ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

NEW QUESTION 1
- (Exam Topic 15)
In addition to life, protection of which of the following elements is MOST important when planning a data center site?

A. Data and hardware
B. Property and operations
C. Profits and assets
D. Resources and reputation

Answer: D

NEW QUESTION 2
- (Exam Topic 15)
Which of the following is an important requirement when designing a secure remote access system?

A. Configure a Demilitarized Zone (DMZ) to ensure that user and service traffic is separated.
B. Provide privileged access rights to computer files and systems.
C. Ensure that logging and audit controls are included.
D. Reduce administrative overhead through password self service.

Answer: C

NEW QUESTION 3
- (Exam Topic 15)
Two computers, each with a single connection on the same physical 10 gigabit Ethernet network segment, need to communicate with each other. The first machine has a single Internet Protocol (IP) Classless
Inter-Domain Routing (CIDR) address of 192.168.1.3/30 and the second machine has an IP/CIDR address 192.168.1.6/30. Which of the following is correct?

A. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network bridge in order to communicate.
B. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network bridge in order to communicate.
C. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network router in order to communicate.
D. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network router in order to communicate.

Answer: B

NEW QUESTION 4
- (Exam Topic 15)
Which of the following access control models is MOST restrictive?

A. Discretionary Access Control (DAC)
B. Mandatory Access Control (MAC)
C. Role Based Access Control (RBAC)
D. Rule based access control

Answer: B

NEW QUESTION 5
- (Exam Topic 15)
A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes. What is the
BEST design approach to securing this environment?

A. Place firewalls around critical devices, isolating them from the rest of the environment.
B. Layer multiple detective and preventative technologies at the environment perimeter.
C. Use reverse proxies to create a secondary "shadow" environment for critical systems.
D. Align risk across all interconnected elements to ensure critical threats are detected and handled.

Answer: B

NEW QUESTION 6
- (Exam Topic 15)
Which of the following provides the MOST secure method for Network Access Control (NAC)?

A. Media Access Control (MAC) filtering
B. 802.IX authentication
C. Application layer filtering
D. Network Address Translation (NAT)

Answer: B

NEW QUESTION 7
- (Exam Topic 15)
Which of the following actions should be undertaken prior to deciding on a physical baseline Protection Profile (PP)?

A. Check the technical design.
B. Conduct a site survey.
C. Categorize assets.
D. Choose a suitable location.

Answer: A

NEW QUESTION 8
- (Exam Topic 15)
During a penetration test, what are the three PRIMARY objectives of the planning phase?

A. Determine testing goals, identify rules of engagement, and conduct an initial discovery scan.
B. Finalize management approval, determine testing goals, and gather port and service information.
C. Identify rules of engagement, finalize management approval, and determine testing goals.
D. Identify rules of engagement, document management approval, and collect system and application information.

Answer: D

NEW QUESTION 9
- (Exam Topic 15)
Which of the following is the BEST way to protect an organization's data assets?

A. Monitor and enforce adherence to security policies.
B. Encrypt data in transit and at rest using up-to-date cryptographic algorithms.
C. Create the Demilitarized Zone (DMZ) with proxies, firewalls and hardened bastion hosts.
D. Require Multi-Factor Authentication (MFA) and Separation of Duties (SoD).

Answer: B

NEW QUESTION 10
- (Exam Topic 15)
Which of the following is the strongest physical access control?

A. Biometrics and badge reader
B. Biometrics, a password, and personal identification number (PIN)
C. Individual password for each user
D. Biometrics, a password, and badge reader

Answer: D

NEW QUESTION 10
- (Exam Topic 15)
In order to support the least privilege security principle when a resource is transferring within the organization from a production support system administration role to a developer role, what changes should be made to the resource’s access to the production operating system (OS) directory structure?

A. From Read Only privileges to No Access Privileges
B. From Author privileges to Administrator privileges
C. From Administrator privileges to No Access privileges
D. From No Access Privileges to Author privileges

Answer: C

NEW QUESTION 15
- (Exam Topic 15)
During a Disaster Recovery (DR) simulation, it is discovered that the shared recovery site lacks adequate data restoration capabilities to support the implementation of multiple plans simultaneously. What would be impacted by this fact if left unchanged?

A. Recovery Point Objective (RPO)
B. Recovery Time Objective (RTO)
C. Business Impact Analysis (BIA)
D. Return on Investment (ROI)
E. A

Answer: E

NEW QUESTION 18
- (Exam Topic 15)
Which of the following is the BEST way to protect against Structured Query language (SQL) injection?

A. Enforce boundary checking.
B. Ratfrict um of SELECT command.
C. Restrict HyperText Markup Language (HTML) source code
D. Use stored procedures.

Answer: D

NEW QUESTION 19
- (Exam Topic 15)
Which of the following security objectives for industrial control systems (ICS) can be adapted to securing any Internet of Things (IoT) system?

A. Prevent unauthorized modification of data.
B. Restore the system after an incident.
C. Detect security events and incidents.
D. Protect individual components from exploitation

Answer: D

NEW QUESTION 23
- (Exam Topic 15)
Why is authentication by ownership stronger than authentication by knowledge?

A. It is easier to change.
B. It can be kept on the user's person.
C. It is more difficult to duplicate.
D. It is simpler to control.

Answer: B

NEW QUESTION 24
- (Exam Topic 15)
What is the BEST control to be implemented at a login page in a web application to mitigate the ability to enumerate users?

A. Implement a generic response for a failed login attempt.
B. Implement a strong password during account registration.
C. Implement numbers and special characters in the user name.
D. Implement two-factor authentication (2FA) to login process.

Answer: A

NEW QUESTION 26
- (Exam Topic 15)
The disaster recovery (DR) process should always include

A. plan maintenance.
B. periodic vendor review.
C. financial data analysis.
D. periodic inventory review.

Answer: A

NEW QUESTION 28
- (Exam Topic 15)
Which of the following phases in the software acquisition process does developing evaluation criteria take place?

A. Follow-On
B. Planning
C. Contracting
D. Monitoring and Acceptance

Answer: D

NEW QUESTION 33
- (Exam Topic 15)
What is the FIRST step that should be considered in a Data Loss Prevention (DLP) program?

A. Configuration management (CM)
B. Information Rights Management (IRM)
C. Policy creation
D. Data classification

Answer: D

NEW QUESTION 37
- (Exam Topic 15)
Using the cipher text and resultant clear text message to derive the non-alphabetic cipher key is an example of which method of cryptanalytic attack?

A. Frequency analysis
B. Ciphertext-only attack
C. Probable-plaintext attack
D. Known-plaintext attack

Answer: D

NEW QUESTION 42
- (Exam Topic 15)
Which of the following is included in change management?

A. Business continuity testing
B. User Acceptance Testing (UAT) before implementation
C. Technical review by business owner
D. Cost-benefit analysis (CBA) after implementation

Answer: A

NEW QUESTION 47
- (Exam Topic 15)
Which of the following is MOST important to follow when developing information security controls for an organization?

A. Exercise due diligence with regard to all risk management information to tailor appropriate controls.
B. Perform a risk assessment and choose a standard that addresses existing gaps.
C. Use industry standard best practices for security controls in the organization.
D. Review all local and international standards and choose the most stringent based on location.

Answer: C

NEW QUESTION 51
- (Exam Topic 15)
What is the MOST important criterion that needs to be adhered to during the data collection process of an active investigation?

A. Capturing an image of the system
B. Maintaining the chain of custody
C. Complying with the organization's security policy
D. Outlining all actions taken during the investigation

Answer: A

NEW QUESTION 55
- (Exam Topic 15)
In which of the following system life cycle processes should security requirements be developed?

A. Risk management
B. Business analysis
C. Information management
D. System analysis

Answer: B

NEW QUESTION 56
- (Exam Topic 15)
Which of the following determines how traffic should flow based on the status of the infrastructure layer?

A. Traffic plane
B. Application plane
C. Data plane
D. Control plane

Answer: A

NEW QUESTION 61
- (Exam Topic 15)
Information Security Continuous Monitoring (1SCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management
decisions. Which of the following is the FIRST step in developing an ISCM strategy and implementing an ISCM program?

A. Define a strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
B. Conduct a vulnerability assessment to discover current threats against the environment and incorporate them into the program.
C. Respond to findings with technical management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
D. Analyze the data collected and report findings, determining the appropriate respons
E. It may be necessary to collect additional information to clarify or supplement existing monitoring data.

Answer: A

NEW QUESTION 65
- (Exam Topic 15)
Which of the following criteria ensures information is protected relative to its importance to the organization?

A. The value of the data to the organization's senior management
B. Legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification

C. Legal requirements determined by the organization headquarters' location
D. Organizational stakeholders, with classification approved by the management board

Answer: D

NEW QUESTION 68
- (Exam Topic 15)
Which of the following would qualify as an exception to the "right to be forgotten" of the General Data Protection Regulation's (GDPR)?

A. For the establishment, exercise, or defense of legal claims
B. The personal data has been lawfully processed and collected
C. The personal data remains necessary to the purpose for which it was collected
D. For the reasons of private interest

Answer: C

NEW QUESTION 73
- (Exam Topic 15)
Which of the following is a common risk with fiber optical communications, and what is the associated mitigation measure?

A. Data emanation, deploying Category (CAT) 6 and higher cable wherever feasible
B. Light leakage, deploying shielded cable wherever feasible
C. Cable damage, deploying ring architecture wherever feasible
D. Electronic eavesdropping, deploying end-to-end encryption wherever feasible

Answer: B

NEW QUESTION 74
- (Exam Topic 15)
Which of the following departments initiates the request, approval, and provisioning business process?

A. Operations
B. Human resources (HR)
C. Information technology (IT)
D. Security

Answer: A

NEW QUESTION 77
- (Exam Topic 15)
Which of the following is the MAIN difference between a network-based firewall and a host-based firewall?

A. A network-based firewall is stateful, while a host-based firewall is stateless.
B. A network-based firewall controls traffic passing through the device, while a host-based firewall controls traffic destined for the device.
C. A network-based firewall verifies network traffic, while a host-based firewall verifies processes and applications.
D. A network-based firewall blocks network intrusions, while a host-based firewall blocks malware.

Answer: B

NEW QUESTION 78
- (Exam Topic 15)
What is the benefit of an operating system (OS) feature that is designed to prevent an application from executing code from a non-executable memory region?

A. Identifies which security patches still need to be installed on the system
B. Stops memory resident viruses from propagating their payload
C. Reduces the risk of polymorphic viruses from encrypting their payload
D. Helps prevent certain exploits that store code in buffers

Answer: C

NEW QUESTION 83
- (Exam Topic 15)
An organization is trying to secure instant messaging (IM) communications through its network perimeter. Which of the following is the MOST significant challenge?

A. IM clients can interoperate between multiple vendors.
B. IM clients can run without administrator privileges.
C. IM clients can utilize random port numbers.
D. IM clients can run as executable that do not require installation.

Answer: B

NEW QUESTION 86
- (Exam Topic 15)
Which of the following is the MOST significant key management problem due to the number of keys created?

A. Keys are more difficult to provision and
B. Storage of the keys require increased security
C. Exponential growth when using asymmetric keys
D. Exponential growth when using symmetric keys

Answer: B

NEW QUESTION 89
- (Exam Topic 15)
An enterprise is developing a baseline cybersecurity standard its suppliers must meet before being awarded a contract. Which of the following statements is TRUE about the baseline cybersecurity standard?

A. It should be expressed as general requirements.
B. It should be expressed in legal terminology.
C. It should be expressed in business terminology.
D. It should be expressed as technical requirements.

Answer: D

NEW QUESTION 91
- (Exam Topic 15)
Which of the following security tools monitors devices and records the information in a central database for further analysis?

A. Security orchestration automation and response
B. Host-based intrusion detection system (HIDS)
C. Antivirus
D. Endpoint detection and response (EDR)

Answer: A

NEW QUESTION 96
- (Exam Topic 15)
Management has decided that a core application will be used on personal cellular phones. As an implementation requirement, regularly scheduled analysis of the security posture needs to be conducted. Management has also directed that continuous monitoring be implemented. Which of the following is required to accomplish management’s directive?

A. Strict integration of application management, configuration management (CM), and phone management
B. Management application installed on user phones that tracks all application events and cellular traffic
C. Enterprise-level security information and event management (SIEM) dashboard that provides full visibility of cellular phone activity
D. Routine reports generated by the user's cellular phone provider that detail security events

Answer: B

NEW QUESTION 101
- (Exam Topic 15)
Which of the following would be considered an incident if reported by a security information and event management (SIEM) system?

A. An administrator is logging in on a server through a virtual private network (VPN).
B. A log source has stopped sending data.
C. A web resource has reported a 404 error.
D. A firewall logs a connection between a client on the Internet and a web server using Transmission Control Protocol (TCP) on port 80.

Answer: C

NEW QUESTION 103
- (Exam Topic 15)
Security Software Development Life Cycle (SDLC) expects application code to be written In a consistent manner to allow ease of auditing and which of the following?

A. Protecting
B. Executing
C. Copying
D. Enhancing

Answer: A

NEW QUESTION 106
- (Exam Topic 15)
A security architect is developing an information system for a client. One of the requirements is to deliver a platform that mitigates against common vulnerabilities and attacks, What is the MOST efficient option used to prevent buffer overflow attacks?

A. Process isolation
B. Address Space Layout Randomization (ASLR)
C. Processor states
D. Access control mechanisms

Answer: B

NEW QUESTION 109
- (Exam Topic 15)
Which of the following minimizes damage to information technology (IT) equipment stored in a data center when a false fire alarm event occurs?

A. A pre-action system is installed.
B. An open system is installed.
C. A dry system is installed.
D. A wet system is installed.

Answer: C

NEW QUESTION 112
- (Exam Topic 15)
Which of the following is the PRIMARY issue when analyzing 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: D

NEW QUESTION 117
- (Exam Topic 15)
A Chief Information Security Officer (CISO) of a firm which decided to migrate to cloud has been tasked with ensuring an optimal level of security. Which of the following would be the FIRST consideration?

A. Define the cloud migration roadmap and set out which applications and data repositories should be moved into the cloud.
B. Ensure that the contract between the cloud vendor and the firm clearly defines responsibilities for operating security controls.
C. Analyze the firm's applications and data repositories to determine the relevant control requirements.
D. Request a security risk assessment of the cloud vendor be completed by an independent third-party.

Answer: A

NEW QUESTION 119
- (Exam Topic 15)
In a large company, a system administrator needs to assign users access to files using Role Based Access Control (RBAC). Which option Is an example of RBAC?

A. Mowing users access to files based on their group membership
B. Allowing users access to files based on username
C. Allowing users access to files based on the users location at time of access
D. Allowing users access to files based on the file type

Answer: A

NEW QUESTION 120
- (Exam Topic 15)
An organization is planning to have an it audit of its as a Service (SaaS) application to demonstrate to external parties that the security controls around availability are designed. The audit report must also cover a certain period of time to show the operational effectiveness of the controls. Which Service Organization Control (SOC) report would BEST fit their needs?

A. SOC 1 Type 1
B. SOC 1 Type 2
C. SOC 2 Type 1
D. SOC 2 Type 2

Answer: D

NEW QUESTION 125
- (Exam Topic 15)
Which of the following is required to verify the authenticity of a digitally signed document?

A. Digital hash of the signed document
B. Sender's private key
C. Recipient's public key
D. Agreed upon shared secret

Answer: A

NEW QUESTION 127
- (Exam Topic 15)
What documentation is produced FIRST when performing an effective physical loss control process?

A. Deterrent controls list
B. Security standards list

C. inventory list
D. Asset valuation list

Answer: C

NEW QUESTION 128
- (Exam Topic 15)
Which of the following attacks, if successful, could give an intruder complete control of a software-defined networking (SDN) architecture?

A. Sniffing the traffic of a compromised host inside the network
B. Sending control messages to open a flow that does not pass a firewall from a compromised host within the network
C. A brute force password attack on the Secure Shell (SSH) port of the controller
D. Remote Authentication Dial-In User Service (RADIUS) token replay attack

Answer: B

NEW QUESTION 130
- (Exam Topic 15)
Where can the Open Web Application Security Project (OWASP) list of associated vulnerabilities be found?

A. OWASP Top 10 Project
B. OWASP Software Assurance Maturity Model (SAMM) Project
C. OWASP Guide Project
D. OWASP Mobile Project

Answer: A

NEW QUESTION 135
- (Exam Topic 15)
Within a large organization, what business unit is BEST positioned to initiate provisioning and deprovisioning of user accounts?

A. Training department
B. Internal audit
C. Human resources
D. Information technology (IT)

Answer: C

NEW QUESTION 139
- (Exam Topic 15)
Which of the following is considered the FIRST step when designing an internal security control assessment?

A. Create a plan based on recent vulnerability scans of the systems in question.
B. Create a plan based on comprehensive knowledge of known breaches.
C. Create a plan based on a recognized framework of known controls.
D. Create a plan based on reconnaissance of the organization's infrastructure.

Answer: D

NEW QUESTION 143
- (Exam Topic 15)
The Chief Information Security Officer (CISO) is concerned about business application availability. The organization was recently subject to a ransomware attack that resulted in the unavailability of applications and services for 10 working days that required paper-based running of all main business processes. There are now aggressive plans to enhance the Recovery Time Objective (RTO) and cater for more frequent data captures. Which of the following solutions should be implemented to fully comply to the new business requirements?

A. Virtualization
B. Antivirus
C. Process isolation
D. Host-based intrusion prevention system (HIPS)

Answer: A

NEW QUESTION 147
- (Exam Topic 15)
Which Wide Area Network (WAN) technology requires the first router in the path to determine the full path the packet will travel, removing the need for other routers in the path to make independent determinations?

A. Multiprotocol Label Switching (MPLS)
B. Synchronous Optical Networking (SONET)
C. Session Initiation Protocol (SIP)
D. Fiber Channel Over Ethernet (FCoE)

Answer: A

NEW QUESTION 149

- (Exam Topic 15)
Which of the following BEST describes the purpose of the reference monitor when defining access control to enforce the security model?

A. Quality design principles to ensure quality by design
B. Policies to validate organization rules
C. Cyber hygiene to ensure organizations can keep systems healthy
D. Strong operational security to keep unit members safe

Answer: B

NEW QUESTION 151
- (Exam Topic 15)
A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

A. OTDR
B. Tone generator
C. Fusion splicer
D. Cable tester
E. PoE injector

Answer: A

NEW QUESTION 156
- (Exam Topic 15)
Which of the following is the MOST common use of the Online Certificate Status Protocol (OCSP)?

A. To obtain the expiration date of an X.509 digital certificate
B. To obtain the revocation status of an X.509 digital certificate
C. To obtain the author name of an X.509 digital certificate
D. To verify the validity of an X.509 digital certificate

Answer: D

NEW QUESTION 161
- (Exam Topic 15)
When resolving ethical conflicts, the information security professional MUST consider many factors. In what order should these considerations be prioritized?

A. Public safety, duties to individuals, duties to the profession, and duties to principals
B. Public safety, duties to principals, duties to individuals, and duties to the profession
C. Public safety, duties to the profession, duties to principals, and duties to individuals
D. Public safety, duties to principals, duties to the profession, and duties to individuals

Answer: C

NEW QUESTION 165
- (Exam Topic 15)
Configuring a Wireless Access Point (WAP) with the same Service Set Identifier (SSID) as another WAP in order to have users unknowingly connect is referred to as which of the following?

A. Jamming
B. Man-irHht-Middk (MITM)
C. War driving
D. Internet Protocol (IP) spoofing

Answer: B

NEW QUESTION 170
- (Exam Topic 15)
Which of the following is a correct feature of a virtual local area network (VLAN)?

A. A VLAN segregates network traffic therefore information security is enhanced significantly.
B. Layer 3 routing is required to allow traffic from one VLAN to another.
C. VLAN has certain security features such as where the devices are physically connected.
D. There is no broadcast allowed within a single VLAN due to network segregation.

Answer: A

NEW QUESTION 173
- (Exam Topic 15)
Which of the following is TRUE for an organization that is using a third-party federated identity service?

A. The organization enforces the rules to other organization's user provisioning
B. The organization establishes a trust relationship with the other organizations
C. The organization defines internal standard for overall user identification
D. The organization specifies alone how to authenticate other organization's users

Answer: C

NEW QUESTION 177
- (Exam Topic 15)
An organization is implementing security review as part of system development. Which of the following is the BEST technique to follow?

A. Engage a third-party auditing firm.
B. Review security architecture.
C. Perform incremental assessments.
D. Conduct penetration testing.

Answer: C

NEW QUESTION 181
- (Exam Topic 15)
A new site's gateway isn't able to form a tunnel to the existing site-to-site Internet Protocol Security (IPsec) virtual private network (VPN) device at headquarters. Devices at the new site have no problem accessing resources on the Internet. When testing connectivity between the remote site's gateway, it was observed that the external Internet Protocol (IP) address of the gateway was set to 192.168.1.1. and was configured to send outbound traffic to the Internet Service Provider (ISP) gateway at4 192.168.1.2. Which of the following would be the BEST way to resolve the issue and get the remote site connected?

A. Enable IPSec tunnel mode on the VPN devices at the new site and the corporate headquarters.
B. Enable Layer 2 Tunneling Protocol (L2TP) on the VPN devices at the new site and the corporate headquarters.
C. Enable Point-to-Point Tunneling Protocol (PPTP) on the VPN devices at the new site and the corporate headquarters.
D. Enable Network Address Translation (NAT) - Traversal on the VPN devices at the new site and the corporate headquarters.

Answer: A

NEW QUESTION 185
- (Exam Topic 15)
A company wants to implement two-factor authentication (2FA) to protect their computers from unauthorized users. Which solution provides the MOST secure means of authentication and meets the criteria they have set?

A. Username and personal identification number (PIN)
B. Fingerprint and retinal scanners
C. Short Message Services (SMS) and smartphone authenticator
D. Hardware token and password

Answer: D

NEW QUESTION 186
- (Exam Topic 15)
What does the result of Cost-Benefit Analysis (C8A) on new security initiatives provide?

A. Quantifiable justification
B. Baseline improvement
C. Risk evaluation
D. Formalized acceptance

Answer: A

NEW QUESTION 190
- (Exam Topic 15)
When auditing the Software Development Life Cycle (SDLC) which of the following is one of the high-level audit phases?

A. Requirements
B. Risk assessment
C. Due diligence
D. Planning

Answer: B

NEW QUESTION 191
- (Exam Topic 15)
Digital non-repudiation requires which of the following?

A. A trusted third-party
B. Appropriate corporate policies
C. Symmetric encryption
D. Multifunction access cards

Answer: A

NEW QUESTION 193
- (Exam Topic 15)
The quality assurance (QA) department is short-staffed and is unable to test all modules before the anticipated release date of an application. What security control is MOST likely to be violated?

A. Separation of environments

B. Program management
C. Mobile code controls
D. Change management

Answer: D

NEW QUESTION 195
- (Exam Topic 15)
Which technique helps system designers consider potential security concerns of their systems and applications?

A. Penetration testing
B. Threat modeling
C. Manual inspections and reviews
D. Source code review

Answer: B

NEW QUESTION 197
- (Exam Topic 15)
The adoption of an enterprise-wide Business Continuity (BC) program requires which of the following?

A. Good communication throughout the organization
B. A completed Business Impact Analysis (BIA)
C. Formation of Disaster Recovery (DR) project team
D. Well-documented information asset classification

Answer: D

NEW QUESTION 202
- (Exam Topic 15)
When assessing web vulnerabilities, how can navigating the dark web add value to a penetration test?

A. The actual origin and tools used for the test can be hidden.
B. Information may be found on related breaches and hacking.
C. Vulnerabilities can be tested without impact on the tested environment.
D. Information may be found on hidden vendor patches.

Answer: D

NEW QUESTION 206
- (Exam Topic 15)
What is the PRIMARY objective of business continuity planning?

A. Establishing a cost estimate for business continuity recovery operations
B. Restoring computer systems to normal operations as soon as possible
C. Strengthening the perceived importance of business continuity planning among senior management
D. Ensuring timely recovery of mission-critical business processes

Answer: B

NEW QUESTION 210
- (Exam Topic 15)
a large organization uses biometrics to allow access to its facilities. It adjusts the biometric value for incorrectly granting or denying access so that the two numbers are the same.
What is this value called?

A. False Rejection Rate (FRR)
B. Accuracy acceptance threshold
C. Equal error rate
D. False Acceptance Rate (FAR)

Answer: C

NEW QUESTION 214
- (Exam Topic 15)
The security architect has been assigned the responsibility of ensuring integrity of the organization's electronic records. Which of the following methods provides the strongest level of integrity?

A. Time stamping
B. Encryption
C. Hashing
D. Digital signature

Answer: D

NEW QUESTION 217

- (Exam Topic 15)
What is the MOST common security risk of a mobile device?

A. Insecure communications link
B. Data leakage
C. Malware infection
D. Data spoofing

Answer: C

NEW QUESTION 221
- (Exam Topic 15)
An organization purchased a commercial off-the-shelf (COTS) software several years ago. The information technology (IT) Director has decided to migrate the application into the cloud, but is concerned about the application security of the software in the organization's dedicated environment with a cloud service provider. What is the BEST way to prevent and correct the software's security weal

A. Implement a dedicated COTS sandbox environment
B. Follow the software end-of-life schedule
C. Transfer the risk to the cloud service provider
D. Examine the software updating and patching process

Answer: A

NEW QUESTION 222
- (Exam Topic 15)
What is the PRIMARY purpose of creating and reporting metrics for a security awareness, training, and education program?

A. Make all stakeholders aware of the program's progress.
B. Measure the effect of the program on the organization's workforce.
C. Facilitate supervision of periodic training events.
D. Comply with legal regulations and document due diligence in security practices.

Answer: C

NEW QUESTION 227
- (Exam Topic 15)
Why would a system be structured to isolate different classes of information from one another and segregate them by user jurisdiction?

A. The organization can avoid e-discovery processes in the event of litigation.
B. The organization's infrastructure is clearly arranged and scope of responsibility is simplified.
C. The organization can vary its system policies to comply with conflicting national laws.
D. The organization is required to provide different services to various third-party organizations.

Answer: C

NEW QUESTION 231
- (Exam Topic 15)
What is considered the BEST explanation when determining whether to provide remote network access to a third-party security service?

A. Contract negotiation
B. Vendor demonstration
C. Supplier request
D. Business need

Answer: D

NEW QUESTION 236
- (Exam Topic 15)
A recent information security risk assessment identified weak system access controls on mobile devices as a high me In order to address this risk and ensure only authorized staff access company information, which of the following should the organization implement?

A. Intrusion prevention system (IPS)
B. Multi-factor authentication (MFA)
C. Data loss protection (DLP)
D. Data at rest encryption

Answer: B

NEW QUESTION 241
- (Exam Topic 15)
The Chief Information Security Officer (CISO) of a small organization is making a case for building a security operations center (SOC). While debating between an in-house, fully outsourced, or a hybrid capability, which of the following would be the MAIN consideration, regardless of the model?

A. Skill set and training
B. Headcount and capacity
C. Tools and technologies
D. Scope and service catalog

Answer: C

NEW QUESTION 245
- (Exam Topic 15)
While dealing with the consequences of a security incident, which of the following security controls are MOST appropriate?

A. Detective and recovery controls
B. Corrective and recovery controls
C. Preventative and corrective controls
D. Recovery and proactive controls

Answer: C

NEW QUESTION 249
- (Exam Topic 15)
A manager identified two conflicting sensitive user functions that were assigned to a single user account that had the potential to result in financial and regulatory risk to the company. The manager MOST likely discovered this during which of the following?

A. Security control assessment.
B. Separation of duties analysis
C. Network Access Control (NAC) review
D. Federated identity management (FIM) evaluation

Answer: B

NEW QUESTION 254
- (Exam Topic 15)
Which of the following is the FIRST step an organization's security professional performs when defining a cyber-security program based upon industry standards?

A. Map the organization's current security practices to industry standards and frameworks.
B. Define the organization's objectives regarding security and risk mitigation.
C. Select from a choice of security best practices.
D. Review the past security assessments.

Answer: A

NEW QUESTION 255
- (Exam Topic 15)
A Certified Information Systems Security Professional (CISSP) with identity and access management (IAM) responsibilities is asked by the Chief Information Security Officer (CISO) to4 perform a vulnerability assessment on a web application to pass a Payment Card Industry (PCI) audit. The CISSP has never performed this before. According to the (ISC)? Code of Professional Ethics, which of the following should the CISSP do?

A. Review the CISSP guidelines for performing a vulnerability assessment before proceeding to complete it
B. Review the PCI requirements before performing the vulnerability assessment
C. Inform the CISO that they are unable to perform the task because they should render only those services for which they are fully competent and qualified
D. Since they are CISSP certified, they have enough knowledge to assist with the request, but will need assistance in order to complete it in a timely manner

Answer: C

NEW QUESTION 260
- (Exam Topic 15)
Which of the following is the BEST method to gather evidence from a computer's hard drive?

A. Disk duplication
B. Disk replacement
C. Forensic signature
D. Forensic imaging

Answer: D

NEW QUESTION 262
- (Exam Topic 15)
A system developer has a requirement for an application to check for a secure digital signature before the application is accessed on a user's laptop. Which security mechanism addresses this requirement?

A. Hardware encryption
B. Certificate revocation list (CRL) policy
C. Trusted Platform Module (TPM)
D. Key exchange

Answer: B

NEW QUESTION 266
- (Exam Topic 15)
A cloud service provider requires its customer organizations to enable maximum audit logging for its data storage service and to retain the logs for the period of

three months. The audit logging generates extremely high amount of logs. What is the MOST appropriate strategy for the log retention?

A. Keep last week's logs in an online storage and the rest in a near-line storage.
B. Keep all logs in an online storage.
C. Keep all logs in an offline storage.
D. Keep last week's logs in an online storage and the rest in an offline storage.

Answer: D

NEW QUESTION 267
- (Exam Topic 15)
Which application type is considered high risk and provides a common way for malware and viruses to enter a network?

A. Instant messaging or chat applications
B. E-mail applications
C. Peer-to-Peer (P2P) file sharing applications
D. End-to-end applications

Answer: A

NEW QUESTION 268
- (Exam Topic 15)
Which of the following describes the BEST method of maintaining the inventory of software and hardware within the organization?

A. Maintaining the inventory through a combination of desktop configuration, administration management, and procurement management tools
B. Maintaining the inventory through a combination of asset owner interviews, open-source system management, and open-source management tools
C. Maintaining the inventory through a combination of on-premise storage configuration, cloud management, and partner management tools
D. Maintaining the inventory through a combination of system configuration, network management, and license management tools

Answer: C

NEW QUESTION 272
- (Exam Topic 15)
What industry-recognized document could be used as a baseline reference that is related to data security and business operations for conducting a security assessment?

A. Service Organization Control (SOC) 1 Type 2
B. Service Organization Control (SOC) 2 Type 1
C. Service Organization Control (SOC) 1 Type 1
D. Service Organization Control (SOC) 2 Type 2

Answer: D

NEW QUESTION 276
- (Exam Topic 15)
In a quarterly system access review, an active privileged account was discovered that did not exist in the prior review on the production system. The account was created one hour after the previous access review. Which of the following is the BEST option to reduce overall risk in addition to quarterly access reviews?

A. Increase logging levels.
B. Implement bi-annual reviews.
C. Create policies for system access.
D. Implement and review risk-based alerts.

Answer: D

NEW QUESTION 280
- (Exam Topic 15)
The Chief Information Security Officer (CISO) of an organization has requested that a Service Organization Control (SOC) report be created to outline the security and availability of a
particular system over a 12-month period. Which type of SOC report should be utilized?

A. SOC 1 Type 1
B. SOC 2 Type 2
C. SOC 2 Type 2
D. SOC 3 Type 1

Answer: C

NEW QUESTION 284
- (Exam Topic 15)
What is the BEST design for securing physical perimeter protection?

A. Crime Prevention through Environmental Design (CPTED)
B. Barriers, fences, gates, and walls
C. Business continuity planning (BCP)
D. Closed-circuit television (CCTV)

Answer: B

NEW QUESTION 288
- (Exam Topic 15)
What is a security concern when considering implementing software-defined networking (SDN)?

A. It increases the attack footprint.
B. It uses open source protocols.
C. It has a decentralized architecture.
D. It is cloud based.

Answer: C

NEW QUESTION 292
- (Exam Topic 15)
Which of the following BEST describes when an organization should conduct a black box security audit on a new software product?

A. When the organization wishes to check for non-functional compliance
B. When the organization wants to enumerate known security vulnerabilities across their infrastructure
C. When the organization has experienced a security incident
D. When the organization is confident the final source code is complete

Answer: B

NEW QUESTION 295
- (Exam Topic 15)
An organization wants to migrate to Session Initiation Protocol (SIP) to save on telephony expenses. Which of the following security related statements should be considered in the decision-making process?

A. Cloud telephony is less secure and more expensive than digital telephony services.
B. SIP services are more secure when used with multi-layer security proxies.
C. H.323 media gateways must be used to ensure end-to-end security tunnels.
D. Given the behavior of SIP traffic, additional security controls would be required.

Answer: C

NEW QUESTION 297
- (Exam Topic 15)
An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex. Which of the following is the MOST likely cause of this issue?

A. The link is improperly terminated
B. One of the devices is misconfigured
C. The cable length is excessive.
D. One of the devices has a hardware issue.

Answer: A

NEW QUESTION 300
- (Exam Topic 15)
Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

A. Centralized network provisioning
B. Centralized network administrator control
C. Reduced network latency when scaled
D. Reduced hardware footprint and cost

Answer: B

NEW QUESTION 303
- (Exam Topic 15)
Which media sanitization methods should be used for data with a high security categorization?

A. Clear or destroy
B. Clear or purge
C. Destroy or delete
D. Purge or destroy

Answer: D

NEW QUESTION 305
- (Exam Topic 15)
An information security professional is reviewing user access controls on a customer-facing application. The application must have multi-factor authentication (MFA) in place. The application currently requires a username and password to login. Which of the following options would BEST implement MFA?

A. Geolocate the user and compare to previous logins
B. Require a pre-selected number as part of the login
C. Have the user answer a secret question that is known to them
D. Enter an automatically generated number from a hardware token

Answer: C

NEW QUESTION 309
- (Exam Topic 15)
What is the HIGHEST priority in agile development?

A. Selecting appropriate coding language
B. Managing costs of product delivery
C. Early and continuous delivery of software
D. Maximizing the amount of code delivered

Answer: C

NEW QUESTION 314
- (Exam Topic 15)
When are security requirements the LEAST expensive to implement?

A. When identified by external consultants
B. During the application rollout phase
C. During each phase of the project cycle
D. When built into application design

Answer: D

NEW QUESTION 315
- (Exam Topic 15)
In Federated Identity Management (FIM), which of the following represents the concept of federation?

A. Collection of information logically grouped into a single entity
B. Collection, maintenance, and deactivation of user objects and attributes in one or more systems, directories or applications
C. Collection of information for common identities in a system
D. Collection of domains that have established trust among themselves

Answer: D

NEW QUESTION 320
- (Exam Topic 15)
Which of the following should exist in order to perform a security audit?

A. Industry framework to audit against
B. External (third-party) auditor
C. Internal certified auditor
D. Neutrality of the auditor

Answer: D

NEW QUESTION 323
- (Exam Topic 15)
Who should perform the design review to uncover security design flaws as part of the Software Development Life Cycle (SDLC)?

A. The business owner
B. security subject matter expert (SME)
C. The application owner
D. A developer subject matter expert (SME)

Answer: B

NEW QUESTION 328
- (Exam Topic 15)
The initial security categorization should be done early in the system life cycle and should be reviewed periodically. Why is it important for this to be done correctly?

A. It determines the security requirements.
B. It affects other steps in the certification and accreditation process.
C. It determines the functional and operational requirements.
D. The system engineering process works with selected security controls.

Answer: B

NEW QUESTION 329

- (Exam Topic 15)
A healthcare insurance organization chose a vendor to develop a software application. Upon review of the draft contract, the information security professional notices that software security is not addressed. What is the BEST approach to address the issue?

A. Update the service level agreement (SLA) to provide the organization the right to audit the vendor.
B. Update the service level agreement (SLA) to require the vendor to provide security capabilities.
C. Update the contract so that the vendor is obligated to provide security capabilities.
D. Update the contract to require the vendor to perform security code reviews.

Answer: C

NEW QUESTION 334
- (Exam Topic 15)
A cloud hosting provider would like to provide a Service Organization Control (SOC) report relevant to its security program. This report should an abbreviated report that can be freely distributed. Which type of report BEST meets this requirement?

A. SOC 1
B. SOC 2 Type I
C. SOC 2 Type II
D. SOC 3

Answer: D

NEW QUESTION 336
- (Exam Topic 15)
Which of the fallowing statements is MOST accurate regarding information assets?

A. International Organization for Standardization (ISO) 27001 compliance specifies which information assets must be included in asset inventory.
B. S3 Information assets include any information that is valuable to the organization,
C. Building an information assets register is a resource-intensive job.
D. Information assets inventory is not required for risk assessment.

Answer: B

NEW QUESTION 341
- (Exam Topic 15)
An internal audit for an organization recently identified malicious actions by a user account. Upon further investigation, it was determined the offending user account was used by multiple people at multiple locations simultaneously for various services and applications. What is the BEST method to prevent this problem in the future?

A. Ensure the security information and event management (SIEM) is set to alert.
B. Inform users only one user should be using the account at a time.
C. Ensure each user has their own unique account,
D. Allow several users to share a generic account.

Answer: A

NEW QUESTION 345
- (Exam Topic 15)
A large organization’s human resources and security teams are planning on implementing technology to eliminate manual user access reviews and improve compliance. Which of the following options is MOST likely to resolve the issues associated with user access?

A. Implement a role-based access control (RBAC) system.
B. Implement identity and access management (IAM) platform.
C. Implement a Privileged Access Management (PAM) system.
D. Implement a single sign-on (SSO) platform.

Answer: B

NEW QUESTION 346
- (Exam Topic 14)
Which one of the following documentation should be included in a Disaster Recovery (DR) package?

A. Source code, compiled code, firmware updates, operational log book and manuals.
B. Data encrypted in original format, auditable transaction data, and recovery instructions for future extraction on demand.
C. Hardware configuration instructions, hardware configuration software, an operating system image, a data restoration option, media retrieval instructions,…..
D. System configuration including hardware, software, hardware, interfaces, software Application Programming Interface (API) configuration, data structure, ….

Answer: C

NEW QUESTION 349
- (Exam Topic 14)
Continuity of operations is BEST supported by which of the following?

A. Confidentiality, availability, and reliability
B. Connectivity, reliability, and redundancy
C. Connectivity, reliability, and recovery

D. Confidentiality, integrity, and availability

Answer: B

NEW QUESTION 352
- (Exam Topic 14)
If a content management system (CMC) is implemented, which one of the following would occur?

A. Developers would no longer have access to production systems
B. The applications placed into production would be secure
C. Patching the systems would be completed more quickly
D. The test and production systems would be running the same software

Answer: D

NEW QUESTION 355
- (Exam Topic 14)
Which of the following is a characteristic of the independent testing of a program?

A. Independent testing increases the likelihood that a test will expose the effect of a hidden feature.
B. Independent testing decreases the likelihood that a test will expose the effect of a hidden feature.
C. Independent testing teams help decrease the cost of creating test data and system design specification.
D. Independent testing teams help identify functional requirements and Service Level Agreements (SLA)

Answer: A

NEW QUESTION 359
- (Exam Topic 14)
A corporate security policy specifies that all devices on the network must have updated operating system patches and anti-malware software. Which technology should be used to enforce this policy?

A. Network Address Translation (NAT)
B. Stateful Inspection
C. Packet filtering
D. Network Access Control (NAC)

Answer: D

NEW QUESTION 363
- (Exam Topic 14)
Which of the following System and Organization Controls (SOC) report types should an organization request if they require a period of time report covering security and availability for a particular system?

A. SOC 1 Type1
B. SOC 1Type2
C. SOC 2 Type 1
D. SOC 2 Type 2

Answer: D

NEW QUESTION 368
- (Exam Topic 14)
Which of the following is mobile device remote fingerprinting?

A. Installing an application to retrieve common characteristics of the device
B. Storing information about a remote device in a cookie file
C. Identifying a device based on common characteristics shared by all devices of a certain type
D. Retrieving the serial number of the mobile device

Answer: C

NEW QUESTION 372
- (Exam Topic 14)
Compared with hardware cryptography, software cryptography is generally

A. less expensive and slower.
B. more expensive and faster.
C. more expensive and slower.
D. less expensive and faster.

Answer: A

Explanation:
Reference:
https://www.ontrack.com/uk/blog/making-data-simple/hardware-encryption-vs-software-encryption-the-simple

NEW QUESTION 377
- (Exam Topic 14)
Which is the MOST critical aspect of computer-generated evidence?

A. Objectivity
B. Integrity
C. Timeliness
D. Relevancy

Answer: B

NEW QUESTION 381
- (Exam Topic 14)
What is the MOST common component of a vulnerability management framework?

A. Risk analysis
B. Patch management
C. Threat analysis
D. Backup management

Answer: B

Explanation:
Reference: https://www.helpnetsecurity.com/2016/10/11/effective-vulnerability-management-process/

NEW QUESTION 385
- (Exam Topic 14)
What is the PRIMARY purpose for an organization to conduct a security audit?

A. To ensure the organization is adhering to a well-defined standard
B. To ensure the organization is applying security controls to mitigate identified risks
C. To ensure the organization is configuring information systems efficiently
D. To ensure the organization is documenting findings

Answer: A

NEW QUESTION 386
- (Exam Topic 14)
Which of the following will have the MOST influence on the definition and creation of data classification and data ownership policies?

A. Data access control policies
B. Threat modeling
C. Common Criteria (CC)
D. Business Impact Analysis (BIA)

Answer: A

NEW QUESTION 391
- (Exam Topic 14)
Which of the following practices provides the development team with a definition of security and identification of threats in designing software?

A. Penetration testing
B. Stakeholder review
C. Threat modeling
D. Requirements review

Answer: C

NEW QUESTION 394
- (Exam Topic 14)
What testing technique enables the designer to develop mitigation strategies for potential vulnerabilities?

A. Manual inspections and reviews
B. Penetration testing
C. Threat modeling
D. Source code review

Answer: C

NEW QUESTION 397
- (Exam Topic 14)
When dealing with shared, privilaged accounts, especially those for emergencies, what is the BEST way to assure non-repudiation of logs?

A. Regularity change the passwords,
B. implement a password vaulting solution.
C. Lock passwords in tamperproof envelopes in a safe.

D. Implement a strict access control policy.

Answer: B

NEW QUESTION 399
- (Exam Topic 14)
Which of the following authorization standards is built to handle Application Programming Interface (API) access for Federated Identity Management (FIM)?

A. Security Assertion Markup Language (SAML)
B. Open Authentication (OAUTH)
C. Remote Authentication Dial-in User service (RADIUS)
D. Terminal Access Control Access Control System Plus (TACACS+)

Answer: B

NEW QUESTION 402
- (Exam Topic 14)
Which of the following is the MOST effective countermeasure against Man-in-the Middle (MITM) attacks while using online banking?

A. Transport Layer Security (TLS)
B. Secure Sockets Layer (SSL)
C. Pretty Good Privacy (PGP)
D. Secure Shell (SSH)

Answer: A

NEW QUESTION 403
- (Exam Topic 14)
An organization operates a legacy Industrial Control System (ICS) to support its core business service, which carrot be replaced. Its management MUST be performed remotely through an administrative console software, which in tum depends on an old version of the Java Runtime Environment (JPE) known to be vulnerable to a number of attacks, How is this risk BEST managed?

A. Isolate the full ICS by moving It onto its own network segment
B. Air-gap and harden the host used for management purposes
C. Convince the management to decommission the ICS and mitigate to a modem technology
D. Deploy a restrictive proxy between all clients and the vulnerable management station

Answer: B

NEW QUESTION 408
- (Exam Topic 14)
Which of the following is the final phase of the identity and access provisioning lifecycle?

A. Recertification
B. Revocation
C. Removal
D. Validation

Answer: B

Explanation:
Reference: https://books.google.com.pk/books?id=W2TvAgAAQBAJ&pg=PA256&lpg=PA256&dq=process+in+the+acce

NEW QUESTION 413
- (Exam Topic 14)
An organization discovers that its secure file transfer protocol (SFTP) server has been accessed by an unauthorized person to download an unreleased game. A recent security audit found weaknesses in some of the organization’s general information technology (IT) controls, specifically pertaining to software change control and security patch management, but not in other control areas.
Which of the following is the MOST probable attack vector used in the security breach?

A. Buffer overflow
B. Weak password able to lack of complexity rules
C. Distributed Denial of Service (DDoS)
D. Cross-Site Scripting (XSS)

Answer: A

NEW QUESTION 414
- (Exam Topic 14)
An organization that has achieved a Capability Maturity model Integration (CMMI) level of 4 has done which of the following?

A. Addressed continuous innovative process improvement
B. Addressed the causes of common process variance
C. Achieved optimized process performance
D. Achieved predictable process performance

Answer:

C

NEW QUESTION 419
- (Exam Topic 14)
Which layer of the Open system Interconnect (OSI) model is responsible for secure data transfer between applications, flow control, and error detection and correction?

A. Layer 2
B. Layer 4
C. Layer 5
D. Layer 6

Answer: B

NEW QUESTION 424
- (Exam Topic 14)
Which of the following MUST a security professional do in order to quantify the value of a security program to organization management?

A. Report using metrics.
B. Rank priorities as high, medium, or low.
C. Communicate compliance obstacles.
D. Report en employee activities

Answer: A

NEW QUESTION 429
- (Exam Topic 14)
Which of the following is considered the last line defense in regard to a Governance, Risk managements, and compliance (GRC) program?

A. Internal audit
B. Internal controls
C. Board review
D. Risk management

Answer: B

NEW QUESTION 431
- (Exam Topic 14)
Which of the following open source software issues pose the MOST risk to an application?

A. The software is beyond end of life and the vendor is out of business.
B. The software is not used or popular in the development community.
C. The software has multiple Common Vulnerabilities and Exposures (CVE) and only some are remediated.
D. The software has multiple Common Vulnerabilities and Exposures (CVE) but the CVEs are classified as low risks.

Answer: D

NEW QUESTION 434
- (Exam Topic 14)
A financial company has decided to move its main business application to the Cloud. The legal department objects, arguing that the move of the platform should comply with several regulatory obligations such as the General Data Protection (GDPR) and ensure data confidentiality. The Chief Information Security Officer (CISO) says that the cloud provider has met all regulations requirements and even provides its own encryption solution with internally-managed encryption keys to address data confidentiality. Did the CISO address all the legal requirements in this situation?

A. No, because the encryption solution is internal to the cloud provider.
B. Yes, because the cloud provider meets all regulations requirements.
C. Yes, because the cloud provider is GDPR compliant.
D. No, because the cloud provider is not certified to host government data.

Answer: B

NEW QUESTION 439
- (Exam Topic 14)
Which layer of the Open systems Interconnection (OSI) model is being targeted in the event of a Synchronization (SYN) flood attack?

A. Session
B. Transport
C. Network
D. Presentation

Answer: B

NEW QUESTION 444
- (Exam Topic 14)
Which type of fire alarm system sensor is intended to detect fire at its earliest stage?

A. Ionization
B. Infrared
C. Thermal
D. Photoelectric

Answer: A

NEW QUESTION 448
- (Exam Topic 14)
What should be the FIRST action for a security administrator who detects an intrusion on the network based on precursors and other indicators?

A. Isolate and contain the intrusion.
B. Notify system and application owners.
C. Apply patches to the Operating Systems (OS).
D. Document and verify the intrusion.

Answer: C

Explanation:
Reference:
https://securityintelligence.com/dont-dwell-on-it-how-to-detect-a-breach-on-your-network-more-efficiently/

NEW QUESTION 453
- (Exam Topic 14)
A vehicle of a private courier company that transports backup data for offsite storage was robbed while in transport backup data for offsite was robbed while in transit. The incident management team is now responsible to estimate the robbery, which of the following would help the incident management team to MOST effectively analyze the business impact of the robbery?

A. Log of backup administrative actions
B. Log of the transported media and its classification marking
C. Log of the transported media and Its detailed contents
D. Log of backed up data and their respective data custodians

Answer: B

NEW QUESTION 455
- (Exam Topic 14)
In fault-tolerant systems, what do rollback capabilities permit?

A. Restoring the system to a previous functional state
B. Identifying the error that caused the problem
C. Allowing the system to an in a reduced manner
D. Isolating the error that caused the problem

Answer: A

NEW QUESTION 460
- (Exam Topic 14)
Which of the following is the MOST important reason for timely installation of software patches?

A. Attackers may be conducting network analysis.
B. Patches ere only available for a specific time.
C. Attackers reverse engineer the exploit from the patch.
D. Patches may not be compatible with proprietary software

Answer: C

NEW QUESTION 461
- (Exam Topic 14)
Which of the following is an accurate statement when an assessment results in the discovery of vulnerabilities in a critical network component?

A. The fact that every other host is sufficiently hardened does not change the fact frat the network is placed at risk of attack.
B. There is little likelihood that the entire network is being placed at a significant risk of attack.
C. A second assessment should immediately be performed after all vulnerabilities are corrected.
D. There is a low possibility that any adjacently connected components have been compromised by an attacker

Answer: C

NEW QUESTION 463
- (Exam Topic 14)
Which of the following initiates the systems recovery phase of a disaster recovery plan?

A. Issuing a formal disaster declaration
B. Activating the organization's hot site
C. Evacuating the disaster site
D. Assessing the extent of damage following the disaster

Answer: A

NEW QUESTION 466
- (Exam Topic 14)
When deploying en Intrusion Detection System (IDS) on a high-volume network, the need to distribute the load across multiple sensors would create which technical problem?

A. Session continuity
B. Proxy authentication failure
C. Sensor overload
D. Synchronized sensor updates

Answer: A

NEW QUESTION 470
- (Exam Topic 14)
Which of the following authorization standards is built to handle Application programming Interface (API) access for federated Identity management (FIM)?

A. Remote Authentication Dial-In User Service (RADIUS)
B. Terminal Access Controller Access Control System Plus (TACACS+)
C. Open Authentication (OAuth)
D. Security Assertion Markup Language (SAML)

Answer: C

NEW QUESTION 473
- (Exam Topic 14)
Assume that a computer was powered off when an information security professional arrived at a crime scene. Which of the following actions should be performed after the crime scene is isolated?

A. Turn the computer on and collect volatile data.
B. Turn the computer on and collect network information.
C. Leave the computer off and prepare the computer for transportation to the laboratory
D. Remove the hard drive, prepare it for transportation, and leave the hardware ta the scene.

Answer: C

NEW QUESTION 475
- (Exam Topic 14)
Digital certificates used transport Layer security (TLS) support which of the following?

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

Answer: A

NEW QUESTION 478
- (Exam Topic 14)
Which of the following is a characteristic of a challenge/response authentication process?

A. Presenting distorted graphics of text for authentication
B. Transmitting a hash based on the user's password
C. Using a password history blacklist
D. Requiring the use of non-consecutive numeric characters

Answer: A

NEW QUESTION 483
- (Exam Topic 14)
Additional padding may be added to the Encapsulating security protocol (ESP) trailer to provide which of the following?

A. Data origin authentication
B. Partial traffic flow confidentiality
C. protection ao>ainst replay attack
D. Access control

Answer: C

NEW QUESTION 484
- (Exam Topic 14)
Which of the following is a peor entity authentication method for Point-to-Point Protocol (PPP)?

A. Challenge Handshake Authentication Protocol (CHAP)

B. Message Authentication Code (MAC)
C. Transport Layer Security (TLS) handshake protocol
D. Challenge-response authentication mechanism

Answer: A

NEW QUESTION 488
- (Exam Topic 14)
Which of the following technologies would provide the BEST alternative to anti-malware software?

A. Host-based Intrusion Detection Systems (HIDS)
B. Application whitelisting
C. Host-based firewalls
D. Application sandboxing

Answer: B

NEW QUESTION 492
- (Exam Topic 14)
Which of the following media is least problematic with data remanence?

A. Magnetic disk
B. Electrically Erasable Programming read-only Memory (EEPROM)
C. Dynamic Random Access Memory (DRAM)
D. Flash memory

Answer: C

NEW QUESTION 493
- (Exam Topic 14)
An organization is required to comply with the Payment Card Industry Data Security Standard (PCI-DSS), what is the MOST effective approach to safeguard digital and paper media that contains cardholder data?

A. Use and regularity update antivirus software.
B. Maintain strict control over storage of media
C. Mandate encryption of cardholder data.
D. Configure firewall rules to protect the data.

Answer: C

NEW QUESTION 496
- (Exam Topic 14)
When can a security program be considered effective?

A. Audits are rec/party performed and reviewed.
B. Vulnerabilities are proactively identified.
C. Risk is lowered to an acceptable level.
D. Badges are regulatory performed and validated

Answer: C

NEW QUESTION 499
- (Exam Topic 14)
What high Availability (HA) option of database allows multiple clients to access multiple database servers simultaneously?

A. Non-Structured Query Language (NoSQL) database
B. Relational database
C. Shadow database
D. Replicated database

Answer: C

NEW QUESTION 501
- (Exam Topic 14)
Why do certificate Authorities (CA) add value to the security of electronic commerce transactions?

A. They maintain the certificate revocation list.
B. They maintain the private keys of transition parties.
C. They verify the transaction parties' private keys.
D. They provide a secure communication enamel to the transaction parties.

Answer: D

NEW QUESTION 506
- (Exam Topic 14)

Which of the following MUST be considered when developing business rules for a data loss prevention (DLP) solution?

A. Data availability
B. Data sensitivity
C. Data ownership
D. Data integrity

Answer: B

NEW QUESTION 508
- (Exam Topic 14)
A development operations team would like to start building new applications delegating the cybersecurity responsibility as much as possible to the service provider. Which of the following environments BEST fits their need?

A. Cloud Virtual Machines (VM)
B. Cloud application container within a Virtual Machine (VM)
C. On premises Virtual Machine (VM)
D. Self-hosted Virtual Machine (VM)

Answer: A

NEW QUESTION 509
- (Exam Topic 14)
Which of the following is applicable to a publicly held company concerned about information handling and storage requirement specific to the financial reporting?

A. Privacy Act of 1974
B. Clinger-Cohan Act of 1996
C. Sarbanes-Oxley (SOX) Act of 2002
D. International Organization for Standardization (ISO) 27001

Answer: C

NEW QUESTION 510
- (Exam Topic 14)
Which of the following will help prevent improper session handling?

A. Ensure that all UlWebView calls do not execute without proper input validation.
B. Ensure that tokens are sufficiently long, complex, and pseudo-random.
C. Ensure JavaScript and plugin support is disabled.
D. Ensure that certificates are valid and fail closed.

Answer: B

NEW QUESTION 515
- (Exam Topic 14)
Which of the following objects should be removed FIRST prior to uploading code to public code repositories?

A. Security credentials
B. Known vulnerabilities
C. Inefficient algorithms
D. Coding mistakes

Answer: A

NEW QUESTION 518
- (Exam Topic 14)
What is maintained by using write blocking devices whan forensic evidence is examined?

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

Answer: B

NEW QUESTION 522
- (Exam Topic 14)
Which programming methodology allows a programmer to use pre-determined blocks of code end consequently reducing development time and programming costs?

A. Application security
B. Object oriented
C. Blocked algorithm
D. Assembly language

Answer: B

NEW QUESTION 527
- (Exam Topic 14)
Which one of the following is an advantage of an effective release control strategy from a configuration control standpoint?

A. Ensures that there is no loss of functionality between releases
B. Allows for future enhancements to existing features
C. Enforces backward compatibility between releases
D. Ensures that a trace for all deliverables is maintained and auditable

Answer: C

NEW QUESTION 528
- (Exam Topic 14)
Which attack defines a piece of code that is inserted into software to trigger a malicious function?

A. Phishing
B. Salami
C. Back door
D. Logic bomb

Answer: D

NEW QUESTION 529
- (Exam Topic 14)
Which of the following presents the PRIMARY concern to an organization when setting up a federated single sign-on (SSO) solution with another

A. Sending assertions to an identity provider
B. Requesting Identity assertions from the partners domain
C. defining the identity mapping scheme
D. Having the resource provider query the Identity provider

Answer: C

NEW QUESTION 534
- (Exam Topic 14)
Which area of embedded devices are most commonly attacked?

A. Application
B. Firmware
C. Protocol
D. Physical Interface

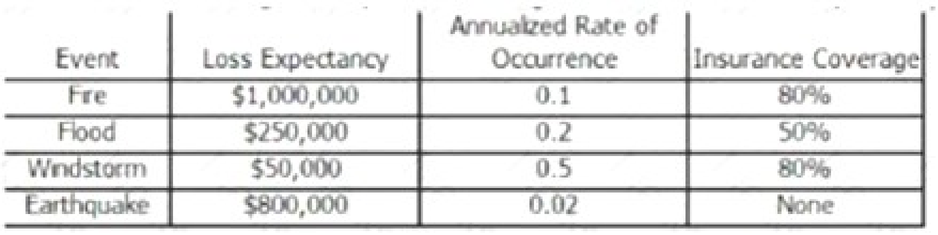
Answer: A

NEW QUESTION 538
- (Exam Topic 14)
Which of the following is the BEST approach for a forensic examiner to obtain the greatest amount of relevant information form malicious software?

A. Analyze the behavior of the program.
B. Examine the file properties and permissions.
C. Review the code to identify its origin.
D. Analyze the logs generated by the software.

Answer: A

NEW QUESTION 543
- (Exam Topic 14)
Which of the following would present the higher annualized loss expectancy (ALE)?



Event	Loss Expectancy	Annualized Rate of Occurrence	Insurance Coverage
Fire	$1,000,000	0.1	80%
Flood	$250,000	0.2	50%
Windstorm	$50,000	0.5	80%
Earthquake	$800,000	0.02	None

A. Fire
B. Earthquake
C. Windstorm
D. Flood

Answer: A

NEW QUESTION 547
- (Exam Topic 14)
Which of the following steps is performed during the forensic data analysis phase?

A. Collect known system files
B. search for relevant strings.
C. Create file lists
D. Recover deleted data.

Answer: B

NEW QUESTION 550
- (Exam Topic 14)
Which of the following attacks is dependent upon the compromise of a secondary target in order to reach the primary target?

A. Watering hole
B. Brute force
C. Spear phishing
D. Address Resolution Protocol (ARP) poisoning

Answer: D

NEW QUESTION 554
- (Exam Topic 14)
Which of the following is a common measure within a Local Area Network (LAN) to provide en additional level of security through segmentation?

A. Building Virtual Local Area Networks (VLAN)
B. Building Demilitarized Zones (DMZ)
C. Implementing a virus scanner
D. Implementing an Intrusion Detection System (IDS)

Answer: A

NEW QUESTION 555
- (Exam Topic 14)
A security professional should consider the protection of which of the following elements FIRST when developing a defense-in-depth strategy for a mobile workforce?

A. Network perimeters
B. Demilitarized Zones (DM2)
C. Databases and back-end servers
D. End-user devices

Answer: D

NEW QUESTION 559
- (Exam Topic 14)
A large corporation is locking for a solution to automate access based on where on request is coming from, who the user is, what device they are connecting with, and what time of day they are attempting this access. What type of solution would suit their needs?

A. Discretionary Access Control (DAC)
B. Role Based Access Control (RBAC)
C. Mandater Access Control (MAC)
D. Network Access Control (NAC)

Answer: D

NEW QUESTION 562
- (Exam Topic 14)
Which of the following BEST describes the responsibilities of data owner?

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

Answer: B

NEW QUESTION 563
- (Exam Topic 14)
Which of the following is the weakest form of protection for an application that handles Personally Identifiable Information (PII)?

A. Transport Layer Security (TLS)
B. Ron Rivest Cipher 4 (RC4) encryption
C. Security Assertion Markup Language (SAML)
D. Multifactor authentication

Answer: B

NEW QUESTION 567

- (Exam Topic 14)
What does the term “100-year floodplain” mean to emergency preparedness officials?

A. The area is expected to be safe from flooding for at least 100 years.
B. The odds of a flood at this level are 1 in 100 in any given year.
C. The odds are that the next significant flood will hit within the next 100 years.
D. The last flood of any kind to hit the area was more than 100 years ago.

Answer: B

NEW QUESTION 572
- (Exam Topic 14)
What is the BEST method if an investigator wishes to analyze a hard drive which may be used as evidence?

A. Leave the hard drive in place and use only verified and authenticated Operating Systems (OS) utilities ...
B. Log into the system and immediately make a copy of all relevant files to a Write Once, Read Many ...
C. Remove the hard drive from the system and make a copy of the hard drive's contents using imaging hardware.
D. Use a separate bootable device to make a copy of the hard drive before booting the system and analyzing the hard drive.

Answer: C

NEW QUESTION 575
- (Exam Topic 13)
From a security perspective, which of the following assumptions MUST be made about input to an application?

A. It is tested
B. It is logged
C. It is verified
D. It is untrusted

Answer: D

NEW QUESTION 578
- (Exam Topic 14)
Individuals have been identified and determined as having a need-to-know for the information. Which of the following access control methods MUST include a consistent set of rules for controlling and limiting access?

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

Answer: D

NEW QUESTION 580
- (Exam Topic 13)
A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report. In which phase of the assessment was this error MOST likely made?

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

Answer: A

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 584
- (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 587
- (Exam Topic 13)
What is the foundation of cryptographic functions?

A. Encryption
B. Cipher
C. Hash

D. Entropy

Answer: D

NEW QUESTION 590
- (Exam Topic 13)
What is the MAIN purpose of a change management policy?

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

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 595
- (Exam Topic 13)
A security analyst for a large financial institution is reviewing network traffic related to an incident. The analyst determines the traffic is irrelevant to the investigation but in the process of the review, the analyst also finds that an applications data, which included full credit card cardholder data, is transferred in clear text between the server and user’s desktop. The analyst knows this violates the Payment Card Industry Data Security Standard (PCI-DSS). Which of the following is the analyst’s next step?

A. Send the log file co-workers for peer review
B. Include the full network traffic logs in the incident report
C. Follow organizational processes to alert the proper teams to address the issue.
D. Ignore data as it is outside the scope of the investigation and the analyst’s role.

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 598
- (Exam Topic 13)
Transport Layer Security (TLS) provides which of the following capabilities for a remote access server?

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

Answer: C

NEW QUESTION 601
- (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 605
- (Exam Topic 13)
What is the PRIMARY goal of fault tolerance?

A. Elimination of single point of failure
B. Isolation using a sandbox
C. Single point of repair
D. Containment to prevent propagation

Answer: A

NEW QUESTION 609
- (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 611
- (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 616
- (Exam Topic 13)
Which of the following entails identification of data and links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

A. Security governance
B. Risk management
C. Security portfolio management
D. Risk assessment

Answer: B

NEW QUESTION 621
- (Exam Topic 13)
An organization adopts a new firewall hardening standard. How can the security professional verify that the technical staff correct implemented the new standard?

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

Answer: A

Explanation:
Section: Security Operations

NEW QUESTION 626
- (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: C

NEW QUESTION 631
- (Exam Topic 13)
During examination of Internet history records, the following string occurs within a Unique Resource Locator (URL):
http://www.companysite.com/products/products.asp?productid=123 or 1=1
What type of attack does this indicate?

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

Answer: C

NEW QUESTION 634
- (Exam Topic 13)
An organization has outsourced its financial transaction processing to a Cloud Service Provider (CSP) who will provide them with Software as a Service (SaaS). If there was a data breach who is responsible for monetary losses?

A. The Data Protection Authority (DPA)
B. The Cloud Service Provider (CSP)
C. The application developers
D. The data owner

Answer: B

NEW QUESTION 636
- (Exam Topic 13)
Which one of the following data integrity models assumes a lattice of integrity levels?

A. Take-Grant
B. Biba
C. Harrison-Ruzzo
D. Bell-LaPadula

Answer: B

NEW QUESTION 640
- (Exam Topic 13)
What are the steps of a risk assessment?

A. identification, analysis, evaluation
B. analysis, evaluation, mitigation
C. classification, identification, risk management
D. identification, evaluation, mitigation

Answer: A

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 641
- (Exam Topic 13)
A security compliance manager of a large enterprise wants to reduce the time it takes to perform network, system, and application security compliance audits while increasing quality and effectiveness of the results. What should be implemented to BEST achieve the desired results?

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

Answer: A

NEW QUESTION 643
- (Exam Topic 13)
An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject’s data?

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

Answer: B

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 648
- (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 651
- (Exam Topic 13)
Which of the following could be considered the MOST significant security challenge when adopting DevOps practices compared to a more traditional control framework?

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

Answer: B

NEW QUESTION 656

- (Exam Topic 13)
In a change-controlled environment, which of the following is MOST likely to lead to unauthorized changes to production programs?

A. Modifying source code without approval
B. Promoting programs to production without approval
C. Developers checking out source code without approval
D. Developers using Rapid Application Development (RAD) methodologies without approval

Answer: A

NEW QUESTION 661
- (Exam Topic 13)
Which of the following is MOST effective in detecting information hiding in Transmission Control Protocol/internet Protocol (TCP/IP) traffic?

A. Stateful inspection firewall
B. Application-level firewall
C. Content-filtering proxy
D. Packet-filter firewall

Answer: A

NEW QUESTION 665
- (Exam Topic 13)
Who has the PRIMARY responsibility to ensure that security objectives are aligned with organization goals?

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

Answer: C

NEW QUESTION 667
- (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 670
- (Exam Topic 13)
An organization recently conducted a review of the security of its network applications. One of the vulnerabilities found was that the session key used in encrypting sensitive information to a third party server
had been hard-coded in the client and server applications. Which of the following would be MOST effective in mitigating this vulnerability?

A. Diffle-Hellman (DH) algorithm
B. Elliptic Curve Cryptography (ECC) algorithm
C. Digital Signature algorithm (DSA)
D. Rivest-Shamir-Adleman (RSA) algorithm

Answer: D

NEW QUESTION 675
- (Exam Topic 13)
What protocol is often used between gateway hosts on the Internet?

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

Answer: B

NEW QUESTION 676
- (Exam Topic 13)
An organization plan on purchasing a custom software product developed by a small vendor to support its business model. Which unique consideration should be made part of the contractual agreement potential
long-term risks associated with creating this dependency?

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

Answer: B

NEW QUESTION 678
- (Exam Topic 13)
Which of the following is MOST appropriate for protecting confidentially of data stored on a hard drive?

A. Triple Data Encryption Standard (3DES)
B. Advanced Encryption Standard (AES)
C. Message Digest 5 (MD5)
D. Secure Hash Algorithm 2(SHA-2)

Answer: B

NEW QUESTION 682
- (Exam Topic 13)
Which of the following techniques is known to be effective in spotting resource exhaustion problems, especially with resources such as processes, memory, and connections?

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

Answer: A

NEW QUESTION 686
- (Exam Topic 13)
Which of the following management process allows ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

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

Answer: A

NEW QUESTION 689
- (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

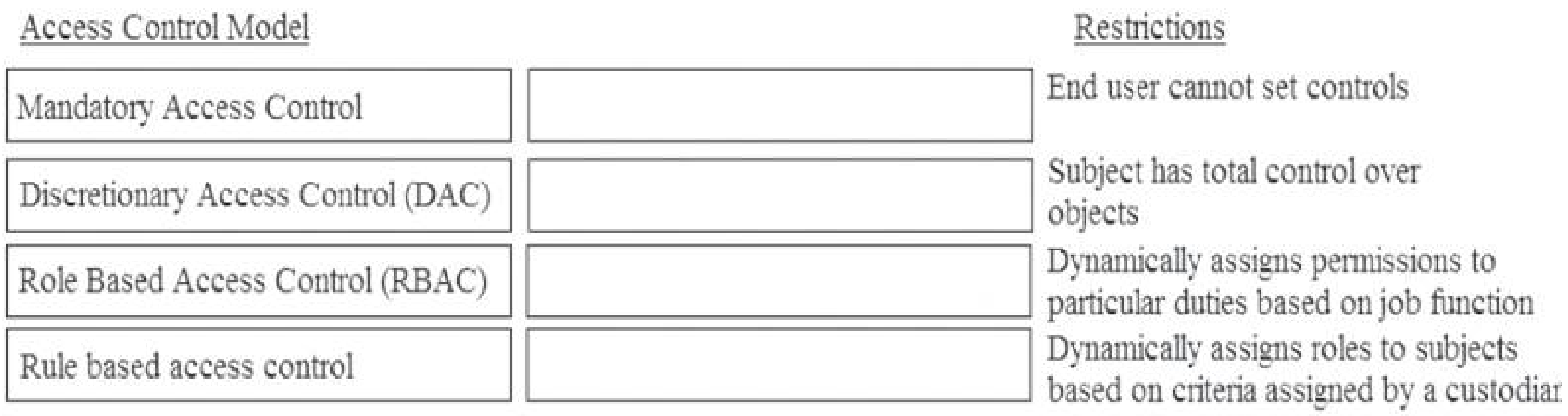
Answer: B

NEW QUESTION 691
- (Exam Topic 13)
“Stateful” differs from “Static” packet filtering firewalls by being aware of which of the following?

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

Answer: A

NEW QUESTION 692
- (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.

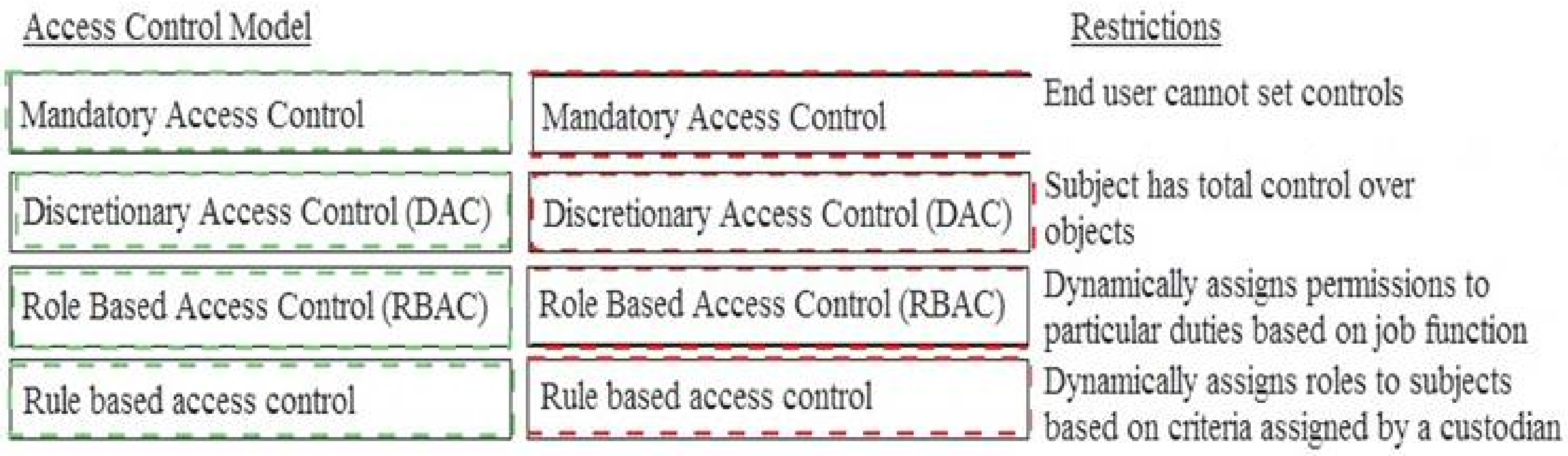


Access Control Model		Restrictions
Mandatory Access Control		End user cannot set controls
Discretionary Access Control (DAC)		Subject has total control over objects
Role Based Access Control (RBAC)		Dynamically assigns permissions to particular duties based on job function
Rule based access control	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

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 694
- (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 695
- (Exam Topic 12)
An organization’s information security strategic plan MUST be reviewed

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

Answer: C

NEW QUESTION 699
- (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 704
- (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 708
- (Exam Topic 12)
A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

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

Answer: A

NEW QUESTION 711
- (Exam Topic 12)
Which of the following media sanitization techniques is MOST likely to be effective for an organization using public cloud services?

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

Answer: B

NEW QUESTION 714
- (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 719
- (Exam Topic 12)
What is the MOST important element when considering the effectiveness of a training program for Business Continuity (BC) and Disaster Recovery (DR)?

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

Answer: B

NEW QUESTION 722
- (Exam Topic 12)
A database administrator is asked by a high-ranking member of management to perform specific changes to the accounting system database. The administrator is specifically instructed to not track or evidence the change in a ticket. Which of the following is the BEST course of action?

A. Ignore the request and do not perform the change.
B. Perform the change as requested, and rely on the next audit to detect and report the situation.
C. Perform the change, but create a change ticket regardless to ensure there is complete traceability.
D. Inform the audit committee or internal audit directly using the corporate whistleblower process.

Answer: D

NEW QUESTION 727
- (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 730
- (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 732
- (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 733
- (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 737
- (Exam Topic 12)
Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

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

Answer: B

NEW QUESTION 739
- (Exam Topic 12)
Which of the following are effective countermeasures against passive network-layer attacks?

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

Answer: C

NEW QUESTION 743
- (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 747
- (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 749
- (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 754
- (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 758
- (Exam Topic 12)
Between which pair of Open System Interconnection (OSI) Reference Model layers are routers used as a communications device?

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

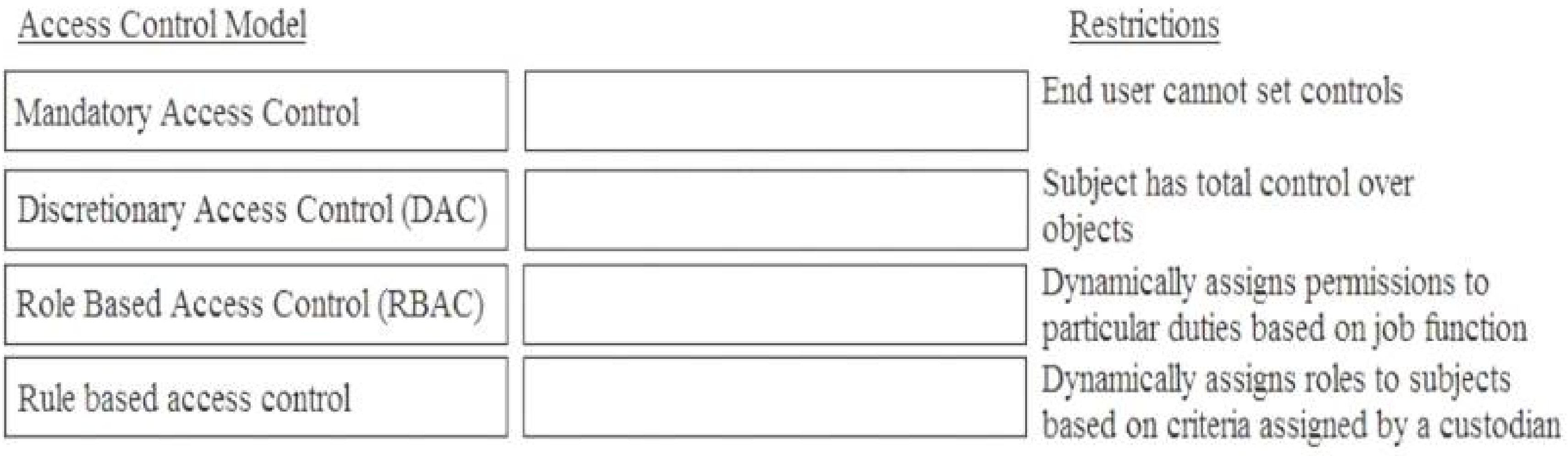
Answer: B

NEW QUESTION 763
- (Exam Topic 12)
Although code using a specific program language may not be susceptible to a buffer overflow attack,

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

Answer: C

NEW QUESTION 766
- (Exam Topic 12)
Match the name of access control model with its associated restriction.
Drag each access control model to its appropriate restriction access on the right.



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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 769
- (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 772
- (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)

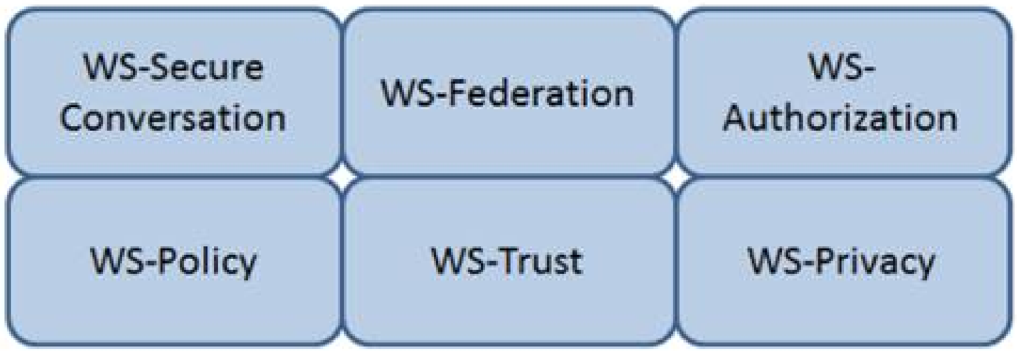
Answer: B

NEW QUESTION 775
- (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 776
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated? Click on the correct specification in the image below.



WS-Secure Conversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 778
- (Exam Topic 11)
While investigating a malicious event, only six days of audit logs from the last month were available. What policy should be updated to address this problem?

A. Retention
B. Reporting
C. Recovery
D. Remediation

Answer: A

NEW QUESTION 783
- (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 788
- (Exam Topic 11)
Which of the following could elicit a Denial of Service (DoS) attack against a credential management system?

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

Answer: B

NEW QUESTION 792
- (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 795
- (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 796
- (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 798
- (Exam Topic 11)
If an identification process using a biometric system detects a 100% match between a presented template and a stored template, what is the interpretation of this result?

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

Answer: B

NEW QUESTION 801
- (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 804

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

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

Answer: A

NEW QUESTION 805
- (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 810
- (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 811
- (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 813
- (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 814
- (Exam Topic 11)
Which of the following is the MOST important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?

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

Answer: D

NEW QUESTION 816
- (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

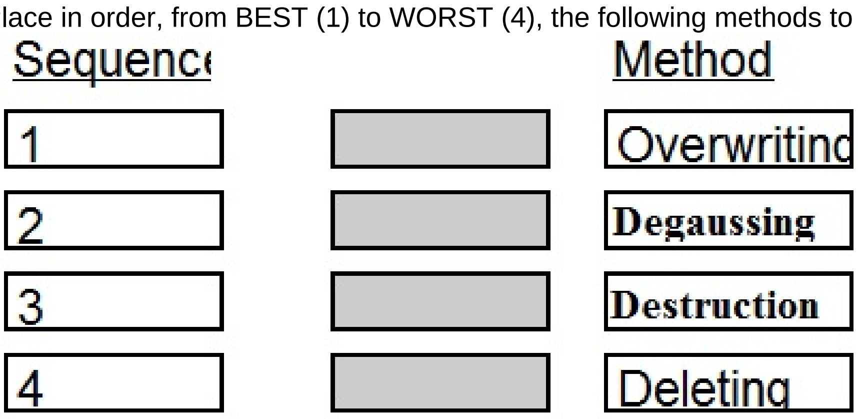
Answer: C

NEW QUESTION 820
- (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 823
- (Exam Topic 11)
Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic media.

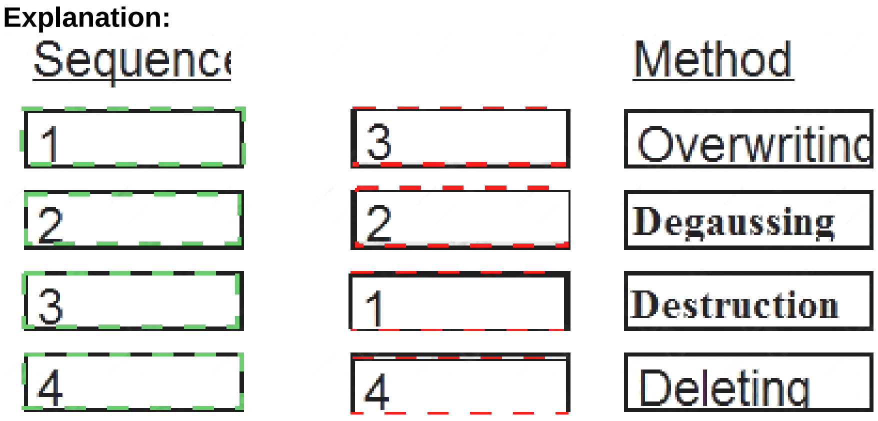


Sequence		Method
1		Overwriting
2		Degaussing
3		Destruction
4		Deleting

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

NEW QUESTION 827
- (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 828
- (Exam Topic 11)
Which of the following is a reason to use manual patch installation instead of automated patch management?

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

Answer: C

NEW QUESTION 829
- (Exam Topic 11)
To protect auditable information, which of the following MUST be configured to only allow read access?

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

Answer: B

NEW QUESTION 830
- (Exam Topic 11)
Which of the following controls is the FIRST step in protecting privacy in an information system?

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

Answer: B

NEW QUESTION 833
- (Exam Topic 11)
A Simple Power Analysis (SPA) attack against a device directly observes which of the following?

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

Answer: B

NEW QUESTION 837
- (Exam Topic 11)
The BEST example of the concept of "something that a user has" when providing an authorized user access to a computing system is

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

Answer: B

NEW QUESTION 842
- (Exam Topic 10)
The use of proximity card to gain access to a building is an example of what type of security control?

A. Legal
B. Logical
C. Physical
D. Procedural

Answer: C

NEW QUESTION 843
- (Exam Topic 10)
Which of the following is a critical factor for implementing a successful data classification program?

A. Executive sponsorship
B. Information security sponsorship
C. End-user acceptance
D. Internal audit acceptance

Answer: A

NEW QUESTION 846
- (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

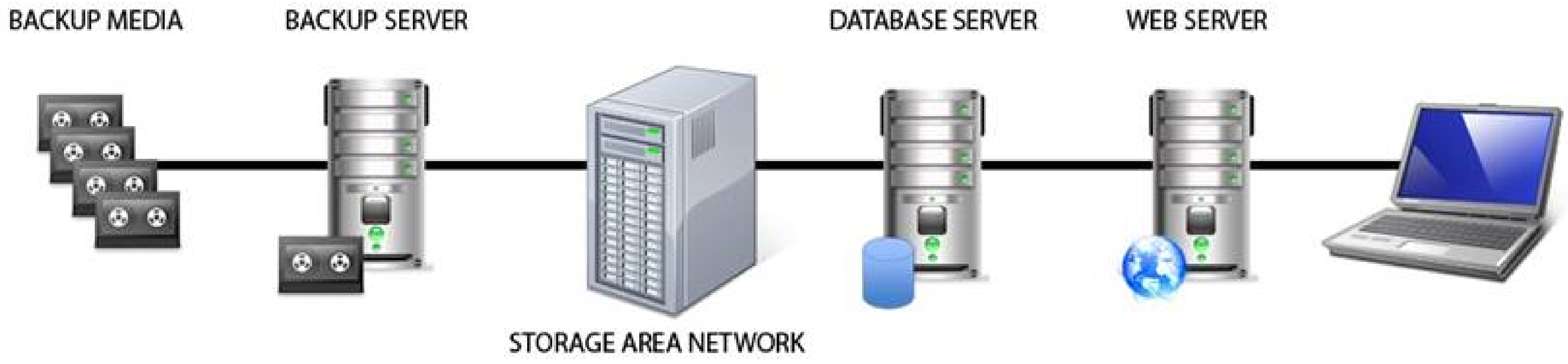
NEW QUESTION 851
- (Exam Topic 10)
Which of the following violates identity and access management best practices?

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

D. Privileged accounts

Answer: C

NEW QUESTION 856
- (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 860
- (Exam Topic 10)
Multi-Factor Authentication (MFA) is necessary in many systems given common types of password attacks. Which of the following is a correct list of password attacks?

A. Masquerading, salami, malware, polymorphism
B. Brute force, dictionary, phishing, keylogger
C. Zeus, netbus, rabbit, turtle
D. Token, biometrics, IDS, DLP

Answer: B

NEW QUESTION 864
- (Exam Topic 10)
What does secure authentication with logging provide?

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

Answer: B

NEW QUESTION 869
- (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 indicate where the IT budget is BEST allocated during this time?

A. Policies
B. Frameworks
C. Metrics
D. Guidelines

Answer: C

NEW QUESTION 870
- (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 871
- (Exam Topic 10)
An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a PRIMARY security concern?

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

Answer: A

NEW QUESTION 875
- (Exam Topic 10)
Which of the following is a MAJOR consideration in implementing a Voice over IP (VoIP) network?

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

Answer: A

NEW QUESTION 878
- (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.

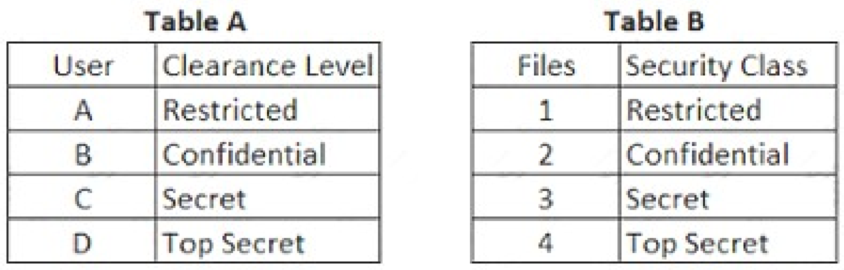


Table A

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

Which of the following is true according to the star property (*property)?

A. User D can write to File 1
B. User B can write to File 1
C. User A can write to File 1
D. User C can write to File 1

Answer: C

NEW QUESTION 883
- (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 885
- (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 887

- (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 889
- (Exam Topic 10)
Which of the following is a detective access control mechanism?

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

Answer: A

NEW QUESTION 892
......