ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (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)
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 3
- (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 4
- (Exam Topic 2)
Which of the following BEST describes the responsibilities of a data owner?

A. Ensuring quality and validation through periodic audits for ongoing data integrity
B. Maintaining fundamental data availability, including data storage and archiving
C. Ensuring accessibility to appropriate users, maintaining appropriate levels of data security
D. Determining the impact the information has on the mission of the organization

Answer: C

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

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

Answer: A

NEW QUESTION 6
- (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 7
- (Exam Topic 4)
An external attacker has compromised an organization’s network security perimeter and installed a sniffer onto an inside computer. Which of the following is the MOST effective layer of security the organization could have implemented to mitigate the attacker’s ability to gain further information?

A. Implement packet filtering on the network firewalls
B. Install Host Based Intrusion Detection Systems (HIDS)

C. Require strong authentication for administrators
D. Implement logical network segmentation at the switches

Answer: D

NEW QUESTION 8
- (Exam Topic 4)
What is the purpose of an Internet Protocol (IP) spoofing attack?

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

Answer: D

NEW QUESTION 9
- (Exam Topic 4)
At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

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

Answer: D

NEW QUESTION 10
- (Exam Topic 5)
What is the BEST approach for controlling access to highly sensitive information when employees have the same level of security clearance?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 6)
Which of the following could cause a Denial of Service (DoS) against an authentication system?

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

Answer: D

NEW QUESTION 13
- (Exam Topic 7)
A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?

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

Answer: D

NEW QUESTION 14
- (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 19
- (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 21
- (Exam Topic 7)
What is the PRIMARY reason for implementing change management?

A. Certify and approve releases to the environment
B. Provide version rollbacks for system changes
C. Ensure that all applications are approved
D. Ensure accountability for changes to the environment

Answer: D

NEW QUESTION 25
- (Exam Topic 7)
Which of the following types of business continuity tests includes assessment of resilience to internal and external risks without endangering live operations?

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

Answer: B

NEW QUESTION 29
- (Exam Topic 9)
What is the FIRST step in developing a security test and its evaluation?

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

Answer: C

NEW QUESTION 34
- (Exam Topic 9)
Which of the following is a method used to prevent Structured Query Language (SQL) injection attacks?

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

Answer: D

NEW QUESTION 39
- (Exam Topic 9)
The three PRIMARY requirements for a penetration test are

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

Answer: A

NEW QUESTION 43
- (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 45
- (Exam Topic 9)

Which of the following is the FIRST action that a system administrator should take when it is revealed during a penetration test that everyone in an organization has unauthorized access to a server holding sensitive data?

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

Answer: A

NEW QUESTION 46
- (Exam Topic 9)
Which of the following MUST be part of a contract to support electronic discovery of data stored in a cloud environment?

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

Answer: D

NEW QUESTION 50
- (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 55
- (Exam Topic 9)
A vulnerability test on an Information System (IS) is conducted to

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

Answer: C

NEW QUESTION 58
- (Exam Topic 9)
An organization allows ping traffic into and out of their network. An attacker has installed a program on the network that uses the payload portion of the ping packet to move data into and out of the network. What type of attack has the organization experienced?

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

Answer: D

NEW QUESTION 60
- (Exam Topic 9)
Which of the following is a physical security control that protects Automated Teller Machines (ATM) from skimming?

A. Anti-tampering
B. Secure card reader
C. Radio Frequency (RF) scanner
D. Intrusion Prevention System (IPS)

Answer: A

NEW QUESTION 63
- (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 66
- (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 67
- (Exam Topic 9)
The PRIMARY purpose of a security awareness program is to

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

Answer: A

NEW QUESTION 72
- (Exam Topic 9)
A practice that permits the owner of a data object to grant other users access to that object would usually provide

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

Answer: D

NEW QUESTION 77
- (Exam Topic 9)
Which of the following assessment metrics is BEST used to understand a system's vulnerability to potential exploits?

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

Answer: C

NEW QUESTION 82
- (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 86
- (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 89
- (Exam Topic 9)
Which of the following is the MOST important consideration when storing and processing Personally Identifiable Information (PII)?

A. Encrypt and hash all PII to avoid disclosure and tampering.
B. Store PII for no more than one year.
C. Avoid storing PII in a Cloud Service Provider.
D. Adherence to collection limitation laws and regulations.

Answer: D

NEW QUESTION 90
- (Exam Topic 9)
What would be the PRIMARY concern when designing and coordinating a security assessment for an Automatic Teller Machine (ATM) system?

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

Answer: A

NEW QUESTION 91
- (Exam Topic 9)
The BEST way to check for good security programming practices, as well as auditing for possible backdoors, is to conduct

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

Answer: B

NEW QUESTION 96
- (Exam Topic 9)
In Business Continuity Planning (BCP), what is the importance of documenting business processes?

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

Answer: D

NEW QUESTION 98
- (Exam Topic 9)
A security consultant has been asked to research an organization's legal obligations to protect privacy-related information. What kind of reading material is MOST relevant to this project?

A. The organization's current security policies concerning privacy issues
B. Privacy-related regulations enforced by governing bodies applicable to the organization
C. Privacy best practices published by recognized security standards organizations
D. Organizational procedures designed to protect privacy information

Answer: B

NEW QUESTION 100
- (Exam Topic 9)
The Hardware Abstraction Layer (HAL) is implemented in the

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

Answer: A

NEW QUESTION 104
- (Exam Topic 9)
Which type of control recognizes that a transaction amount is excessive in accordance with corporate policy?

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

Answer: A

NEW QUESTION 105
- (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 109
- (Exam Topic 9)
Which of the following is a network intrusion detection technique?

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

Answer: A

NEW QUESTION 113
- (Exam Topic 9)
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 114
- (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 117
- (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 118
- (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 122
- (Exam Topic 9)
Who must approve modifications to an organization's production infrastructure configuration?

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

Answer: B

NEW QUESTION 127
- (Exam Topic 9)
An Intrusion Detection System (IDS) is generating alarms that a user account has over 100 failed login attempts per minute. A sniffer is placed on the network, and a variety of passwords for that user are noted. Which of the following is MOST likely occurring?

A. A dictionary attack
B. A Denial of Service (DoS) attack

C. A spoofing attack
D. A backdoor installation

Answer: A

NEW QUESTION 128
- (Exam Topic 9)
What is the MOST important purpose of testing the Disaster Recovery Plan (DRP)?

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

Answer: C

NEW QUESTION 131
- (Exam Topic 9)
Which of the following is a potential risk when a program runs in privileged mode?

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

Answer: D

NEW QUESTION 136
- (Exam Topic 9)
When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?

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

Answer: B

NEW QUESTION 139
- (Exam Topic 9)
When constructing an Information Protection Policy (IPP), it is important that the stated rules are necessary, adequate, and

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

Answer: D

NEW QUESTION 141
- (Exam Topic 9)
A system has been scanned for vulnerabilities and has been found to contain a number of communication ports that have been opened without authority. To which of the following might this system have been subjected?

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

Answer: A

NEW QUESTION 146
- (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 149
- (Exam Topic 9)
At a MINIMUM, a formal review of any Disaster Recovery Plan (DRP) should be conducted

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

Answer: C

NEW QUESTION 153
- (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 155
- (Exam Topic 10)
What do Capability Maturity Models (CMM) serve as a benchmark for in an organization?

A. Experience in the industry
B. Definition of security profiles
C. Human resource planning efforts
D. Procedures in systems development

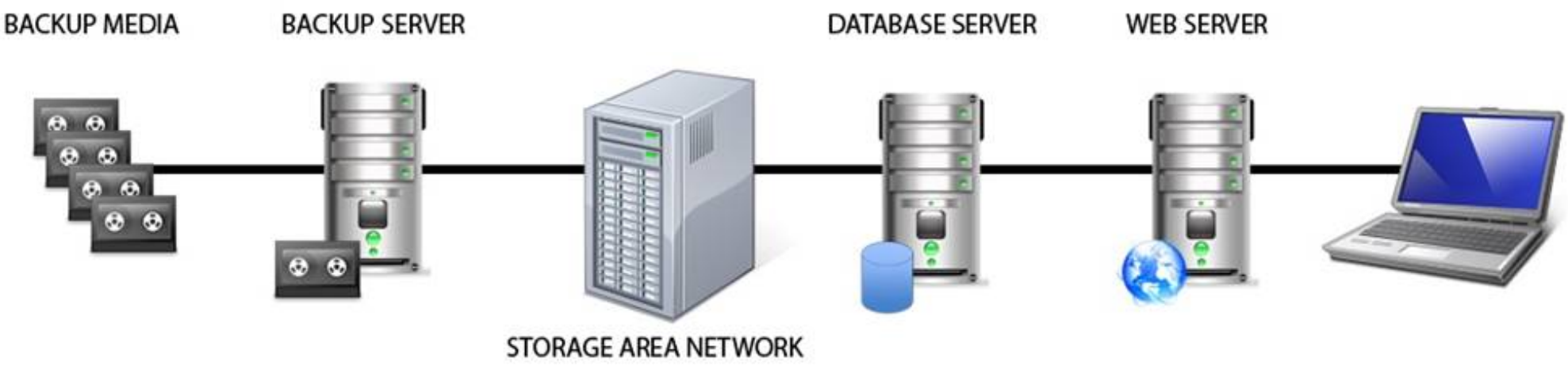
Answer: D

NEW QUESTION 159
- (Exam Topic 10)
Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following solutions would have MOST likely detected the use of peer-to-peer programs when the computer was connected to the office network?

A. Anti-virus software
B. Intrusion Prevention System (IPS)
C. Anti-spyware software
D. Integrity checking software

Answer: B

NEW QUESTION 160
- (Exam Topic 10)
Identify the component that MOST likely lacks digital accountability related to information access. Click on the correct device in the image below.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 161
- (Exam Topic 10)
Which of the following is the BEST reason to review audit logs periodically?

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

Answer: C

NEW QUESTION 164
- (Exam Topic 10)
Which of the following is an example of two-factor authentication?

A. Retina scan and a palm print
B. Fingerprint and a smart card
C. Magnetic stripe card and an ID badge
D. Password and Completely Automated Public Turing test to tell Computers and Humans Apart(CAPTCHA)

Answer: B

NEW QUESTION 166
- (Exam Topic 10)
Which of the following MOST influences the design of the organization's electronic monitoring policies?

A. Workplace privacy laws
B. Level of organizational trust
C. Results of background checks
D. Business ethical considerations

Answer: A

NEW QUESTION 167
- (Exam Topic 10)
According to best practice, which of the following groups is the MOST effective in performing an information security compliance audit?

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

Answer: D

NEW QUESTION 170
- (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 171
- (Exam Topic 10)
According to best practice, which of the following is required when implementing third party software in a production environment?

A. Scan the application for vulnerabilities
B. Contract the vendor for patching
C. Negotiate end user application training
D. Escrow a copy of the software

Answer: A

NEW QUESTION 174
- (Exam Topic 10)
Which of the following is the MOST difficult to enforce when using cloud computing?

A. Data access
B. Data backup
C. Data recovery
D. Data disposal

Answer: D

NEW QUESTION 179

- (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 180
- (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 185
- (Exam Topic 10)
Which of the following is required to determine classification and ownership?

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

Answer: A

NEW QUESTION 188
- (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 191
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
What MUST the access control logs contain in addition to the identifier?

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

Answer: A

NEW QUESTION 194
- (Exam Topic 10)
What component of a web application that stores the session state in a cookie can be bypassed by an attacker?

A. An initialization check
B. An identification check
C. An authentication check
D. An authorization check

Answer: C

NEW QUESTION 198
- (Exam Topic 10)
A business has implemented Payment Card Industry Data Security Standard (PCI-DSS) compliant handheld credit card processing on their Wireless Local Area Network (WLAN) topology. The network team partitioned the WLAN to create a private segment for credit card processing using a firewall to control device access and route traffic to the card processor on the Internet. What components are in the scope of PCI-DSS?

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

Answer: C

NEW QUESTION 202
- (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 205
- (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 209
- (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 210
- (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 211
- (Exam Topic 10)
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
In the plan, what is the BEST approach to mitigate future internal client-based attacks?

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

Answer: D

NEW QUESTION 215
- (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 218
- (Exam Topic 10)
Refer to the information below to answer the question.
In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

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

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

Answer: D

NEW QUESTION 219
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Which of the following is considered the MOST important priority for the information security officer?

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

Answer: A

NEW QUESTION 220
- (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

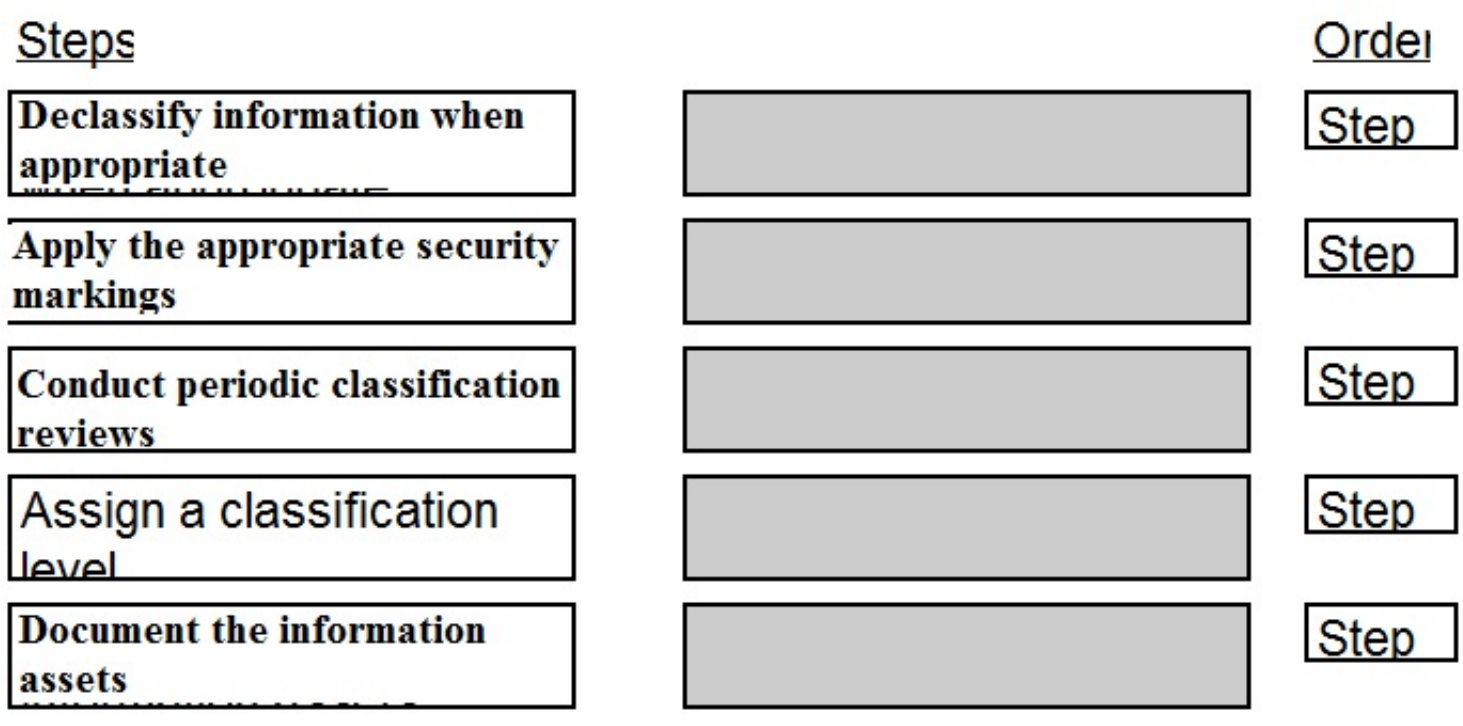
Answer: B

NEW QUESTION 224
- (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

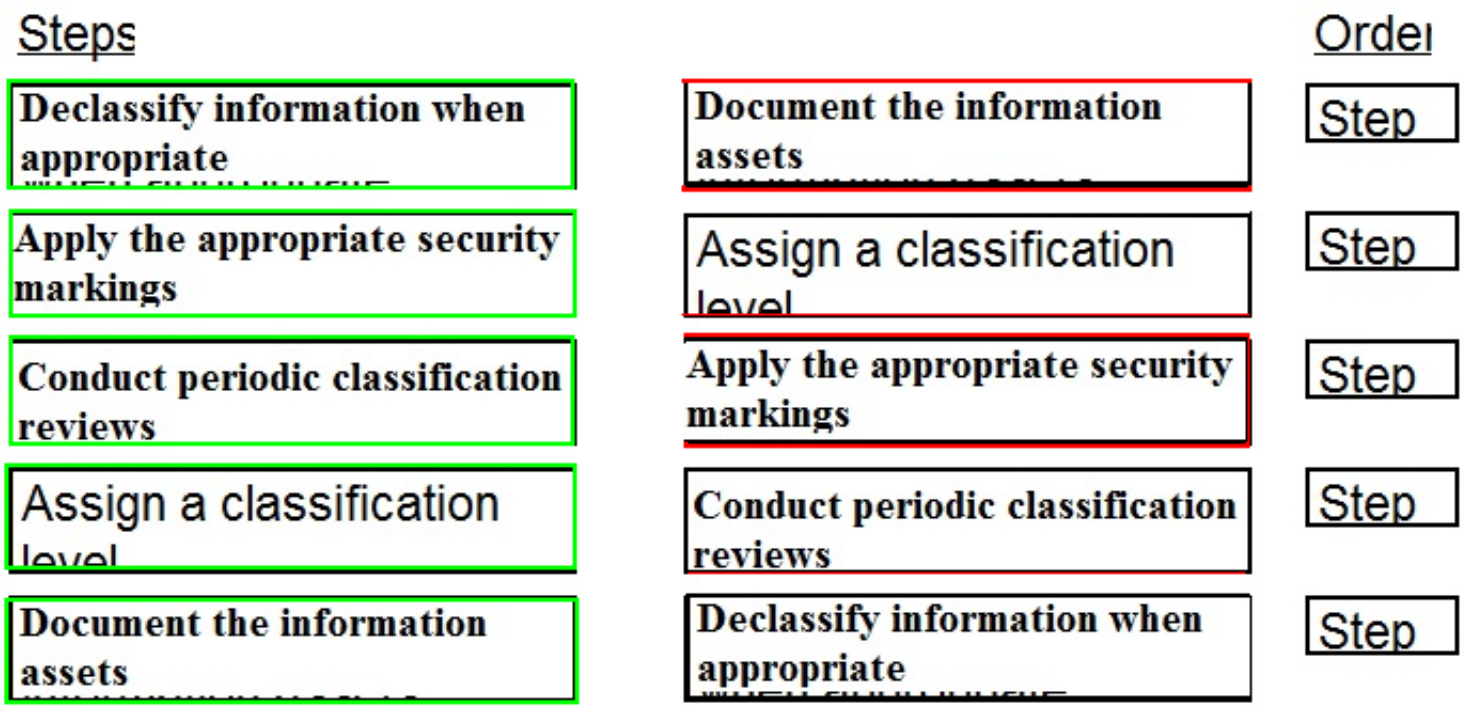
NEW QUESTION 228
- (Exam Topic 10)
Place the following information classification steps in sequential order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 232
- (Exam Topic 10)
Refer to the information below to answer the question.
Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.
After magnetic drives were degaussed twice according to the product manufacturer's directions, what is the MOST LIKELY security issue with degaussing?

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

Answer: B

NEW QUESTION 233
- (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 235
- (Exam Topic 10)

An organization's data policy MUST include a data retention period which is based on

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

Answer: D

NEW QUESTION 240
- (Exam Topic 10)
What is the PRIMARY reason for ethics awareness and related policy implementation?

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

Answer: B

NEW QUESTION 244
- (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 246
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
When determining appropriate resource allocation, which of the following is MOST important to monitor?

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

Answer: B

NEW QUESTION 249
- (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 250
- (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 255
- (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 260
- (Exam Topic 10)
Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
What additional considerations are there if the third party is located in a different country?

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

Answer: C

NEW QUESTION 264
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
The effectiveness of the security program can PRIMARILY be measured through

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

Answer: A

NEW QUESTION 265
- (Exam Topic 10)
Which of the following is the BEST countermeasure to brute force login attacks?

A. Changing all canonical passwords
B. Decreasing the number of concurrent user sessions
C. Restricting initial password delivery only in person
D. Introducing a delay after failed system access attempts

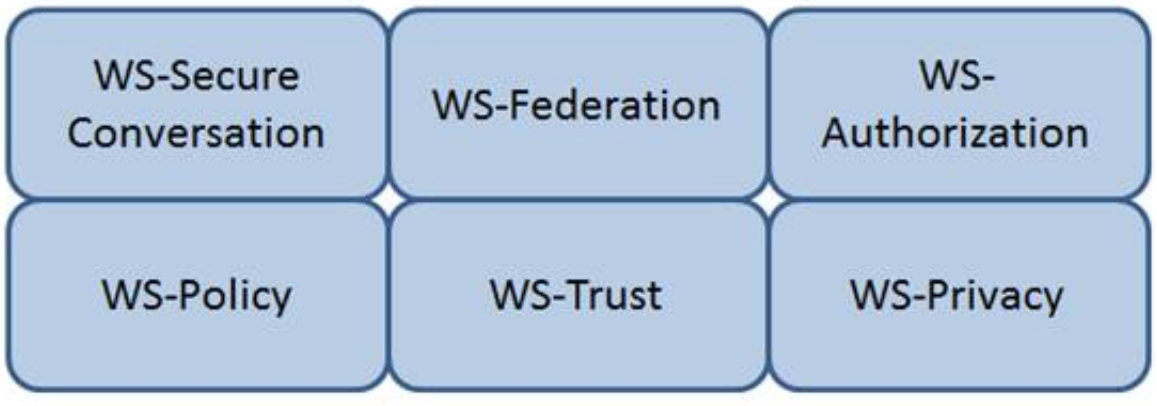
Answer: D

NEW QUESTION 268
- (Exam Topic 10)
What is the MOST important reason to configure unique user IDs?

A. Supporting accountability
B. Reducing authentication errors
C. Preventing password compromise
D. Supporting Single Sign On (SSO)

Answer: A

NEW QUESTION 269
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 270
- (Exam Topic 11)
The application of which of the following standards would BEST reduce the potential for data breaches?

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

Answer: D

NEW QUESTION 275
- (Exam Topic 11)
What is the MOST effective method of testing custom application code?

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

Answer: B

NEW QUESTION 280
- (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 281
- (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 283
- (Exam Topic 11)
Which of the following is the BEST approach to take in order to effectively incorporate the concepts of business continuity into the organization?

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

Answer: C

NEW QUESTION 286
- (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 287
- (Exam Topic 11)
Which of the following is a reason to use manual patch installation instead of automated patch management?

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

Answer: C

NEW QUESTION 292
- (Exam Topic 11)
After a thorough analysis, it was discovered that a perpetrator compromised a network by gaining access to the network through a Secure Socket Layer (SSL) Virtual Private Network (VPN) gateway. The perpetrator guessed a username and brute forced the password to gain access. Which of the following BEST mitigates this issue?

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

Answer: D

NEW QUESTION 295
- (Exam Topic 11)
Which of the following has the GREATEST impact on an organization's security posture?

A. International and country-specific compliance requirements
B. Security violations by employees and contractors
C. Resource constraints due to increasing costs of supporting security
D. Audit findings related to employee access and permissions process

Answer: A

NEW QUESTION 299
- (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 304
- (Exam Topic 11)
How does an organization verify that an information system's current hardware and software match the standard system configuration?

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

Answer: C

NEW QUESTION 306
- (Exam Topic 11)
Regarding asset security and appropriate retention, which of the following INITIAL top three areas are important to focus on?

A. Security control baselines, access controls, employee awareness and training
B. Human resources, asset management, production management
C. Supply chain lead time, inventory control, encryption
D. Polygraphs, crime statistics, forensics

Answer: A

NEW QUESTION 307
- (Exam Topic 11)
Which of the following analyses is performed to protect information assets?

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

Answer: A

NEW QUESTION 311
- (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 313
- (Exam Topic 11)
Discretionary Access Control (DAC) restricts access according to

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

Answer: C

NEW QUESTION 316
- (Exam Topic 11)
The World Trade Organization's (WTO) agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires authors of computer software to be given the

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

Answer: A

NEW QUESTION 317
- (Exam Topic 11)
An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?

A. Limits and scope of the testing.
B. Physical location of server room and wiring closet.
C. Logical location of filters and concentrators.
D. Employee directory and organizational chart.

Answer: A

NEW QUESTION 321

- (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 326
- (Exam Topic 11)
When planning a penetration test, the tester will be MOST interested in which information?

A. Places to install back doors
B. The main network access points
C. Job application handouts and tours
D. Exploits that can attack weaknesses

Answer: B

NEW QUESTION 329
- (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 332
- (Exam Topic 11)
Which of the following describes the BEST configuration management practice?

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

Answer: D

NEW QUESTION 337
- (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 341
- (Exam Topic 11)
Which of the following is the BEST example of weak management commitment to the protection of security assets and resources?

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

Answer: A

NEW QUESTION 345
- (Exam Topic 11)
Which of the following explains why record destruction requirements are included in a data retention policy?

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

Answer: A

NEW QUESTION 347
- (Exam Topic 11)
Which of the following is an essential step before performing Structured Query Language (SQL) penetration tests on a production system?

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

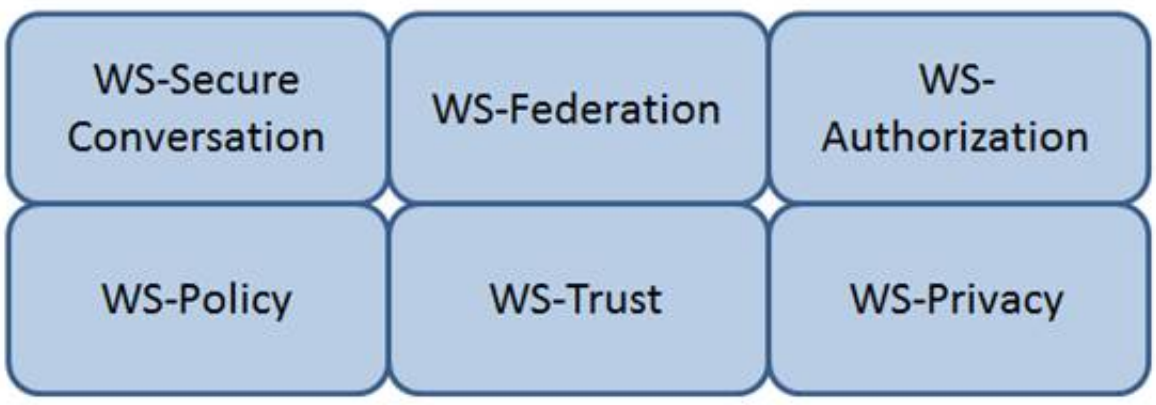
Answer: C

NEW QUESTION 351
- (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 356
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 359
- (Exam Topic 11)
Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).

Secure Architecture		**Do you advertise shared security services with guidance for project teams?**
Education & Guidance		**Are most people tested to ensure a baseline skill- set for secure development practices?**
Strategy & Metrics		**Does most of the organization know about what's required based on risk ratings?**
Vulnerability Management		**Are most project teams aware of their security point(s) of contact and response team(s)?**

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 361
- (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 363
- (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 366
- (Exam Topic 11)
Secure Sockets Layer (SSL) encryption protects

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

Answer: C

NEW QUESTION 367
- (Exam Topic 11)
Which methodology is recommended for penetration testing to be effective in the development phase of the life-cycle process?

A. White-box testing
B. Software fuzz testing
C. Black-box testing
D. Visual testing

Answer: A

NEW QUESTION 369
- (Exam Topic 11)
The PRIMARY characteristic of a Distributed Denial of Service (DDoS) attack is that it

A. exploits weak authentication to penetrate networks.
B. can be detected with signature analysis.
C. looks like normal network activity.
D. is commonly confused with viruses or worms.

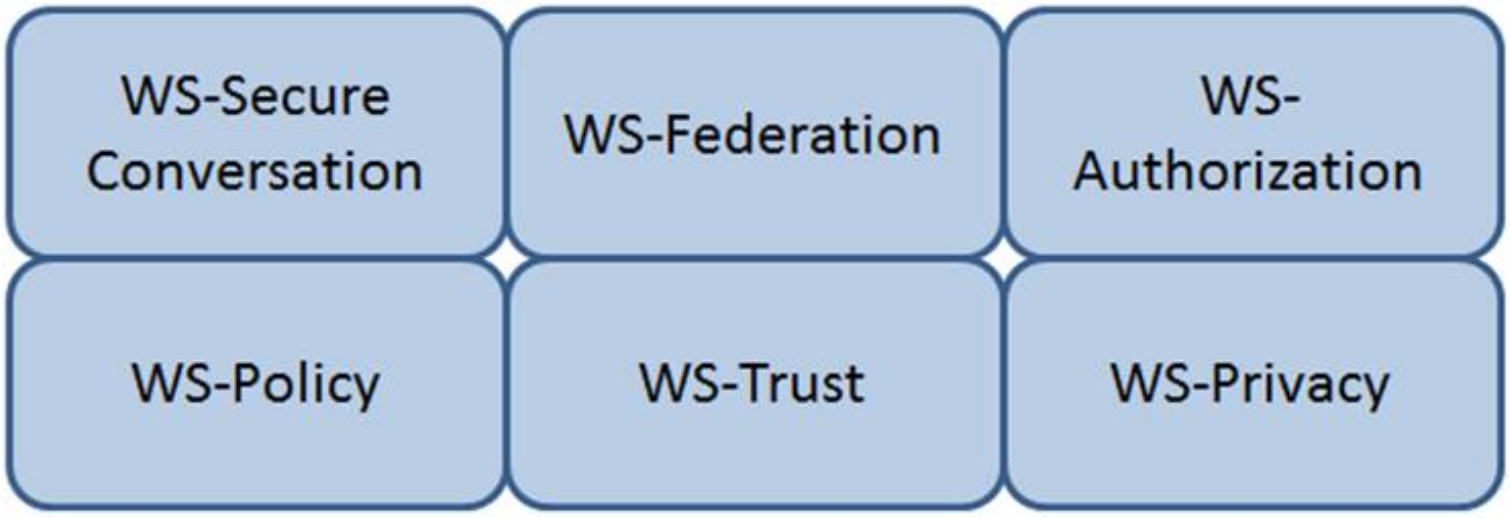
Answer: C

NEW QUESTION 372
- (Exam Topic 11)
The implementation of which features of an identity management system reduces costs and administration overhead while improving audit and accountability?

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

Answer: C

NEW QUESTION 374
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated? Click on the correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 378
- (Exam Topic 11)
Software Code signing is used as a method of verifying what security concept?

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

Answer: A

NEW QUESTION 379
- (Exam Topic 11)
An organization has decided to contract with a cloud-based service provider to leverage their identity as a service offering. They will use Open Authentication (OAuth) 2.0 to authenticate external users to the organization's services.
As part of the authentication process, which of the following must the end user provide?

A. An access token
B. A username and password

C. A username
D. A password

Answer: A

NEW QUESTION 382
- (Exam Topic 11)
Which one of the following is a common risk with network configuration management?

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

Answer: D

NEW QUESTION 386
- (Exam Topic 11)
The goal of a Business Continuity Plan (BCP) training and awareness program is to

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

Answer: A

NEW QUESTION 387
- (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 389
- (Exam Topic 11)
What is the GREATEST challenge of an agent-based patch management solution?

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

Answer: B

NEW QUESTION 392
- (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 396
- (Exam Topic 11)
A Simple Power Analysis (SPA) attack against a device directly observes which of the following?

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

Answer: B

NEW QUESTION 398
- (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

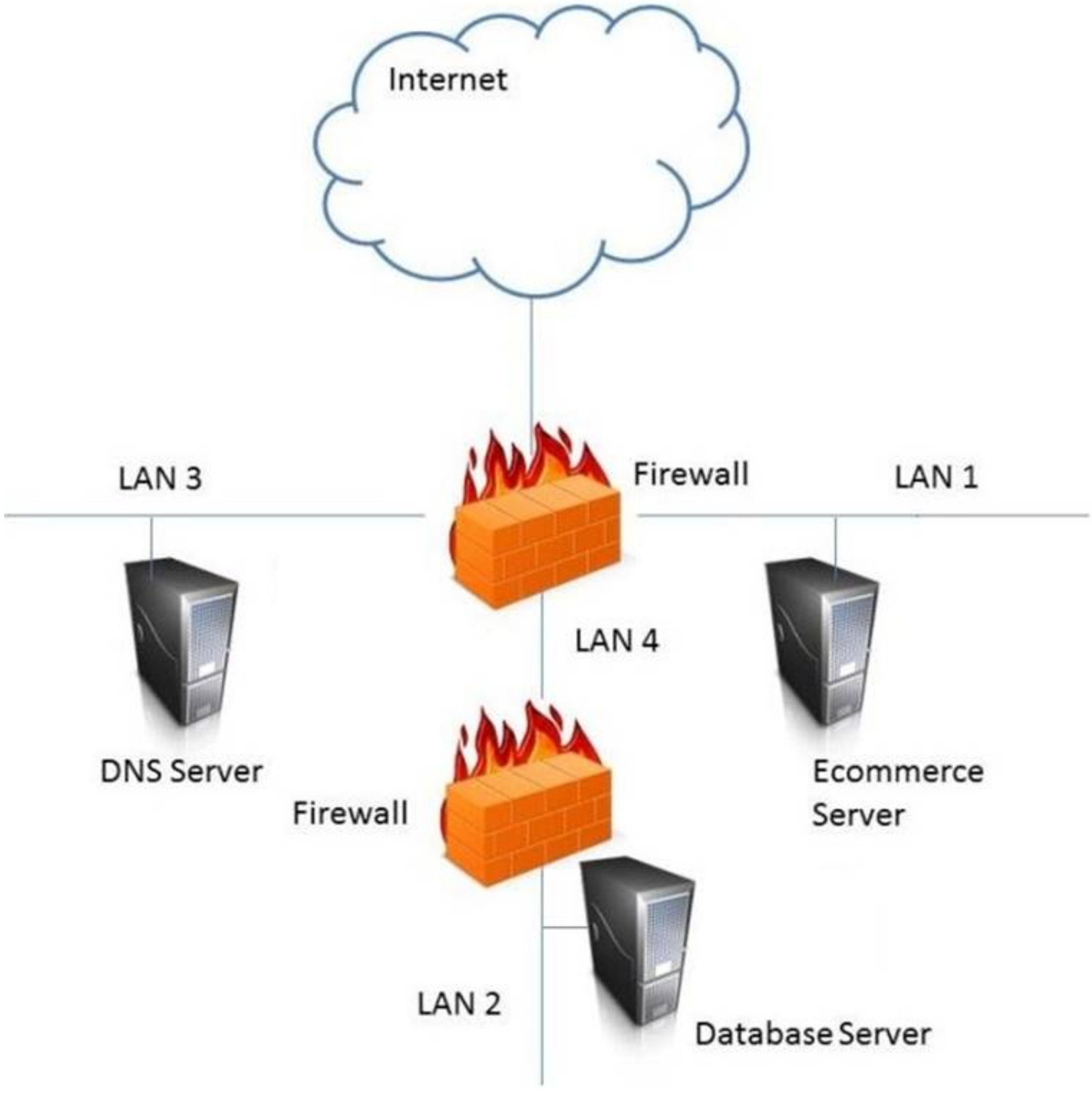
Answer: C

NEW QUESTION 402
- (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 404
- (Exam Topic 11)
In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?



A. Mastered
B. Not Mastered

Answer: A

Explanation:
LAN 4

NEW QUESTION 409
- (Exam Topic 11)
Which of the following is the PRIMARY issue when collecting detailed log information?

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

Answer: B

NEW QUESTION 414
- (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 417
- (Exam Topic 11)
The MAIN reason an organization conducts a security authorization process is to

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

Answer: A

NEW QUESTION 419
- (Exam Topic 11)
Which of the following could elicit a Denial of Service (DoS) attack against a credential management system?

A. Delayed revocation or destruction of credentials
B. Modification of Certificate Revocation List
C. Unauthorized renewal or re-issuance
D. Token use after decommissioning

Answer: B

NEW QUESTION 424
- (Exam Topic 11)
Which of the following provides the minimum set of privileges required to perform a job function and restricts the user to a domain with the required privileges?

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

Answer: B

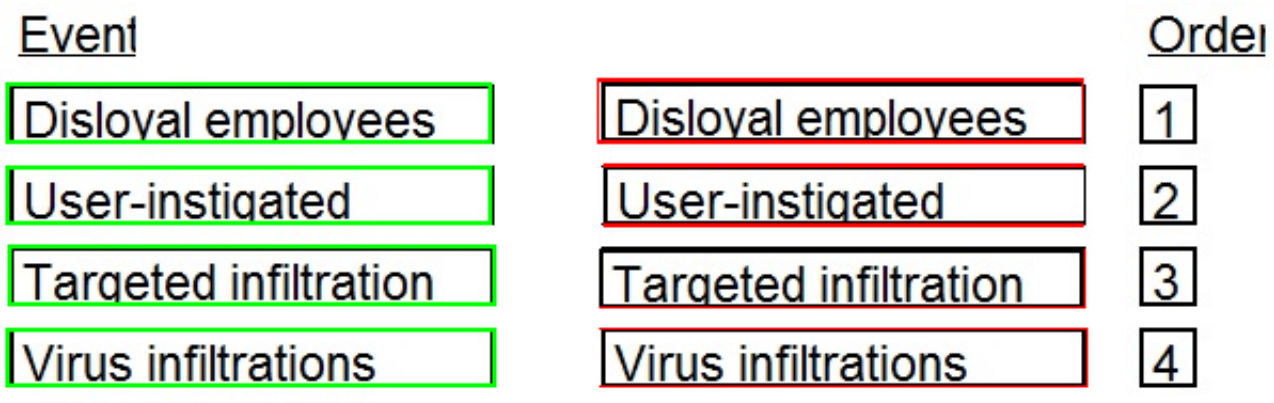
NEW QUESTION 429
- (Exam Topic 11)
In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?

Event		Order
Disloyal employees		1
User-instigated		2
Targeted infiltration		3
Virus infiltrations		4

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 431
- (Exam Topic 12)
As a best practice, the Security Assessment Report (SAR) should include which of the following sections?

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

Answer: B

NEW QUESTION 434
- (Exam Topic 12)
What is the difference between media marking and media labeling?

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

Answer: D

NEW QUESTION 435
- (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 437
- (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 441
- (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 443
- (Exam Topic 12)
A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

A. Enterprise asset management framework
B. Asset baseline using commercial off the shelf software

C. Asset ownership database using domain login records
D. A script to report active user logins on assets

Answer: A

NEW QUESTION 446
- (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 447
- (Exam Topic 12)
Which of the following adds end-to-end security inside a Layer 2 Tunneling Protocol (L2TP) Internet Protocol Security (IPSec) connection?

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

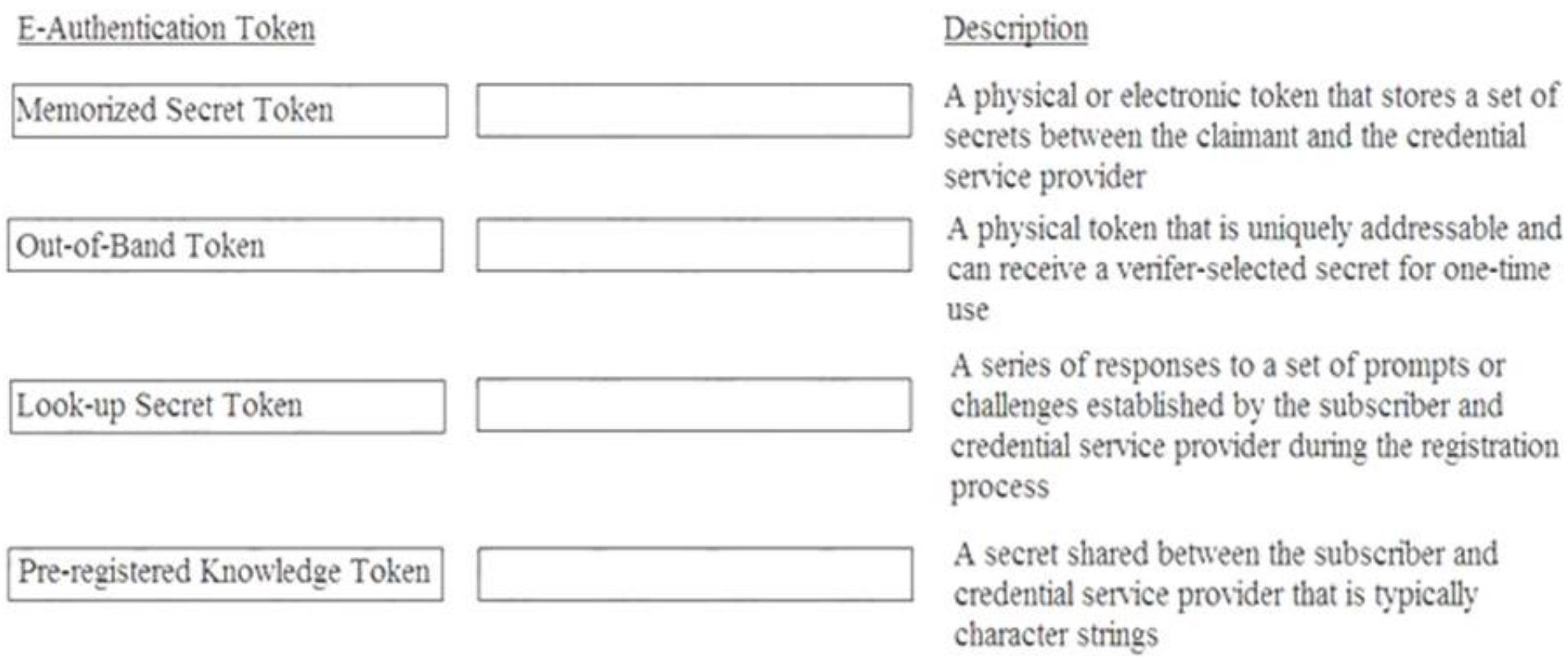
Answer: B

NEW QUESTION 448
- (Exam Topic 12)
Which of the following sets of controls should allow an investigation if an attack is not blocked by preventive controls or detected by monitoring?

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

Answer: C

NEW QUESTION 452
- (Exam Topic 12)
Match the types of e-authentication tokens to their description.
Drag each e-authentication token on the left to its corresponding description on the right.



A. Mastered
B. Not Mastered

Answer: A

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

Memorized Secret Token - A secret shared between the subscriber and credential service provider that is typically character strings

NEW QUESTION 454
- (Exam Topic 12)
Which of the following restricts the ability of an individual to carry out all the steps of a particular process?

A. Job rotation
B. Separation of duties
C. Least privilege
D. Mandatory vacations

Answer: B

NEW QUESTION 458
- (Exam Topic 12)
During which of the following processes is least privilege implemented for a user account?

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

Answer: A

NEW QUESTION 463
- (Exam Topic 12)
Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

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

Answer: B

NEW QUESTION 466
- (Exam Topic 12)
Which of the following is an advantage of on-premise Credential Management Systems?

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

Answer: B

NEW QUESTION 467
- (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 468
- (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 473
- (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 477
- (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 479
- (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 482
- (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 484
- (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 488
- (Exam Topic 12)
Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

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

Answer: A

NEW QUESTION 489
- (Exam Topic 12)
A security architect plans to reference a Mandatory Access Control (MAC) model for implementation. This indicates that which of the following properties are being prioritized?

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

Answer: C

NEW QUESTION 493
- (Exam Topic 12)
In order to assure authenticity, which of the following are required?

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

Answer: D

NEW QUESTION 494
- (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 498
- (Exam Topic 12)
Which of the following are effective countermeasures against passive network-layer attacks?

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

Answer: C

NEW QUESTION 500
- (Exam Topic 12)
From a cryptographic perspective, the service of non-repudiation includes which of the following features?

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

Answer: C

NEW QUESTION 504
- (Exam Topic 12)
When evaluating third-party applications, which of the following is the GREATEST responsibility of Information Security?

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

Answer: C

NEW QUESTION 509
- (Exam Topic 12)
Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?

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

Answer: C

NEW QUESTION 513
- (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 517
- (Exam Topic 12)

What is a characteristic of Secure Socket Layer (SSL) and Transport Layer Security (TLS)?

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

Answer: A

NEW QUESTION 522
- (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 523
- (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 524
- (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 528
- (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 533
- (Exam Topic 13)
Due to system constraints, a group of system administrators must share a high-level access set of credentials. Which of the following would be MOST appropriate to implement?

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

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 534
- (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 538
- (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 541
- (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 544
- (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 549
- (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 550
- (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 551
- (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 555

- (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 557
- (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 559
- (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 560
- (Exam Topic 13)
A Denial of Service (DoS) attack on a syslog server exploits weakness in which of the following protocols?

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

Answer: B

NEW QUESTION 564
- (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 566
- (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 567
- (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 571
- (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 575
- (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 580
- (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

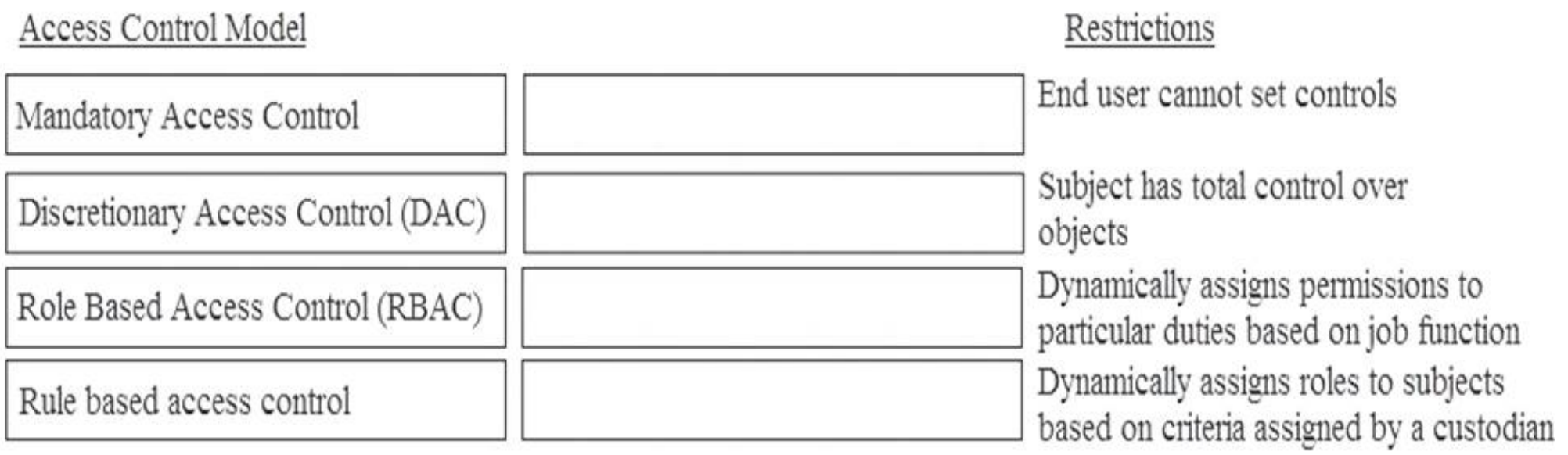
NEW QUESTION 584
- (Exam Topic 13)
Which of the following is a responsibility of the information owner?

A. Ensure that users and personnel complete the required security training to access the Information System (IS)

B. Defining proper access to the Information System (IS), including privileges or access rights
C. Managing identification, implementation, and assessment of common security controls
D. Ensuring the Information System (IS) is operated according to agreed upon security requirements

Answer: C

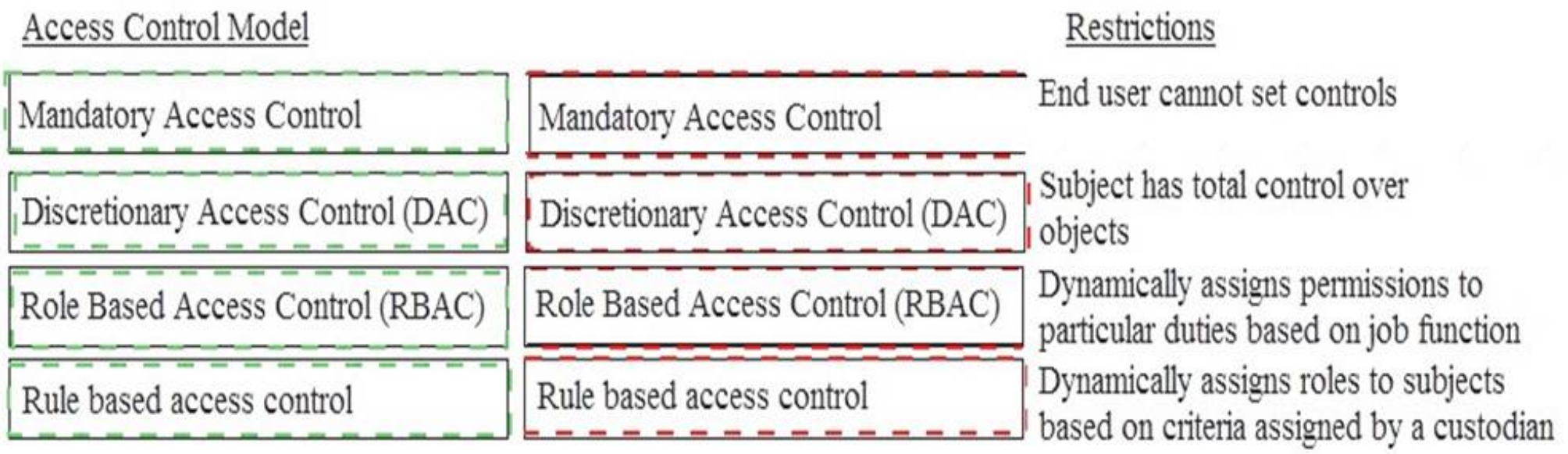
NEW QUESTION 586
- (Exam Topic 13)
Match the name of access control model with its associated restriction.
Drag each access control model to its appropriate restriction access on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 591
- (Exam Topic 13)
Which type of test would an organization perform in order to locate and target exploitable defects?

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

Answer: A

NEW QUESTION 595
- (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 600

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

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

Answer: D

NEW QUESTION 602
- (Exam Topic 13)
Which of the following is the MOST challenging issue in apprehending cyber criminals?

A. They often use sophisticated method to commit a crime.
B. It is often hard to collect and maintain integrity of digital evidence.
C. The crime is often committed from a different jurisdiction.
D. There is often no physical evidence involved.

Answer: C

NEW QUESTION 603
- (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 607
- (Exam Topic 13)
Which of the following MUST be scalable to address security concerns raised by the integration of third-party identity services?

A. Mandatory Access Controls (MAC)
B. Enterprise security architecture
C. Enterprise security procedures
D. Role Based Access Controls (RBAC)

Answer: D

NEW QUESTION 612
- (Exam Topic 13)
What MUST each information owner do when a system contains data from multiple information owners?

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

Answer: C

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 616
- (Exam Topic 13)
When developing a business case for updating a security program, the security program owner MUST do which of the following?

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

Answer: A

NEW QUESTION 619
- (Exam Topic 13)
A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report.
In which phase of the assessment was this error MOST likely made?

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

Answer: A

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 623
- (Exam Topic 13)
When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

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

Answer: D

NEW QUESTION 625
- (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 628
- (Exam Topic 13)
Which Identity and Access Management (IAM) process can be used to maintain the principle of least privilege?

A. identity provisioning
B. access recovery
C. multi-factor authentication (MFA)
D. user access review

Answer: A

NEW QUESTION 632
- (Exam Topic 13)
A chemical plan wants to upgrade the Industrial Control System (ICS) to transmit data using Ethernet instead of RS422. The project manager wants to simplify administration and maintenance by utilizing the office network infrastructure and staff to implement this upgrade.
Which of the following is the GREATEST impact on security for the network?

A. The network administrators have no knowledge of ICS
B. The ICS is now accessible from the office network
C. The ICS does not support the office password policy
D. RS422 is more reliable than Ethernet

Answer: B

NEW QUESTION 637
- (Exam Topic 13)
Which of the following is part of a Trusted Platform Module (TPM)?

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

Answer: A

NEW QUESTION 642
- (Exam Topic 13)
An organization adopts a new firewall hardening standard. How can the security professional verify that the technical staff correct implemented the new standard?

A. Perform a compliance review
B. Perform a penetration test
C. Train the technical staff
D. Survey the technical staff

Answer:

B

Explanation:
Section: Security Operations

NEW QUESTION 644
- (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 648
- (Exam Topic 13)
Which of the following is the GREATEST benefit of implementing a Role Based Access Control (RBAC) system?

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

Answer: D

NEW QUESTION 651
- (Exam Topic 13)
In a High Availability (HA) environment, what is the PRIMARY goal of working with a virtual router address as the gateway to a network?

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

Answer: C

NEW QUESTION 654
- (Exam Topic 13)
During examination of Internet history records, the following string occurs within a Unique Resource Locator (URL):
http://www.companysite.com/products/products.asp?productid=123
or 1=1
What type of attack does this indicate?

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

Answer: C

NEW QUESTION 659
- (Exam Topic 13)
Who would be the BEST person to approve an organizations information security policy?

A. Chief Information Officer (CIO)
B. Chief Information Security Officer (CISO)
C. Chief internal auditor
D. Chief Executive Officer (CEO)

Answer: B

Explanation:
Section: Security Operations

NEW QUESTION 662
- (Exam Topic 13)
In Disaster Recovery (DR) and Business Continuity (DC) training, which BEST describes a functional drill?

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

Answer:

D

NEW QUESTION 665
- (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 666
- (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 671
- (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 673
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISSP Practice Exam Features:

* CISSP Questions and Answers Updated Frequently

* CISSP Practice Questions Verified by Expert Senior Certified Staff

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

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