ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

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

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

Answer: B

NEW QUESTION 2
- (Exam Topic 1)
Which of the following actions will reduce risk to a laptop before traveling to a high risk area?

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

Answer: D

NEW QUESTION 3
- (Exam Topic 2)
In a data classification scheme, the data is owned by the

A. system security managers
B. business managers
C. Information Technology (IT) managers
D. end users

Answer: B

NEW QUESTION 4
- (Exam Topic 2)
When implementing a data classification program, why is it important to avoid too much granularity?

A. The process will require too many resources
B. It will be difficult to apply to both hardware and software
C. It will be difficult to assign ownership to the data
D. The process will be perceived as having value

Answer: A

NEW QUESTION 5
- (Exam Topic 2)
An organization has doubled in size due to a rapid market share increase. The size of the Information Technology (IT) staff has maintained pace with this growth. The organization hires several contractors whose onsite time is limited. The IT department has pushed its limits building servers and rolling out workstations and has a backlog of account management requests.
Which contract is BEST in offloading the task from the IT staff?

A. Platform as a Service (PaaS)
B. Identity as a Service (IDaaS)
C. Desktop as a Service (DaaS)
D. Software as a Service (SaaS)

Answer: B

NEW QUESTION 6
- (Exam Topic 3)
Which of the following mobile code security models relies only on trust?

A. Code signing
B. Class authentication
C. Sandboxing
D. Type safety

Answer: A

NEW QUESTION 7
- (Exam Topic 3)
Which security service is served by the process of encryption plaintext with the sender’s private key and decrypting cipher text with the sender’s public key?

A. Confidentiality
B. Integrity

C. Identification
D. Availability

Answer: A

NEW QUESTION 8
- (Exam Topic 3)
Which technique can be used to make an encryption scheme more resistant to a known plaintext attack?

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

Answer: A

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

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

Answer: A

NEW QUESTION 10
- (Exam Topic 4)
What is the purpose of an Internet Protocol (IP) spoofing attack?

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

Answer: D

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

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

Answer: A

NEW QUESTION 14
- (Exam Topic 6)
Which of the following could cause a Denial of Service (DoS) against an authentication system?

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

Answer: D

NEW QUESTION 19
- (Exam Topic 7)
Which of the following is a PRIMARY advantage of using a third-party identity service?

A. Consolidation of multiple providers
B. Directory synchronization
C. Web based logon
D. Automated account management

Answer: D

NEW QUESTION 23
- (Exam Topic 7)
What is the MOST important step during forensic analysis when trying to learn the purpose of an unknown application?

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

Answer: D

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

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

Answer: D

NEW QUESTION 31
- (Exam Topic 8)
Which of the following is a web application control that should be put into place to prevent exploitation of Operating System (OS) bugs?

A. Check arguments in function calls
B. Test for the security patch level of the environment
C. Include logging functions
D. Digitally sign each application module

Answer: B

NEW QUESTION 34
- (Exam Topic 8)
Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

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

Answer: D

NEW QUESTION 39
- (Exam Topic 9)
Internet Protocol (IP) source address spoofing is used to defeat

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

Answer: A

NEW QUESTION 42
- (Exam Topic 9)
Which of the following is ensured when hashing files during chain of custody handling?

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

Answer: C

NEW QUESTION 44
- (Exam Topic 9)
Which of the following MUST be part of a contract to support electronic discovery of data stored in a cloud environment?

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

Answer: D

NEW QUESTION 48

- (Exam Topic 9)
Logical access control programs are MOST effective when they are

A. approved by external auditors.
B. combined with security token technology.
C. maintained by computer security officers.
D. made part of the operating system.

Answer: D

NEW QUESTION 51
- (Exam Topic 9)
A vulnerability test on an Information System (IS) is conducted to

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

Answer: C

NEW QUESTION 53
- (Exam Topic 9)
Contingency plan exercises are intended to do which of the following?

A. Train personnel in roles and responsibilities
B. Validate service level agreements
C. Train maintenance personnel
D. Validate operation metrics

Answer: A

NEW QUESTION 56
- (Exam Topic 9)
In the area of disaster planning and recovery, what strategy entails the presentation of information about the plan?

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

Answer: A

NEW QUESTION 58
- (Exam Topic 9)
Which of the following is a physical security control that protects Automated Teller Machines (ATM) from skimming?

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

Answer: A

NEW QUESTION 61
- (Exam Topic 9)
Copyright provides protection for which of the following?

A. Ideas expressed in literary works
B. A particular expression of an idea
C. New and non-obvious inventions
D. Discoveries of natural phenomena

Answer: B

NEW QUESTION 63
- (Exam Topic 9)
The key benefits of a signed and encrypted e-mail include

A. confidentiality, authentication, and authorization.
B. confidentiality, non-repudiation, and authentication.
C. non-repudiation, authorization, and authentication.
D. non-repudiation, confidentiality, and authorization.

Answer: B

NEW QUESTION 66
- (Exam Topic 9)
An internal Service Level Agreement (SLA) covering security is signed by senior managers and is in place. When should compliance to the SLA be reviewed to ensure that a good security posture is being delivered?

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

Answer: D

NEW QUESTION 68
- (Exam Topic 9)
Which one of the following transmission media is MOST effective in preventing data interception?

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

Answer: C

NEW QUESTION 73
- (Exam Topic 9)
Which layer of the Open Systems Interconnections (OSI) model implementation adds information concerning the logical connection between the sender and receiver?

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

Answer: C

NEW QUESTION 75
- (Exam Topic 9)
Which one of the following considerations has the LEAST impact when considering transmission security?

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

Answer: C

NEW QUESTION 76
- (Exam Topic 9)
Which of the following is considered best practice for preventing e-mail spoofing?

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

Answer: B

NEW QUESTION 81
- (Exam Topic 9)
The process of mutual authentication involves a computer system authenticating a user and authenticating the

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

Answer: B

NEW QUESTION 83
- (Exam Topic 9)
Which of the following is an authentication protocol in which a new random number is generated uniquely for each login session?

A. Challenge Handshake Authentication Protocol (CHAP)
B. Point-to-Point Protocol (PPP)
C. Extensible Authentication Protocol (EAP)
D. Password Authentication Protocol (PAP)

Answer: A

NEW QUESTION 84
- (Exam Topic 9)
The BEST method of demonstrating a company's security level to potential customers is

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

Answer: A

NEW QUESTION 89
- (Exam Topic 9)
An organization is selecting a service provider to assist in the consolidation of multiple computing sites including development, implementation and ongoing support of various computer systems. Which of the following MUST be verified by the Information Security Department?

A. The service provider's policies are consistent with ISO/IEC27001 and there is evidence that the service provider is following those policies.
B. The service provider will segregate the data within its systems and ensure that each region's policies are met.
C. The service provider will impose controls and protections that meet or exceed the current systemscontrols and produce audit logs as verification.
D. The service provider's policies can meet the requirements imposed by the new environment even if they differ from the organization's current policies.

Answer: D

NEW QUESTION 91
- (Exam Topic 9)
Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?

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

Answer: D

NEW QUESTION 93
- (Exam Topic 9)
The use of strong authentication, the encryption of Personally Identifiable Information (PII) on database servers, application security reviews, and the encryption of data transmitted across networks provide

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

Answer: B

NEW QUESTION 96
- (Exam Topic 9)
Which of the following is the MOST important consideration when storing and processing Personally Identifiable Information (PII)?

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

Answer: D

NEW QUESTION 99
- (Exam Topic 9)
What would be the PRIMARY concern when designing and coordinating a security assessment for an Automatic Teller Machine (ATM) system?

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

Answer: A

NEW QUESTION 101
- (Exam Topic 9)
An external attacker has compromised an organization's network security perimeter and installed a sniffer onto an inside computer. Which of the following is the MOST effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information?

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

Answer: D

NEW QUESTION 105
- (Exam Topic 9)
The Hardware Abstraction Layer (HAL) is implemented in the

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

Answer: A

NEW QUESTION 109
- (Exam Topic 9)
When transmitting information over public networks, the decision to encrypt it should be based on

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

Answer: C

NEW QUESTION 111
- (Exam Topic 9)
Which of the following would be the FIRST step to take when implementing a patch management program?

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

Answer: D

NEW QUESTION 116
- (Exam Topic 9)
Why MUST a Kerberos server be well protected from unauthorized access?

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

Answer: A

NEW QUESTION 121
- (Exam Topic 9)
An Intrusion Detection System (IDS) is generating alarms that a user account has over 100 failed login attempts per minute. A sniffer is placed on the network, and a variety of passwords for that user are noted. Which of the following is MOST likely occurring?

A. A dictionary attack
B. A Denial of Service (DoS) attack
C. A spoofing attack
D. A backdoor installation

Answer: A

NEW QUESTION 124
- (Exam Topic 9)
Which of the following is the BEST mitigation from phishing attacks?

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

Answer: B

NEW QUESTION 128

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

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

Answer: A

NEW QUESTION 131
- (Exam Topic 9)
By allowing storage communications to run on top of Transmission Control Protocol/Internet Protocol (TCP/IP) with a Storage Area Network (SAN), the

A. confidentiality of the traffic is protected.
B. opportunity to sniff network traffic exists.
C. opportunity for device identity spoofing is eliminated.
D. storage devices are protected against availability attacks.

Answer: B

NEW QUESTION 134
- (Exam Topic 9)
Which of the following BEST represents the principle of open design?

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

Answer: D

NEW QUESTION 136
- (Exam Topic 9)
Which of the following wraps the decryption key of a full disk encryption implementation and ties the hard disk drive to a particular device?

A. Trusted Platform Module (TPM)
B. Preboot eXecution Environment (PXE)
C. Key Distribution Center (KDC)
D. Simple Key-Management for Internet Protocol (SKIP)

Answer: A

NEW QUESTION 138
- (Exam Topic 9)
Which Hyper Text Markup Language 5 (HTML5) option presents a security challenge for network data leakage prevention and/or monitoring?

A. Cross Origin Resource Sharing (CORS)
B. WebSockets
C. Document Object Model (DOM) trees
D. Web Interface Definition Language (IDL)

Answer: B

NEW QUESTION 143
- (Exam Topic 9)
At a MINIMUM, a formal review of any Disaster Recovery Plan (DRP) should be conducted

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

Answer: C

NEW QUESTION 146
- (Exam Topic 9)
In Disaster Recovery (DR) and business continuity training, which BEST describes a functional drill?

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

Answer: B

NEW QUESTION 147
- (Exam Topic 10)
What is the MAIN feature that onion routing networks offer?

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

Answer: C

NEW QUESTION 151
- (Exam Topic 10)
What do Capability Maturity Models (CMM) serve as a benchmark for in an organization?

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

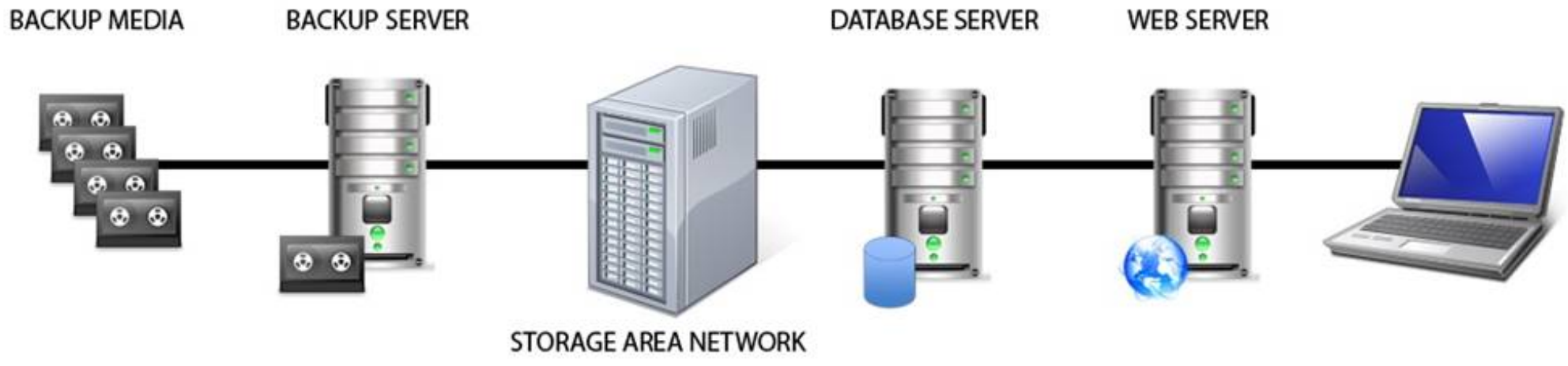
Answer: D

NEW QUESTION 154
- (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 155
- (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 160
- (Exam Topic 10)
When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?

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

Answer: B

NEW QUESTION 161
- (Exam Topic 10)
Which of the following provides effective management assurance for a Wireless Local Area Network (WLAN)?

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

Answer: A

NEW QUESTION 166
- (Exam Topic 10)
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
If it is discovered that large quantities of information have been copied by the unauthorized individual, what attribute of the data has been compromised?

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

Answer: D

NEW QUESTION 171
- (Exam Topic 10)
Which of the following is required to determine classification and ownership?

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

Answer: A

NEW QUESTION 173
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
What MUST the access control logs contain in addition to the identifier?

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

Answer: A

NEW QUESTION 175
- (Exam Topic 10)
What is a common challenge when implementing Security Assertion Markup Language (SAML) for identity integration between on-premise environment and an external identity provider service?

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

Answer: A

NEW QUESTION 178
- (Exam Topic 10)
A business has implemented Payment Card Industry Data Security Standard (PCI-DSS) compliant handheld credit card processing on their Wireless Local Area Network (WLAN) topology. The network team partitioned the WLAN to create a private segment for credit card processing using a firewall to control device access and route traffic to the card processor on the Internet. What components are in the scope of PCI-DSS?

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

Answer: C

NEW QUESTION 180
- (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 185
- (Exam Topic 10)
Which of the following is the BEST solution to provide redundancy for telecommunications links?

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

Answer: D

NEW QUESTION 190
- (Exam Topic 10)
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
In the plan, what is the BEST approach to mitigate future internal client-based attacks?

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

Answer: D

NEW QUESTION 193
- (Exam Topic 10)
With data labeling, which of the following MUST be the key decision maker?

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

Answer: D

NEW QUESTION 194
- (Exam Topic 10)
Which of the following is the MOST crucial for a successful audit plan?

A. Defining the scope of the audit to be performed
B. Identifying the security controls to be implemented
C. Working with the system owner on new controls
D. Acquiring evidence of systems that are not compliant

Answer: A

NEW QUESTION 197
- (Exam Topic 10)
A Business Continuity Plan (BCP) is based on

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

Answer: C

NEW QUESTION 199
- (Exam Topic 10)
A large university needs to enable student access to university resources from their homes. Which of the following provides the BEST option for low maintenance and ease of deployment?

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

Answer: B

NEW QUESTION 203

- (Exam Topic 10)
An organization decides to implement a partial Public Key Infrastructure (PKI) with only the servers having digital certificates. What is the security benefit of this implementation?

A. Clients can authenticate themselves to the servers.
B. Mutual authentication is available between the clients and servers.
C. Servers are able to issue digital certificates to the client.
D. Servers can authenticate themselves to the client.

Answer: D

NEW QUESTION 206
- (Exam Topic 10)
From a security perspective, which of the following is a best practice to configure a Domain Name Service (DNS) system?

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

Answer: D

NEW QUESTION 210
- (Exam Topic 10)
A thorough review of an organization's audit logs finds that a disgruntled network administrator has intercepted emails meant for the Chief Executive Officer (CEO) and changed them before forwarding them to their intended recipient. What type of attack has MOST likely occurred?

A. Spoofing
B. Eavesdropping
C. Man-in-the-middle
D. Denial of service

Answer: C

NEW QUESTION 213
- (Exam Topic 10)
An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a PRIMARY security concern?

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

Answer: C

NEW QUESTION 217
- (Exam Topic 10)
Which of the following is the BEST countermeasure to brute force login attacks?

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

Answer: D

NEW QUESTION 222
- (Exam Topic 10)
What is the MOST important reason to configure unique user IDs?

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

Answer: A

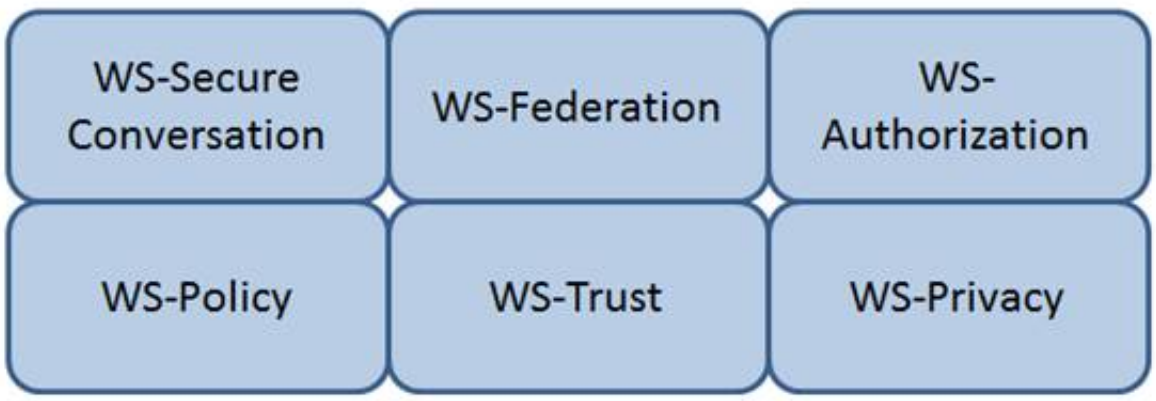
NEW QUESTION 226
- (Exam Topic 10)
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
Aside from the potential records which may have been viewed, which of the following should be the PRIMARY concern regarding the database information?

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

D. Confidentiality of the incident

Answer: A

NEW QUESTION 228
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 229
- (Exam Topic 11)
Which of the following BEST describes the purpose of performing security certification?

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

Answer: B

NEW QUESTION 234
- (Exam Topic 11)
Which of the following prevents improper aggregation of privileges in Role Based Access Control (RBAC)?

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

Answer: B

NEW QUESTION 237
- (Exam Topic 11)
A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

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

Answer: A

NEW QUESTION 241

- (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 242
- (Exam Topic 11)
Which of the following is generally indicative of a replay attack when dealing with biometric authentication?

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

Answer: D

NEW QUESTION 247
- (Exam Topic 11)
A security professional has been asked to evaluate the options for the location of a new data center within a multifloor building. Concerns for the data center include emanations and physical access controls.
Which of the following is the BEST location?

A. On the top floor
B. In the basement
C. In the core of the building
D. In an exterior room with windows

Answer: C

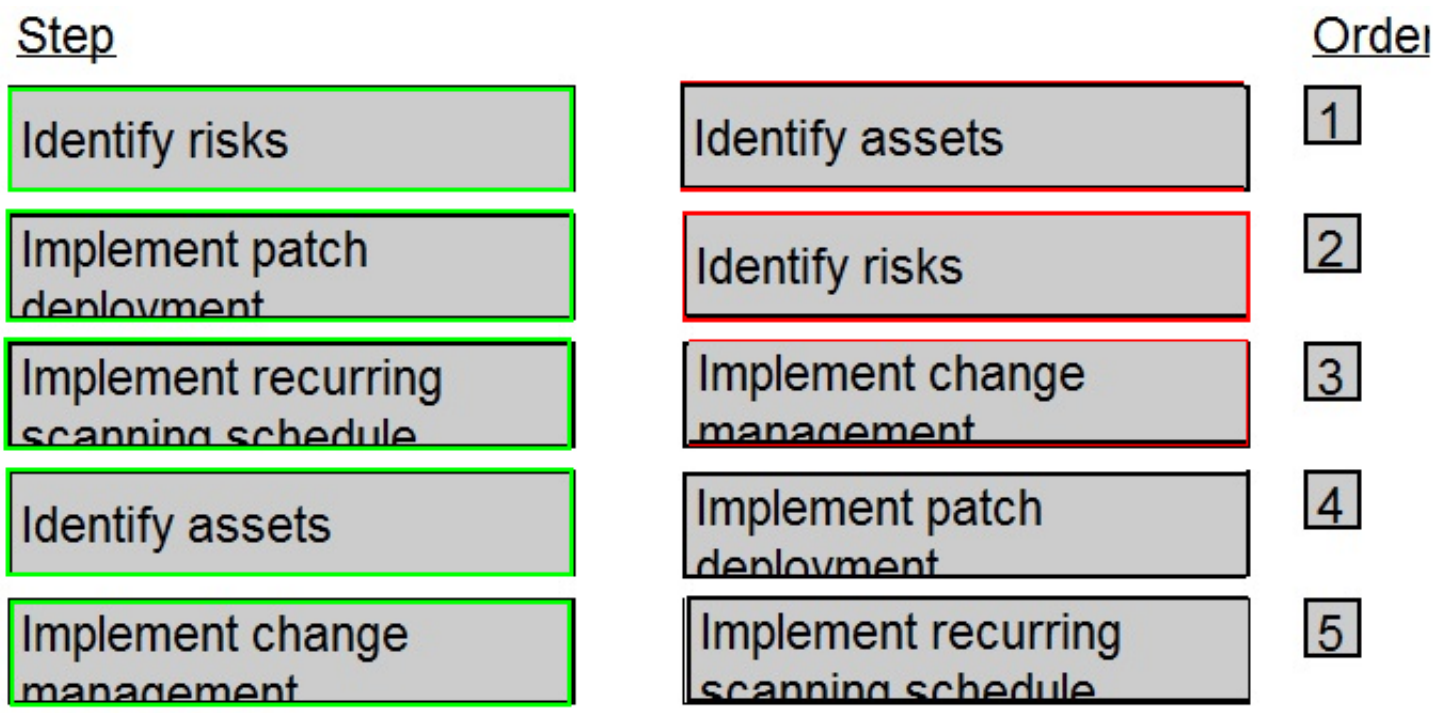
NEW QUESTION 252
- (Exam Topic 11)
Order the below steps to create an effective vulnerability management process.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 253
- (Exam Topic 11)
Which of the following is the BEST approach to take in order to effectively incorporate the concepts of business continuity into the organization?

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

Answer: C

NEW QUESTION 258
- (Exam Topic 11)
What should happen when an emergency change to a system must be performed?

A. The change must be given priority at the next meeting of the change control board.
B. Testing and approvals must be performed quickly.
C. The change must be performed immediately and then submitted to the change board.
D. The change is performed and a notation is made in the system log.

Answer: B

NEW QUESTION 260
- (Exam Topic 11)
If compromised, which of the following would lead to the exploitation of multiple virtual machines?

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

Answer: B

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

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

Answer: C

NEW QUESTION 266
- (Exam Topic 11)
Regarding asset security and appropriate retention, which of the following INITIAL top three areas are important to focus on?

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

Answer: A

NEW QUESTION 268
- (Exam Topic 11)
Which of the following is the BEST method to assess the effectiveness of an organization's vulnerability management program?

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

Answer: B

NEW QUESTION 273
- (Exam Topic 11)
Which of the following is the MOST likely cause of a non-malicious data breach when the source of the data breach was an un-marked file cabinet containing sensitive documents?

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

Answer: A

NEW QUESTION 274
- (Exam Topic 11)
What is an important characteristic of Role Based Access Control (RBAC)?

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

Answer: B

NEW QUESTION 278
- (Exam Topic 11)
Which of the following is the BIGGEST weakness when using native Lightweight Directory Access Protocol (LDAP) for authentication?

A. Authorizations are not included in the server response
B. Unsalted hashes are passed over the network
C. The authentication session can be replayed
D. Passwords are passed in cleartext

Answer: D

NEW QUESTION 283
- (Exam Topic 11)
Which of the following disaster recovery test plans will be MOST effective while providing minimal risk?

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

Answer: B

NEW QUESTION 285
- (Exam Topic 11)
Which of the following standards/guidelines requires an Information Security Management System (ISMS) to be defined?

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

Answer: A

NEW QUESTION 288
- (Exam Topic 11)
What is the PRIMARY difference between security policies and security procedures?

A. Policies are used to enforce violations, and procedures create penalties
B. Policies point to guidelines, and procedures are more contractual in nature
C. Policies are included in awareness training, and procedures give guidance
D. Policies are generic in nature, and procedures contain operational details

Answer: D

NEW QUESTION 292
- (Exam Topic 11)
An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?

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

Answer: A

NEW QUESTION 296
- (Exam Topic 11)
How does Encapsulating Security Payload (ESP) in transport mode affect the Internet Protocol (IP)?

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

Answer: B

NEW QUESTION 300
- (Exam Topic 11)
Which of the following command line tools can be used in the reconnaisance phase of a network vulnerability assessment?

A. dig
B. ifconfig
C. ipconfig
D. nbtstat

Answer: A

NEW QUESTION 302
- (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 304
- (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 308
- (Exam Topic 11)
An organization has developed a major application that has undergone accreditation testing. After receiving the results of the evaluation, what is the final step before the application can be accredited?

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

Answer: A

NEW QUESTION 310
- (Exam Topic 11)
Which methodology is recommended for penetration testing to be effective in the development phase of the life-cycle process?

A. White-box testing
B. Software fuzz testing

C. Black-box testing
D. Visual testing

Answer: A

NEW QUESTION 315
- (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 319
- (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 324
- (Exam Topic 11)
The PRIMARY outcome of a certification process is that it provides documented

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

Answer: D

NEW QUESTION 325
- (Exam Topic 11)
Discretionary Access Control (DAC) is based on which of the following?

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

Answer: B

NEW QUESTION 329
- (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 332
- (Exam Topic 11)
When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?

A. After the system preliminary design has been developed and the data security categorization has been performed
B. After the business functional analysis and the data security categorization have been performed
C. After the vulnerability analysis has been performed and before the system detailed design begins
D. After the system preliminary design has been developed and before the data security categorization begins

Answer: B

NEW QUESTION 337
- (Exam Topic 11)
Who is ultimately responsible to ensure that information assets are categorized and adequate measures are taken to protect them?

A. Data Custodian
B. Executive Management
C. Chief Information Security Officer
D. Data/Information/Business Owners

Answer: B

NEW QUESTION 339
- (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 343
- (Exam Topic 11)
Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?

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

Answer: C

NEW QUESTION 346
- (Exam Topic 11)
In the Open System Interconnection (OSI) model, which layer is responsible for the transmission of binary data over a communications network?

A. Application Layer
B. Physical Layer
C. Data-Link Layer
D. Network Layer

Answer: B

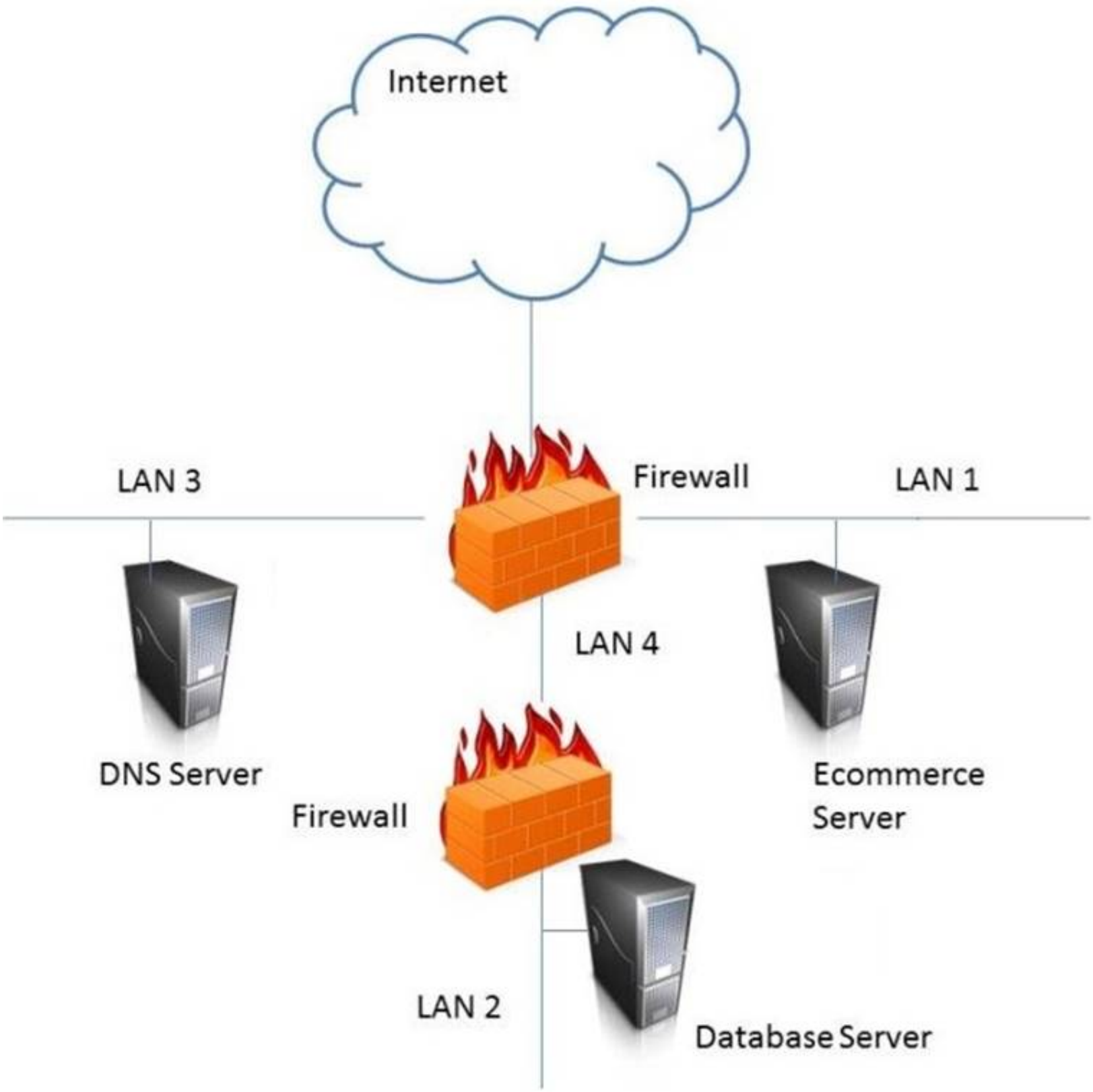
NEW QUESTION 347
- (Exam Topic 11)
Which of the following secures web transactions at the Transport Layer?

A. Secure HyperText Transfer Protocol (S-HTTP)
B. Secure Sockets Layer (SSL)
C. Socket Security (SOCKS)
D. Secure Shell (SSH)

Answer: B

NEW QUESTION 349
- (Exam Topic 11)

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



A. Mastered
B. Not Mastered

Answer: A

Explanation:
LAN 4

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

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

Answer: D

NEW QUESTION 359
- (Exam Topic 11)
Which of the following is the PRIMARY issue when collecting detailed log information?

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

Answer: B

NEW QUESTION 362
- (Exam Topic 11)
Which of the following is the PRIMARY benefit of implementing data-in-use controls?

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

Answer: C

NEW QUESTION 364
- (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 369
- (Exam Topic 12)
Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

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

Answer: A

NEW QUESTION 370
- (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 371
- (Exam Topic 12)
Which Radio Frequency Interference (RFI) phenomenon associated with bundled cable runs can create information leakage?

A. Transference
B. Covert channel
C. Bleeding
D. Cross-talk

Answer: D

NEW QUESTION 374
- (Exam Topic 12)
Which of the following is the MOST important goal of information asset valuation?

A. Developing a consistent and uniform method of controlling access on information assets
B. Developing appropriate access control policies and guidelines
C. Assigning a financial value to an organization’s information assets
D. Determining the appropriate level of protection

Answer: D

NEW QUESTION 375
- (Exam Topic 12)
Which of the following is MOST important when deploying digital certificates?

A. Validate compliance with X.509 digital certificate standards

B. Establish a certificate life cycle management framework
C. Use a third-party Certificate Authority (CA)
D. Use no less than 256-bit strength encryption when creating a certificate

Answer: B

NEW QUESTION 377
- (Exam Topic 12)
What type of wireless network attack BEST describes an Electromagnetic Pulse (EMP) attack?

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

Answer: B

NEW QUESTION 380
- (Exam Topic 12)
Match the access control type to the example of the control type. Drag each access control type net to its corresponding example.

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 382
- (Exam Topic 12)
Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

A. dig
B. ipconfig
C. ifconfig
D. nbstat

Answer: A

NEW QUESTION 385
- (Exam Topic 12)
At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

A. Transport Layer
B. Data-Link Layer
C. Network Layer
D. Application Layer

Answer: C

NEW QUESTION 389
- (Exam Topic 12)
When writing security assessment procedures, what is the MAIN purpose of the test outputs and reports?

A. To force the software to fail and document the process
B. To find areas of compromise in confidentiality and integrity
C. To allow for objective pass or fail decisions
D. To identify malware or hidden code within the test results

Answer: C

NEW QUESTION 392
- (Exam Topic 12)
Which of the following BEST represents the concept of least privilege?

A. Access to an object is denied unless access is specifically allowed.
B. Access to an object is only available to the owner.
C. Access to an object is allowed unless it is protected by the information security policy.
D. Access to an object is only allowed to authenticated users via an Access Control List (ACL).

Answer: A

NEW QUESTION 394
- (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 399
- (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 403
- (Exam Topic 12)
When evaluating third-party applications, which of the following is the GREATEST responsibility of Information Security?

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

Answer: C

NEW QUESTION 406
- (Exam Topic 12)
Reciprocal backup site agreements are considered to be

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

Answer: B

NEW QUESTION 410
- (Exam Topic 12)
Backup information that is critical to the organization is identified through a

A. Vulnerability Assessment (VA).
B. Business Continuity Plan (BCP).
C. Business Impact Analysis (BIA).
D. data recovery analysis.

Answer: D

NEW QUESTION 413
- (Exam Topic 12)

In which identity management process is the subject's identity established?

A. Trust
B. Provisioning
C. Authorization
D. Enrollment

Answer: D

NEW QUESTION 417
- (Exam Topic 12)
Which of the following is the PRIMARY reason to perform regular vulnerability scanning of an organization network?

A. Provide vulnerability reports to management.
B. Validate vulnerability remediation activities.
C. Prevent attackers from discovering vulnerabilities.
D. Remediate known vulnerabilities.

Answer: B

NEW QUESTION 422
- (Exam Topic 12)
What is a characteristic of Secure Socket Layer (SSL) and Transport Layer Security (TLS)?

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

Answer: A

NEW QUESTION 425
- (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 429
- (Exam Topic 13)
Which of the following is the MOST important security goal when performing application interface testing?

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

Answer: B

NEW QUESTION 431
- (Exam Topic 13)
Why is planning in Disaster Recovery (DR) an interactive process?

A. It details off-site storage plans
B. It identifies omissions in the plan
C. It defines the objectives of the plan
D. It forms part of the awareness process

Answer: B

NEW QUESTION 435
- (Exam Topic 13)
What is the MAIN goal of information security awareness and training?

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

Answer: B

NEW QUESTION 437

- (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 440
- (Exam Topic 13)
A company seizes a mobile device suspected of being used in committing fraud. What would be the BEST method used by a forensic examiner to isolate the powered-on device from the network and preserve the evidence?

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

Answer: A

NEW QUESTION 443
- (Exam Topic 13)
Which of the following are important criteria when designing procedures and acceptance criteria for acquired software?

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

Answer: A

NEW QUESTION 444
- (Exam Topic 13)
Even though a particular digital watermark is difficult to detect, which of the following represents a way it might still be inadvertently removed?

A. Truncating parts of the data
B. Applying Access Control Lists (ACL) to the data
C. Appending non-watermarked data to watermarked data
D. Storing the data in a database

Answer: A

NEW QUESTION 446
- (Exam Topic 13)
Unused space in a disk cluster is important in media analysis because it may contain which of the following?

A. Residual data that has not been overwritten
B. Hidden viruses and Trojan horses
C. Information about the File Allocation table (FAT)
D. Information about patches and upgrades to the system

Answer: A

NEW QUESTION 451
- (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 456
- (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 457
- (Exam Topic 13)
It is MOST important to perform which of the following to minimize potential impact when implementing a new vulnerability scanning tool in a production environment?

A. Negotiate schedule with the Information Technology (IT) operation's team
B. Log vulnerability summary reports to a secured server
C. Enable scanning during off-peak hours
D. Establish access for Information Technology (IT) management

Answer: A

Explanation:
Section: Security Operations

NEW QUESTION 459
- (Exam Topic 13)
Which factors MUST be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?

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

Answer: A

NEW QUESTION 463
- (Exam Topic 13)
Which of the following is the MOST efficient mechanism to account for all staff during a speedy nonemergency evacuation from a large security facility?

A. Large mantrap where groups of individuals leaving are identified using facial recognition technology
B. Radio Frequency Identification (RFID) sensors worn by each employee scanned by sensors at each exitdoor
C. Emergency exits with push bars with coordinates at each exit checking off the individual against a predefined list
D. Card-activated turnstile where individuals are validated upon exit

Answer: B

Explanation:
Section: Security Operations

NEW QUESTION 465
- (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 468
- (Exam Topic 13)
What can happen when an Intrusion Detection System (IDS) is installed inside a firewall-protected internal network?

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

Answer: A

NEW QUESTION 471
- (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 473

- (Exam Topic 13)
The organization would like to deploy an authorization mechanism for an Information Technology (IT) infrastructure project with high employee turnover. Which access control mechanism would be preferred?

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

Answer: D

NEW QUESTION 474
- (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 479
- (Exam Topic 13)
What is the MOST significant benefit of an application upgrade that replaces randomly generated session keys with certificate based encryption for communications with backend servers?

A. Non-repudiation
B. Efficiency
C. Confidentially
D. Privacy

Answer: A

NEW QUESTION 480
- (Exam Topic 13)
Which type of test would an organization perform in order to locate and target exploitable defects?

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

Answer: A

NEW QUESTION 484
- (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 488
- (Exam Topic 13)
What is the second step in the identity and access provisioning lifecycle?

A. Provisioning
B. Review
C. Approval
D. Revocation

Answer: B

NEW QUESTION 492
- (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 495
- (Exam Topic 13)
When developing a business case for updating a security program, the security program owner MUST do which of the following?

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

Answer: A

NEW QUESTION 497
- (Exam Topic 13)
When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

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

Answer: D

NEW QUESTION 502
- (Exam Topic 13)
A security professional determines that a number of outsourcing contracts inherited from a previous merger do not adhere to the current security requirements. Which of the following BEST minimizes the risk of this happening again?

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

Answer: D

NEW QUESTION 507
- (Exam Topic 13)
A minimal implementation of endpoint security includes which of the following?

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

Answer: A

NEW QUESTION 511
- (Exam Topic 13)
An organization has discovered that users are visiting unauthorized websites using anonymous proxies. Which of the following is the BEST way to prevent future occurrences?

A. Remove the anonymity from the proxy
B. Analyze Internet Protocol (IP) traffic for proxy requests
C. Disable the proxy server on the firewall
D. Block the Internet Protocol (IP) address of known anonymous proxies

Answer: C

NEW QUESTION 515
- (Exam Topic 13)
A Security Operations Center (SOC) receives an incident response notification on a server with an active intruder who has planted a backdoor. Initial notifications are sent and communications are established. What MUST be considered or evaluated before performing the next step?

A. Notifying law enforcement is crucial before hashing the contents of the server hard drive
B. Identifying who executed the incident is more important than how the incident happened
C. Removing the server from the network may prevent catching the intruder
D. Copying the contents of the hard drive to another storage device may damage the evidence

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 516
- (Exam Topic 13)
In Disaster Recovery (DR) and Business Continuity (DC) training, which BEST describes a functional drill?

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

Answer: D

NEW QUESTION 517
- (Exam Topic 13)
Which of the following is BEST achieved through the use of eXtensible Access Markup Language (XACML)?

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

Answer: D

NEW QUESTION 522
- (Exam Topic 13)
Which of the following provides the MOST comprehensive filtering of Peer-to-Peer (P2P) traffic?

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

Answer: A

NEW QUESTION 525
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISSP Practice Exam Features:

* CISSP Questions and Answers Updated Frequently

* CISSP Practice Questions Verified by Expert Senior Certified Staff

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

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