

CISSP Dumps

Certified Information Systems Security Professional (CISSP)

<https://www.certleader.com/CISSP-dumps.html>



NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 2

- (Exam Topic 1)

Which of the following actions will reduce risk to a laptop before traveling to a high risk area?

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

Answer: D

NEW QUESTION 3

- (Exam Topic 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)

Which one of the following affects the classification of data?

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

Answer: D

NEW QUESTION 5

- (Exam Topic 2)

Which of the following is an initial consideration when developing an information security management system?

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

Answer: B

NEW QUESTION 6

- (Exam Topic 2)

Which of the following is MOST important when assigning ownership of an asset to a department?

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

Answer: B

NEW QUESTION 7

- (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 8

- (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 9

- (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 10

- (Exam Topic 3)

Which component of the Security Content Automation Protocol (SCAP) specification contains the data required to estimate the severity of vulnerabilities identified automated vulnerability assessments?

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

Answer: B

NEW QUESTION 10

- (Exam Topic 3)

Which technique can be used to make an encryption scheme more resistant to a known plaintext attack?

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

Answer: A

NEW QUESTION 15

- (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 16

- (Exam Topic 4)

Which of the following operates at the Network Layer of the Open System Interconnection (OSI) model?

- A. Packet filtering
- B. Port services filtering
- C. Content filtering
- D. Application access control

Answer: A

NEW QUESTION 20

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 21

- (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 23

- (Exam Topic 5)

What is the BEST approach for controlling access to highly sensitive information when employees have the same level of security clearance?

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

Answer: B

NEW QUESTION 27

- (Exam Topic 6)

Which of the following is of GREATEST assistance to auditors when reviewing system configurations?

- A. Change management processes
- B. User administration procedures
- C. Operating System (OS) baselines
- D. System backup documentation

Answer: A

NEW QUESTION 31

- (Exam Topic 7)

What would be the MOST cost effective solution for a Disaster Recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours?

- A. Warm site
- B. Hot site
- C. Mirror site
- D. Cold site

Answer: A

NEW QUESTION 34

- (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 39

- (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 43

- (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 48

- (Exam Topic 8)

When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?

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

Answer: C

NEW QUESTION 52

- (Exam Topic 8)

Which of the following is the BEST method to prevent malware from being introduced into a production environment?

- A. Purchase software from a limited list of retailers
- B. Verify the hash key or certificate key of all updates
- C. Do not permit programs, patches, or updates from the Internet
- D. Test all new software in a segregated environment

Answer: D

NEW QUESTION 54

- (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 58

- (Exam Topic 9)

What is the FIRST step in developing a security test and its evaluation?

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

Answer: C

NEW QUESTION 61

- (Exam Topic 9)

Which of the following is a method used to prevent Structured Query Language (SQL) injection attacks?

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

Answer: D

NEW QUESTION 64

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 67

- (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 69

- (Exam Topic 9)

To prevent inadvertent disclosure of restricted information, which of the following would be the LEAST effective process for eliminating data prior to the media being discarded?

- A. Multiple-pass overwriting
- B. Degaussing
- C. High-level formatting
- D. Physical destruction

Answer: C

NEW QUESTION 72

- (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 74

- (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 79

- (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 83

- (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 86

- (Exam Topic 9)

What is the term commonly used to refer to a technique of authenticating one machine to another by forging packets from a trusted source?

- A. Man-in-the-Middle (MITM) attack

- B. Smurfing
- C. Session redirect
- D. Spoofing

Answer: D

NEW QUESTION 88

- (Exam Topic 9)

Checking routing information on e-mail to determine it is in a valid format and contains valid information is an example of which of the following anti-spam approaches?

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

Answer: D

NEW QUESTION 89

- (Exam Topic 9)

The overall goal of a penetration test is to determine a system's

- A. ability to withstand an attack.
- B. capacity management.
- C. error recovery capabilities.
- D. reliability under stress.

Answer: A

NEW QUESTION 91

- (Exam Topic 9)

The stringency of an Information Technology (IT) security assessment will be determined by the

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

Answer: C

NEW QUESTION 92

- (Exam Topic 9)

Including a Trusted Platform Module (TPM) in the design of a computer system is an example of a technique to what?

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

Answer: D

NEW QUESTION 96

- (Exam Topic 9)

An advantage of link encryption in a communications network is that it

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

Answer: D

NEW QUESTION 101

- (Exam Topic 9)

Which of the following is an attacker MOST likely to target to gain privileged access to a system?

- A. Programs that write to system resources
- B. Programs that write to user directories
- C. Log files containing sensitive information
- D. Log files containing system calls

Answer: A

NEW QUESTION 104

- (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 107

- (Exam Topic 9)

Which of the following is the best practice for testing a Business Continuity Plan (BCP)?

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

Answer: B

NEW QUESTION 108

- (Exam Topic 9)

What security management control is MOST often broken by collusion?

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

Answer: B

NEW QUESTION 111

- (Exam Topic 9)

Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

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

Answer: C

NEW QUESTION 114

- (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 119

- (Exam Topic 9)

Which of the following does the Encapsulating Security Payload (ESP) provide?

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

Answer: C

NEW QUESTION 120

- (Exam Topic 9)

Which one of the following is the MOST important in designing a biometric access system if it is essential that no one other than authorized individuals are admitted?

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

Answer: A

NEW QUESTION 124

- (Exam Topic 9)

Which one of the following security mechanisms provides the BEST way to restrict the execution of privileged procedures?

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

Answer: A

NEW QUESTION 127

- (Exam Topic 9)

Which of the following statements is TRUE for point-to-point microwave transmissions?

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

Answer: D

NEW QUESTION 130

- (Exam Topic 9)

Which of the following is the BEST way to verify the integrity of a software patch?

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

Answer: A

NEW QUESTION 134

- (Exam Topic 9)

The FIRST step in building a firewall is to

- A. assign the roles and responsibilities of the firewall administrators.
- B. define the intended audience who will read the firewall policy.
- C. identify mechanisms to encourage compliance with the policy.
- D. perform a risk analysis to identify issues to be addressed.

Answer: D

NEW QUESTION 137

- (Exam Topic 9)

Which one of the following describes granularity?

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

Answer: D

NEW QUESTION 139

- (Exam Topic 9)

Which of the following is the 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 140

- (Exam Topic 9)

Which of the following is the MAIN reason that system re-certification and re-accreditation are needed?

- A. To assist data owners in making future sensitivity and criticality determinations
- B. To assure the software development team that all security issues have been addressed
- C. To verify that security protection remains acceptable to the organizational security policy
- D. To help the security team accept or reject new systems for implementation and production

Answer: C

NEW QUESTION 145

- (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 146

- (Exam Topic 9)

Which one of the following effectively obscures network addresses from external exposure when implemented on a firewall or router?

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

Answer: A

NEW QUESTION 149

- (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 153

- (Exam Topic 9)

What is an effective practice when returning electronic storage media to third parties for repair?

- A. Ensuring the media is not labeled in any way that indicates the organization's name.
- B. Disassembling the media and removing parts that may contain sensitive data.
- C. Physically breaking parts of the media that may contain sensitive data.
- D. Establishing a contract with the third party regarding the secure handling of the media.

Answer: D

NEW QUESTION 155

- (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 159

- (Exam Topic 9)

Alternate encoding such as hexadecimal representations is MOST often observed in which of the following forms of attack?

- A. Smurf
- B. Rootkit exploit
- C. Denial of Service (DoS)
- D. Cross site scripting (XSS)

Answer: D

NEW QUESTION 164

- (Exam Topic 9)

Which of the following elements MUST a compliant EU-US Safe Harbor Privacy Policy contain?

- A. An Explanation: of how long the data subject's collected information will be retained for and how it will be eventually disposed.
- B. An Explanation: of who can be contacted at the organization collecting the information if corrections are required by the data subject.
- C. An Explanation: of the regulatory frameworks and compliance standards the information collecting organization adheres to.
- D. An Explanation: of all the technologies employed by the collecting organization in gathering information on the data subject.

Answer: B

NEW QUESTION 166

- (Exam Topic 9)

Which of the following is a network intrusion detection technique?

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

Answer: A

NEW QUESTION 168

- (Exam Topic 9)

Following the completion of a network security assessment, which of the following can BEST be demonstrated?

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

Answer: A

NEW QUESTION 172

- (Exam Topic 9)

In a data classification scheme, the data is owned by the

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

Answer: B

NEW QUESTION 176

- (Exam Topic 9)

When implementing controls in a heterogeneous end-point network for an organization, it is critical that

- A. hosts are able to establish network communications.
- B. users can make modifications to their security software configurations.
- C. common software security components be implemented across all hosts.
- D. firewalls running on each host are fully customizable by the user.

Answer: C

NEW QUESTION 177

- (Exam Topic 9)

Which of the following defines the key exchange for Internet Protocol Security (IPSec)?

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

Answer: B

NEW QUESTION 182

- (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 184

- (Exam Topic 9)

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

- A. Create a user profile.
- B. Create a user access matrix.

- C. Develop an Access Control List (ACL).
- D. Develop a Role Based Access Control (RBAC) list.

Answer: B

NEW QUESTION 185

- (Exam Topic 9)

Which of the following actions should be performed when implementing a change to a database schema in a production system?

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

Answer: D

NEW QUESTION 187

- (Exam Topic 9)

Which of the following is an effective method for avoiding magnetic media data remanence?

- A. Degaussing
- B. Encryption
- C. Data Loss Prevention (DLP)
- D. Authentication

Answer: A

NEW QUESTION 188

- (Exam Topic 9)

What is the MOST important purpose of testing the Disaster Recovery Plan (DRP)?

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

Answer: C

NEW QUESTION 189

- (Exam Topic 9)

Which of the following is a potential risk when a program runs in privileged mode?

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

Answer: D

NEW QUESTION 192

- (Exam Topic 9)

What is the MOST effective countermeasure to a malicious code attack against a mobile system?

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

Answer: A

NEW QUESTION 197

- (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 199

- (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 203

- (Exam Topic 9)

Which of the following does Temporal Key Integrity Protocol (TKIP) support?

- A. Multicast and broadcast messages
- B. Coordination of IEEE 802.11 protocols
- C. Wired Equivalent Privacy (WEP) systems
- D. Synchronization of multiple devices

Answer: C

NEW QUESTION 205

- (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 210

- (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 215

- (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 218

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 223

- (Exam Topic 9)

What should be the INITIAL response to Intrusion Detection System/Intrusion Prevention System (IDS/IPS) alerts?

- A. Ensure that the Incident Response Plan is available and current.
- B. Determine the traffic's initial source and block the appropriate port.
- C. Disable or disconnect suspected target and source systems.
- D. Verify the threat and determine the scope of the attack.

Answer: D

NEW QUESTION 227

- (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 230

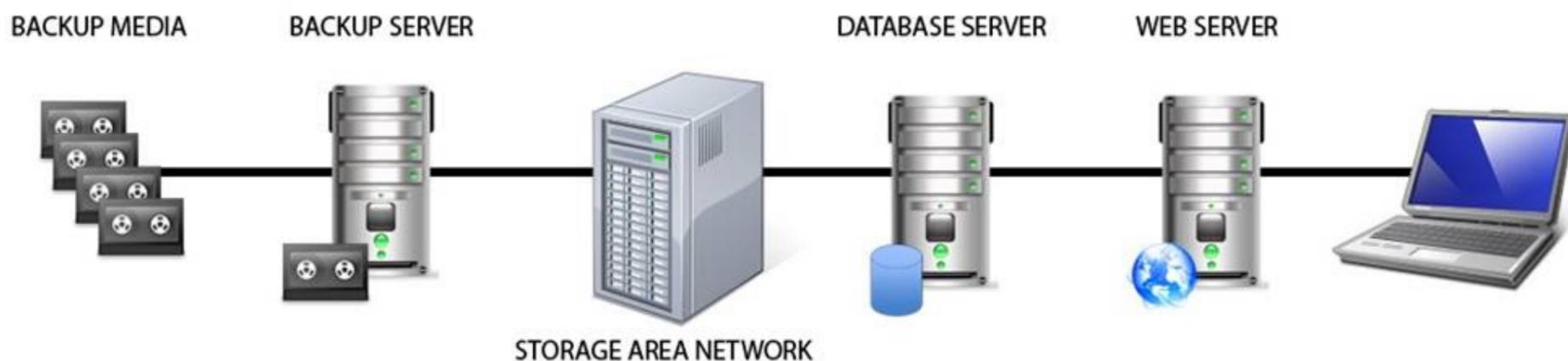
- (Exam Topic 10)
Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?

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

Answer: A

NEW QUESTION 233

- (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 236

- (Exam Topic 10)
Which of the following describes the concept of a Single Sign-On (SSO) system?

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

Answer: C

NEW QUESTION 239

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

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

Answer: C

NEW QUESTION 242

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

- A. Retina scan and a palm print

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

Answer: B

NEW QUESTION 247

- (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 251

- (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 254

- (Exam Topic 10)

Which of the following MOST influences the design of the organization's electronic monitoring policies?

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

Answer: A

NEW QUESTION 256

- (Exam Topic 10)

According to best practice, which of the following groups is the MOST effective in performing an information security compliance audit?

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

Answer: D

NEW QUESTION 260

- (Exam Topic 10)

During an investigation of database theft from an organization's web site, it was determined that the Structured Query Language (SQL) injection technique was used despite input validation with client-side scripting. Which of the following provides the GREATEST protection against the same attack occurring again?

- A. Encrypt communications between the servers
- B. Encrypt the web server traffic
- C. Implement server-side filtering
- D. Filter outgoing traffic at the perimeter firewall

Answer: C

NEW QUESTION 265

- (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 270

- (Exam Topic 10)

Refer to the information below to answer the question.

A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns. In addition to web browsers, what PRIMARY areas need to be addressed concerning mobile code used for malicious purposes?

- A. Text editors, database, and Internet phone applications
- B. Email, presentation, and database applications
- C. Image libraries, presentation and spreadsheet applications
- D. Email, media players, and instant messaging applications

Answer: D

NEW QUESTION 275

- (Exam Topic 10)

According to best practice, which of the following is required when implementing third party software in a production environment?

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

Answer: A

NEW QUESTION 278

- (Exam Topic 10)

Which item below is a federated identity standard?

- A. 802.11i
- B. Kerberos
- C. Lightweight Directory Access Protocol (LDAP)
- D. Security Assertion Markup Language (SAML)

Answer: D

NEW QUESTION 280

- (Exam Topic 10)

Which of the following assures that rules are followed in an identity management architecture?

- A. Policy database
- B. Digital signature
- C. Policy decision point
- D. Policy enforcement point

Answer: D

NEW QUESTION 285

- (Exam Topic 10)

Which of the following is the MOST difficult to enforce when using cloud computing?

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

Answer: D

NEW QUESTION 289

- (Exam Topic 10)

Refer to the information below to answer the question.

A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns. What MUST the plan include in order to reduce client-side exploitation?

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

Answer: D

NEW QUESTION 294

- (Exam Topic 10)

What is the MOST effective method for gaining unauthorized access to a file protected with a long complex password?

- A. Brute force attack
- B. Frequency analysis

- C. Social engineering
- D. Dictionary attack

Answer: C

NEW QUESTION 298

- (Exam Topic 10)

Which of the following are required components for implementing software configuration management systems?

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

Answer: C

NEW QUESTION 301

- (Exam Topic 10)

Which of the following BEST mitigates a replay attack against a system using identity federation and Security Assertion Markup Language (SAML) implementation?

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

Answer: C

NEW QUESTION 302

- (Exam Topic 10)

Given the various means to protect physical and logical assets, match the access management area to the technology.

Area		Technolog
Facilities		Encryption
Devices		Window
Information		Firewall
Systems		Authenticatid

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Area		Technolog
Facilities	Information	Encryption
Devices	Facilities	Window
Information	Devices	Firewall
Systems	Systems	Authenticatid

NEW QUESTION 307

- (Exam Topic 10)

What is the PRIMARY advantage of using automated application security testing tools?

- A. The application can be protected in the production environment.
- B. Large amounts of code can be tested using fewer resources.
- C. The application will fail less when tested using these tools.
- D. Detailed testing of code functions can be performed.

Answer: B

NEW QUESTION 309

- (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 310

- (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 311

- (Exam Topic 10)

Refer to the information below to answer the question.

During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.

If the intrusion causes the system processes to hang, which of the following has been affected?

- A. System integrity
- B. System availability
- C. System confidentiality
- D. System auditability

Answer: B

NEW QUESTION 315

- (Exam Topic 10)

Which of the following is a MAJOR consideration in implementing a Voice over IP (VoIP) network?

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

Answer: B

NEW QUESTION 319

- (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 322

- (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 324

- (Exam Topic 10)

During the procurement of a new information system, it was determined that some of the security requirements were not addressed in the system specification. Which of the following is the MOST likely reason for this?

- A. The procurement officer lacks technical knowledge.
- B. The security requirements have changed during the procurement process.

- C. There were no security professionals in the vendor's bidding team.
- D. The description of the security requirements was insufficient.

Answer: D

NEW QUESTION 326

- (Exam Topic 10)

When implementing a secure wireless network, which of the following supports authentication and authorization for individual client endpoints?

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

Answer: C

NEW QUESTION 330

- (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 334

- (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 338

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.

Which of the following is considered the **MOST** important priority for the information security officer?

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

Answer: A

NEW QUESTION 339

- (Exam Topic 10)

Which of the following **BEST** describes Recovery Time Objective (RTO)?

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

Answer: C

NEW QUESTION 342

- (Exam Topic 10)

What is the **BEST** method to detect the most common improper initialization problems in programming languages?

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

Answer: B

NEW QUESTION 346

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.

Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?

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

Answer: A

NEW QUESTION 347

- (Exam Topic 10)

Refer to the information below to answer the question.

A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.

Which of the following methods is the MOST effective way of removing the Peer-to-Peer (P2P) program from the computer?

- A. Run software uninstall
- B. Re-image the computer
- C. Find and remove all installation files
- D. Delete all cookies stored in the web browser cache

Answer: B

NEW QUESTION 351

- (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 352

- (Exam Topic 10)

Which of the following is the MAIN goal of a data retention policy?

- A. Ensure that data is destroyed properly.
- B. Ensure that data recovery can be done on the data.
- C. Ensure the integrity and availability of data for a predetermined amount of time.
- D. Ensure the integrity and confidentiality of data for a predetermined amount of time.

Answer: C

NEW QUESTION 353

- (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 356

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.

The security program can be considered effective when

- A. vulnerabilities are proactively identified.
- B. audits are regularly performed and reviewed.
- C. backups are regularly performed and validated.
- D. risk is lowered to an acceptable level.

Answer: D

NEW QUESTION 361

- (Exam Topic 10)

For a service provider, which of the following MOST effectively addresses confidentiality concerns for customers using cloud computing?

- A. Hash functions
- B. Data segregation
- C. File system permissions
- D. Non-repudiation controls

Answer: B

NEW QUESTION 362

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 365

- (Exam Topic 10)

Which of the following is the BEST way to determine if a particular system is able to identify malicious software without executing it?

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

Answer: B

NEW QUESTION 367

- (Exam Topic 10)

A risk assessment report recommends upgrading all perimeter firewalls to mitigate a particular finding. Which of the following BEST supports this recommendation?

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

Answer: C

NEW QUESTION 372

- (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 376

- (Exam Topic 10)

During an audit, the auditor finds evidence of potentially illegal activity. Which of the following is the MOST appropriate action to take?

- A. Immediately call the police
- B. Work with the client to resolve the issue internally
- C. Advise the person performing the illegal activity to cease and desist
- D. Work with the client to report the activity to the appropriate authority

Answer: D

NEW QUESTION 377

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

D. The quantity of data that must be provided to the third party and how it is to be used

Answer: C

NEW QUESTION 380

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement. The effectiveness of the security program can PRIMARILY be measured through

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

Answer: A

NEW QUESTION 385

- (Exam Topic 10)

When using third-party software developers, which of the following is the MOST effective method of providing software development Quality Assurance (QA)?

- A. Retain intellectual property rights through contractual wording.
- B. Perform overlapping code reviews by both parties.
- C. Verify that the contractors attend development planning meetings.
- D. Create a separate contractor development environment.

Answer: B

NEW QUESTION 386

- (Exam Topic 10)

Refer to the information below to answer the question.

Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed. Organizational policy requires the deletion of user data from Personal Digital Assistant (PDA) devices before disposal. It may not be possible to delete the user data if the device is malfunctioning. Which destruction method below provides the BEST assurance that the data has been removed?

- A. Knurling
- B. Grinding
- C. Shredding
- D. Degaussing

Answer: C

NEW QUESTION 390

- (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 391

- (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 394

- (Exam Topic 11)

The application of which of the following standards would BEST reduce the potential for data breaches?

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

Answer: D

NEW QUESTION 395

- (Exam Topic 11)

Which of the following BEST describes a Protection Profile (PP)?

- A. A document that expresses an implementation independent set of security requirements for an IT product that meets specific consumer needs.
- B. A document that is used to develop an IT security product from its security requirements definition.
- C. A document that expresses an implementation dependent set of security requirements which contains only the security functional requirements.
- D. A document that represents evaluated products where there is a one-to-one correspondence between a PP and a Security Target (ST).

Answer: A

NEW QUESTION 399

- (Exam Topic 11)

Changes to a Trusted Computing Base (TCB) system that could impact the security posture of that system and trigger a recertification activity are documented in the

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

Answer: A

NEW QUESTION 401

- (Exam Topic 11)

Order the below steps to create an effective vulnerability management process.

<u>Step</u>		<u>Order</u>
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:

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

NEW QUESTION 406

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 408

- (Exam Topic 11)

Which of the following has the GREATEST impact on an organization's security posture?

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

Answer: A

NEW QUESTION 412

- (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 414

- (Exam Topic 11)

How does an organization verify that an information system's current hardware and software match the standard system configuration?

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

Answer: C

NEW QUESTION 418

- (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 419

- (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 423

- (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 428

- (Exam Topic 11)

Which of the following analyses is performed to protect information assets?

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

Answer: A

NEW QUESTION 433

- (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 434

- (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 435

- (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 440

- (Exam Topic 11)

Discretionary Access Control (DAC) restricts access according to

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

Answer: C

NEW QUESTION 445

- (Exam Topic 11)

What is the MOST efficient way to secure a production program and its data?

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

Answer: B

NEW QUESTION 449

- (Exam Topic 11)

An organization lacks a data retention policy. Of the following, who is the BEST person to consult for such requirement?

- A. Application Manager
- B. Database Administrator

- C. Privacy Officer
- D. Finance Manager

Answer: C

NEW QUESTION 452

- (Exam Topic 11)

Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

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

Answer: B

NEW QUESTION 457

- (Exam Topic 11)

When planning a penetration test, the tester will be MOST interested in which information?

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

Answer: B

NEW QUESTION 458

- (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 460

- (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 461

- (Exam Topic 11)

After acquiring the latest security updates, what must be done before deploying to production systems?

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

Answer: B

NEW QUESTION 466

- (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 470

- (Exam Topic 11)

Which of the following is the BEST example of weak management commitment to the protection of security assets and resources?

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

Answer: A

NEW QUESTION 473

- (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 475

- (Exam Topic 11)

What type of encryption is used to protect sensitive data in transit over a network?

- A. Payload encryption and transport encryption
- B. Authentication Headers (AH)
- C. Keyed-Hashing for Message Authentication
- D. Point-to-Point Encryption (P2PE)

Answer: A

NEW QUESTION 478

- (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 480

- (Exam Topic 11)

Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).

Secure Architecture

Do you advertise shared security services with guidance for project teams?

Education & Guidance

Are most people tested to ensure a baseline skill- set for secure development practices?

Strategy & Metrics

Does most of the organization know about what's required based on risk ratings?

Vulnerability Management

Are most project teams aware of their security point(s) of contact and response team(s)?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Secure Architecture

Secure Architecture

Do you advertise shared security services with guidance for project teams?

Education & Guidance

Education & Guidance

Are most people tested to ensure a baseline skill- set for secure development practices?

Strategy & Metrics

Strategy & Metrics

Does most of the organization know about what's required based on risk ratings?

Vulnerability Management

Vulnerability Management

Are most project teams aware of their security point(s) of contact and response team(s)?

NEW QUESTION 481

- (Exam Topic 11)

A security professional is asked to provide a solution that restricts a bank teller to only perform a savings deposit transaction but allows a supervisor to perform corrections after the transaction. Which of the following is the MOST effective solution?

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

Answer: C

NEW QUESTION 483

- (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 485

- (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 486

- (Exam Topic 11)

Drag the following Security Engineering terms on the left to the BEST definition on the right.

Security Engineering

Definition

Security Risk Treatment



The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**

Threat Assessment



A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**

Protection Needs



The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**

Risk



The method used to identify feasible security **risk mitigation options and plans.**

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Security Engineering

Definition

Security Risk Treatment

Protection Needs

The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.

Threat Assessment

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

Protection Needs

Threat Assessment

The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.

Risk

Security Risk Treatment

The method used to identify feasible security risk mitigation options and plans.

NEW QUESTION 488

- (Exam Topic 11)

Which of the following is an advantage of on-premise Credential Management Systems?

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

Answer: B

NEW QUESTION 492

- (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 494

- (Exam Topic 11)

Which of the following statements is TRUE regarding value boundary analysis as a functional software testing technique?

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

Answer: C

NEW QUESTION 499

- (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 504

- (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 509

- (Exam Topic 11)

Which one of the following is a common risk with network configuration management?

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

Answer: D

NEW QUESTION 510

- (Exam Topic 11)

What security risk does the role-based access approach mitigate MOST effectively?

- A. Excessive access rights to systems and data
- B. Segregation of duties conflicts within business applications
- C. Lack of system administrator activity monitoring
- D. Inappropriate access requests

Answer: A

NEW QUESTION 513

- (Exam Topic 11)

What is the PRIMARY goal for using Domain Name System Security Extensions (DNSSEC) to sign records?

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

Answer: A

NEW QUESTION 514

- (Exam Topic 11)

Which of the following BEST avoids data remanence disclosure for cloud hosted resources?

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

Answer: A

NEW QUESTION 515

- (Exam Topic 11)

What is the GREATEST challenge of an agent-based patch management solution?

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

Answer: B

NEW QUESTION 517

- (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 518

- (Exam Topic 11)

Which of the following is a recommended alternative to an integrated email encryption system?

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

Answer: C

NEW QUESTION 522

- (Exam Topic 11)

Which of the following protocols would allow an organization to maintain a centralized list of users that can read a protected webpage?

- A. Lightweight Directory Access Control (LDAP)
- B. Security Assertion Markup Language (SAML)
- C. Hypertext Transfer Protocol (HTTP)
- D. Kerberos

Answer: A

NEW QUESTION 524

- (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 527

- (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 532

- (Exam Topic 11)

While inventorying storage equipment, it is found that there are unlabeled, disconnected, and powered off devices. Which of the following is the correct procedure for handling such equipment?

- A. They should be recycled to save energy.
- B. They should be recycled according to NIST SP 800-88.
- C. They should be inspected and sanitized following the organizational policy.
- D. They should be inspected and categorized properly to sell them for reuse.

Answer:

C

NEW QUESTION 533

- (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 536

- (Exam Topic 11)

Are companies legally required to report all data breaches?

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

Answer: A

NEW QUESTION 539

- (Exam Topic 11)

The 802.1x standard provides a framework for what?

- A. Network authentication for only wireless networks
- B. Network authentication for wired and wireless networks
- C. Wireless encryption using the Advanced Encryption Standard (AES)
- D. Wireless network encryption using Secure Sockets Layer (SSL)

Answer: B

NEW QUESTION 543

- (Exam Topic 11)

In order for a security policy to be effective within an organization, it MUST include

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

Answer: D

NEW QUESTION 546

- (Exam Topic 11)

The MAIN reason an organization conducts a security authorization process is to

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

Answer: A

NEW QUESTION 548

- (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 553

- (Exam Topic 12)

A proxy firewall operates at what layer of the Open System Interconnection (OSI) model?

- A. Transport
- B. Data link
- C. Network
- D. Application

Answer: D

NEW QUESTION 555

- (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.

<u>Access Control Model</u>	<u>Restrictions</u>
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 556

- (Exam Topic 12)

A vulnerability in which of the following components would be MOST difficult to detect?

- A. Kernel
- B. Shared libraries
- C. Hardware
- D. System application

Answer: A

NEW QUESTION 560

- (Exam Topic 12)

Which of the following information MUST be provided for user account provisioning?

- A. Full name
- B. Unique identifier
- C. Security question
- D. Date of birth

Answer: B

NEW QUESTION 563

- (Exam Topic 12)

The restoration priorities of a Disaster Recovery Plan (DRP) are based on which of the following documents?

- A. Service Level Agreement (SLA)
- B. Business Continuity Plan (BCP)
- C. Business Impact Analysis (BIA)
- D. Crisis management plan

Answer: B

NEW QUESTION 565

- (Exam Topic 12)

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

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

D. Ping flood attack

Answer: A

NEW QUESTION 567

- (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 572

- (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 573

- (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 577

- (Exam Topic 12)

How should an organization determine the priority of its remediation efforts after a vulnerability assessment has been conducted?

- A. Use an impact-based approach.
- B. Use a risk-based approach.
- C. Use a criticality-based approach.
- D. Use a threat-based approach.

Answer: B

NEW QUESTION 579

- (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 580

- (Exam Topic 12)

Which of the following is the MAIN reason for using configuration management?

- A. To provide centralized administration
- B. To reduce the number of changes
- C. To reduce errors during upgrades
- D. To provide consistency in security controls

Answer: D

NEW QUESTION 584

- (Exam Topic 12)

The PRIMARY outcome of a certification process is that it provides documented

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

Answer: D

NEW QUESTION 586

- (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 591

- (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 593

- (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 596

- (Exam Topic 12)

Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

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

Answer: B

NEW QUESTION 597

- (Exam Topic 12)

What does the Maximum Tolerable Downtime (MTD) determine?

- A. The estimated period of time a business critical database can remain down before customers are affected.
- B. The fixed length of time a company can endure a disaster without any Disaster Recovery (DR) planning
- C. The estimated period of time a business can remain interrupted beyond which it risks never recovering
- D. The fixed length of time in a DR process before redundant systems are engaged

Answer: C

NEW QUESTION 602

- (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 605

- (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.

<u>Access Control Type</u>		<u>Example</u>
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 (RFID) badge

NEW QUESTION 606

- (Exam Topic 12)

Which of the following BEST describes a chosen plaintext attack?

- A. The cryptanalyst can generate ciphertext from arbitrary text.
- B. The cryptanalyst examines the communication being sent back and forth.
- C. The cryptanalyst can choose the key and algorithm to mount the attack.
- D. The cryptanalyst is presented with the ciphertext from which the original message is determined.

Answer: A

NEW QUESTION 611

- (Exam Topic 12)

What operations role is responsible for protecting the enterprise from corrupt or contaminated media?

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

Answer: B

NEW QUESTION 614

- (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 618

- (Exam Topic 12)

Determining outage costs caused by a disaster can BEST be measured by the

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

Answer: C

NEW QUESTION 619

- (Exam Topic 12)

A company was ranked as high in the following National Institute of Standards and Technology (NIST) functions: Protect, Detect, Respond and Recover. However, a low maturity grade was attributed to the Identify function. In which of the following the controls categories does this company need to improve when analyzing its processes individually?

- A. Asset Management, Business Environment, Governance and Risk Assessment
- B. Access Control, Awareness and Training, Data Security and Maintenance
- C. Anomalies and Events, Security Continuous Monitoring and Detection Processes
- D. Recovery Planning, Improvements and Communications

Answer: A

NEW QUESTION 620

- (Exam Topic 12)

What is the BEST way to encrypt web application communications?

- A. Secure Hash Algorithm 1 (SHA-1)
- B. Secure Sockets Layer (SSL)
- C. Cipher Block Chaining Message Authentication Code (CBC-MAC)
- D. Transport Layer Security (TLS)

Answer: D

NEW QUESTION 624

- (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 625

- (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 626

- (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 630

- (Exam Topic 12)

Which one of the following activities would present a significant security risk to organizations when employing a Virtual Private Network (VPN) solution?

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

Answer: B

NEW QUESTION 631

- (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 634

- (Exam Topic 12)

Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

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

Answer: A

NEW QUESTION 636

- (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 641

- (Exam Topic 12)

An organization regularly conducts its own penetration tests. Which of the following scenarios MUST be covered for the test to be effective?

- A. Third-party vendor with access to the system
- B. System administrator access compromised
- C. Internal attacker with access to the system
- D. Internal user accidentally accessing data

Answer: C

NEW QUESTION 645

- (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 647

- (Exam Topic 12)

An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a PRIMARY security concern?

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

Answer: C

NEW QUESTION 652

- (Exam Topic 12)

When using Generic Routing Encapsulation (GRE) tunneling over Internet Protocol version 4 (IPv4), where is the GRE header inserted?

- A. Into the options field
- B. Between the delivery header and payload
- C. Between the source and destination addresses
- D. Into the destination address

Answer: B

NEW QUESTION 654

- (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 656

- (Exam Topic 12)

The application of a security patch to a product previously validate at Common Criteria (CC) Evaluation Assurance Level (EAL) 4 would

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

Answer: B

NEW QUESTION 658

- (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 661

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 663

- (Exam Topic 12)

For network based evidence, which of the following contains traffic details of all network sessions in order to detect anomalies?

- A. Alert data
- B. User data
- C. Content data
- D. Statistical data

Answer: D

NEW QUESTION 666

- (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 671

- (Exam Topic 12)

Knowing the language in which an encrypted message was originally produced might help a cryptanalyst to perform a

- A. clear-text attack.
- B. known cipher attack.
- C. frequency analysis.
- D. stochastic assessment.

Answer: C

NEW QUESTION 674

- (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 676

- (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 677

- (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 679

- (Exam Topic 12)

What balance MUST be considered when web application developers determine how informative application error messages should be constructed?

- A. Risk versus benefit
- B. Availability versus auditability
- C. Confidentiality versus integrity
- D. Performance versus user satisfaction

Answer: A

NEW QUESTION 683

- (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 685

- (Exam Topic 13)

Which of the following is the BEST reason for writing an information security policy?

- A. To support information security governance
- B. To reduce the number of audit findings
- C. To deter attackers
- D. To implement effective information security controls

Answer: A

NEW QUESTION 688

- (Exam Topic 13)

Which of the following is the MOST effective method to mitigate Cross-Site Scripting (XSS) attacks?

- A. Use Software as a Service (SaaS)
- B. Whitelist input validation
- C. Require client certificates
- D. Validate data output

Answer: B

NEW QUESTION 689

- (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 691

- (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 696

- (Exam Topic 13)

A control to protect from a Denial-of-Service (DoS) attack has been determined to stop 50% of attacks, and additionally reduces the impact of an attack by 50%. What is the residual risk?

- A. 25%
- B. 50%
- C. 75%
- D. 100%

Answer: A

NEW QUESTION 700

- (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 701

- (Exam Topic 13)

Which of the following MUST be in place to recognize a system attack?

- A. Stateful firewall
- B. Distributed antivirus
- C. Log analysis
- D. Passive honeypot

Answer: A

NEW QUESTION 702

- (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 704

- (Exam Topic 13)

What capability would typically be included in a commercially available software package designed for access control?

- A. Password encryption

- B. File encryption
- C. Source library control
- D. File authentication

Answer: A

NEW QUESTION 709

- (Exam Topic 13)

Which of the following is a direct monetary cost of a security incident?

- A. Morale
- B. Reputation
- C. Equipment
- D. Information

Answer: C

NEW QUESTION 712

- (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 715

- (Exam Topic 13)

What is the PRIMARY role of a scrum master in agile development?

- A. To choose the primary development language
- B. To choose the integrated development environment
- C. To match the software requirements to the delivery plan
- D. To project manage the software delivery

Answer: D

NEW QUESTION 717

- (Exam Topic 13)

Which of the following is the MOST common method of memory protection?

- A. Compartmentalization
- B. Segmentation
- C. Error correction
- D. Virtual Local Area Network (VLAN) tagging

Answer: B

NEW QUESTION 720

- (Exam Topic 13)

Which security access policy contains fixed security attributes that are used by the system to determine a user's access to a file or object?

- A. Mandatory Access Control (MAC)
- B. Access Control List (ACL)
- C. Discretionary Access Control (DAC)
- D. Authorized user control

Answer: A

NEW QUESTION 722

- (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 723

- (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 727

- (Exam Topic 13)

Which of the following combinations would MOST negatively affect availability?

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

Answer: A

NEW QUESTION 731

- (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 735

- (Exam Topic 13)

The design review for an application has been completed and is ready for release. What technique should an organization use to assure application integrity?

- A. Application authentication
- B. Input validation
- C. Digital signing
- D. Device encryption

Answer: C

NEW QUESTION 736

- (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 741

- (Exam Topic 13)

Which of the following mechanisms will BEST prevent a Cross-Site Request Forgery (CSRF) attack?

- A. parameterized database queries
- B. whitelist input values
- C. synchronized session tokens
- D. use strong ciphers

Answer: C

NEW QUESTION 746

- (Exam Topic 13)

Which security modes is MOST commonly used in a commercial environment because it protects the integrity of financial and accounting data?

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

Answer:

C

NEW QUESTION 751

- (Exam Topic 13)

What is the process of removing sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique?

- A. Purging
- B. Encryption
- C. Destruction
- D. Clearing

Answer: A

NEW QUESTION 756

- (Exam Topic 13)

Which of the following is a benefit in implementing an enterprise Identity and Access Management (IAM) solution?

- A. Password requirements are simplified.
- B. Risk associated with orphan accounts is reduced.
- C. Segregation of duties is automatically enforced.
- D. Data confidentiality is increased.

Answer: A

NEW QUESTION 761

- (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 764

- (Exam Topic 13)

Which of the following is a characteristic of an internal audit?

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

Answer: D

NEW QUESTION 766

- (Exam Topic 13)

When developing solutions for mobile devices, in which phase of the Software Development Life Cycle (SDLC) should technical limitations related to devices be specified?

- A. Implementation
- B. Initiation
- C. Review
- D. Development

Answer: A

NEW QUESTION 771

- (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 774

- (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 775

- (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 780

- (Exam Topic 13)

Which of the following is a common characteristic of privacy?

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

Answer: A

NEW QUESTION 784

- (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 786

- (Exam Topic 13)

What does electronic vaulting accomplish?

- A. It protects critical files.
- B. It ensures the fault tolerance of Redundant Array of Independent Disks (RAID) systems
- C. It stripes all database records
- D. It automates the Disaster Recovery Process (DRP)

Answer: A

Explanation:

Section: Security Operations

NEW QUESTION 787

- (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.

<u>Access Control Model</u>	<u>Restrictions</u>
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:

<u>Access Control Model</u>		<u>Restrictions</u>
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 789

- (Exam Topic 13)

Proven application security principles include which of the following?

- A. Minimizing attack surface area
- B. Hardening the network perimeter
- C. Accepting infrastructure security controls
- D. Developing independent modules

Answer: A

NEW QUESTION 793

- (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 794

- (Exam Topic 13)

The core component of Role Based Access Control (RBAC) must be constructed of defined data elements. Which elements are required?

- A. Users, permissions, operations, and protected objects
- B. Roles, accounts, permissions, and protected objects
- C. Users, roles, operations, and protected objects
- D. Roles, operations, accounts, and protected objects

Answer: C

NEW QUESTION 797

- (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 800

- (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: B

NEW QUESTION 805

- (Exam Topic 13)

Assessing a third party's risk by counting bugs in the code may not be the best measure of an attack surface within the supply chain. Which of the following is LEAST associated with the attack surface?

- A. Input protocols
- B. Target processes
- C. Error messages
- D. Access rights

Answer: C

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 809

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

Answer: A

NEW QUESTION 813

- (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 816

- (Exam Topic 13)

Which of the following is MOST appropriate for protecting confidentiality 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 819

- (Exam Topic 13)

What is the expected outcome of security awareness in support of a security awareness program?

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

Answer: C

NEW QUESTION 821

- (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 823

- (Exam Topic 13)

Which of the following MUST be scalable to address security concerns raised by the integration of third-party identity services?

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

Answer: D

NEW QUESTION 828

- (Exam Topic 13)

What MUST each information owner do when a system contains data from multiple information owners?

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

Answer: C

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 832

- (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 837

- (Exam Topic 13)

At a MINIMUM, audits of permissions to individual or group accounts should be scheduled

- A. annually
- B. to correspond with staff promotions
- C. to correspond with terminations
- D. continually

Answer: A

NEW QUESTION 842

- (Exam Topic 13)

Who is accountable for the information within an Information System (IS)?

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

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 845

- (Exam Topic 13)

Digital certificates used in Transport Layer Security (TLS) support which of the following?

- A. Information input validation
- B. Non-repudiation controls and data encryption
- C. Multi-Factor Authentication (MFA)
- D. Server identity and data confidentiality

Answer: D

NEW QUESTION 848

- (Exam Topic 13)

A chemical plant wants to upgrade the Industrial Control System (ICS) to transmit data using Ethernet instead of RS422. The project manager wants to simplify

administration and maintenance by utilizing the office network infrastructure and staff to implement this upgrade. Which of the following is the GREATEST impact on security for the network?

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

Answer: B

NEW QUESTION 852

- (Exam Topic 13)

Which of the following is part of a Trusted Platform Module (TPM)?

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

Answer: A

NEW QUESTION 857

- (Exam Topic 13)

Which of the following is a responsibility of a data steward?

- A. Ensure alignment of the data governance effort to the organization.
- B. Conduct data governance interviews with the organization.
- C. Document data governance requirements.
- D. Ensure that data decisions and impacts are communicated to the organization.

Answer: A

NEW QUESTION 860

- (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 864

- (Exam Topic 13)

Which of the following is the MOST appropriate action when reusing media that contains sensitive data?

- A. Erase
- B. Sanitize
- C. Encrypt
- D. Degauss

Answer: B

NEW QUESTION 866

- (Exam Topic 13)

A user has infected a computer with malware by connecting a Universal Serial Bus (USB) storage device. Which of the following is MOST effective to mitigate future infections?

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

Answer: C

NEW QUESTION 867

- (Exam Topic 13)

Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) only provides which of the following?

- A. Mutual authentication
- B. Server authentication
- C. User authentication
- D. Streaming ciphertext data

Answer: C

NEW QUESTION 872

- (Exam Topic 13)

What is the correct order of steps in an information security assessment?

Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.

<u>Actions</u>		<u>Steps</u>
Define the perimeter.		Step 1
Identify the vulnerability.		Step 2
Assess the risk.		Step 3
Determine the actions.		Step 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<u>Actions</u>		<u>Steps</u>
Define the perimeter.	Identify the vulnerability.	Step 1
Identify the vulnerability.	Define the perimeter.	Step 2
Assess the risk.	Assess the risk.	Step 3
Determine the actions.	Determine the actions.	Step 4

NEW QUESTION 875

- (Exam Topic 13)

In a High Availability (HA) environment, what is the PRIMARY goal of working with a virtual router address as the gateway to a network?

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

Answer: C

NEW QUESTION 877

- (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 880

- (Exam Topic 13)

Attack trees are MOST useful for which of the following?

- A. Determining system security scopes
- B. Generating attack libraries
- C. Enumerating threats
- D. Evaluating Denial of Service (DoS) attacks

Answer: A

NEW QUESTION 883

- (Exam Topic 13)

Which of the following would BEST support effective testing of patch compatibility when patches are applied to an organization's systems?

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

Answer: A

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 887

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISSP Exam with Our Prep Materials Via below:

<https://www.certleader.com/CISSP-dumps.html>