ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

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

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

Answer: C

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

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

Answer: B

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

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

Answer: D

NEW QUESTION 4
- (Exam Topic 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 5
- (Exam Topic 1)
What is the MOST important consideration from a data security perspective when an organization plans to relocate?

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

Answer: C

NEW QUESTION 6
- (Exam Topic 2)
Which of the following is an initial consideration when developing an information security management system?

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

Answer: B

NEW QUESTION 7
- (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 8
- (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 9
- (Exam Topic 3)
Which component of the Security Content Automation Protocol (SCAP) specification contains the data required to estimate the severity of vulnerabilities identified automated vulnerability assessments?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 3)
Which technique can be used to make an encryption scheme more resistant to a known plaintext attack?

A. Hashing the data before encryption
B. Hashing the data after encryption
C. Compressing the data after encryption
D. Compressing the data before encryption

Answer: A

NEW QUESTION 10
- (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 15
- (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 17
- (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 21
- (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 25
- (Exam Topic 4)
Which of the following factors contributes to the weakness of Wired Equivalent Privacy (WEP) protocol?

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

Answer: A

NEW QUESTION 28
- (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 31
- (Exam Topic 5)
Which of the following BEST describes an access control method utilizing cryptographic keys derived from a smart card private key that is embedded within mobile devices?

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

Answer: A

NEW QUESTION 33
- (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 35
- (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 38
- (Exam Topic 6)
Which of the following is a PRIMARY benefit of using a formalized security testing report format and structure?

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

Answer: D

NEW QUESTION 42
- (Exam Topic 7)
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 46
- (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 51
- (Exam Topic 7)
What is the MOST important step during forensic analysis when trying to learn the purpose of an unknown application?

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

Answer: D

NEW QUESTION 55
- (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 60
- (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 65
- (Exam Topic 7)
When is a Business Continuity Plan (BCP) considered to be valid?

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

Answer: D

NEW QUESTION 68
- (Exam Topic 7)
What should be the FIRST action to protect the chain of evidence when a desktop computer is involved?

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

Answer: C

NEW QUESTION 71
- (Exam Topic 7)
Which of the following is the FIRST step in the incident response process?

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

Answer: D

NEW QUESTION 73
- (Exam Topic 8)
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 vulnerability analysis has been performed and before the system detailed design begins
C. After the system preliminary design has been developed and before the data security categorization begins
D. After the business functional analysis and the data security categorization have been performed

Answer: C

NEW QUESTION 75
- (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 76
- (Exam Topic 8)
Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

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

Answer: D

NEW QUESTION 77
- (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 82
- (Exam Topic 9)
Which of the following is ensured when hashing files during chain of custody handling?

A. Availability
B. Accountability
C. Integrity
D. Non-repudiation

Answer: C

NEW QUESTION 86
- (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 88
- (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 89
- (Exam Topic 9)
In the area of disaster planning and recovery, what strategy entails the presentation of information about the plan?

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

Answer: A

NEW QUESTION 92
- (Exam Topic 9)
An internal Service Level Agreement (SLA) covering security is signed by senior managers and is in place. When should compliance to the SLA be reviewed to ensure that a good security posture is being delivered?

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

Answer: D

NEW QUESTION 93
- (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 98
- (Exam Topic 9)
Which one of the following transmission media is MOST effective in preventing data interception?

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

Answer: C

NEW QUESTION 102
- (Exam Topic 9)
Which layer of the Open Systems Interconnections (OSI) model implementation adds information concerning the logical connection between the sender and receiver?

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

Answer: C

NEW QUESTION 103
- (Exam Topic 9)
Checking routing information on e-mail to determine it is in a valid format and contains valid information is an example of which of the following anti-spam

approaches?

A. Simple Mail Transfer Protocol (SMTP) blacklist
B. Reverse Domain Name System (DNS) lookup
C. Hashing algorithm
D. Header analysis

Answer: D

NEW QUESTION 108
- (Exam Topic 9)
Which security action should be taken FIRST when computer personnel are terminated from their jobs?

A. Remove their computer access
B. Require them to turn in their badge
C. Conduct an exit interview
D. Reduce their physical access level to the facility

Answer: A

NEW QUESTION 112
- (Exam Topic 9)
The type of authorized interactions a subject can have with an object is

A. control.
B. permission.
C. procedure.
D. protocol.

Answer: B

NEW QUESTION 115
- (Exam Topic 9)
Which one of the following considerations has the LEAST impact when considering transmission security?

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

Answer: C

NEW QUESTION 119
- (Exam Topic 9)
Which of the following is considered best practice for preventing e-mail spoofing?

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

Answer: B

NEW QUESTION 122
- (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 123
- (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 127

- (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 130
- (Exam Topic 9)
An advantage of link encryption in a communications network is that it

A. makes key management and distribution easier.
B. protects data from start to finish through the entire network.
C. improves the efficiency of the transmission.
D. encrypts all information, including headers and routing information.

Answer: D

NEW QUESTION 135
- (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 140
- (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 141
- (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 144
- (Exam Topic 9)
A security professional has just completed their organization's Business Impact Analysis (BIA). Following Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) best practices, what would be the professional's NEXT step?

A. Identify and select recovery strategies.
B. Present the findings to management for funding.
C. Select members for the organization's recovery teams.
D. Prepare a plan to test the organization's ability to recover its operations.

Answer: A

NEW QUESTION 146
- (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 151
- (Exam Topic 9)
When building a data center, site location and construction factors that increase the level of vulnerability to physical threats include

A. hardened building construction with consideration of seismic factors.
B. adequate distance from and lack of access to adjacent buildings.
C. curved roads approaching the data center.
D. proximity to high crime areas of the city.

Answer: D

NEW QUESTION 154
- (Exam Topic 9)
Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

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

Answer: C

NEW QUESTION 155
- (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 156
- (Exam Topic 9)
Which of the following does the Encapsulating Security Payload (ESP) provide?

A. Authorization and integrity
B. Availability and integrity
C. Integrity and confidentiality
D. Authorization and confidentiality

Answer: C

NEW QUESTION 159
- (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 163
- (Exam Topic 9)
Which one of the following security mechanisms provides the BEST way to restrict the execution of privileged procedures?

A. Role Based Access Control (RBAC)
B. Biometric access control
C. Federated Identity Management (IdM)
D. Application hardening

Answer: A

NEW QUESTION 166
- (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 170
- (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 173
- (Exam Topic 9)
Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?

A. Transparent Database Encryption (TDE)
B. Column level database encryption
C. Volume encryption
D. Data tokenization

Answer: D

NEW QUESTION 177
- (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 178
- (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 179
- (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 181
- (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 184
- (Exam Topic 9)
Which one of the following effectively obscures network addresses from external exposure when implemented on a firewall or router?

A. Network Address Translation (NAT)
B. Application Proxy
C. Routing Information Protocol (RIP) Version 2

D. Address Masking

Answer: A

NEW QUESTION 189
- (Exam Topic 9)
Which of the following can BEST prevent security flaws occurring in outsourced software development?

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

Answer: C

NEW QUESTION 191
- (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 193
- (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 197
- (Exam Topic 9)
The birthday attack is MOST effective against which one of the following cipher technologies?

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

Answer: C

NEW QUESTION 200
- (Exam Topic 9)
A disadvantage of an application filtering firewall is that it can lead to

A. a crash of the network as a result of user activities.
B. performance degradation due to the rules applied.
C. loss of packets on the network due to insufficient bandwidth.
D. Internet Protocol (IP) spoofing by hackers.

Answer: B

NEW QUESTION 205
- (Exam Topic 9)
Which one of the following is a fundamental objective in handling an incident?

A. To restore control of the affected systems
B. To confiscate the suspect's computers
C. To prosecute the attacker
D. To perform full backups of the system

Answer: A

NEW QUESTION 208
- (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 210
- (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 214
- (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 219
- (Exam Topic 9)
In a basic SYN flood attack, what is the attacker attempting to achieve?

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

Answer: A

NEW QUESTION 221
- (Exam Topic 9)
While impersonating an Information Security Officer (ISO), an attacker obtains information from company employees about their User IDs and passwords. Which method of information gathering has the attacker used?

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

Answer: C

NEW QUESTION 226
- (Exam Topic 9)
Which of the following defines the key exchange for Internet Protocol Security (IPSec)?

A. Secure Sockets Layer (SSL) key exchange
B. Internet Key Exchange (IKE)
C. Security Key Exchange (SKE)
D. Internet Control Message Protocol (ICMP)

Answer: B

NEW QUESTION 229
- (Exam Topic 9)
Why MUST a Kerberos server be well protected from unauthorized access?

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

Answer: A

NEW QUESTION 233

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

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

Answer: A

NEW QUESTION 235
- (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 238
- (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 241
- (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 245
- (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 248
- (Exam Topic 9)
Which of the following MUST be done when promoting a security awareness program to senior management?

A. Show the need for security; identify the message and the audience
B. Ensure that the security presentation is designed to be all-inclusive
C. Notify them that their compliance is mandatory
D. Explain how hackers have enhanced information security

Answer: A

NEW QUESTION 253
- (Exam Topic 9)
What is the MOST effective countermeasure to a malicious code attack against a mobile system?

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

Answer: A

NEW QUESTION 257
- (Exam Topic 9)
Which of the following is the BEST mitigation from phishing attacks?

A. Network activity monitoring
B. Security awareness training
C. Corporate policy and procedures
D. Strong file and directory permissions

Answer: B

NEW QUESTION 261
- (Exam Topic 9)
Which of the following BEST represents the principle of open design?

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

Answer: D

NEW QUESTION 266
- (Exam Topic 9)
Why must all users be positively identified prior to using multi-user computers?

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

Answer: C

NEW QUESTION 267
- (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 269
- (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 270
- (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 272
- (Exam Topic 10)
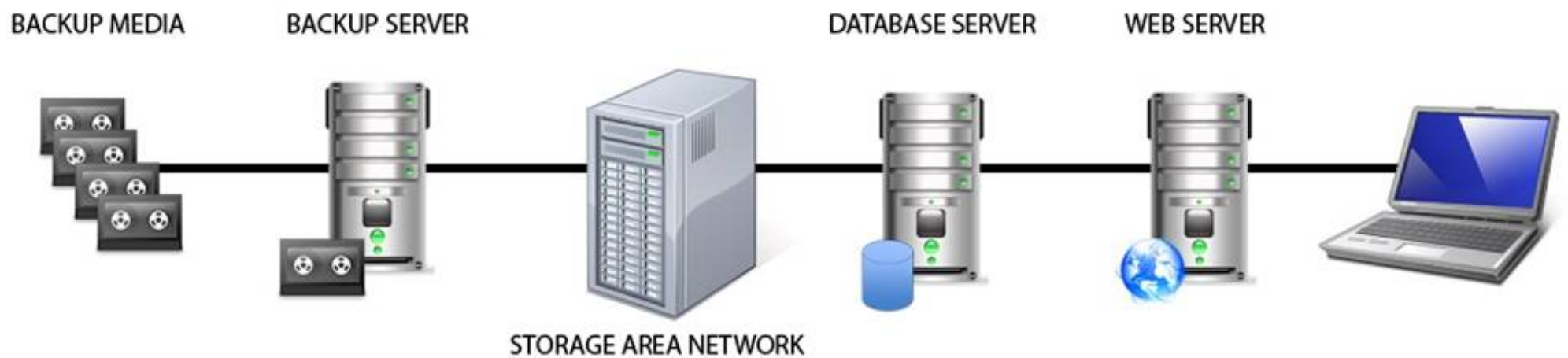What do Capability Maturity Models (CMM) serve as a benchmark for in an organization?

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

Answer: D

NEW QUESTION 277
- (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 281
- (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 285
- (Exam Topic 10)
Which of the following describes the concept of a Single Sign-On (SSO) system?

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

Answer: C

NEW QUESTION 286
- (Exam Topic 10)
Which of the following is the MOST beneficial to review when performing an IT audit?

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

Answer: C

NEW QUESTION 288
- (Exam Topic 10)
When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?

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

Answer: B

NEW QUESTION 291
- (Exam Topic 10)
What physical characteristic does a retinal scan biometric device measure?

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

Answer: C

NEW QUESTION 292
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration
functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
Which of the following will be the PRIMARY security concern as staff is released from the organization?

A. Inadequate IT support
B. Loss of data and separation of duties
C. Undocumented security controls
D. Additional responsibilities for remaining staff

Answer: B

NEW QUESTION 295
- (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 299
- (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 302
- (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 305
- (Exam Topic 10)
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
What MUST the plan include in order to reduce client-side exploitation?

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

Answer: D

NEW QUESTION 306
- (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 308
- (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 313
- (Exam Topic 10)
Which of the following BEST mitigates a replay attack against a system using identity federation and Security Assertion Markup Language (SAML) implementation?

A. Two-factor authentication
B. Digital certificates and hardware tokens
C. Timed sessions and Secure Socket Layer (SSL)
D. Passwords with alpha-numeric and special characters

Answer: C

NEW QUESTION 316
- (Exam Topic 10)
Given the various means to protect physical and logical assets, match the access management area to the technology.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 317
- (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 321
- (Exam Topic 10)
What is the BEST first step for determining if the appropriate security controls are in place for protecting data at rest?

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

Answer: B

NEW QUESTION 326
- (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 327
- (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 332
- (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 337
- (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 338
- (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 342
- (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 344
- (Exam Topic 10)
When implementing a secure wireless network, which of the following supports authentication and authorization for individual client endpoints?

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

Answer: C

NEW QUESTION 348
- (Exam Topic 10)
Refer to the information below to answer the question.
In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

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

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

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

Answer: D

NEW QUESTION 349
- (Exam Topic 10)
Which of the following is a BEST practice when traveling internationally with laptops containing Personally Identifiable Information (PII)?

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

Answer: B

NEW QUESTION 350
- (Exam Topic 10)
With data labeling, which of the following MUST be the key decision maker?

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

Answer: D

NEW QUESTION 352
- (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 355
- (Exam Topic 10)
A system is developed so that its business users can perform business functions but not user administration functions. Application administrators can perform administration functions but not user business functions. These capabilities are BEST described as

A. least privilege.
B. rule based access controls.
C. Mandatory Access Control (MAC).
D. separation of duties.

Answer: D

NEW QUESTION 356
- (Exam Topic 10)
What is the BEST method to detect the most common improper initialization problems in programming languages?

A. Use and specify a strong character encoding.
B. Use automated static analysis tools that target this type of weakness.
C. Perform input validation on any numeric inputs by assuring that they are within the expected range.
D. Use data flow analysis to minimize the number of false positives.

Answer: B

NEW QUESTION 360
- (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 364
- (Exam Topic 10)
Which of the following MUST system and database administrators be aware of and apply when configuring systems used for storing personal employee data?

A. Secondary use of the data by business users
B. The organization's security policies and standards
C. The business purpose for which the data is to be used
D. The overall protection of corporate resources and data

Answer: B

NEW QUESTION 365
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?

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

Answer: A

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

A. Removing employee's full access to the computer
B. Supervising their child's use of the computer
C. Limiting computer's access to only the employee
D. Ensuring employee understands their business conduct guidelines

Answer: A

NEW QUESTION 372
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
Which of the following BEST describes the access control methodology used?

A. Least privilege
B. Lattice Based Access Control (LBAC)
C. Role Based Access Control (RBAC)
D. Lightweight Directory Access Control (LDAP)

Answer: C

NEW QUESTION 377
- (Exam Topic 10)
Host-Based Intrusion Protection (HIPS) systems are often deployed in monitoring or learning mode during their initial implementation. What is the objective of starting in this mode?

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

Answer: D

NEW QUESTION 379
- (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 383
- (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 386
- (Exam Topic 10)
A large university needs to enable student access to university resources from their homes. Which of the following provides the BEST option for low maintenance and ease of deployment?

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

Answer: B

NEW QUESTION 389
- (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 has the MOST restrictions when writing data to any of the four files?

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

Answer: D

NEW QUESTION 393
- (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 394
- (Exam Topic 10)
Which of the following secure startup mechanisms are PRIMARILY designed to thwart attacks?

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

Answer: B

NEW QUESTION 395
- (Exam Topic 10)
From a security perspective, which of the following is a best practice to configure a Domain Name Service (DNS) system?

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

Answer: D

NEW QUESTION 396
- (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 400
- (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 403
- (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 408
- (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 413
- (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 418
- (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 422
- (Exam Topic 10)
A risk assessment report recommends upgrading all perimeter firewalls to mitigate a particular finding. Which of the following BEST supports this recommendation?

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

Answer: C

NEW QUESTION 423
- (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 426
- (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 431
- (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 436
- (Exam Topic 10)
Refer to the information below to answer the question.
Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.
Organizational policy requires the deletion of user data from Personal Digital Assistant (PDA) devices before disposal. It may not be possible to delete the user data if the device is malfunctioning. Which destruction method below provides the BEST assurance that the data has been removed?
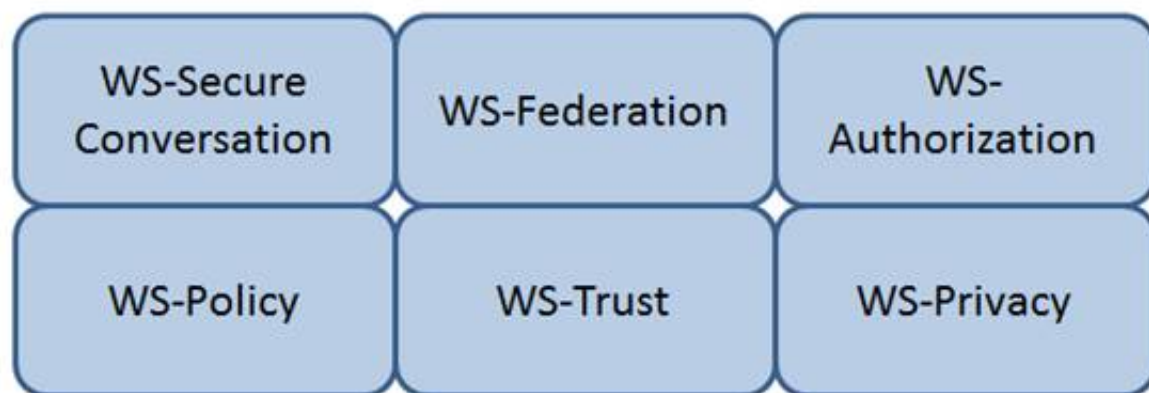
A. Knurling
B. Grinding
C. Shredding
D. Degaussing

Answer: C

NEW QUESTION 440
- (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 442
- (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 447
- (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 452
- (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 453
- (Exam Topic 11)
Which of the following is generally indicative of a replay attack when dealing with biometric authentication?

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

Answer: D

NEW QUESTION 455
- (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 457
- (Exam Topic 11)
Changes to a Trusted Computing Base (TCB) system that could impact the security posture of that system and trigger a recertification activity are documented in the

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

Answer: A

NEW QUESTION 460
- (Exam Topic 11)
Data remanence refers to which of the following?

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

Answer: D

NEW QUESTION 462

- (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 463
- (Exam Topic 11)
If compromised, which of the following would lead to the exploitation of multiple virtual machines?

A. Virtual device drivers
B. Virtual machine monitor
C. Virtual machine instance
D. Virtual machine file system

Answer: B

NEW QUESTION 467
- (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 470
- (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 473
- (Exam Topic 11)
How can lessons learned from business continuity training and actual recovery incidents BEST be used?

A. As a means for improvement
B. As alternative options for awareness and training
C. As indicators of a need for policy
D. As business function gap indicators

Answer: A

NEW QUESTION 478
- (Exam Topic 11)
Which of the following PRIMARILY contributes to security incidents in web-based applications?

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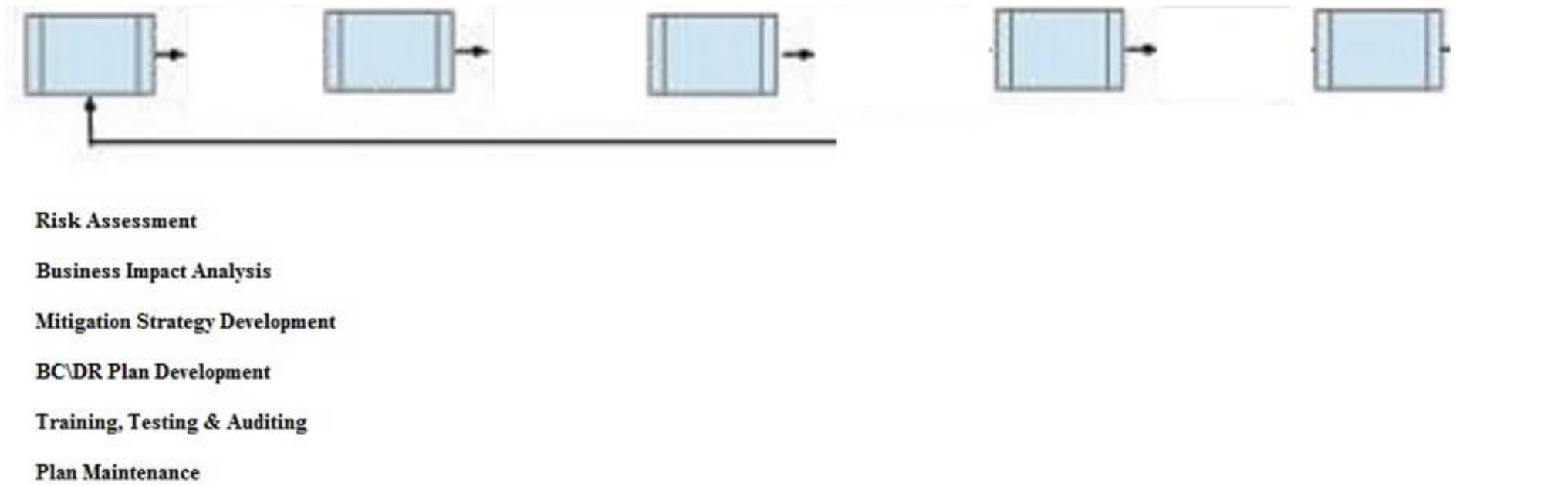D. Improper stress testing and application interfaces

Answer: C

NEW QUESTION 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.
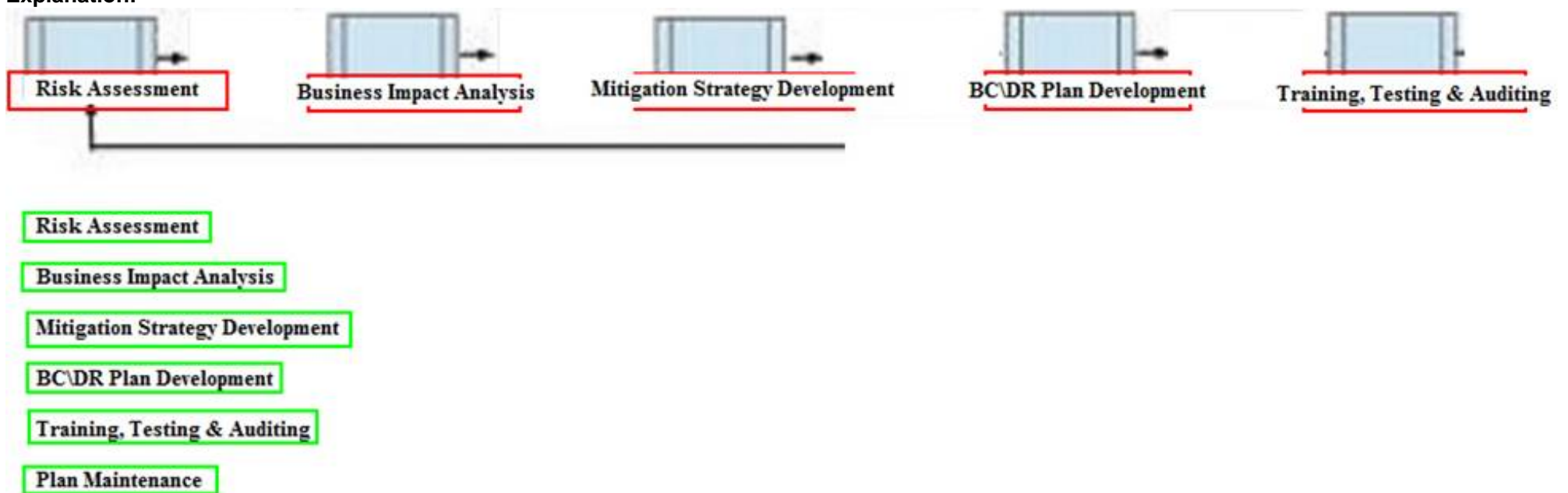What is the best approach for the CISO?
Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.

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 484
- (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 486
- (Exam Topic 11)
Disaster Recovery Plan (DRP) training material should be

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

Answer: A

NEW QUESTION 487
- (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 488
- (Exam Topic 11)
Which of the following is the BEST method to assess the effectiveness of an organization's vulnerability management program?

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

Answer: B

NEW QUESTION 490
- (Exam Topic 11)
Which of the following is the MOST likely cause of a non-malicious data breach when the source of the data breach was an un-marked file cabinet containing sensitive documents?

A. Ineffective data classification
B. Lack of data access controls
C. Ineffective identity management controls
D. Lack of Data Loss Prevention (DLP) tools

Answer: A

NEW QUESTION 493
- (Exam Topic 11)
Single Sign-On (SSO) is PRIMARILY designed to address which of the following?

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

Answer: D

NEW QUESTION 495
- (Exam Topic 11)
Which of the following standards/guidelines requires an Information Security Management System (ISMS) to be defined?

A. International Organization for Standardization (ISO) 27000 family
B. Information Technology Infrastructure Library (ITIL)
C. Payment Card Industry Data Security Standard (PCIDSS)
D. ISO/IEC 20000

Answer: A

NEW QUESTION 496
- (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 499
- (Exam Topic 11)
Which security approach will BEST minimize Personally Identifiable Information (PII) loss from a data breach?

A. A strong breach notification process
B. Limited collection of individuals' confidential data
C. End-to-end data encryption for data in transit
D. Continuous monitoring of potential vulnerabilities

Answer: B

NEW QUESTION 504
- (Exam Topic 11)
Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

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

Answer: B

NEW QUESTION 506
- (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 507
- (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 510
- (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 512
- (Exam Topic 11)
Which of the following BEST describes a rogue Access Point (AP)?

A. An AP that is not protected by a firewall
B. An AP not configured to use Wired Equivalent Privacy (WEP) with Triple Data Encryption Algorithm (3DES)
C. An AP connected to the wired infrastructure but not under the management of authorized network administrators
D. An AP infected by any kind of Trojan or Malware

Answer: C

NEW QUESTION 513
- (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 514
- (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 517
- (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 521
- (Exam Topic 11)
Retaining system logs for six months or longer can be valuable for what activities?

A. Disaster recovery and business continuity
B. Forensics and incident response
C. Identity and authorization management
D. Physical and logical access control

Answer: B

NEW QUESTION 523
- (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 528
- (Exam Topic 11)
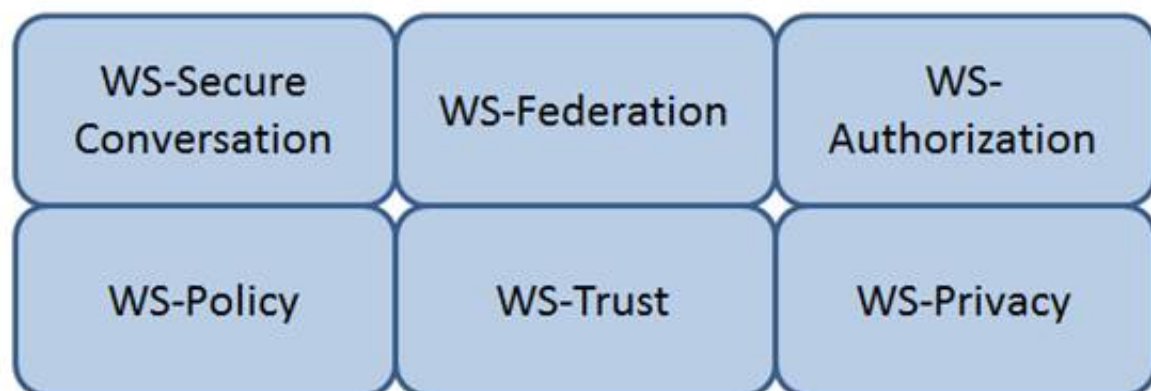What type of encryption is used to protect sensitive data in transit over a network?

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 532
- (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 536

- (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 537
- (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 542
- (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 546
- (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 547
- (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 552
- (Exam Topic 11)
Application of which of the following Institute of Electrical and Electronics Engineers (IEEE) standards will prevent an unauthorized wireless device from being attached to a network?

A. IEEE 802.1F
B. IEEE 802.1H
C. IEEE 802.1Q
D. IEEE 802.1X

Answer: D

NEW QUESTION 556
- (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
Security 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	**Security Risk Treatment**	The method used to identify feasible security risk mitigation options and plans.

NEW QUESTION 560
- (Exam Topic 11)
The PRIMARY security concern for handheld devices is the

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

Answer: C

NEW QUESTION 563
- (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 566

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

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

Answer: B

NEW QUESTION 571
- (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 575
- (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 577
- (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 579
- (Exam Topic 11)
Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic mediA.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 582
- (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 586
- (Exam Topic 11)
Which one of the following operates at the session, transport, or network layer of the Open System Interconnection (OSI) model?

A. Data at rest encryption
B. Configuration Management
C. Integrity checking software
D. Cyclic redundancy check (CRC)

Answer: D

NEW QUESTION 589
- (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 590
- (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 592
- (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 595
- (Exam Topic 11)
Which of the following BEST avoids data remanence disclosure for cloud hosted resources?

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

Answer: A

NEW QUESTION 597
- (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 602
- (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 605
- (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 607
- (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 612
- (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 615
- (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 618
- (Exam Topic 11)
The 802.1x standard provides a framework for what?
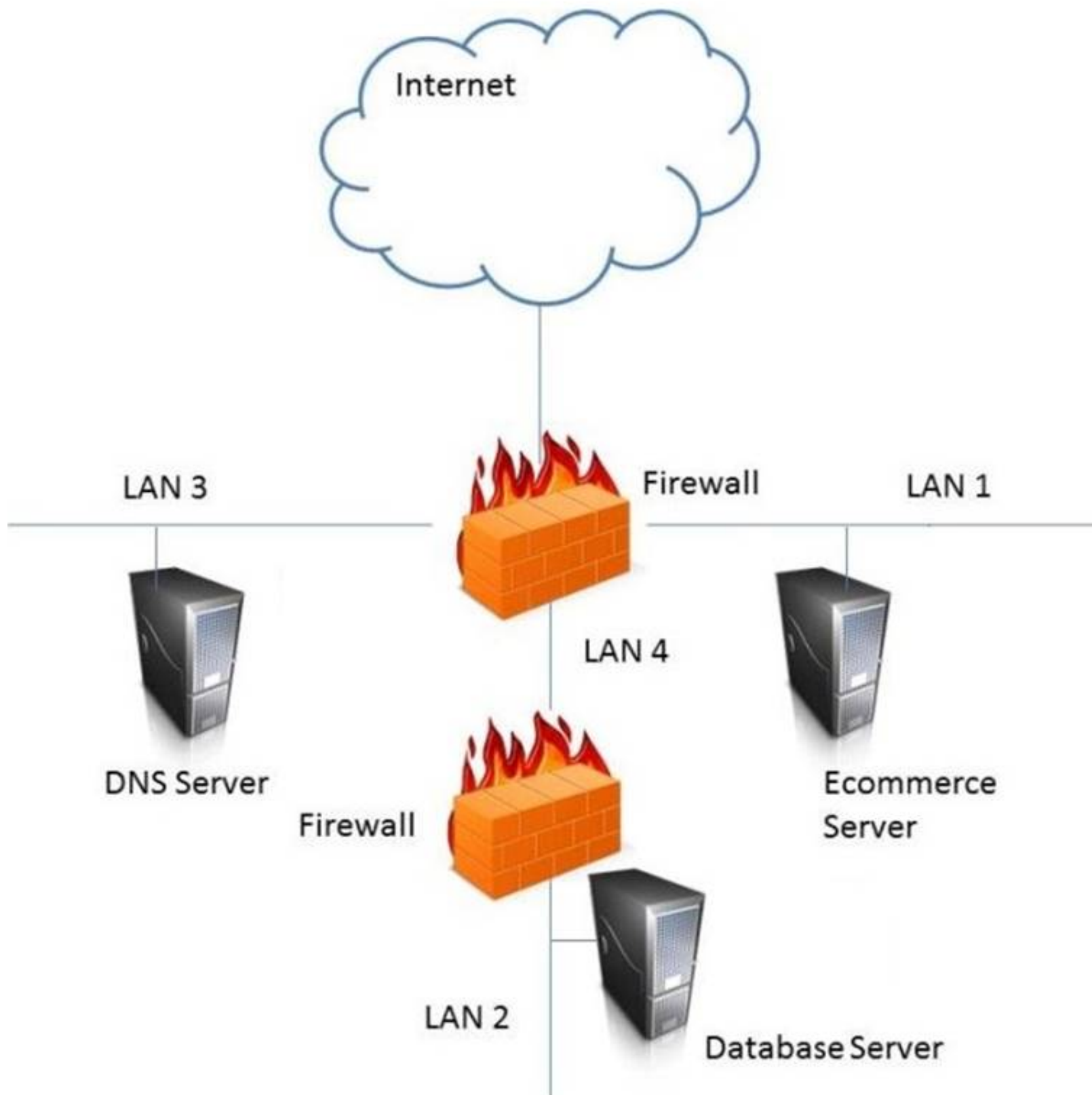
A. Network authentication for only wireless networks
B. Network authentication for wired and wireless networks
C. Wireless encryption using the Advanced Encryption Standard (AES)
D. Wireless network encryption using Secure Sockets Layer (SSL)

Answer: B

NEW QUESTION 620
- (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 622
- (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 626
- (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 630
- (Exam Topic 11)
In order for a security policy to be effective within an organization, it MUST include

A. strong statements that clearly define the problem.
B. a list of all standards that apply to the policy.
C. owner information and date of last revision.
D. disciplinary measures for non compliance.

Answer: D

NEW QUESTION 635
- (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 637
- (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 641
- (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 644
- (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 648
- (Exam Topic 12)
Which of the following is the BEST method to reduce the effectiveness of phishing attacks?

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

Answer: A

NEW QUESTION 650
- (Exam Topic 12)
An Intrusion Detection System (IDS) has recently been deployed in a Demilitarized Zone (DMZ). The IDS detects a flood of malformed packets. Which of the following BEST describes what has occurred?

A. Denial of Service (DoS) attack
B. Address Resolution Protocol (ARP) spoof
C. Buffer overflow
D. Ping flood attack

Answer: A

NEW QUESTION 651
- (Exam Topic 12)
Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

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

Answer: A

NEW QUESTION 656
- (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 660
- (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 665
- (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 666
- (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.

E-Authentication Token

Memorized Secret Token

Out-of-Band Token

Look-up Secret Token

Pre-registered Knowledge Token

Description

A physical or electronic token that stores a set of secrets between the claimant and the credential service provider

A physical token that is uniquely addressable and can receive a verifer-selected secret for one-time use

A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process

A secret shared between the subscriber and credential service provider that is typically character strings

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 667
- (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 671
- (Exam Topic 12)
What type of wireless network attack BEST describes an Electromagnetic Pulse (EMP) attack?

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

Answer: B

NEW QUESTION 676
- (Exam Topic 12)
Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item?

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

Answer: D

NEW QUESTION 678
- (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 679
- (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 681
- (Exam Topic 12)
What operations role is responsible for protecting the enterprise from corrupt or contaminated media?

A. Information security practitioner
B. Information librarian
C. Computer operator
D. Network administrator

Answer: B

NEW QUESTION 683
- (Exam Topic 12)
Which of the following BEST describes Recovery Time Objective (RTO)?

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

Answer: A

NEW QUESTION 684
- (Exam Topic 12)
Determining outage costs caused by a disaster can BEST be measured by the

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

Answer: C

NEW QUESTION 686
- (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 691
- (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 694
- (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 698
- (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 702
- (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 704
- (Exam Topic 12)
Which of the following is the PRIMARY benefit of a formalized information classification program?

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

Answer: B

NEW QUESTION 708
- (Exam Topic 12)
Which of the following is needed to securely distribute symmetric cryptographic keys?

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

Answer: C

NEW QUESTION 713
- (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 716
- (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 721
- (Exam Topic 12)
What is an advantage of Elliptic Curve Cryptography (ECC)?

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

Answer: C

NEW QUESTION 723
- (Exam Topic 12)
Which of the following is BEST suited for exchanging authentication and authorization messages in a multi-party decentralized environment?

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

Answer: B

NEW QUESTION 726
- (Exam Topic 12)
Which of the following is the MOST important consideration when developing a Disaster Recovery Plan (DRP)?

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

Answer: C

NEW QUESTION 730
- (Exam Topic 12)
In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of

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

Answer: D

NEW QUESTION 731
- (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 732
- (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 735
- (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 740
- (Exam Topic 12)
Which of the following is a characteristic of the initialization vector when using Data Encryption Standard (DES)?

A. It must be known to both sender and receiver.
B. It can be transmitted in the clear as a random number.
C. It must be retained until the last block is transmitted.
D. It can be used to encrypt and decrypt information.

Answer: B

NEW QUESTION 742
- (Exam Topic 12)
In configuration management, what baseline configuration information MUST be maintained for each computer system?

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

Answer: A

NEW QUESTION 745
- (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 748
- (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 753
- (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 758
- (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 759
- (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 764
- (Exam Topic 12)
When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?

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

Answer: D

NEW QUESTION 765
- (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 766

- (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 769
- (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 770
- (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 771
- (Exam Topic 13)
Which of the following is the MOST effective practice in managing user accounts when an employee is terminated?

A. Implement processes for automated removal of access for terminated employees.
B. Delete employee network and system IDs upon termination.
C. Manually remove terminated employee user-access to all systems and applications.
D. Disable terminated employee network ID to remove all access.

Answer: B

NEW QUESTION 772
- (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 776
- (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 779
- (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 783
- (Exam Topic 13)
An organization's security policy delegates to the data owner the ability to assign which user roles have access to a particular resource. What type of authorization mechanism is being used?

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

Answer: A

NEW QUESTION 788
- (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 793
- (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 796
- (Exam Topic 13)
What is the MAIN reason for testing a Disaster Recovery Plan (DRP)?

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

Answer: B

NEW QUESTION 801
- (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 806
- (Exam Topic 13)
Which of the following are important criteria when designing procedures and acceptance criteria for acquired software?

A. Code quality, security, and origin
B. Architecture, hardware, and firmware
C. Data quality, provenance, and scaling
D. Distributed, agile, and bench testing

Answer: A

NEW QUESTION 811
- (Exam Topic 13)
Which of the following combinations would MOST negatively affect availability?

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

Answer: A

NEW QUESTION 816
- (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 819
- (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 820
- (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 825
- (Exam Topic 13)
Which security modes is MOST commonly used in a commercial environment because it protects the integrity
of financial and accounting data?

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

Answer: C

NEW QUESTION 830
- (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 835
- (Exam Topic 13)
When determining who can accept the risk associated with a vulnerability, which of the following is MOST
important?

A. Countermeasure effectiveness
B. Type of potential loss
C. Incident likelihood
D. Information ownership

Answer:

C

NEW QUESTION 837
- (Exam Topic 13)
Which of the following is a characteristic of an internal audit?

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

Answer: D

NEW QUESTION 838
- (Exam Topic 13)
A security practitioner is tasked with securing the organization's Wireless Access Points (WAP). Which of these is the MOST effective way of restricting this environment to authorized users?

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

Answer: D

NEW QUESTION 840
- (Exam Topic 13)
What can happen when an Intrusion Detection System (IDS) is installed inside a firewall-protected internal network?

A. The IDS can detect failed administrator logon attempts from servers.
B. The IDS can increase the number of packets to analyze.
C. The firewall can increase the number of packets to analyze.
D. The firewall can detect failed administrator login attempts from servers

Answer: A

NEW QUESTION 844
- (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 848
- (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 851
- (Exam Topic 13)
Which of the following is a common characteristic of privacy?

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

Answer: A

NEW QUESTION 854
- (Exam Topic 13)
What does electronic vaulting accomplish?

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

D. It automates the Disaster Recovery Process (DRP)

Answer: A

Explanation:
Section: Security Operations

NEW QUESTION 859
- (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 863
- (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.

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:

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

NEW QUESTION 868
......

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

Answer: C

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

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

Answer: B

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

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

Answer: D

NEW QUESTION 4
- (Exam Topic 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 5
- (Exam Topic 1)
What is the MOST important consideration from a data security perspective when an organization plans to relocate?

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

Answer: C

NEW QUESTION 6
- (Exam Topic 2)
Which of the following is an initial consideration when developing an information security management system?

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

Answer: B

NEW QUESTION 7
- (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 8
- (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 9
- (Exam Topic 3)
Which component of the Security Content Automation Protocol (SCAP) specification contains the data required to estimate the severity of vulnerabilities identified automated vulnerability assessments?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 3)
Which technique can be used to make an encryption scheme more resistant to a known plaintext attack?

A. Hashing the data before encryption
B. Hashing the data after encryption
C. Compressing the data after encryption
D. Compressing the data before encryption

Answer: A

NEW QUESTION 10
- (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 15
- (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 17
- (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 21
- (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 25
- (Exam Topic 4)
Which of the following factors contributes to the weakness of Wired Equivalent Privacy (WEP) protocol?

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

Answer: A

NEW QUESTION 28
- (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 31
- (Exam Topic 5)
Which of the following BEST describes an access control method utilizing cryptographic keys derived from a smart card private key that is embedded within mobile devices?

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

Answer: A

NEW QUESTION 33
- (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 35
- (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 38
- (Exam Topic 6)
Which of the following is a PRIMARY benefit of using a formalized security testing report format and structure?

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

Answer: D

NEW QUESTION 42
- (Exam Topic 7)
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 46
- (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 51
- (Exam Topic 7)
What is the MOST important step during forensic analysis when trying to learn the purpose of an unknown application?

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

Answer: D

NEW QUESTION 55
- (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 60
- (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 65
- (Exam Topic 7)
When is a Business Continuity Plan (BCP) considered to be valid?

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

Answer: D

NEW QUESTION 68
- (Exam Topic 7)
What should be the FIRST action to protect the chain of evidence when a desktop computer is involved?

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

Answer: C

NEW QUESTION 71
- (Exam Topic 7)
Which of the following is the FIRST step in the incident response process?

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

Answer: D

NEW QUESTION 73
- (Exam Topic 8)
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 vulnerability analysis has been performed and before the system detailed design begins
C. After the system preliminary design has been developed and before the data security categorization begins
D. After the business functional analysis and the data security categorization have been performed

Answer: C

NEW QUESTION 75
- (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 76
- (Exam Topic 8)
Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

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

Answer: D

NEW QUESTION 77
- (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 82
- (Exam Topic 9)
Which of the following is ensured when hashing files during chain of custody handling?

A. Availability
B. Accountability
C. Integrity
D. Non-repudiation

Answer: C

NEW QUESTION 86
- (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 88
- (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 89
- (Exam Topic 9)
In the area of disaster planning and recovery, what strategy entails the presentation of information about the plan?

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

Answer: A

NEW QUESTION 92
- (Exam Topic 9)
An internal Service Level Agreement (SLA) covering security is signed by senior managers and is in place. When should compliance to the SLA be reviewed to ensure that a good security posture is being delivered?

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

Answer: D

NEW QUESTION 93
- (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 98
- (Exam Topic 9)
Which one of the following transmission media is MOST effective in preventing data interception?

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

Answer: C

NEW QUESTION 102
- (Exam Topic 9)
Which layer of the Open Systems Interconnections (OSI) model implementation adds information concerning the logical connection between the sender and receiver?

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

Answer: C

NEW QUESTION 103
- (Exam Topic 9)
Checking routing information on e-mail to determine it is in a valid format and contains valid information is an example of which of the following anti-spam

approaches?

A. Simple Mail Transfer Protocol (SMTP) blacklist
B. Reverse Domain Name System (DNS) lookup
C. Hashing algorithm
D. Header analysis

Answer: D

NEW QUESTION 108
- (Exam Topic 9)
Which security action should be taken FIRST when computer personnel are terminated from their jobs?

A. Remove their computer access
B. Require them to turn in their badge
C. Conduct an exit interview
D. Reduce their physical access level to the facility

Answer: A

NEW QUESTION 112
- (Exam Topic 9)
The type of authorized interactions a subject can have with an object is

A. control.
B. permission.
C. procedure.
D. protocol.

Answer: B

NEW QUESTION 115
- (Exam Topic 9)
Which one of the following considerations has the LEAST impact when considering transmission security?

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

Answer: C

NEW QUESTION 119
- (Exam Topic 9)
Which of the following is considered best practice for preventing e-mail spoofing?

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

Answer: B

NEW QUESTION 122
- (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 123
- (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 127

- (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 130
- (Exam Topic 9)
An advantage of link encryption in a communications network is that it

A. makes key management and distribution easier.
B. protects data from start to finish through the entire network.
C. improves the efficiency of the transmission.
D. encrypts all information, including headers and routing information.

Answer: D

NEW QUESTION 135
- (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 140
- (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 141
- (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 144
- (Exam Topic 9)
A security professional has just completed their organization's Business Impact Analysis (BIA). Following Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) best practices, what would be the professional's NEXT step?

A. Identify and select recovery strategies.
B. Present the findings to management for funding.
C. Select members for the organization's recovery teams.
D. Prepare a plan to test the organization's ability to recover its operations.

Answer: A

NEW QUESTION 146
- (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 151
- (Exam Topic 9)
When building a data center, site location and construction factors that increase the level of vulnerability to physical threats include

A. hardened building construction with consideration of seismic factors.
B. adequate distance from and lack of access to adjacent buildings.
C. curved roads approaching the data center.
D. proximity to high crime areas of the city.

Answer: D

NEW QUESTION 154
- (Exam Topic 9)
Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

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

Answer: C

NEW QUESTION 155
- (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 156
- (Exam Topic 9)
Which of the following does the Encapsulating Security Payload (ESP) provide?

A. Authorization and integrity
B. Availability and integrity
C. Integrity and confidentiality
D. Authorization and confidentiality

Answer: C

NEW QUESTION 159
- (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 163
- (Exam Topic 9)
Which one of the following security mechanisms provides the BEST way to restrict the execution of privileged procedures?

A. Role Based Access Control (RBAC)
B. Biometric access control
C. Federated Identity Management (IdM)
D. Application hardening

Answer: A

NEW QUESTION 166
- (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 170
- (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 173
- (Exam Topic 9)
Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?

A. Transparent Database Encryption (TDE)
B. Column level database encryption
C. Volume encryption
D. Data tokenization

Answer: D

NEW QUESTION 177
- (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 178
- (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 179
- (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 181
- (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 184
- (Exam Topic 9)
Which one of the following effectively obscures network addresses from external exposure when implemented on a firewall or router?

A. Network Address Translation (NAT)
B. Application Proxy
C. Routing Information Protocol (RIP) Version 2

D. Address Masking

Answer: A

NEW QUESTION 189
- (Exam Topic 9)
Which of the following can BEST prevent security flaws occurring in outsourced software development?

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

Answer: C

NEW QUESTION 191
- (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 193
- (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 197
- (Exam Topic 9)
The birthday attack is MOST effective against which one of the following cipher technologies?

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

Answer: C

NEW QUESTION 200
- (Exam Topic 9)
A disadvantage of an application filtering firewall is that it can lead to

A. a crash of the network as a result of user activities.
B. performance degradation due to the rules applied.
C. loss of packets on the network due to insufficient bandwidth.
D. Internet Protocol (IP) spoofing by hackers.

Answer: B

NEW QUESTION 205
- (Exam Topic 9)
Which one of the following is a fundamental objective in handling an incident?

A. To restore control of the affected systems
B. To confiscate the suspect's computers
C. To prosecute the attacker
D. To perform full backups of the system

Answer: A

NEW QUESTION 208
- (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 210
- (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 214
- (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 219
- (Exam Topic 9)
In a basic SYN flood attack, what is the attacker attempting to achieve?

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

Answer: A

NEW QUESTION 221
- (Exam Topic 9)
While impersonating an Information Security Officer (ISO), an attacker obtains information from company employees about their User IDs and passwords. Which method of information gathering has the attacker used?

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

Answer: C

NEW QUESTION 226
- (Exam Topic 9)
Which of the following defines the key exchange for Internet Protocol Security (IPSec)?

A. Secure Sockets Layer (SSL) key exchange
B. Internet Key Exchange (IKE)
C. Security Key Exchange (SKE)
D. Internet Control Message Protocol (ICMP)

Answer: B

NEW QUESTION 229
- (Exam Topic 9)
Why MUST a Kerberos server be well protected from unauthorized access?

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

Answer: A

NEW QUESTION 233

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

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

Answer: A

NEW QUESTION 235
- (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 238
- (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 241
- (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 245
- (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 248
- (Exam Topic 9)
Which of the following MUST be done when promoting a security awareness program to senior management?

A. Show the need for security; identify the message and the audience
B. Ensure that the security presentation is designed to be all-inclusive
C. Notify them that their compliance is mandatory
D. Explain how hackers have enhanced information security

Answer: A

NEW QUESTION 253
- (Exam Topic 9)
What is the MOST effective countermeasure to a malicious code attack against a mobile system?

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

Answer: A

NEW QUESTION 257
- (Exam Topic 9)
Which of the following is the BEST mitigation from phishing attacks?

A. Network activity monitoring
B. Security awareness training
C. Corporate policy and procedures
D. Strong file and directory permissions

Answer: B

NEW QUESTION 261
- (Exam Topic 9)
Which of the following BEST represents the principle of open design?

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

Answer: D

NEW QUESTION 266
- (Exam Topic 9)
Why must all users be positively identified prior to using multi-user computers?

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

Answer: C

NEW QUESTION 267
- (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 269
- (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 270
- (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 272
- (Exam Topic 10)
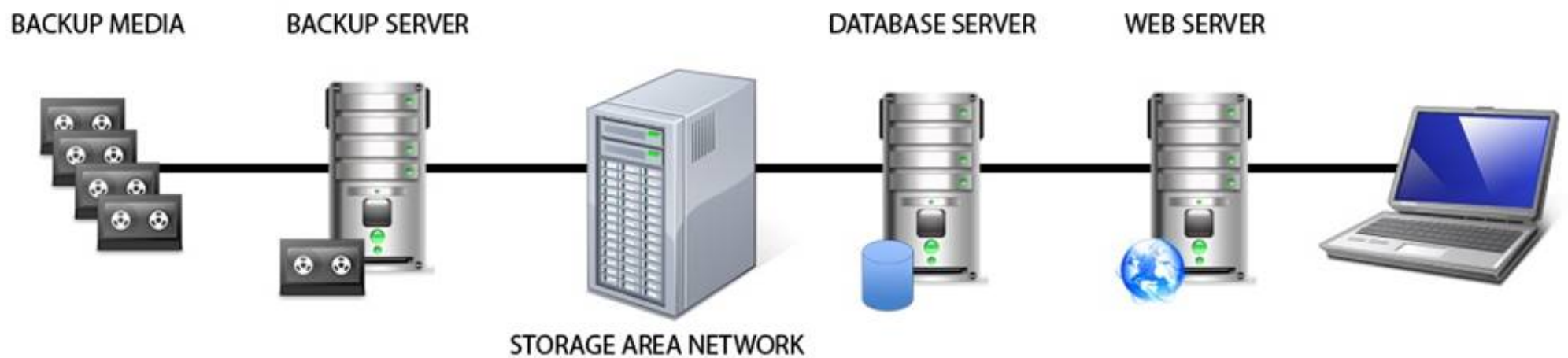What do Capability Maturity Models (CMM) serve as a benchmark for in an organization?

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

Answer: D

NEW QUESTION 277
- (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 281
- (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 285
- (Exam Topic 10)
Which of the following describes the concept of a Single Sign-On (SSO) system?

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

Answer: C

NEW QUESTION 286
- (Exam Topic 10)
Which of the following is the MOST beneficial to review when performing an IT audit?

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

Answer: C

NEW QUESTION 288
- (Exam Topic 10)
When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?

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

Answer: B

NEW QUESTION 291
- (Exam Topic 10)
What physical characteristic does a retinal scan biometric device measure?

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

Answer: C

NEW QUESTION 292
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration
functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
Which of the following will be the PRIMARY security concern as staff is released from the organization?

A. Inadequate IT support
B. Loss of data and separation of duties
C. Undocumented security controls
D. Additional responsibilities for remaining staff

Answer: B

NEW QUESTION 295
- (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 299
- (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 302
- (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 305
- (Exam Topic 10)
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
What MUST the plan include in order to reduce client-side exploitation?

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

Answer: D

NEW QUESTION 306
- (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 308
- (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 313
- (Exam Topic 10)
Which of the following BEST mitigates a replay attack against a system using identity federation and Security Assertion Markup Language (SAML) implementation?

A. Two-factor authentication
B. Digital certificates and hardware tokens
C. Timed sessions and Secure Socket Layer (SSL)
D. Passwords with alpha-numeric and special characters

Answer: C

NEW QUESTION 316
- (Exam Topic 10)
Given the various means to protect physical and logical assets, match the access management area to the technology.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 317
- (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 321
- (Exam Topic 10)
What is the BEST first step for determining if the appropriate security controls are in place for protecting data at rest?

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

Answer: B

NEW QUESTION 326
- (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 327
- (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 332
- (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 337
- (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 338
- (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 342
- (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 344
- (Exam Topic 10)
When implementing a secure wireless network, which of the following supports authentication and authorization for individual client endpoints?

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

Answer: C

NEW QUESTION 348
- (Exam Topic 10)
Refer to the information below to answer the question.
In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

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

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

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

Answer: D

NEW QUESTION 349
- (Exam Topic 10)
Which of the following is a BEST practice when traveling internationally with laptops containing Personally Identifiable Information (PII)?

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

Answer: B

NEW QUESTION 350
- (Exam Topic 10)
With data labeling, which of the following MUST be the key decision maker?

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

Answer: D

NEW QUESTION 352
- (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 355
- (Exam Topic 10)
A system is developed so that its business users can perform business functions but not user administration functions. Application administrators can perform administration functions but not user business functions. These capabilities are BEST described as

A. least privilege.
B. rule based access controls.
C. Mandatory Access Control (MAC).
D. separation of duties.

Answer: D

NEW QUESTION 356
- (Exam Topic 10)
What is the BEST method to detect the most common improper initialization problems in programming languages?

A. Use and specify a strong character encoding.
B. Use automated static analysis tools that target this type of weakness.
C. Perform input validation on any numeric inputs by assuring that they are within the expected range.
D. Use data flow analysis to minimize the number of false positives.

Answer: B

NEW QUESTION 360
- (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 364
- (Exam Topic 10)
Which of the following MUST system and database administrators be aware of and apply when configuring systems used for storing personal employee data?

A. Secondary use of the data by business users
B. The organization's security policies and standards
C. The business purpose for which the data is to be used
D. The overall protection of corporate resources and data

Answer: B

NEW QUESTION 365
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?

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

Answer: A

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

A. Removing employee's full access to the computer
B. Supervising their child's use of the computer
C. Limiting computer's access to only the employee
D. Ensuring employee understands their business conduct guidelines

Answer: A

NEW QUESTION 372
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
Which of the following BEST describes the access control methodology used?

A. Least privilege
B. Lattice Based Access Control (LBAC)
C. Role Based Access Control (RBAC)
D. Lightweight Directory Access Control (LDAP)

Answer: C

NEW QUESTION 377
- (Exam Topic 10)
Host-Based Intrusion Protection (HIPS) systems are often deployed in monitoring or learning mode during their initial implementation. What is the objective of starting in this mode?

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

Answer: D

NEW QUESTION 379
- (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 383
- (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 386
- (Exam Topic 10)
A large university needs to enable student access to university resources from their homes. Which of the following provides the BEST option for low maintenance and ease of deployment?

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

Answer: B

NEW QUESTION 389
- (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 has the MOST restrictions when writing data to any of the four files?

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

Answer: D

NEW QUESTION 393
- (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 394
- (Exam Topic 10)
Which of the following secure startup mechanisms are PRIMARILY designed to thwart attacks?

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

Answer: B

NEW QUESTION 395
- (Exam Topic 10)
From a security perspective, which of the following is a best practice to configure a Domain Name Service (DNS) system?

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

Answer: D

NEW QUESTION 396
- (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 400
- (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 403
- (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 408
- (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 413
- (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 418
- (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 422
- (Exam Topic 10)
A risk assessment report recommends upgrading all perimeter firewalls to mitigate a particular finding. Which of the following BEST supports this recommendation?

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

Answer: C

NEW QUESTION 423
- (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 426
- (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 431
- (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 436
- (Exam Topic 10)
Refer to the information below to answer the question.
Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.
Organizational policy requires the deletion of user data from Personal Digital Assistant (PDA) devices before disposal. It may not be possible to delete the user data if the device is malfunctioning. Which destruction method below provides the BEST assurance that the data has been removed?
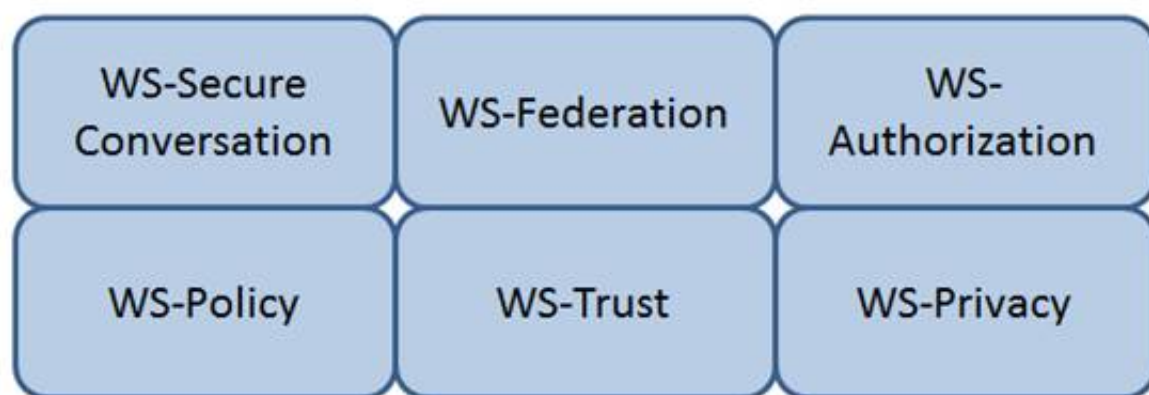
A. Knurling
B. Grinding
C. Shredding
D. Degaussing

Answer: C

NEW QUESTION 440
- (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 442
- (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 447
- (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 452
- (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 453
- (Exam Topic 11)
Which of the following is generally indicative of a replay attack when dealing with biometric authentication?

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

Answer: D

NEW QUESTION 455
- (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 457
- (Exam Topic 11)
Changes to a Trusted Computing Base (TCB) system that could impact the security posture of that system and trigger a recertification activity are documented in the

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

Answer: A

NEW QUESTION 460
- (Exam Topic 11)
Data remanence refers to which of the following?

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

Answer: D

NEW QUESTION 462

- (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 463
- (Exam Topic 11)
If compromised, which of the following would lead to the exploitation of multiple virtual machines?

A. Virtual device drivers
B. Virtual machine monitor
C. Virtual machine instance
D. Virtual machine file system

Answer: B

NEW QUESTION 467
- (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 470
- (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 473
- (Exam Topic 11)
How can lessons learned from business continuity training and actual recovery incidents BEST be used?

A. As a means for improvement
B. As alternative options for awareness and training
C. As indicators of a need for policy
D. As business function gap indicators

Answer: A

NEW QUESTION 478
- (Exam Topic 11)
Which of the following PRIMARILY contributes to security incidents in web-based applications?

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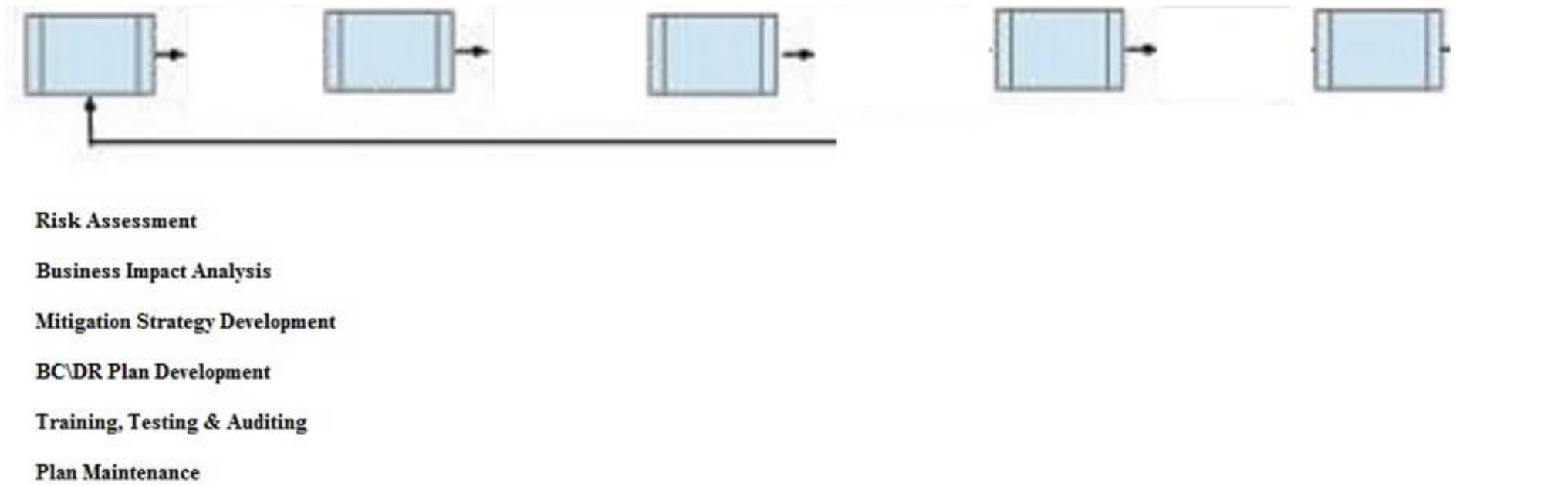D. Improper stress testing and application interfaces

Answer: C

NEW QUESTION 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.
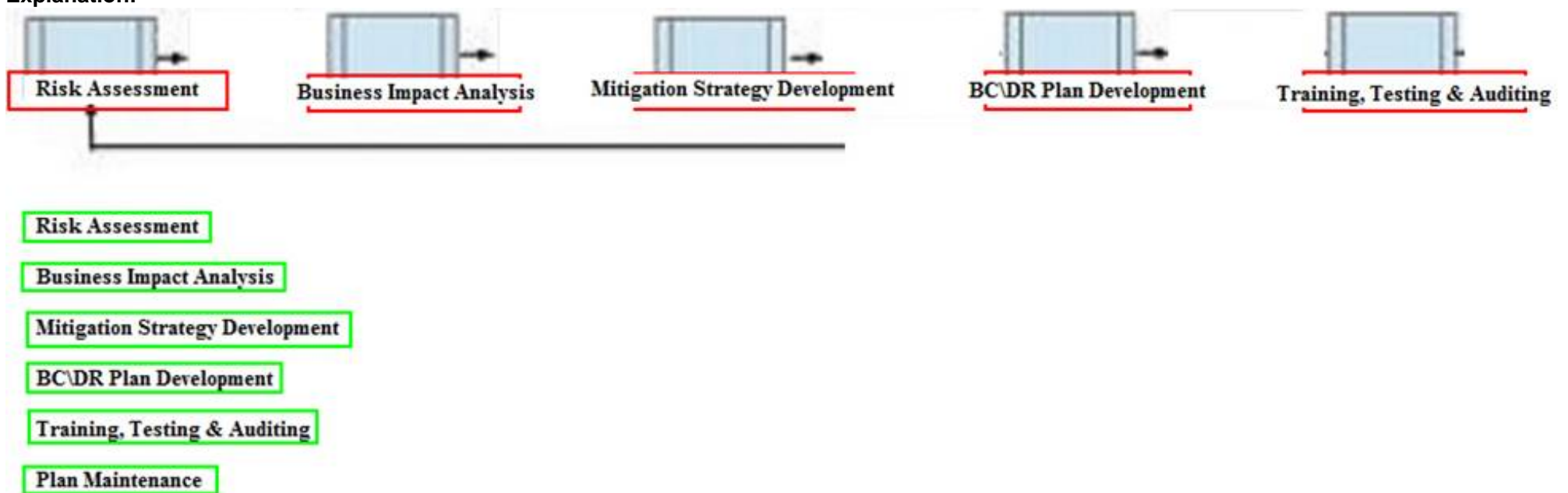What is the best approach for the CISO?
Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.

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:

Risk Assessment | Business Impact Analysis | Mitigation Strategy Development | BC\DR Plan Development | Training, Testing & Auditing

Risk Assessment

Business Impact Analysis

Mitigation Strategy Development

BC\DR Plan Development

Training, Testing & Auditing

Plan Maintenance

NEW QUESTION 484
- (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 486
- (Exam Topic 11)
Disaster Recovery Plan (DRP) training material should be

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

Answer: A

NEW QUESTION 487
- (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 488
- (Exam Topic 11)
Which of the following is the BEST method to assess the effectiveness of an organization's vulnerability management program?

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

Answer: B

NEW QUESTION 490
- (Exam Topic 11)
Which of the following is the MOST likely cause of a non-malicious data breach when the source of the data breach was an un-marked file cabinet containing sensitive documents?

A. Ineffective data classification
B. Lack of data access controls
C. Ineffective identity management controls
D. Lack of Data Loss Prevention (DLP) tools

Answer: A

NEW QUESTION 493
- (Exam Topic 11)
Single Sign-On (SSO) is PRIMARILY designed to address which of the following?

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

Answer: D

NEW QUESTION 495
- (Exam Topic 11)
Which of the following standards/guidelines requires an Information Security Management System (ISMS) to be defined?

A. International Organization for Standardization (ISO) 27000 family
B. Information Technology Infrastructure Library (ITIL)
C. Payment Card Industry Data Security Standard (PCIDSS)
D. ISO/IEC 20000

Answer: A

NEW QUESTION 496
- (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 499
- (Exam Topic 11)
Which security approach will BEST minimize Personally Identifiable Information (PII) loss from a data breach?

A. A strong breach notification process
B. Limited collection of individuals' confidential data
C. End-to-end data encryption for data in transit
D. Continuous monitoring of potential vulnerabilities

Answer: B

NEW QUESTION 504
- (Exam Topic 11)
Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

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

Answer: B

NEW QUESTION 506
- (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 507
- (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 510
- (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 512
- (Exam Topic 11)
Which of the following BEST describes a rogue Access Point (AP)?

A. An AP that is not protected by a firewall
B. An AP not configured to use Wired Equivalent Privacy (WEP) with Triple Data Encryption Algorithm (3DES)
C. An AP connected to the wired infrastructure but not under the management of authorized network administrators
D. An AP infected by any kind of Trojan or Malware

Answer: C

NEW QUESTION 513
- (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 514
- (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 517
- (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 521
- (Exam Topic 11)
Retaining system logs for six months or longer can be valuable for what activities?

A. Disaster recovery and business continuity
B. Forensics and incident response
C. Identity and authorization management
D. Physical and logical access control

Answer: B

NEW QUESTION 523
- (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 528
- (Exam Topic 11)
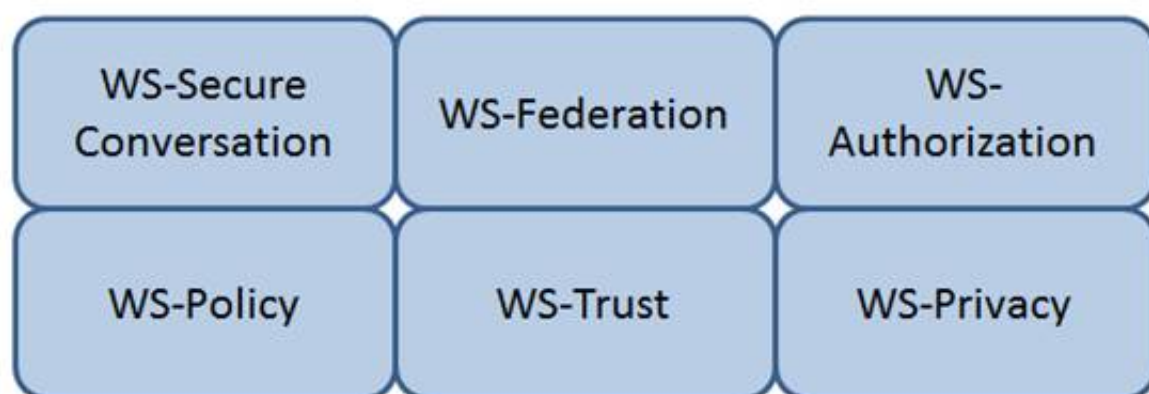What type of encryption is used to protect sensitive data in transit over a network?

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 532
- (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 536

- (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 537
- (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 542
- (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 546
- (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 547
- (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 552
- (Exam Topic 11)

Application of which of the following Institute of Electrical and Electronics Engineers (IEEE) standards will prevent an unauthorized wireless device from being attached to a network?

A. IEEE 802.1F
B. IEEE 802.1H
C. IEEE 802.1Q
D. IEEE 802.1X

Answer: D

NEW QUESTION 556
- (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

| Security Risk Treatment | Protection Needs | Definition |

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

NEW QUESTION 560
- (Exam Topic 11)
The PRIMARY security concern for handheld devices is the

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

Answer: C

NEW QUESTION 563
- (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 566

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

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

Answer: B

NEW QUESTION 571
- (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 575
- (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 577
- (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 579
- (Exam Topic 11)
Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic mediA.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 582
- (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 586
- (Exam Topic 11)
Which one of the following operates at the session, transport, or network layer of the Open System Interconnection (OSI) model?

A. Data at rest encryption
B. Configuration Management
C. Integrity checking software
D. Cyclic redundancy check (CRC)

Answer: D

NEW QUESTION 589
- (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 590
- (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 592
- (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 595
- (Exam Topic 11)
Which of the following BEST avoids data remanence disclosure for cloud hosted resources?

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

Answer: A

NEW QUESTION 597
- (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 602
- (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 605
- (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 607
- (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 612
- (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 615
- (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 618
- (Exam Topic 11)
The 802.1x standard provides a framework for what?
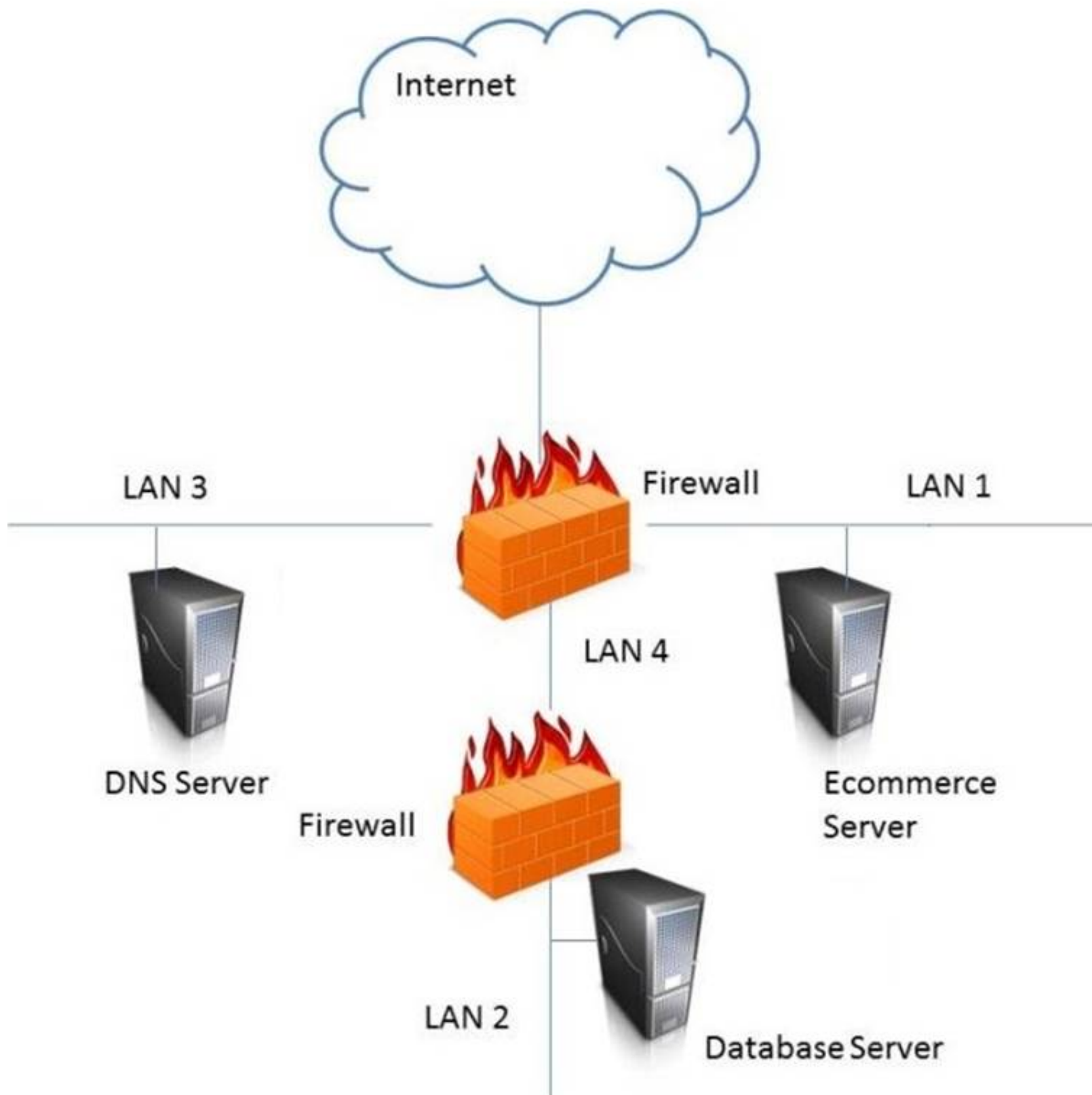
A. Network authentication for only wireless networks
B. Network authentication for wired and wireless networks
C. Wireless encryption using the Advanced Encryption Standard (AES)
D. Wireless network encryption using Secure Sockets Layer (SSL)

Answer: B

NEW QUESTION 620
- (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 622
- (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 626
- (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 630
- (Exam Topic 11)
In order for a security policy to be effective within an organization, it MUST include

A. strong statements that clearly define the problem.
B. a list of all standards that apply to the policy.
C. owner information and date of last revision.
D. disciplinary measures for non compliance.

Answer: D

NEW QUESTION 635
- (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 637
- (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 641
- (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 644
- (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 648
- (Exam Topic 12)
Which of the following is the BEST method to reduce the effectiveness of phishing attacks?

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

Answer: A

NEW QUESTION 650
- (Exam Topic 12)
An Intrusion Detection System (IDS) has recently been deployed in a Demilitarized Zone (DMZ). The IDS detects a flood of malformed packets. Which of the following BEST describes what has occurred?

A. Denial of Service (DoS) attack
B. Address Resolution Protocol (ARP) spoof
C. Buffer overflow
D. Ping flood attack

Answer: A

NEW QUESTION 651
- (Exam Topic 12)
Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

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

Answer: A

NEW QUESTION 656
- (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 660
- (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 665
- (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 666
- (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 667
- (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 671
- (Exam Topic 12)
What type of wireless network attack BEST describes an Electromagnetic Pulse (EMP) attack?

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

Answer: B

NEW QUESTION 676
- (Exam Topic 12)
Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item?

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

Answer: D

NEW QUESTION 678
- (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 679
- (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 681
- (Exam Topic 12)
What operations role is responsible for protecting the enterprise from corrupt or contaminated media?

A. Information security practitioner
B. Information librarian
C. Computer operator
D. Network administrator

Answer: B

NEW QUESTION 683
- (Exam Topic 12)
Which of the following BEST describes Recovery Time Objective (RTO)?

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

Answer: A

NEW QUESTION 684
- (Exam Topic 12)
Determining outage costs caused by a disaster can BEST be measured by the

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

Answer: C

NEW QUESTION 686
- (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 691
- (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 694
- (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 698
- (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 702
- (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 704
- (Exam Topic 12)
Which of the following is the PRIMARY benefit of a formalized information classification program?

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

Answer: B

NEW QUESTION 708
- (Exam Topic 12)
Which of the following is needed to securely distribute symmetric cryptographic keys?

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

Answer: C

NEW QUESTION 713
- (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 716
- (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 721
- (Exam Topic 12)
What is an advantage of Elliptic Curve Cryptography (ECC)?

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

Answer: C

NEW QUESTION 723
- (Exam Topic 12)
Which of the following is BEST suited for exchanging authentication and authorization messages in a multi-party decentralized environment?

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

Answer: B

NEW QUESTION 726
- (Exam Topic 12)
Which of the following is the MOST important consideration when developing a Disaster Recovery Plan (DRP)?

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

Answer: C

NEW QUESTION 730
- (Exam Topic 12)
In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of

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

Answer: D

NEW QUESTION 731
- (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 732
- (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 735
- (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 740
- (Exam Topic 12)
Which of the following is a characteristic of the initialization vector when using Data Encryption Standard (DES)?

A. It must be known to both sender and receiver.
B. It can be transmitted in the clear as a random number.
C. It must be retained until the last block is transmitted.
D. It can be used to encrypt and decrypt information.

Answer: B

NEW QUESTION 742
- (Exam Topic 12)
In configuration management, what baseline configuration information MUST be maintained for each computer system?

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

Answer: A

NEW QUESTION 745
- (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 748
- (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 753
- (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 758
- (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 759
- (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 764
- (Exam Topic 12)
When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?

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

Answer: D

NEW QUESTION 765
- (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 766

- (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 769
- (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 770
- (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 771
- (Exam Topic 13)
Which of the following is the MOST effective practice in managing user accounts when an employee is terminated?

A. Implement processes for automated removal of access for terminated employees.
B. Delete employee network and system IDs upon termination.
C. Manually remove terminated employee user-access to all systems and applications.
D. Disable terminated employee network ID to remove all access.

Answer: B

NEW QUESTION 772
- (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 776
- (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 779
- (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 783
- (Exam Topic 13)
An organization's security policy delegates to the data owner the ability to assign which user roles have access to a particular resource. What type of authorization mechanism is being used?

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

Answer: A

NEW QUESTION 788
- (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 793
- (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 796
- (Exam Topic 13)
What is the MAIN reason for testing a Disaster Recovery Plan (DRP)?

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

Answer: B

NEW QUESTION 801
- (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 806
- (Exam Topic 13)
Which of the following are important criteria when designing procedures and acceptance criteria for acquired software?

A. Code quality, security, and origin
B. Architecture, hardware, and firmware
C. Data quality, provenance, and scaling
D. Distributed, agile, and bench testing

Answer: A

NEW QUESTION 811
- (Exam Topic 13)
Which of the following combinations would MOST negatively affect availability?

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

Answer: A

NEW QUESTION 816
- (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 819
- (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 820
- (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 825
- (Exam Topic 13)
Which security modes is MOST commonly used in a commercial environment because it protects the integrity
of financial and accounting data?

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

Answer: C

NEW QUESTION 830
- (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 835
- (Exam Topic 13)
When determining who can accept the risk associated with a vulnerability, which of the following is MOST
important?

A. Countermeasure effectiveness
B. Type of potential loss
C. Incident likelihood
D. Information ownership

Answer:

C

NEW QUESTION 837
- (Exam Topic 13)
Which of the following is a characteristic of an internal audit?

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

Answer: D

NEW QUESTION 838
- (Exam Topic 13)
A security practitioner is tasked with securing the organization's Wireless Access Points (WAP). Which of these is the MOST effective way of restricting this environment to authorized users?

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

Answer: D

NEW QUESTION 840
- (Exam Topic 13)
What can happen when an Intrusion Detection System (IDS) is installed inside a firewall-protected internal network?

A. The IDS can detect failed administrator logon attempts from servers.
B. The IDS can increase the number of packets to analyze.
C. The firewall can increase the number of packets to analyze.
D. The firewall can detect failed administrator login attempts from servers

Answer: A

NEW QUESTION 844
- (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 848
- (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 851
- (Exam Topic 13)
Which of the following is a common characteristic of privacy?

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

Answer: A

NEW QUESTION 854
- (Exam Topic 13)
What does electronic vaulting accomplish?

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

D. It automates the Disaster Recovery Process (DRP)

Answer: A

Explanation:
Section: Security Operations

NEW QUESTION 859
- (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 863
- (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.

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:

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

NEW QUESTION 868
......

Relate Links

100% Pass Your CISSP Exam with Exambible Prep Materials

https://www.exambible.com/CISSP-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/