitted?

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

Answer: A

NEW QUESTION 115
- (Exam Topic 9)
Which of the following is an essential element of a privileged identity lifecycle management?

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

Answer:

A

NEW QUESTION 118
- (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 120
- (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 123
- (Exam Topic 9)
Which of the following statements is TRUE for point-to-point microwave transmissions?

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

Answer: D

NEW QUESTION 124
- (Exam Topic 9)
The use of strong authentication, the encryption of Personally Identifiable Information (PII) on database servers, application security reviews, and the encryption of data transmitted across networks provide

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

Answer: B

NEW QUESTION 127
- (Exam Topic 9)
Which of the following is the BEST way to verify the integrity of a software patch?

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

Answer: A

NEW QUESTION 131
- (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 133
- (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 138
- (Exam Topic 9)
Which one of the following describes granularity?

A. Maximum number of entries available in an Access Control List (ACL)
B. Fineness to which a trusted system can authenticate users
C. Number of violations divided by the number of total accesses
D. Fineness to which an access control system can be adjusted

Answer: D

NEW QUESTION 139
- (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 141
- (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 143
- (Exam Topic 9)
When transmitting information over public networks, the decision to encrypt it should be based on

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

Answer: C

NEW QUESTION 146
- (Exam Topic 9)
Which of the following would be the FIRST step to take when implementing a patch management program?

A. Perform automatic deployment of patches.
B. Monitor for vulnerabilities and threats.
C. Prioritize vulnerability remediation.
D. Create a system inventory.

Answer: D

NEW QUESTION 147
- (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 149
- (Exam Topic 9)
What is the ultimate objective of information classification?

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

Answer: B

NEW QUESTION 150
- (Exam Topic 9)
Following the completion of a network security assessment, which of the following can BEST be demonstrated?

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

Answer: A

NEW QUESTION 154
- (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 158
- (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 159
- (Exam Topic 9)
When designing a networked Information System (IS) where there will be several different types of individual access, what is the FIRST step that should be taken to ensure all access control requirements are addressed?

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

Answer: B

NEW QUESTION 160
- (Exam Topic 9)
Which of the following actions should be performed when implementing a change to a database schema in a production system?

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

Answer: D

NEW QUESTION 163
- (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 168

- (Exam Topic 9)
Passive Infrared Sensors (PIR) used in a non-climate controlled environment should

A. reduce the detected object temperature in relation to the background temperature.
B. increase the detected object temperature in relation to the background temperature.
C. automatically compensate for variance in background temperature.
D. detect objects of a specific temperature independent of the background temperature.

Answer: C

NEW QUESTION 171
- (Exam Topic 9)
Which one of the following affects the classification of data?

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

Answer: A

NEW QUESTION 175
- (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 180
- (Exam Topic 9)
The goal of software assurance in application development is to

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

Answer: C

NEW QUESTION 185
- (Exam Topic 9)
An engineer in a software company has created a virus creation tool. The tool can generate thousands of polymorphic viruses. The engineer is planning to use the tool in a controlled environment to test the company's next generation virus scanning software. Which would BEST describe the behavior of the engineer and why?

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

Answer: A

NEW QUESTION 186
- (Exam Topic 9)
Which of the following Disaster Recovery (DR) sites is the MOST difficult to test?

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

Answer: B

NEW QUESTION 189
- (Exam Topic 9)
Which of the following statements is TRUE of black box testing?

A. Only the functional specifications are known to the test planner.
B. Only the source code and the design documents are known to the test planner.
C. Only the source code and functional specifications are known to the test planner.
D. Only the design documents and the functional specifications are known to the test planner.

Answer: A

NEW QUESTION 193
- (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 194
- (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 199
- (Exam Topic 9)
In Disaster Recovery (DR) and business continuity training, which BEST describes a functional drill?

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

Answer: B

NEW QUESTION 204
- (Exam Topic 10)
What is the MAIN feature that onion routing networks offer?

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

Answer: C

NEW QUESTION 205
- (Exam Topic 10)
Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?

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

Answer: A

NEW QUESTION 207
- (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 212
- (Exam Topic 10)
Which of the following provides effective management assurance for a Wireless Local Area Network (WLAN)?

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

Answer: A

NEW QUESTION 217
- (Exam Topic 10)
If an attacker in a SYN flood attack uses someone else's valid host address as the source address, the system under attack will send a large number of Synchronize/Acknowledge (SYN/ACK) packets to the

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

Answer: D

NEW QUESTION 221
- (Exam Topic 10)
An online retail company has formulated a record retention schedule for customer transactions. Which of the following is a valid reason a customer transaction is kept beyond the retention schedule?

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

Answer: A

NEW QUESTION 224
- (Exam Topic 10)
What does secure authentication with logging provide?

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

Answer: B

NEW QUESTION 227
- (Exam Topic 10)
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
If it is discovered that large quantities of information have been copied by the unauthorized individual, what attribute of the data has been compromised?

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

Answer: D

NEW QUESTION 232
- (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 234
- (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 238

- (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 241
- (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 246
- (Exam Topic 10)
Which of the following are required components for implementing software configuration management systems?

A. Audit control and signoff
B. User training and acceptance
C. Rollback and recovery processes
D. Regression testing and evaluation

Answer: C

NEW QUESTION 248
- (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 249
- (Exam Topic 10)
What is a common challenge when implementing Security Assertion Markup Language (SAML) for identity integration between on-premise environment and an external identity provider service?

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

Answer: A

NEW QUESTION 251
- (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 252
- (Exam Topic 10)
Which of the following methods provides the MOST protection for user credentials?

A. Forms-based authentication

B. Digest authentication
C. Basic authentication
D. Self-registration

Answer: B

NEW QUESTION 255
- (Exam Topic 10)
Which of the following is a MAJOR consideration in implementing a Voice over IP (VoIP) network?

A. Use of a unified messaging.
B. Use of separation for the voice network.
C. Use of Network Access Control (NAC) on switches.
D. Use of Request for Comments (RFC) 1918 addressing.

Answer: B

NEW QUESTION 257
- (Exam Topic 10)
Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization’s Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following documents explains the proper use of the organization's assets?

A. Human resources policy
B. Acceptable use policy
C. Code of ethics
D. Access control policy

Answer: B

NEW QUESTION 258
- (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 263
- (Exam Topic 10)
Which of the following is a detective access control mechanism?

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

Answer: A

NEW QUESTION 266
- (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 271
- (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 274
- (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 277
- (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 282
- (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 286
- (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 291
- (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

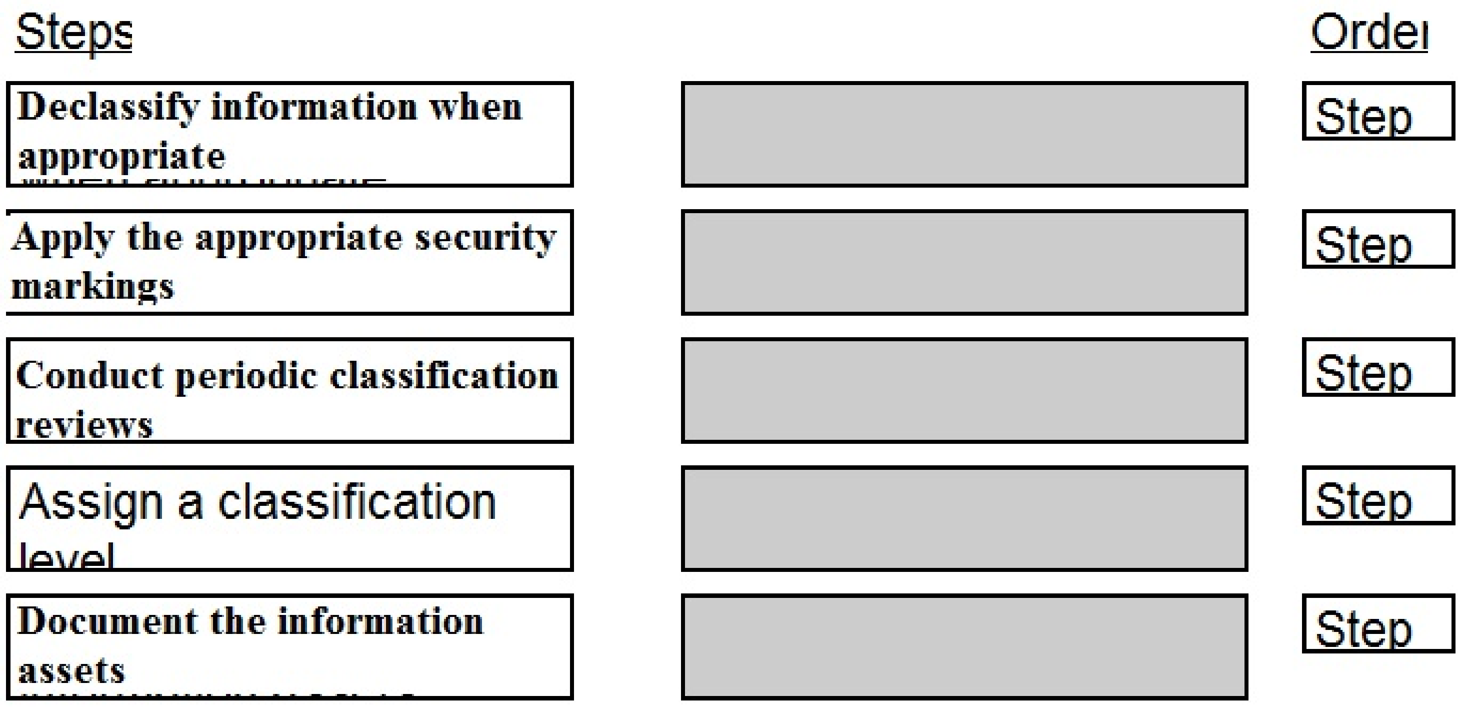
Answer: B

NEW QUESTION 293
- (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 295
- (Exam Topic 10)
Place the following information classification steps in sequential order.

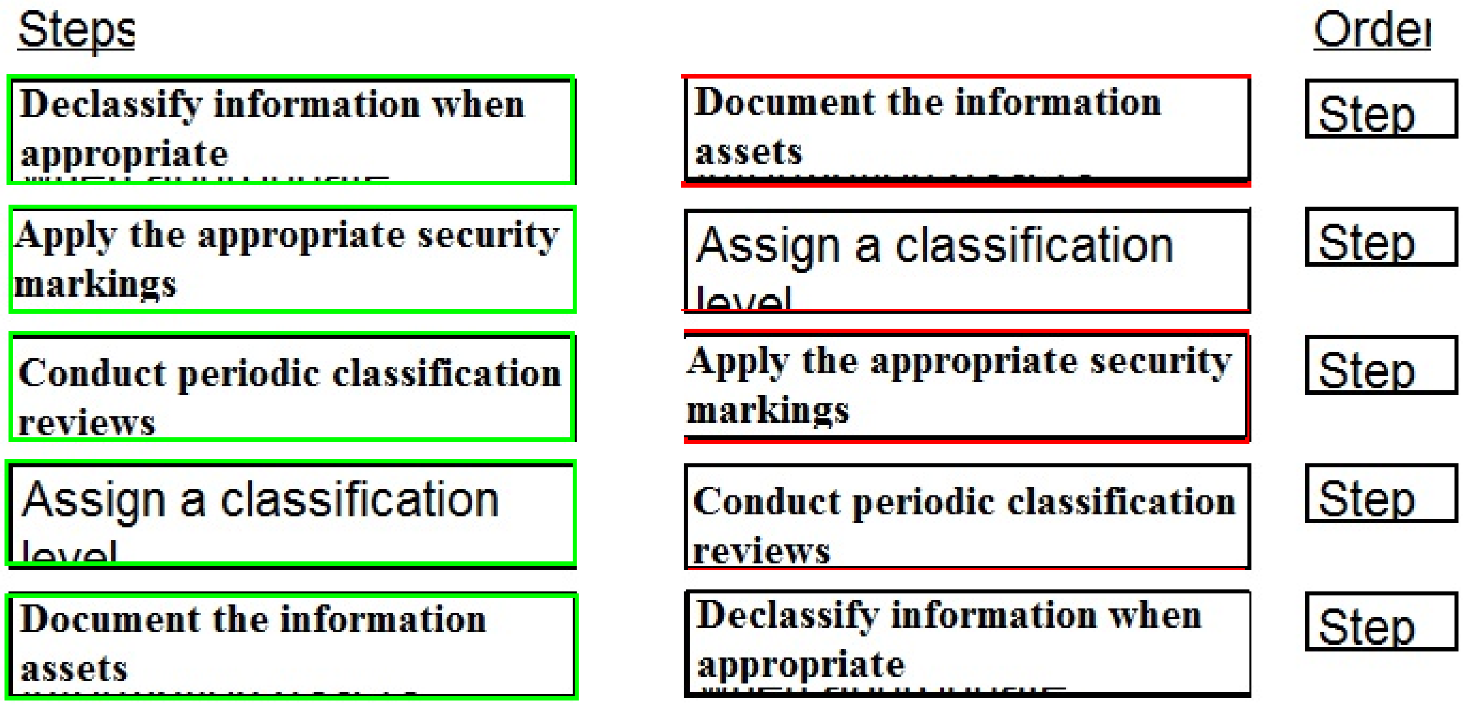


Steps		Order
Declassify information when appropriate		Step
Apply the appropriate security markings		Step
Conduct periodic classification reviews		Step
Assign a classification level		Step
Document the information assets		Step

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 296
- (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 298
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
In addition to authentication at the start of the user session, best practice would require re-authentication

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

Answer: D

NEW QUESTION 302
- (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 303
- (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 308
- (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 311
- (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 316
- (Exam Topic 10)
Which of the following is the BEST way to determine if a particular system is able to identify malicious software without executing it?

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

Answer: B

NEW QUESTION 319
- (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 321
- (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 325
- (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 327
- (Exam Topic 11)
Which of the following BEST describes the purpose of performing security certification?

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

Answer: B

NEW QUESTION 328
- (Exam Topic 11)
Which of the following prevents improper aggregation of privileges in Role Based Access Control (RBAC)?

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

Answer: B

NEW QUESTION 331
- (Exam Topic 11)
A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

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

Answer: A

NEW QUESTION 334
- (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 338
- (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 339
- (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 342
- (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).

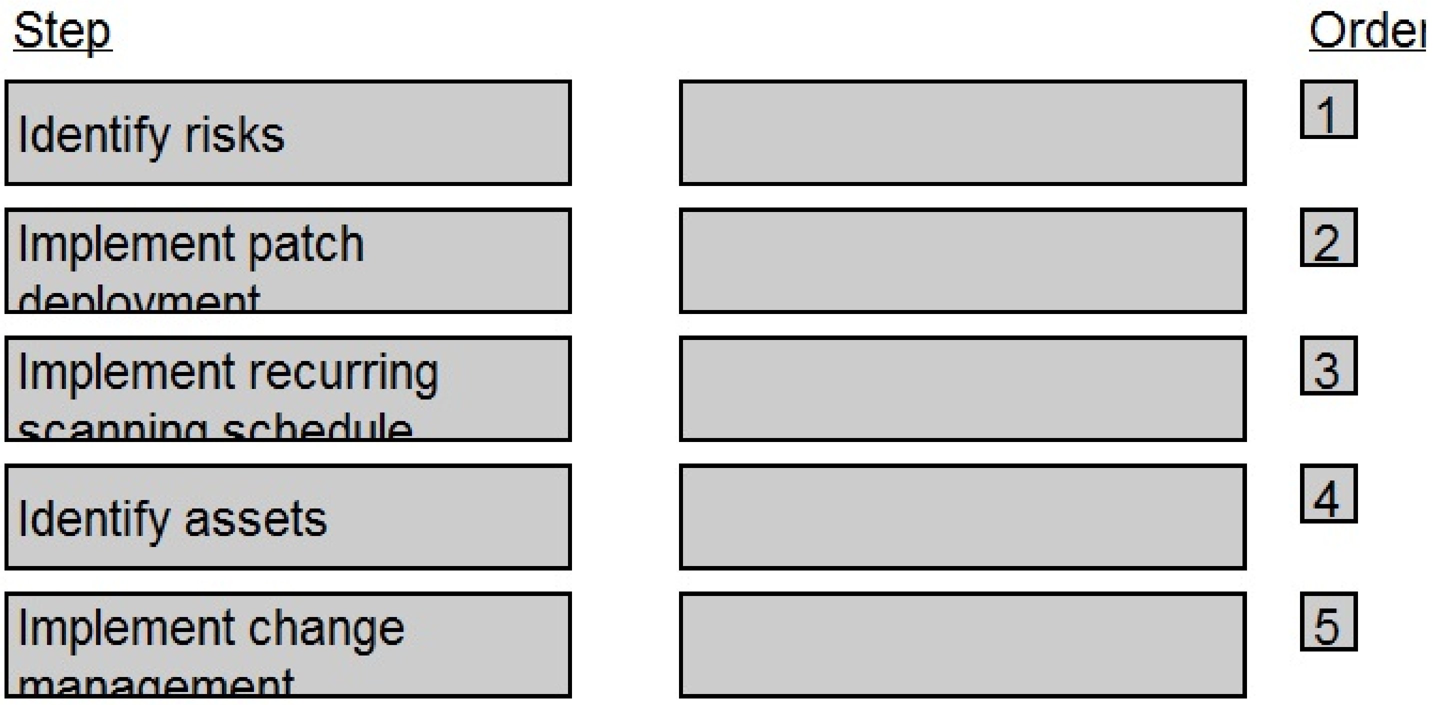
Answer: A

NEW QUESTION 343
- (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 345
- (Exam Topic 11)
Order the below steps to create an effective vulnerability management process.



Step

Identify risks

Implement patch deployment

Implement recurring scanning schedule

Identify assets

Implement change management

Order

1

2

3

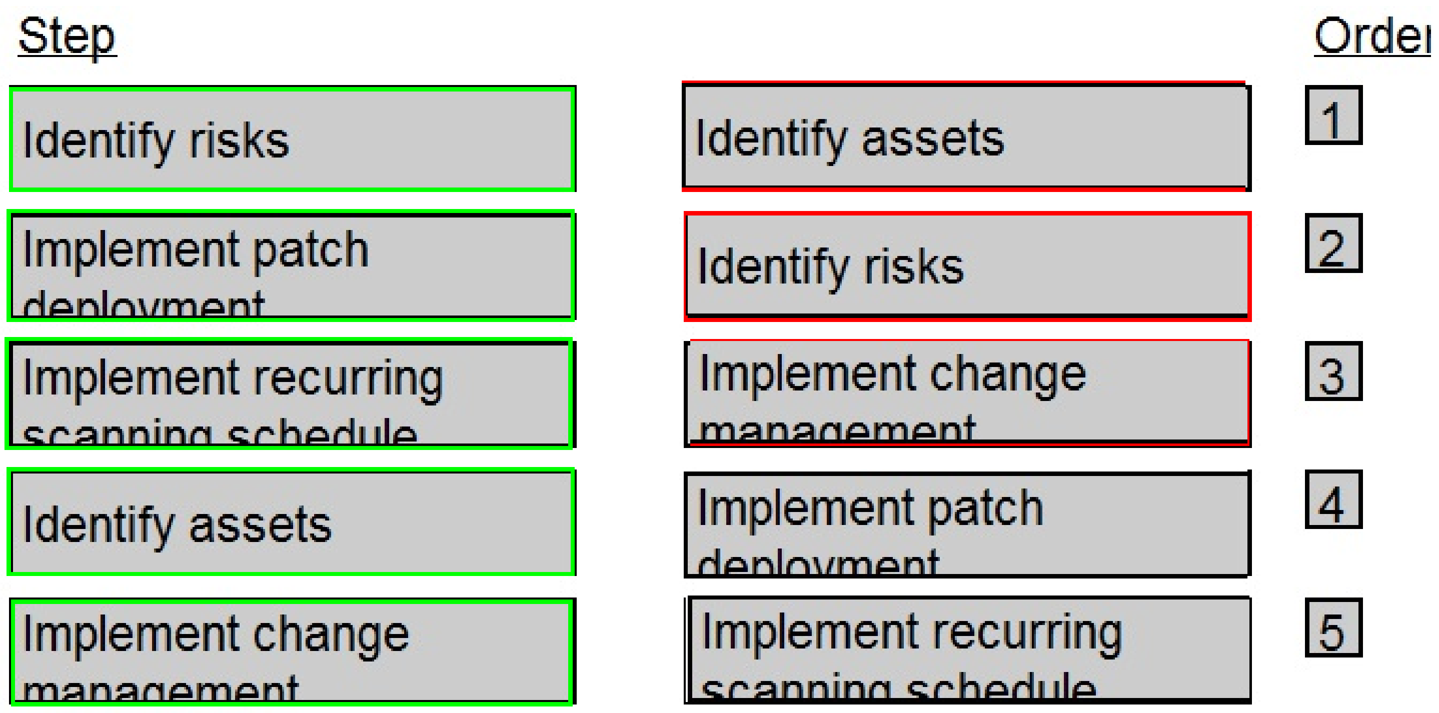
4

5

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Step		Orde
Identify risks	Identify assets	1
Implement patch deployment	Identify risks	2
Implement recurring scanning schedule	Implement change management	3
Identify assets	Implement patch deployment	4
Implement change management	Implement recurring scanning schedule	5

NEW QUESTION 346
- (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

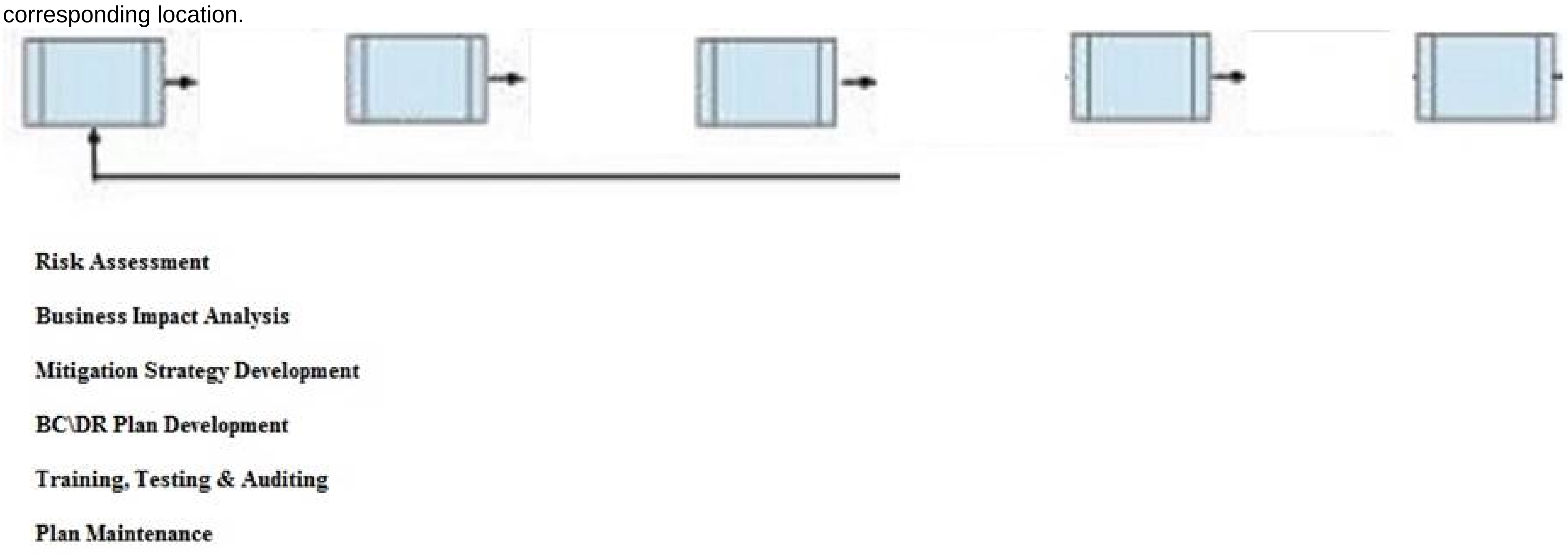
Answer: C

NEW QUESTION 349
- (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 354
- (Exam Topic 11)
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.
What is the best approach for the CISO?
Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.



Risk Assessment

Business Impact Analysis

Mitigation Strategy Development

BC\DR Plan Development

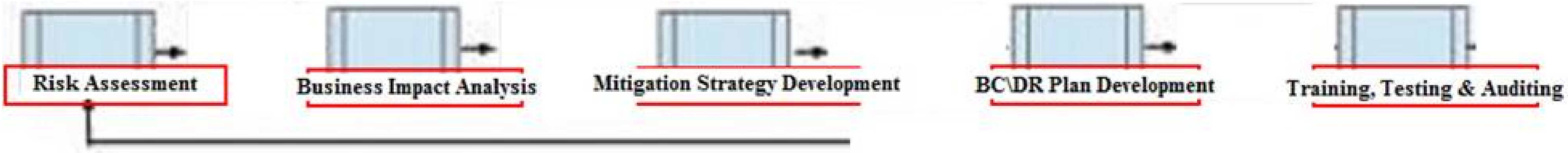
Training, Testing & Auditing

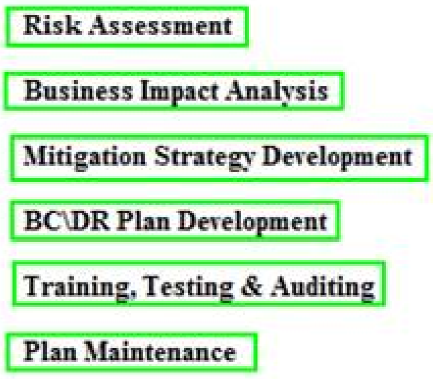
Plan Maintenance

A. Mastered
B. Not Mastered

Answer: A

Explanation:





NEW QUESTION 358
- (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 360
- (Exam Topic 11)
Which of the following is most helpful in applying the principle of LEAST privilege?

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

Answer: A

NEW QUESTION 365
- (Exam Topic 11)
What is an important characteristic of Role Based Access Control (RBAC)?

A. Supports Mandatory Access Control (MAC)
B. Simplifies the management of access rights
C. Relies on rotation of duties
D. Requires two factor authentication

Answer: B

NEW QUESTION 368
- (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 372
- (Exam Topic 11)
Which of the following disaster recovery test plans will be MOST effective while providing minimal risk?

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

Answer: B

NEW QUESTION 374
- (Exam Topic 11)
What is the MOST efficient way to secure a production program and its data?

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

Answer: B

NEW QUESTION 376
- (Exam Topic 11)
An organization lacks a data retention policy. Of the following, who is the BEST person to consult for such requirement?

A. Application Manager
B. Database Administrator
C. Privacy Officer
D. Finance Manager

Answer: C

NEW QUESTION 378
- (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 380
- (Exam Topic 11)
How does Encapsulating Security Payload (ESP) in transport mode affect the Internet Protocol (IP)?

A. Encrypts and optionally authenticates the IP header, but not the IP payload
B. Encrypts and optionally authenticates the IP payload, but not the IP header
C. Authenticates the IP payload and selected portions of the IP header
D. Encrypts and optionally authenticates the complete IP packet

Answer: B

NEW QUESTION 381
- (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 385
- (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 390
- (Exam Topic 11)
After acquiring the latest security updates, what must be done before deploying to production systems?

A. Use tools to detect missing system patches
B. Install the patches on a test system
C. Subscribe to notifications for vulnerabilities
D. Assess the severity of the situation

Answer: B

NEW QUESTION 394
- (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 398
- (Exam Topic 11)
The BEST example of the concept of "something that a user has" when providing an authorized user access to a computing system is

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

Answer: B

NEW QUESTION 399
- (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 404
- (Exam Topic 11)
An organization has developed a major application that has undergone accreditation testing. After receiving the results of the evaluation, what is the final step before the application can be accredited?

A. Acceptance of risk by the authorizing official
B. Remediation of vulnerabilities
C. Adoption of standardized policies and procedures
D. Approval of the System Security Plan (SSP)

Answer: A

NEW QUESTION 405
- (Exam Topic 11)
A security professional is asked to provide a solution that restricts a bank teller to only perform a savings deposit transaction but allows a supervisor to perform corrections after the transaction. Which of the following is the MOST effective solution?

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

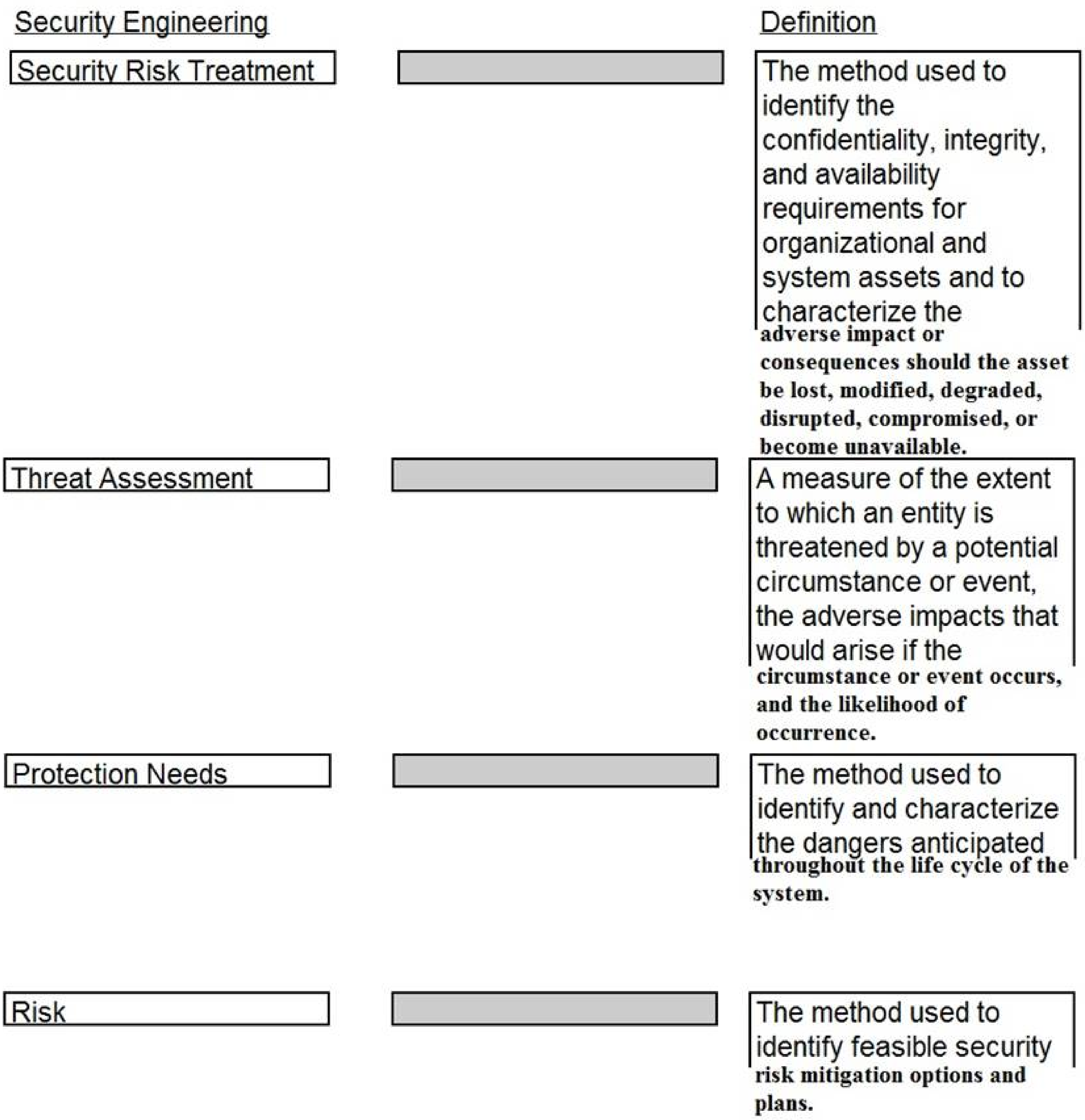
Answer: C

NEW QUESTION 410
- (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 411
- (Exam Topic 11)
Drag the following Security Engineering terms on the left to the BEST definition on the right.

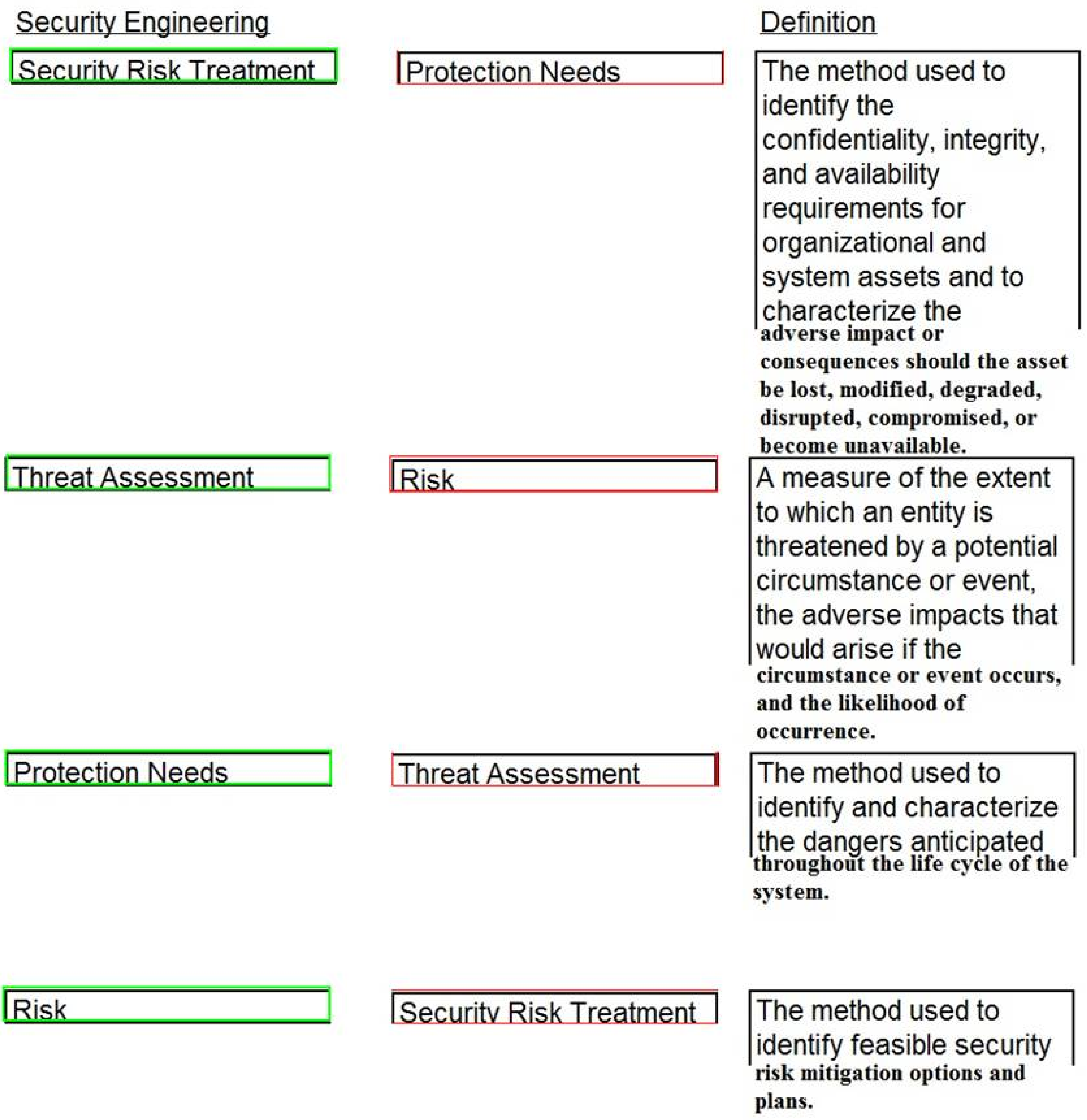


Security Engineering		Definition
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised,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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



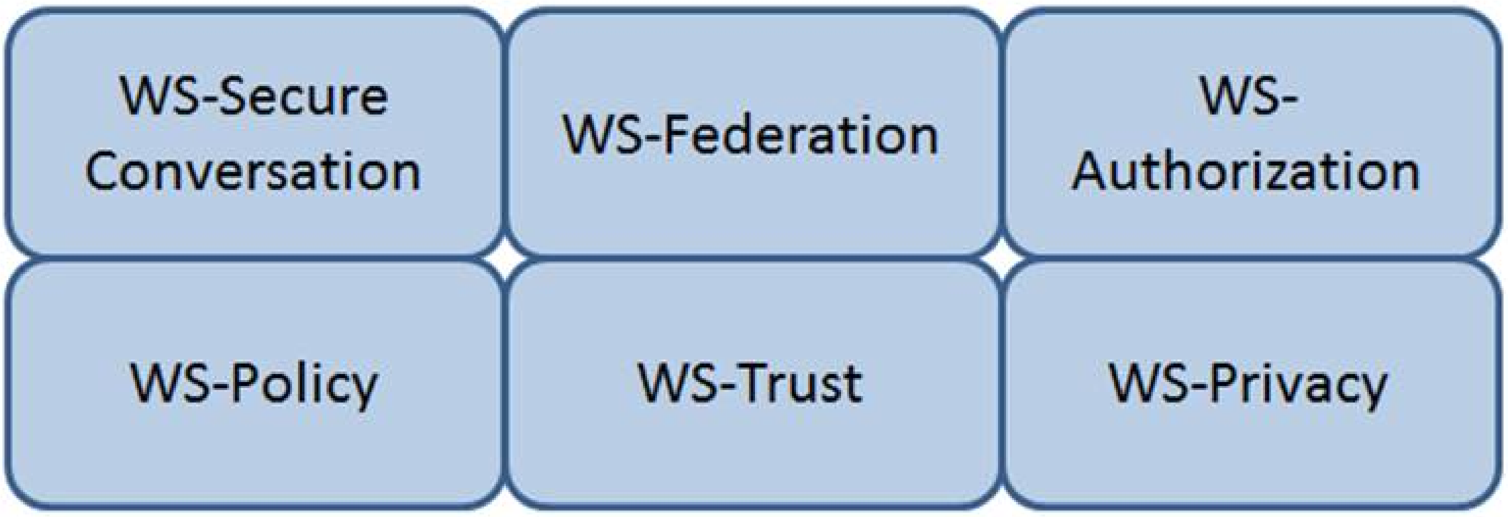
Security Engineering		Definition
Securitv Risk Treatment	Protection Needs	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded,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

NEW QUESTION 416
- (Exam Topic 11)
Which of the following statements is TRUE regarding value boundary analysis as a functional software testing technique?

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

Answer: C

NEW QUESTION 417
- (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.



WS-Secure Conversation

WS-Federation

WS-Authorization

WS-Policy

WS-Trust

WS-Privacy

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 419
- (Exam Topic 11)
Which of the following controls is the FIRST step in protecting privacy in an information system?

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

Answer: B

NEW QUESTION 422
- (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 424
- (Exam Topic 11)
What is one way to mitigate the risk of security flaws in custom software?

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

Answer: B

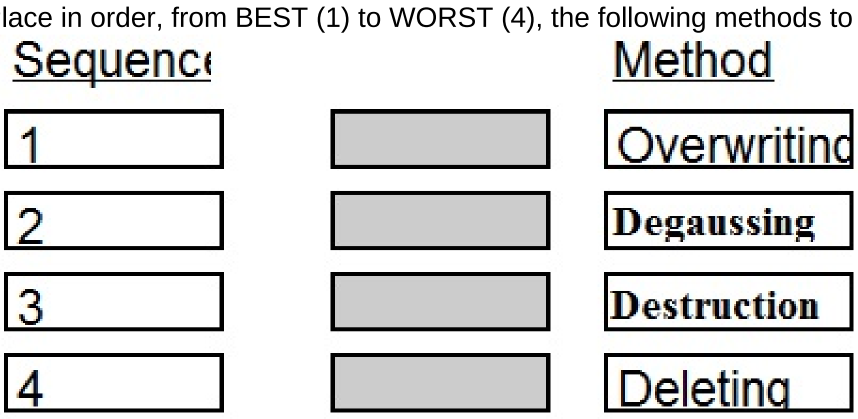
NEW QUESTION 425

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

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

Answer: D

NEW QUESTION 428
- (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.

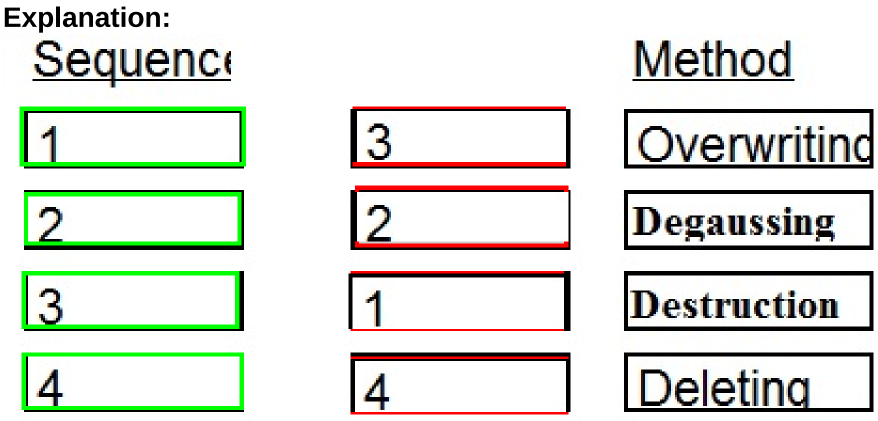


Sequence		Method
1		Overwriting
2		Degaussing
3		Destruction
4		Deleting

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Sequence		Method
1	3	Overwriting
2	2	Degaussing
3	1	Destruction
4	4	Deleting

NEW QUESTION 431
- (Exam Topic 11)
The PRIMARY outcome of a certification process is that it provides documented

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

Answer: D

NEW QUESTION 435
- (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 437
- (Exam Topic 11)
Which of the following methods can be used to achieve confidentiality and integrity for data in transit?

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

Answer: B

NEW QUESTION 440
- (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 445
- (Exam Topic 11)
Discretionary Access Control (DAC) is based on which of the following?

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

Answer: B

NEW QUESTION 446
- (Exam Topic 11)
What type of test assesses a Disaster Recovery (DR) plan using realistic disaster scenarios while maintaining minimal impact to business operations?

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

Answer: C

NEW QUESTION 447
- (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 448
- (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 450
- (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 453
- (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 457
- (Exam Topic 11)
Which of the following BEST describes the purpose of the security functional requirements of Common Criteria?

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

Answer: C

NEW QUESTION 460
- (Exam Topic 11)
Which of the following is a recommended alternative to an integrated email encryption system?

A. Sign emails containing sensitive data
B. Send sensitive data in separate emails
C. Encrypt sensitive data separately in attachments
D. Store sensitive information to be sent in encrypted drives

Answer: C

NEW QUESTION 463
- (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 464
- (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 469
- (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 472
- (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 474
- (Exam Topic 11)
Are companies legally required to report all data breaches?

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

Answer: A

NEW QUESTION 479
- (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 480
- (Exam Topic 11)
Which of the following is the PRIMARY benefit of implementing data-in-use controls?

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

Answer: C

NEW QUESTION 483
- (Exam Topic 11)
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.
What is the best approach for the CISO?
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.
What is the best approach for the CISO?

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

Answer: B

NEW QUESTION 487
- (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 489
- (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 494
- (Exam Topic 11)
A global organization wants to implement hardware tokens as part of a multifactor authentication solution for remote access. The PRIMARY advantage of this implementation is

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

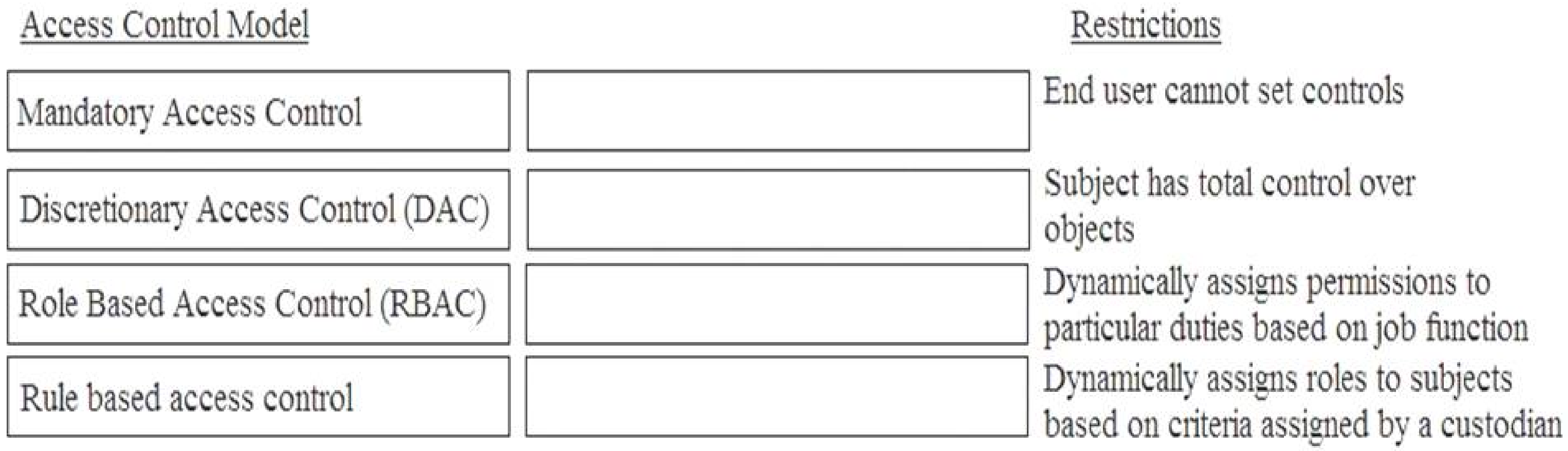
Answer: C

NEW QUESTION 497
- (Exam Topic 12)
Which of the following is a remote access protocol that uses a static authentication?

A. Point-to-Point Tunneling Protocol (PPTP)
B. Routing Information Protocol (RIP)
C. Password Authentication Protocol (PAP)
D. Challenge Handshake Authentication Protocol (CHAP)

Answer: C

NEW QUESTION 502
- (Exam Topic 12)
Match the name of access control model with its associated restriction.
Drag each access control model to its appropriate restriction access on the right.



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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 507
- (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 511
- (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 512
- (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 517
- (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 521
- (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 526
- (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 529
- (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 532
- (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

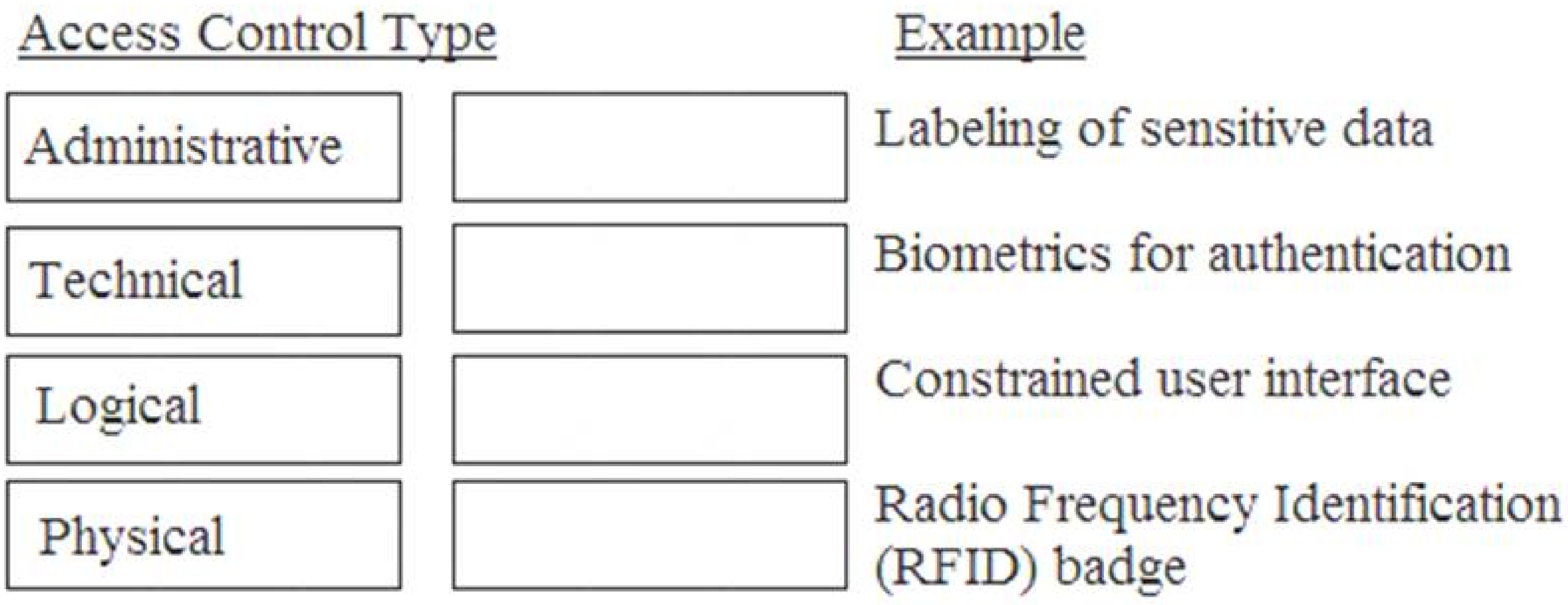
Answer: C

NEW QUESTION 533
- (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 538
- (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 539
- (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 544
- (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 549
- (Exam Topic 12)
In general, servers that are facing the Internet should be placed in a demilitarized zone (DMZ). What is MAIN purpose of the DMZ?

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

Answer: A

NEW QUESTION 550
- (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 555
- (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 558
- (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 563
- (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 565
- (Exam Topic 12)
How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

A. Examines log messages or other indications on the system.
B. Monitors alarms sent to the system administrator
C. Matches traffic patterns to virus signature files
D. Examines the Access Control List (ACL)

Answer: C

NEW QUESTION 568
- (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 572
- (Exam Topic 12)
An employee of a retail company has been granted an extended leave of absence by Human Resources (HR). This information has been formally communicated to the access provisioning team. Which of the following is the BEST action to take?

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

Answer: D

NEW QUESTION 576
- (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 579
- (Exam Topic 12)
Which one of the following activities would present a significant security risk to organizations when employing a Virtual Private Network (VPN) solution?

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

Answer: B

NEW QUESTION 583
- (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 586
- (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 590
- (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 592
- (Exam Topic 12)
The application of a security patch to a product previously validate at Common Criteria (CC) Evaluation Assurance Level (EAL) 4 would

A. require an update of the Protection Profile (PP).
B. require recertification.
C. retain its current EAL rating.
D. reduce the product to EAL 3.

Answer: B

NEW QUESTION 594
- (Exam Topic 12)
A user sends an e-mail request asking for read-only access to files that are not considered sensitive. A Discretionary Access Control (DAC) methodology is in place. Which is the MOST suitable approach that the administrator should take?

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

Answer: A

NEW QUESTION 599
- (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 600
- (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 604
- (Exam Topic 12)
What is the MOST important element when considering the effectiveness of a training program for Business Continuity (BC) and Disaster Recovery (DR)?

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

Answer: B

NEW QUESTION 606
- (Exam Topic 12)
When building a data classification scheme, which of the following is the PRIMARY concern?

A. Purpose
B. Cost effectiveness
C. Availability
D. Authenticity

Answer: D

NEW QUESTION 610
- (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 611
- (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 616
- (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 620
- (Exam Topic 13)
Which of the following steps should be performed FIRST when purchasing Commercial Off-The-Shelf (COTS) software?

A. undergo a security assessment as part of authorization process
B. establish a risk management strategy
C. harden the hosting server, and perform hosting and application vulnerability scans

D. establish policies and procedures on system and services acquisition

Answer: D

NEW QUESTION 625
- (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 627
- (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 631
- (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 632
- (Exam Topic 13)
What is the MAIN goal of information security awareness and training?

A. To inform users of the latest malware threats
B. To inform users of information assurance responsibilities
C. To comply with the organization information security policy
D. To prepare students for certification

Answer: B

NEW QUESTION 634
- (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 638
- (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 642
- (Exam Topic 13)
In an organization where Network Access Control (NAC) has been deployed, a device trying to connect to the network is being placed into an isolated domain. What could be done on this device in order to obtain proper connectivity?

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

Answer: B

NEW QUESTION 646
- (Exam Topic 13)
As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

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

Answer: D

NEW QUESTION 648
- (Exam Topic 13)
A company seizes a mobile device suspected of being used in committing fraud. What would be the BEST method used by a forensic examiner to isolate the powered-on device from the network and preserve the evidence?

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

Answer: A

NEW QUESTION 649
- (Exam Topic 13)
An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject’s data?

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

Answer: C

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 651
- (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 653
- (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 654
- (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

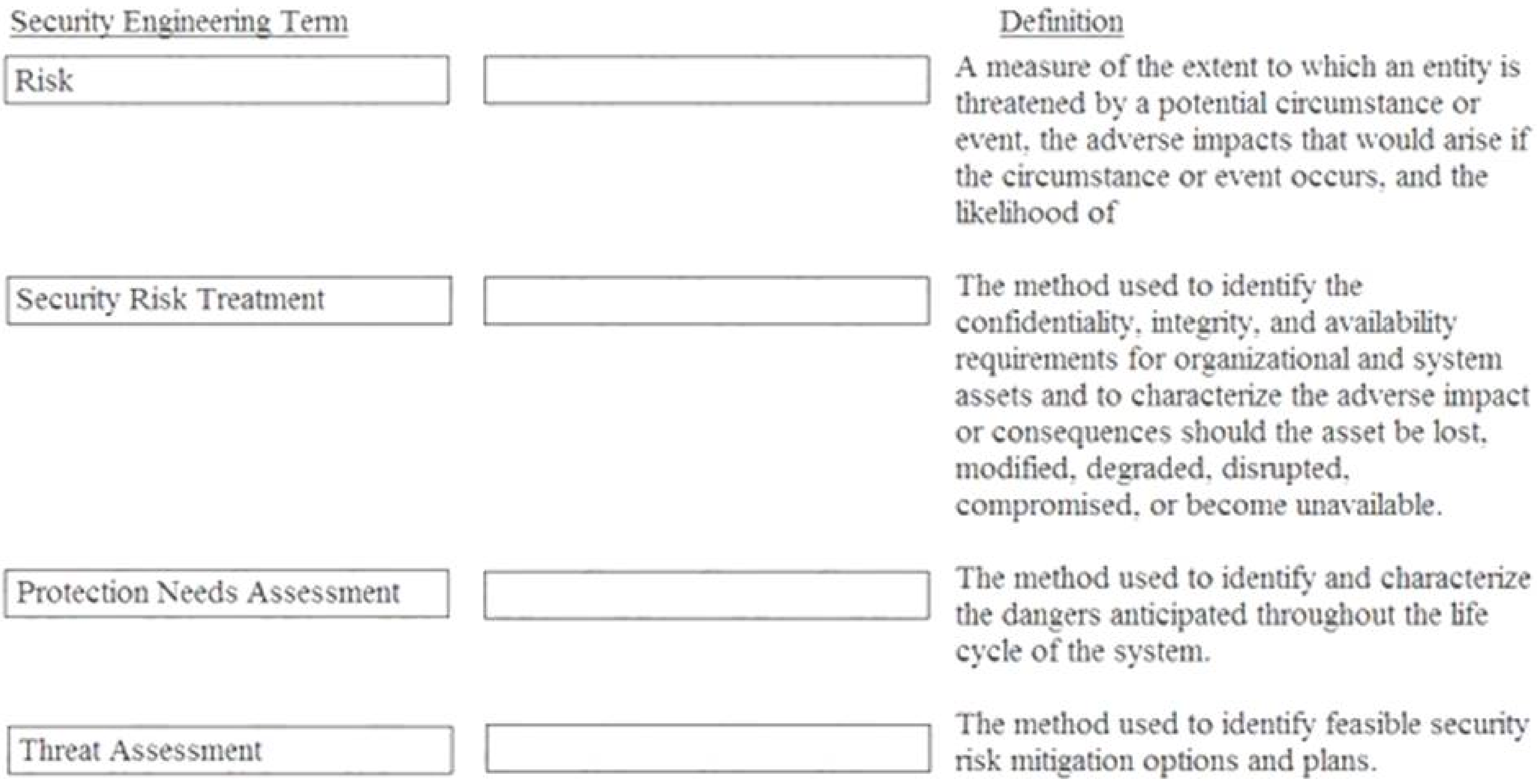
Answer: A

NEW QUESTION 655
- (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 658
- (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 663
- (Exam Topic 13)
Which of the following could be considered the MOST significant security challenge when adopting DevOps practices compared to a more traditional control framework?

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

Answer: B

NEW QUESTION 665
- (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 669
- (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 674
- (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 676
- (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 681
- (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 686
- (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 690
- (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 691
- (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 694
- (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 699
- (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 703
- (Exam Topic 13)
The organization would like to deploy an authorization mechanism for an Information Technology (IT) infrastructure project with high employee turnover.
Which access control mechanism would be preferred?

A. Attribute Based Access Control (ABAC)
B. Discretionary Access Control (DAC)
C. Mandatory Access Control (MAC)
D. Role-Based Access Control (RBAC)

Answer: D

NEW QUESTION 707
- (Exam Topic 13)
Which of the following methods of suppressing a fire is environmentally friendly and the MOST appropriate for a data center?

A. Inert gas fire suppression system
B. Halon gas fire suppression system
C. Dry-pipe sprinklers
D. Wet-pipe sprinklers

Answer: C

NEW QUESTION 710
- (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

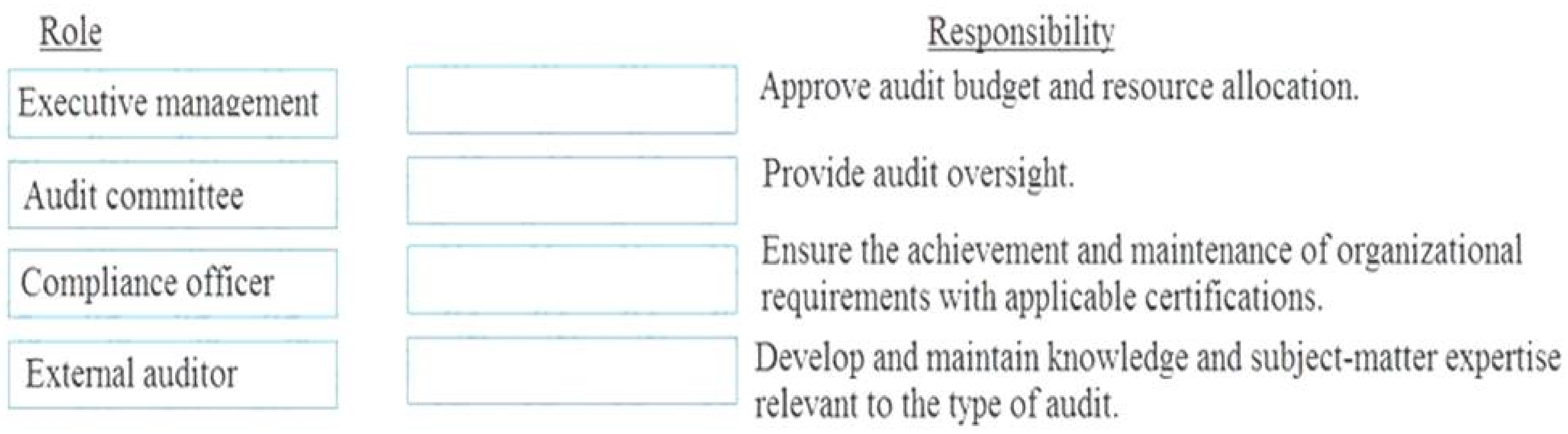
NEW QUESTION 712
- (Exam Topic 13)
Proven application security principles include which of the following?

A. Minimizing attack surface area

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

Answer: A

NEW QUESTION 714
- (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:

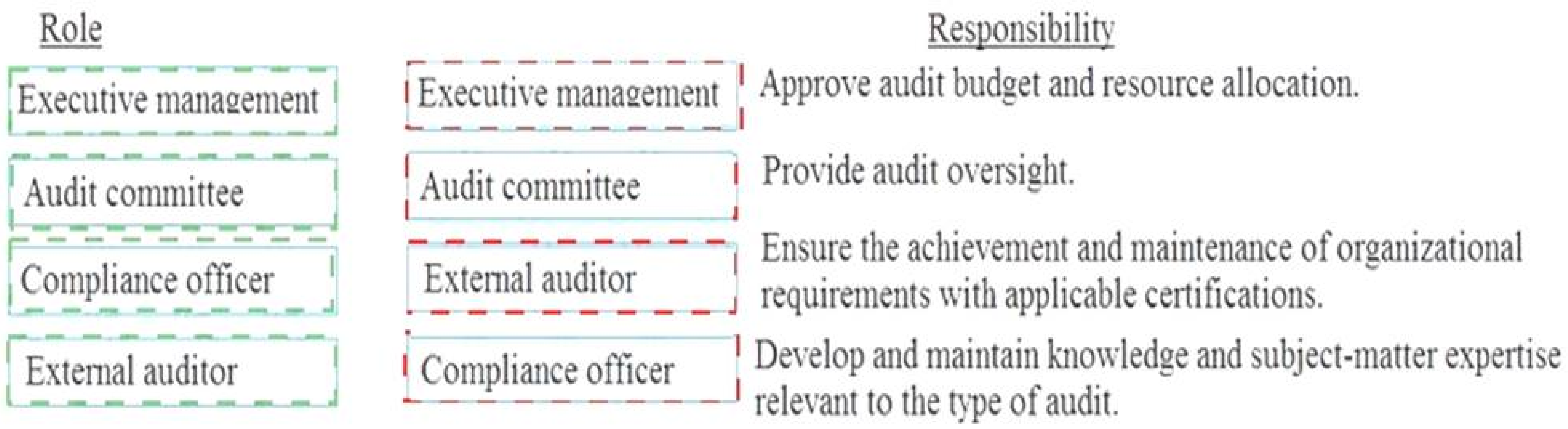


Role		Responsibility
Executive management		Approve audit budget and resource allocation.
Audit committee		Provide audit oversight.
Compliance officer		Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor		Develop and maintain knowledge 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 718
- (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 719
- (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 721
- (Exam Topic 13)
What is the expected outcome of security awareness in support of a security awareness program?

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

Answer: C

NEW QUESTION 722
- (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 724
- (Exam Topic 13)
Transport Layer Security (TLS) provides which of the following capabilities for a remote access server?

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

Answer: C

NEW QUESTION 726
- (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 728
- (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 733
- (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 738
- (Exam Topic 13)
Who is accountable for the information within an Information System (IS)?

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

Answer: B

Explanation:
Section: Security Operations

NEW QUESTION 742
- (Exam Topic 13)
A security professional determines that a number of outsourcing contracts inherited from a previous merger do not adhere to the current security requirements. Which of the following BEST minimizes the risk of this
happening again?

A. Define additional security controls directly after the merger
B. Include a procurement officer in the merger team
C. Verify all contracts before a merger occurs
D. Assign a compliancy officer to review the merger conditions

Answer: D

NEW QUESTION 745
- (Exam Topic 13)
What does a Synchronous (SYN) flood attack do?

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

Answer: B

NEW QUESTION 749
- (Exam Topic 13)
A minimal implementation of endpoint security includes which of the following?

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

Answer: A

NEW QUESTION 753
- (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 758
- (Exam Topic 13)
A user has infected a computer with malware by connecting a Universal Serial Bus (USB) storage device. Which of the following is MOST effective to mitigate future infections?

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

Answer: C

NEW QUESTION 761
- (Exam Topic 13)
Which of the following is the BEST metric to obtain when gaining support for an Identify and Access
Management (IAM) solution?

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

Answer: D

NEW QUESTION 763
- (Exam Topic 13)
Which of the following management process allows ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

A. Configuration
B. Identity
C. Compliance
D. Patch

Answer: A

NEW QUESTION 766
- (Exam Topic 13)
Which of the following would BEST support effective testing of patch compatibility when patches are applied to an organization’s systems?

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

Answer: A

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 770
- (Exam Topic 13)
Which of the following provides the MOST comprehensive filtering of Peer-to-Peer (P2P) traffic?

A. Application proxy
B. Port filter
C. Network boundary router
D. Access layer switch

Answer: A

NEW QUESTION 775
- (Exam Topic 13)
Which one of the following considerations has the LEAST impact when considering transmission security?

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

Answer: C

NEW QUESTION 777
- (Exam Topic 13)
Which of the following techniques is known to be effective in spotting resource exhaustion problems, especially with resources such as processes, memory, and connections?

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

Answer: A

NEW QUESTION 779
- (Exam Topic 13)
A post-implementation review has identified that the Voice Over Internet Protocol (VoIP) system was designed to have gratuitous Address Resolution Protocol (ARP) disabled.
Why did the network architect likely design the VoIP system with gratuitous ARP disabled?

A. Gratuitous ARP requires the use of Virtual Local Area Network (VLAN) 1.
B. Gratuitous ARP requires the use of insecure layer 3 protocols.
C. Gratuitous ARP requires the likelihood of a successful brute-force attack on the phone.
D. Gratuitous ARP requires the risk of a Man-in-the-Middle (MITM) attack.

Answer: D

NEW QUESTION 781
- (Exam Topic 13)
“Stateful” differs from “Static” packet filtering firewalls by being aware of which of the following?

A. Difference between a new and an established connection
B. Originating network location
C. Difference between a malicious and a benign packet payload
D. Originating application session

Answer: A

NEW QUESTION 783
- (Exam Topic 13)
The security accreditation task of the System Development Life Cycle (SDLC) process is completed at the end of which phase?

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

Answer: B

NEW QUESTION 786
......