



ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

NEW QUESTION 1

- (Exam Topic 1)

When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined?

- A. Only when assets are clearly defined
- B. Only when standards are defined
- C. Only when controls are put in place
- D. Only procedures are defined

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

All of the following items should be included in a Business Impact Analysis (BIA) questionnaire EXCEPT questions that

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

Answer: B

NEW QUESTION 3

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 4

- (Exam Topic 1)

Intellectual property rights are PRIMARY concerned with which of the following?

- A. Owner's ability to realize financial gain
- B. Owner's ability to maintain copyright
- C. Right of the owner to enjoy their creation
- D. Right of the owner to control delivery method

Answer: D

NEW QUESTION 5

- (Exam Topic 1)

What is the MOST important consideration from a data security perspective when an organization plans to relocate?

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

Answer: C

NEW QUESTION 6

- (Exam Topic 2)

Which 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 7

- (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 8

- (Exam Topic 2)

Which of the following is an effective control in preventing electronic cloning of Radio Frequency Identification (RFID) based access cards?

- A. Personal Identity Verification (PIV)
- B. Cardholder Unique Identifier (CHUID) authentication
- C. Physical Access Control System (PACS) repeated attempt detection
- D. Asymmetric Card Authentication Key (CAK) challenge-response

Answer: C

NEW QUESTION 9

- (Exam Topic 2)

When implementing a data classification program, why is it important to avoid too much granularity?

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

Answer: A

NEW QUESTION 10

- (Exam Topic 2)

Which of the following BEST describes the responsibilities of a data owner?

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

Answer: C

NEW QUESTION 10

- (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 15

- (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 17

- (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 19

- (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 22

- (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 27

- (Exam Topic 4)

Which of the following is used by the Point-to-Point Protocol (PPP) to determine packet formats?

- A. Layer 2 Tunneling Protocol (L2TP)
- B. Link Control Protocol (LCP)
- C. Challenge Handshake Authentication Protocol (CHAP)
- D. Packet Transfer Protocol (PTP)

Answer: B

NEW QUESTION 28

- (Exam Topic 4)

What is the purpose of an Internet Protocol (IP) spoofing attack?

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

Answer: D

NEW QUESTION 30

- (Exam Topic 4)

At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

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

Answer: D

NEW QUESTION 31

- (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 32

- (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 33

- (Exam Topic 6)

Which of the following could cause a Denial of Service (DoS) against an authentication system?

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

Answer: D

NEW QUESTION 37

- (Exam Topic 6)

A Virtual Machine (VM) environment has five guest Operating Systems (OS) and provides strong isolation. What **MUST** an administrator review to audit a user's access to data files?

- A. Host VM monitor audit logs
- B. Guest OS access controls
- C. Host VM access controls
- D. Guest OS audit logs

Answer: A

NEW QUESTION 42

- (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 43

- (Exam Topic 6)

In which of the following programs is it **MOST** important to include the collection of security process data?

- A. Quarterly access reviews
- B. Security continuous monitoring
- C. Business continuity testing
- D. Annual security training

Answer: A

NEW QUESTION 47

- (Exam Topic 7)

Recovery strategies of a Disaster Recovery planning (DRIP) **MUST** be aligned with which of the following?

- A. Hardware and software compatibility issues
- B. Applications' critically and downtime tolerance
- C. Budget constraints and requirements
- D. Cost/benefit analysis and business objectives

Answer: D

NEW QUESTION 49

- (Exam Topic 7)

A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?

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

Answer: D

NEW QUESTION 51

- (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 56

- (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 57

- (Exam Topic 7)

With what frequency should monitoring of a control occur when implementing Information Security Continuous Monitoring (ISCM) solutions?

- A. Continuously without exception for all security controls
- B. Before and after each change of the control
- C. At a rate concurrent with the volatility of the security control
- D. Only during system implementation and decommissioning

Answer: B

NEW QUESTION 61

- (Exam Topic 7)

When is a Business Continuity Plan (BCP) considered to be valid?

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

Answer: D

NEW QUESTION 65

- (Exam Topic 7)

What should be the FIRST action to protect the chain of evidence when a desktop computer is involved?

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

Answer: C

NEW QUESTION 66

- (Exam Topic 8)

Which of the following is a web application control that should be put into place to prevent exploitation of Operating System (OS) bugs?

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

Answer: B

NEW QUESTION 68

- (Exam Topic 8)

What is the BEST approach to addressing security issues in legacy web applications?

- A. Debug the security issues
- B. Migrate to newer, supported applications where possible
- C. Conduct a security assessment
- D. Protect the legacy application with a web application firewall

Answer: D

NEW QUESTION 70

- (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 75

- (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 78

- (Exam Topic 8)

The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle (SDLC)?

- A. System acquisition and development
- B. System operations and maintenance
- C. System initiation
- D. System implementation

Answer: A

Explanation:

Reference <https://online.concordia.edu/computer-science/system-development-life-cycle-phases/>

NEW QUESTION 81

- (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 84

- (Exam Topic 9)

The three PRIMARY requirements for a penetration test are

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

Answer: A

NEW QUESTION 88

- (Exam Topic 9)

Internet Protocol (IP) source address spoofing is used to defeat

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

Answer: A

NEW QUESTION 93

- (Exam Topic 9)

Copyright provides protection for which of the following?

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

Answer: B

NEW QUESTION 94

- (Exam Topic 9)

What technique BEST describes antivirus software that detects viruses by watching anomalous behavior?

- A. Signature
- B. Inference

- C. Induction
- D. Heuristic

Answer: D

NEW QUESTION 96

- (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 100

- (Exam Topic 9)

Which one of the following transmission media is MOST effective in preventing data interception?

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

Answer: C

NEW QUESTION 105

- (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 108

- (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 111

- (Exam Topic 9)

The Structured Query Language (SQL) implements Discretionary Access Controls (DAC) using

- A. INSERT and DELETE.
- B. GRANT and REVOKE.
- C. PUBLIC and PRIVATE.
- D. ROLLBACK and TERMINATE.

Answer: B

NEW QUESTION 113

- (Exam Topic 9)

Which of the following is considered best practice for preventing e-mail spoofing?

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

Answer: B

NEW QUESTION 117

- (Exam Topic 9)

Multi-threaded applications are more at risk than single-threaded applications to

- A. race conditions.
- B. virus infection.
- C. packet sniffing.
- D. database injection.

Answer: A

NEW QUESTION 119

- (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 122

- (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 126

- (Exam Topic 9)

The process of mutual authentication involves a computer system authenticating a user and authenticating the

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

Answer: B

NEW QUESTION 130

- (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 132

- (Exam Topic 9)

A security professional has just completed their organization's Business Impact Analysis (BIA). Following Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) best practices, what would be the professional's NEXT step?

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

Answer: A

NEW QUESTION 137

- (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 139

- (Exam Topic 9)

An organization is selecting a service provider to assist in the consolidation of multiple computing sites including development, implementation and ongoing support of various computer systems. Which of the following **MUST** be verified by the Information Security Department?

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

Answer: D

NEW QUESTION 140

- (Exam Topic 9)

Which of the following assessment metrics is **BEST** used to understand a system's vulnerability to potential exploits?

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

Answer: C

NEW QUESTION 141

- (Exam Topic 9)

Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?

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

Answer: D

NEW QUESTION 142

- (Exam Topic 9)

An auditor carrying out a compliance audit requests passwords that are encrypted in the system to verify that the passwords are compliant with policy. Which of the following is the **BEST** response to the auditor?

- A. Provide the encrypted passwords and analysis tools to the auditor for analysis.
- B. Analyze the encrypted passwords for the auditor and show them the results.
- C. Demonstrate that non-compliant passwords cannot be created in the system.
- D. Demonstrate that non-compliant passwords cannot be encrypted in the system.

Answer: C

NEW QUESTION 143

- (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 147

- (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 149

- (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 150

- (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 153

- (Exam Topic 9)

Which of the following is a security limitation of File Transfer Protocol (FTP)?

- A. Passive FTP is not compatible with web browsers.
- B. Anonymous access is allowed.
- C. FTP uses Transmission Control Protocol (TCP) ports 20 and 21.
- D. Authentication is not encrypted.

Answer: D

NEW QUESTION 157

- (Exam Topic 9)

In Business Continuity Planning (BCP), what is the importance of documenting business processes?

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

Answer: D

NEW QUESTION 158

- (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 159

- (Exam Topic 9)

The birthday attack is MOST effective against which one of the following cipher technologies?

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

Answer: C

NEW QUESTION 161

- (Exam Topic 9)

A disadvantage of an application filtering firewall is that it can lead to

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

Answer: B

NEW QUESTION 165

- (Exam Topic 9)

Which one of the following is a fundamental objective in handling an incident?

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

Answer: A

NEW QUESTION 170

- (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 172

- (Exam Topic 9)

Which of the following would be the **FIRST** step to take when implementing a patch management program?

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

Answer: D

NEW QUESTION 176

- (Exam Topic 9)

In a basic SYN flood attack, what is the attacker attempting to achieve?

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

Answer: A

NEW QUESTION 178

- (Exam Topic 9)

Which of the following is an appropriate source for test data?

- A. Production data that is secured and maintained only in the production environment.
- B. Test data that has no similarities to production data.
- C. Test data that is mirrored and kept up-to-date with production data.
- D. Production data that has been sanitized before loading into a test environment.

Answer: D

NEW QUESTION 179

- (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 184

- (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 185

- (Exam Topic 9)

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

- A. Trusted path
- B. Malicious logic

- C. Social engineering
- D. Passive misuse

Answer: C

NEW QUESTION 187

- (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 191

- (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 195

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 199

- (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 200

- (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 204

- (Exam Topic 9)

Passive Infrared Sensors (PIR) used in a non-climate controlled environment should

- A. reduce the detected object temperature in relation to the background temperature.
- B. increase the detected object temperature in relation to the background temperature.
- C. automatically compensate for variance in background temperature.
- D. detect objects of a specific temperature independent of the background temperature.

Answer: C

NEW QUESTION 205

- (Exam Topic 9)

When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?

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

Answer: B

NEW QUESTION 207

- (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 209

- (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 212

- (Exam Topic 9)

The goal of software assurance in application development is to

- A. enable the development of High Availability (HA) systems.
- B. facilitate the creation of Trusted Computing Base (TCB) systems.
- C. prevent the creation of vulnerable applications.
- D. encourage the development of open source applications.

Answer: C

NEW QUESTION 213

- (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 220

- (Exam Topic 9)

Which of the following Disaster Recovery (DR) sites is the MOST difficult to test?

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

Answer: B

NEW QUESTION 221

- (Exam Topic 9)

Which of the following statements is TRUE of black box testing?

- A. Only the functional specifications are known to the test planner.
- B. Only the source code and the design documents are known to the test planner.
- C. Only the source code and functional specifications are known to the test planner.
- D. Only the design documents and the functional specifications are known to the test planner.

Answer: A

NEW QUESTION 225

- (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 10)

What is the MAIN feature that onion routing networks offer?

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

Answer: C

NEW QUESTION 229

- (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 231

- (Exam Topic 10)

What do Capability Maturity Models (CMM) serve as a benchmark for in an organization?

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

Answer: D

NEW QUESTION 234

- (Exam Topic 10)

Refer to the information below to answer the question.

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

Which of the following solutions would have MOST likely detected the use of peer-to-peer programs when the computer was connected to the office network?

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

Answer: B

NEW QUESTION 238

- (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 240

- (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 245

- (Exam Topic 10)

Refer to the information below to answer the question.

In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

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

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

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

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

Answer: C

NEW QUESTION 247

- (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 250

- (Exam Topic 10)

An online retail company has formulated a record retention schedule for customer transactions. Which of the following is a valid reason a customer transaction is kept beyond the retention schedule?

- A. Pending legal hold
- B. Long term data mining needs
- C. Customer makes request to retain
- D. Useful for future business initiatives

Answer: A

NEW QUESTION 252

- (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 253

- (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 255

- (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 257

- (Exam Topic 10)

Which of the following is required to determine classification and ownership?

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

Answer: A

NEW QUESTION 262

- (Exam Topic 10)

Refer to the information below to answer the question.

A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.

The third party needs to have

- A. processes that are identical to that of the organization doing the outsourcing.
- B. access to the original personnel that were on staff at the organization.
- C. the ability to maintain all of the applications in languages they are familiar with.
- D. access to the skill sets consistent with the programming languages used by the organization.

Answer: D

NEW QUESTION 263

- (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 265

- (Exam Topic 10)

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

<u>Area</u>		<u>Technolog</u>
Facilities	<input type="text"/>	Encryption
Devices	<input type="text"/>	Window
Information	<input type="text"/>	Firewall
Systems	<input type="text"/>	Authenticatio

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 269

- (Exam Topic 10)

What is the MOST critical factor to achieve the goals of a security program?

- A. Capabilities of security resources
- B. Executive management support
- C. Effectiveness of security management
- D. Budget approved for security resources

Answer: B

NEW QUESTION 271

- (Exam Topic 10)

What is the BEST first step for determining if the appropriate security controls are in place for protecting data at rest?

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

Answer: B

NEW QUESTION 274

- (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 277

- (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 282

- (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 284

- (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 288

- (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 292

- (Exam Topic 10)

Which of the following actions MUST be taken if a vulnerability is discovered during the maintenance stage in a System Development Life Cycle (SDLC)?

- A. Make changes following principle and design guidelines.
- B. Stop the application until the vulnerability is fixed.
- C. Report the vulnerability to product owner.
- D. Monitor the application and review code.

Answer: C

NEW QUESTION 296

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.

Which of the following will indicate where the IT budget is BEST allocated during this time?

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

Answer: C

NEW QUESTION 297

- (Exam Topic 10)

Which of the following is the MOST effective attack against cryptographic hardware modules?

- A. Plaintext
- B. Brute force
- C. Power analysis
- D. Man-in-the-middle (MITM)

Answer: C

NEW QUESTION 298

- (Exam Topic 10)

Refer to the information below to answer the question.

In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

Table A

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

Table B

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

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

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

Answer: D

NEW QUESTION 303

- (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 308

- (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 311

- (Exam Topic 10)

Refer to the information below to answer the question.

A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.

Following best practice, where should the permitted access for each department and job classification combination be specified?

- A. Security procedures
- B. Security standards
- C. Human resource policy
- D. Human resource standards

Answer: B

NEW QUESTION 316

- (Exam Topic 10)

Which of the following **MUST** system and database administrators be aware of and apply when configuring systems used for storing personal employee data?

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

Answer: B

NEW QUESTION 317

- (Exam Topic 10)

Refer to the information below to answer the question.

A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.

Which of the following **BEST** describes the access control methodology used?

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

Answer: C

NEW QUESTION 318

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 323

- (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 328

- (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 333

- (Exam Topic 10)

The amount of data that will be collected during an audit is PRIMARILY determined by the

- A. audit scope.
- B. auditor's experience level.
- C. availability of the data.
- D. integrity of the data.

Answer: A

NEW QUESTION 338

- (Exam Topic 10)

Refer to the information below to answer the question.

Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.

After magnetic drives were degaussed twice according to the product manufacturer's directions, what is the MOST LIKELY security issue with degaussing?

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

Answer: B

NEW QUESTION 341

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 342

- (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 345

- (Exam Topic 10)

Without proper signal protection, embedded systems may be prone to which type of attack?

- A. Brute force
- B. Tampering
- C. Information disclosure
- D. Denial of Service (DoS)

Answer: C

NEW QUESTION 347

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.

When determining appropriate resource allocation, which of the following is MOST important to monitor?

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

Answer: B

NEW QUESTION 352

- (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 355

- (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 356

- (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 357

- (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 358

- (Exam Topic 10)

Which of the following is the BEST countermeasure to brute force login attacks?

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

Answer: D

NEW QUESTION 363

- (Exam Topic 10)

Which of the following is critical for establishing an initial baseline for software components in the operation and maintenance of applications?

- A. Application monitoring procedures
- B. Configuration control procedures
- C. Security audit procedures
- D. Software patching procedures

Answer: B

NEW QUESTION 366

- (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 371

- (Exam Topic 11)

What is the process called when impact values are assigned to the security objectives for information types?

- A. Qualitative analysis
- B. Quantitative analysis
- C. Remediation
- D. System security categorization

Answer: D

NEW QUESTION 376

- (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 381

- (Exam Topic 11)

A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

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

Answer: A

NEW QUESTION 384

- (Exam Topic 11)

Which of the following is generally indicative of a replay attack when dealing with biometric authentication?

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

Answer: D

NEW QUESTION 387

- (Exam Topic 11)

Which of the following is a function of Security Assertion Markup Language (SAML)?

- A. File allocation
- B. Redundancy check
- C. Extended validation
- D. Policy enforcement

Answer: D

NEW QUESTION 390

- (Exam Topic 11)

Data remanence refers to which of the following?

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

Answer: D

NEW QUESTION 395

- (Exam Topic 11)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step		Order
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 398

- (Exam Topic 11)

Which of the following is the MOST important element of change management documentation?

- A. List of components involved
- B. Number of changes being made
- C. Business case justification
- D. A stakeholder communication

Answer: C

NEW QUESTION 402

- (Exam Topic 11)

Which of the following is a reason to use manual patch installation instead of automated patch management?

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

Answer: C

NEW QUESTION 406

- (Exam Topic 11)

If compromised, which of the following would lead to the exploitation of multiple virtual machines?

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

Answer: B

NEW QUESTION 411

- (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)

A mobile device application that restricts the storage of user information to just that which is needed to accomplish lawful business goals adheres to what privacy principle?

- A. Onward transfer
- B. Collection Limitation
- C. Collector Accountability
- D. Individual Participation

Answer: B

NEW QUESTION 414

- (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 417

- (Exam Topic 11)

Which of the following is the BEST method to assess the effectiveness of an organization's vulnerability management program?

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

Answer: B

NEW QUESTION 421

- (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 424

- (Exam Topic 11)

What is an important characteristic of Role Based Access Control (RBAC)?

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

Answer: B

NEW QUESTION 427

- (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 428

- (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 433

- (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 436

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 441

- (Exam Topic 11)

How does Encapsulating Security Payload (ESP) in transport mode affect the Internet Protocol (IP)?

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

Answer: B

NEW QUESTION 446

- (Exam Topic 11)

Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

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

Answer: A

NEW QUESTION 447

- (Exam Topic 11)

Which of the following is the PRIMARY concern when using an Internet browser to access a cloud-based service?

- A. Insecure implementation of Application Programming Interfaces (API)
- B. Improper use and storage of management keys
- C. Misconfiguration of infrastructure allowing for unauthorized access
- D. Vulnerabilities within protocols that can expose confidential data

Answer: D

NEW QUESTION 449

- (Exam Topic 11)

Which of the following is an essential step before performing Structured Query Language (SQL) penetration tests on a production system?

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

Answer: C

NEW QUESTION 452

- (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 455

- (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 459

- (Exam Topic 11)

For privacy protected data, which of the following roles has the highest authority for establishing dissemination rules for the data?

- A. Information Systems Security Officer
- B. Data Owner
- C. System Security Architect
- D. Security Requirements Analyst

Answer: B

NEW QUESTION 464

- (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 466

- (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 471

- (Exam Topic 11)

The PRIMARY security concern for handheld devices is the

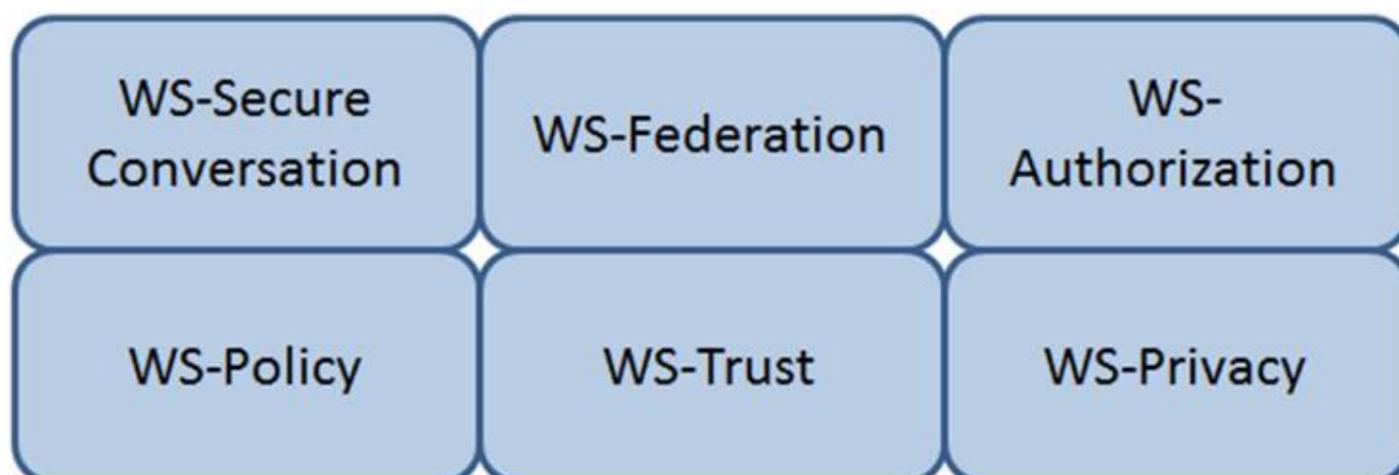
- A. strength of the encryption algorithm.
- B. spread of malware during synchronization.
- C. ability to bypass the authentication mechanism.
- D. strength of the Personal Identification Number (PIN).

Answer: C

NEW QUESTION 475

- (Exam Topic 11)

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

WS-Trust

The protocol used for issuing security tokens is based on WS-Trust. WS-Trust is a Web service specification that builds on WS-Security. It describes a protocol used for issuance, exchange, and validation of security tokens. WS-Trust provides a solution for interoperability by defining a protocol for issuing and exchanging security tokens, based on token format, namespace, or trust boundaries.

Reference: <https://msdn.microsoft.com/en-us/library/ff650503.aspx>

NEW QUESTION 478

- (Exam Topic 11)

Sensitive customer data is going to be added to a database. What is the MOST effective implementation for ensuring data privacy?

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

Answer: B

NEW QUESTION 480

- (Exam Topic 11)

What does an organization FIRST review to assure compliance with privacy requirements?

- A. Best practices
- B. Business objectives
- C. Legal and regulatory mandates
- D. Employee's compliance to policies and standards

Answer: C

NEW QUESTION 484

- (Exam Topic 11)

Discretionary Access Control (DAC) is based on which of the following?

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

Answer: B

NEW QUESTION 487

- (Exam Topic 11)

For an organization considering two-factor authentication for secure network access, which of the following is MOST secure?

- A. Challenge response and private key
- B. Digital certificates and Single Sign-On (SSO)
- C. Tokens and passphrase
- D. Smart card and biometrics

Answer: D

NEW QUESTION 489

- (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 491

- (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 494

- (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 496

- (Exam Topic 11)

Which of the following BEST describes the purpose of the security functional requirements of Common Criteria?

- A. Level of assurance of the Target of Evaluation (TOE) in intended operational environment
- B. Selection to meet the security objectives stated in test documents
- C. Security behavior expected of a TOE
- D. Definition of the roles and responsibilities

Answer: C

NEW QUESTION 500

- (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 505

- (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 510

- (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 514

- (Exam Topic 11)

In the Open System Interconnection (OSI) model, which layer is responsible for the transmission of binary data over a communications network?

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

Answer: B

NEW QUESTION 516

- (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 519

- (Exam Topic 11)

While investigating a malicious event, only six days of audit logs from the last month were available. What policy should be updated to address this problem?

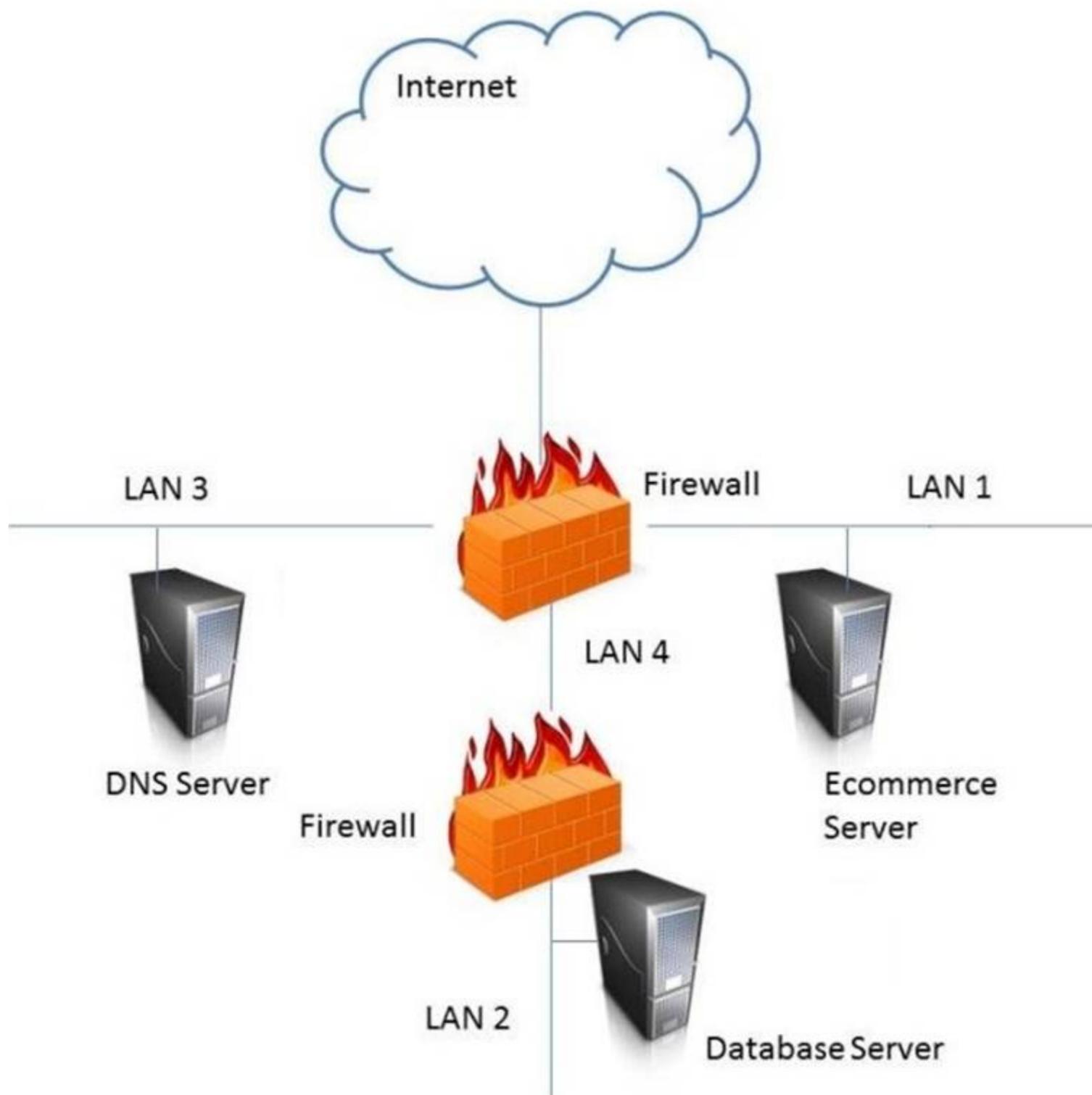
- A. Retention
- B. Reporting
- C. Recovery
- D. Remediation

Answer: A

NEW QUESTION 521

- (Exam Topic 11)

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
LAN 4

NEW QUESTION 526

- (Exam Topic 11)

Which of the following is the MOST important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?

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

Answer: D

NEW QUESTION 530

- (Exam Topic 11)

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

Answer: D

NEW QUESTION 535

- (Exam Topic 11)

Which of the following is the PRIMARY benefit of implementing data-in-use controls?

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

Answer: C

NEW QUESTION 539

- (Exam Topic 11)

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

- A. Document the system as high risk
- B. Perform a vulnerability assessment
- C. Perform a quantitative threat assessment
- D. Notate the information and move on

Answer: B

NEW QUESTION 542

- (Exam Topic 11)

The BEST method to mitigate the risk of a dictionary attack on a system is to

- A. use a hardware token.
- B. use complex passphrases.
- C. implement password history.
- D. encrypt the access control list (ACL).

Answer: A

NEW QUESTION 544

- (Exam Topic 11)

A global organization wants to implement hardware tokens as part of a multifactor authentication solution for remote access. The PRIMARY advantage of this implementation is

- A. the scalability of token enrollment.
- B. increased accountability of end users.
- C. it protects against unauthorized access.
- D. it simplifies user access administration.

Answer: C

NEW QUESTION 548

- (Exam Topic 11)

Which of the following provides the minimum set of privileges required to perform a job function and restricts the user to a domain with the required privileges?

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

Answer: B

NEW QUESTION 550

- (Exam Topic 11)

In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Mandatory Access Control – End user cannot set controls

Discretionary Access Control (DAC) – Subject has total control over objects

Role Based Access Control (RBAC) – Dynamically assigns roles permissions to particular duties based on job function

Rule Based access control – Dynamically assigns roles to subjects based on criteria assigned by a custodian.

NEW QUESTION 558

- (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 561

- (Exam Topic 12)

Which of the following is the BEST method to reduce the effectiveness of phishing attacks?

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

Answer: A

NEW QUESTION 563

- (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 565

- (Exam Topic 12)

Which of the following adds end-to-end security inside a Layer 2 Tunneling Protocol (L2TP) Internet Protocol Security (IPSec) connection?

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

Answer: B

NEW QUESTION 566

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 567

- (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 570

- (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 574

- (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 579

- (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 581

- (Exam Topic 12)

Which of the following restricts the ability of an individual to carry out all the steps of a particular process?

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

Answer: B

NEW QUESTION 585

- (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 586

- (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 589

- (Exam Topic 12)

The PRIMARY purpose of accreditation is to:

- A. comply with applicable laws and regulations.
- B. allow senior management to make an informed decision regarding whether to accept the risk of operating the system.
- C. protect an organization's sensitive data.
- D. verify that all security controls have been implemented properly and are operating in the correct manner.

Answer: B

NEW QUESTION 592

- (Exam Topic 12)

Which of the following media sanitization techniques is MOST likely to be effective for an organization using public cloud services?

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

Answer: B

NEW QUESTION 593

- (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 594

- (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 597

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 601

- (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 602

- (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 604

- (Exam Topic 12)

Which of the following would BEST describe the role directly responsible for data within an organization?

- A. Data custodian
- B. Information owner
- C. Database administrator
- D. Quality control

Answer: A

NEW QUESTION 608

- (Exam Topic 12)

At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

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

Answer: C

NEW QUESTION 609

- (Exam Topic 12)

How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

- A. Examines log messages or other indications on the system.
- B. Monitors alarms sent to the system administrator
- C. Matches traffic patterns to virus signature files
- D. Examines the Access Control List (ACL)

Answer: C

NEW QUESTION 612

- (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 615

- (Exam Topic 12)

An employee of a retail company has been granted an extended leave of absence by Human Resources (HR). This information has been formally communicated to the access provisioning team. Which of the following is the BEST action to take?

- A. Revoke access temporarily.
- B. Block user access and delete user account after six months.
- C. Block access to the offices immediately.
- D. Monitor account usage temporarily.

Answer: D

NEW QUESTION 619

- (Exam Topic 12)

Which of the following is the PRIMARY benefit of a formalized information classification program?

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

Answer: B

NEW QUESTION 620

- (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 624

- (Exam Topic 12)

Which of the following approaches is the MOST effective way to dispose of data on multiple hard drives?

- A. Delete every file on each drive.
- B. Destroy the partition table for each drive using the command line.
- C. Degauss each drive individually.
- D. Perform multiple passes on each drive using approved formatting methods.

Answer: D

NEW QUESTION 627

- (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 632

- (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 636

- (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 637

- (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 639

- (Exam Topic 12)

When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?

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

Answer: D

NEW QUESTION 640

- (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 641

- (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 646

- (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 651

- (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 655

- (Exam Topic 12)

Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?

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

Answer: C

NEW QUESTION 658

- (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 661

- (Exam Topic 12)

Which of the following is the PRIMARY reason to perform regular vulnerability scanning of an organization network?

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

Answer: B

NEW QUESTION 662

- (Exam Topic 13)

Which one of the following data integrity models assumes a lattice of integrity levels?

- A. Take-Grant
- B. Biba
- C. Harrison-Ruzzo

D. Bell-LaPadula

Answer: B

NEW QUESTION 664

- (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 665

- (Exam Topic 13)

Which of the following steps should be performed FIRST when purchasing Commercial Off-The-Shelf (COTS) software?

- A. undergo a security assessment as part of authorization process
- B. establish a risk management strategy
- C. harden the hosting server, and perform hosting and application vulnerability scans
- D. establish policies and procedures on system and services acquisition

Answer: D

NEW QUESTION 667

- (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 670

- (Exam Topic 13)

Which of the following is the MOST important security goal when performing application interface testing?

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

Answer: B

NEW QUESTION 674

- (Exam Topic 13)

An organization's security policy delegates to the data owner the ability to assign which user roles have access to a particular resource. What type of authorization mechanism is being used?

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

Answer: A

NEW QUESTION 679

- (Exam Topic 13)

Due to system constraints, a group of system administrators must share a high-level access set of credentials. Which of the following would be MOST appropriate to implement?

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

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 680

- (Exam Topic 13)

Who is responsible for the protection of information when it is shared with or provided to other organizations?

- A. Systems owner
- B. Authorizing Official (AO)
- C. Information owner
- D. Security officer

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 685

- (Exam Topic 13)

What protocol is often used between gateway hosts on the Internet?

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

Answer: B

NEW QUESTION 686

- (Exam Topic 13)

As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

- A. Use a web scanner to scan for vulnerabilities within the website.
- B. Perform a code review to ensure that the database references are properly addressed.
- C. Establish a secure connection to the web server to validate that only the approved ports are open.
- D. Enter only numbers in the web form and verify that the website prompts the user to enter a valid input.

Answer: D

NEW QUESTION 687

- (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 688

- (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 693

- (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 698

- (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 701

- (Exam Topic 13)

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

<u>Security Engineering Term</u>	<u>Definition</u>
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment	The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment	The method used to identify feasible security risk mitigation options and plans.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

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

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

NEW QUESTION 706

- (Exam Topic 13)

Which of the following could be considered the MOST significant security challenge when adopting DevOps practices compared to a more traditional control framework?

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

Answer: B

NEW QUESTION 710

- (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 712

- (Exam Topic 13)

Which factors **MUST** be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?

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

Answer: A

NEW QUESTION 713

- (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 718

- (Exam Topic 13)

A security practitioner is tasked with securing the organization's Wireless Access Points (WAP). Which of these is the **MOST** effective way of restricting this environment to authorized users?

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

Answer: D

NEW QUESTION 721

- (Exam Topic 13)

What is the **MAIN** purpose of a change management policy?

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

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 725

- (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 730

- (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 733

- (Exam Topic 13)

Which of the following methods of suppressing a fire is environmentally friendly and the **MOST** appropriate for a data center?

- A. Inert gas fire suppression system

- B. Halon gas fire suppression system
- C. Dry-pipe sprinklers
- D. Wet-pipe sprinklers

Answer: C

NEW QUESTION 735

- (Exam Topic 13)

What are the steps of a risk assessment?

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

Answer: A

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 737

- (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 740

- (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 741

- (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 744

- (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 749

- (Exam Topic 13)

Which of the following is considered a secure coding practice?

- A. Use concurrent access for shared variables and resources
- B. Use checksums to verify the integrity of libraries
- C. Use new code for common tasks
- D. Use dynamic execution functions to pass user supplied data

Answer: B

NEW QUESTION 751

- (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 754

- (Exam Topic 13)

Match the functional roles in an external audit to their responsibilities. Drag each role on the left to its corresponding responsibility on the right. Select and Place:

<u>Role</u>		<u>Responsibility</u>
Executive management	<input type="text"/>	Approve audit budget and resource allocation.
Audit committee	<input type="text"/>	Provide audit oversight.
Compliance officer	<input type="text"/>	Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor	<input type="text"/>	Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<u>Role</u>		<u>Responsibility</u>
Executive management	Executive management	Approve audit budget and resource allocation.
Audit committee	Audit committee	Provide audit oversight.
Compliance officer	External auditor	Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor	Compliance officer	Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

NEW QUESTION 755

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 759

- (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 763

- (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 764

- (Exam Topic 13)

An Information Technology (IT) professional attends a cybersecurity seminar on current incident response methodologies. What code of ethics canon is being observed?

- A. Provide diligent and competent service to principals
- B. Protect society, the commonwealth, and the infrastructure
- C. Advance and protect the profession
- D. Act honorable, honesty, justly, responsibly, and legally

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 769

- (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 772

- (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 776

- (Exam Topic 13)

A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report. In which phase of the assessment was this error **MOST** likely made?

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

Answer: A

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 780

- (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 783

- (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 788

- (Exam Topic 13)

An organization adopts a new firewall hardening standard. How can the security professional verify that the technical staff correct implemented the new standard?

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

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 790

- (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 791

- (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 792

- (Exam Topic 13)

Which of the following alarm systems is recommended to detect intrusions through windows in a high-noise, occupied environment?

- A. Acoustic sensor
- B. Motion sensor
- C. Shock sensor
- D. Photoelectric sensor

Answer: C

NEW QUESTION 795

- (Exam Topic 13)

Which of the following is the MOST important part of an awareness and training plan to prepare employees for emergency situations?

- A. Having emergency contacts established for the general employee population to get information
- B. Conducting business continuity and disaster recovery training for those who have a direct role in the recovery
- C. Designing business continuity and disaster recovery training programs for different audiences
- D. Publishing a corporate business continuity and disaster recovery plan on the corporate website

Answer: C

NEW QUESTION 800

- (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.

Actions

- Define the perimeter.
- Identify the vulnerability.
- Assess the risk.
- Determine the actions.

Steps

- Step 1
- Step 2
- Step 3
- Step 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

- Define the perimeter.
- Identify the vulnerability.
- Assess the risk.
- Determine the actions.

Steps

- Identify the vulnerability.
- Define the perimeter.
- Assess the risk.
- Determine the actions.
- Step 1
- Step 2
- Step 3
- Step 4

NEW QUESTION 802

- (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 807

- (Exam Topic 13)

Which of the following is the BEST metric to obtain when gaining support for an Identify and Access Management (IAM) solution?

- A. Application connection successes resulting in data leakage
- B. Administrative costs for restoring systems after connection failure
- C. Employee system timeouts from implementing wrong limits
- D. Help desk costs required to support password reset requests

Answer: D

NEW QUESTION 809

- (Exam Topic 13)

Which of the following management process allows ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

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

Answer: A

NEW QUESTION 810

- (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 811

- (Exam Topic 13)

Which one of the following considerations has the LEAST impact when considering transmission security?

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

Answer: C

NEW QUESTION 816

- (Exam Topic 13)

Which of the following techniques is known to be effective in spotting resource exhaustion problems, especially with resources such as processes, memory, and connections?

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

Answer: A

NEW QUESTION 821

.....

About ExamBible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

- (Exam Topic 1)

When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined?

- A. Only when assets are clearly defined
- B. Only when standards are defined
- C. Only when controls are put in place
- D. Only procedures are defined

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

All of the following items should be included in a Business Impact Analysis (BIA) questionnaire EXCEPT questions that

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

Answer: B

NEW QUESTION 3

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 4

- (Exam Topic 1)

Intellectual property rights are PRIMARY concerned with which of the following?

- A. Owner's ability to realize financial gain
- B. Owner's ability to maintain copyright
- C. Right of the owner to enjoy their creation
- D. Right of the owner to control delivery method

Answer: D

NEW QUESTION 5

- (Exam Topic 1)

What is the MOST important consideration from a data security perspective when an organization plans to relocate?

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

Answer: C

NEW QUESTION 6

- (Exam Topic 2)

Which 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 7

- (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 8

- (Exam Topic 2)

Which of the following is an effective control in preventing electronic cloning of Radio Frequency Identification (RFID) based access cards?

- A. Personal Identity Verification (PIV)
- B. Cardholder Unique Identifier (CHUID) authentication
- C. Physical Access Control System (PACS) repeated attempt detection
- D. Asymmetric Card Authentication Key (CAK) challenge-response

Answer: C

NEW QUESTION 9

- (Exam Topic 2)

When implementing a data classification program, why is it important to avoid too much granularity?

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

Answer: A

NEW QUESTION 10

- (Exam Topic 2)

Which of the following BEST describes the responsibilities of a data owner?

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

Answer: C

NEW QUESTION 10

- (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 15

- (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 17

- (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 19

- (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 22

- (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 27

- (Exam Topic 4)

Which of the following is used by the Point-to-Point Protocol (PPP) to determine packet formats?

- A. Layer 2 Tunneling Protocol (L2TP)
- B. Link Control Protocol (LCP)
- C. Challenge Handshake Authentication Protocol (CHAP)
- D. Packet Transfer Protocol (PTP)

Answer: B

NEW QUESTION 28

- (Exam Topic 4)

What is the purpose of an Internet Protocol (IP) spoofing attack?

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

Answer: D

NEW QUESTION 30

- (Exam Topic 4)

At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

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

Answer: D

NEW QUESTION 31

- (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 32

- (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 33

- (Exam Topic 6)

Which of the following could cause a Denial of Service (DoS) against an authentication system?

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

Answer: D

NEW QUESTION 37

- (Exam Topic 6)

A Virtual Machine (VM) environment has five guest Operating Systems (OS) and provides strong isolation. What **MUST** an administrator review to audit a user's access to data files?

- A. Host VM monitor audit logs
- B. Guest OS access controls
- C. Host VM access controls
- D. Guest OS audit logs

Answer: A

NEW QUESTION 42

- (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 43

- (Exam Topic 6)

In which of the following programs is it **MOST** important to include the collection of security process data?

- A. Quarterly access reviews
- B. Security continuous monitoring
- C. Business continuity testing
- D. Annual security training

Answer: A

NEW QUESTION 47

- (Exam Topic 7)

Recovery strategies of a Disaster Recovery planning (DRIP) **MUST** be aligned with which of the following?

- A. Hardware and software compatibility issues
- B. Applications' critically and downtime tolerance
- C. Budget constraints and requirements
- D. Cost/benefit analysis and business objectives

Answer: D

NEW QUESTION 49

- (Exam Topic 7)

A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?

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

Answer: D

NEW QUESTION 51

- (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 56

- (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 57

- (Exam Topic 7)

With what frequency should monitoring of a control occur when implementing Information Security Continuous Monitoring (ISCM) solutions?

- A. Continuously without exception for all security controls
- B. Before and after each change of the control
- C. At a rate concurrent with the volatility of the security control
- D. Only during system implementation and decommissioning

Answer: B

NEW QUESTION 61

- (Exam Topic 7)

When is a Business Continuity Plan (BCP) considered to be valid?

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

Answer: D

NEW QUESTION 65

- (Exam Topic 7)

What should be the FIRST action to protect the chain of evidence when a desktop computer is involved?

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

Answer: C

NEW QUESTION 66

- (Exam Topic 8)

Which of the following is a web application control that should be put into place to prevent exploitation of Operating System (OS) bugs?

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

Answer: B

NEW QUESTION 68

- (Exam Topic 8)

What is the BEST approach to addressing security issues in legacy web applications?

- A. Debug the security issues
- B. Migrate to newer, supported applications where possible
- C. Conduct a security assessment
- D. Protect the legacy application with a web application firewall

Answer: D

NEW QUESTION 70

- (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 75

- (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 78

- (Exam Topic 8)

The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle (SDLC)?

- A. System acquisition and development
- B. System operations and maintenance
- C. System initiation
- D. System implementation

Answer: A

Explanation:

Reference <https://online.concordia.edu/computer-science/system-development-life-cycle-phases/>

NEW QUESTION 81

- (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 84

- (Exam Topic 9)

The three PRIMARY requirements for a penetration test are

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

Answer: A

NEW QUESTION 88

- (Exam Topic 9)

Internet Protocol (IP) source address spoofing is used to defeat

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

Answer: A

NEW QUESTION 93

- (Exam Topic 9)

Copyright provides protection for which of the following?

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

Answer: B

NEW QUESTION 94

- (Exam Topic 9)

What technique BEST describes antivirus software that detects viruses by watching anomalous behavior?

- A. Signature
- B. Inference

- C. Induction
- D. Heuristic

Answer: D

NEW QUESTION 96

- (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 100

- (Exam Topic 9)

Which one of the following transmission media is MOST effective in preventing data interception?

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

Answer: C

NEW QUESTION 105

- (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 108

- (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 111

- (Exam Topic 9)

The Structured Query Language (SQL) implements Discretionary Access Controls (DAC) using

- A. INSERT and DELETE.
- B. GRANT and REVOKE.
- C. PUBLIC and PRIVATE.
- D. ROLLBACK and TERMINATE.

Answer: B

NEW QUESTION 113

- (Exam Topic 9)

Which of the following is considered best practice for preventing e-mail spoofing?

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

Answer: B

NEW QUESTION 117

- (Exam Topic 9)

Multi-threaded applications are more at risk than single-threaded applications to

- A. race conditions.
- B. virus infection.
- C. packet sniffing.
- D. database injection.

Answer: A

NEW QUESTION 119

- (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 122

- (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 126

- (Exam Topic 9)

The process of mutual authentication involves a computer system authenticating a user and authenticating the

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

Answer: B

NEW QUESTION 130

- (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 132

- (Exam Topic 9)

A security professional has just completed their organization's Business Impact Analysis (BIA). Following Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) best practices, what would be the professional's NEXT step?

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

Answer: A

NEW QUESTION 137

- (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 139

- (Exam Topic 9)

An organization is selecting a service provider to assist in the consolidation of multiple computing sites including development, implementation and ongoing support of various computer systems. Which of the following **MUST** be verified by the Information Security Department?

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

Answer: D

NEW QUESTION 140

- (Exam Topic 9)

Which of the following assessment metrics is **BEST** used to understand a system's vulnerability to potential exploits?

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

Answer: C

NEW QUESTION 141

- (Exam Topic 9)

Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?

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

Answer: D

NEW QUESTION 142

- (Exam Topic 9)

An auditor carrying out a compliance audit requests passwords that are encrypted in the system to verify that the passwords are compliant with policy. Which of the following is the **BEST** response to the auditor?

- A. Provide the encrypted passwords and analysis tools to the auditor for analysis.
- B. Analyze the encrypted passwords for the auditor and show them the results.
- C. Demonstrate that non-compliant passwords cannot be created in the system.
- D. Demonstrate that non-compliant passwords cannot be encrypted in the system.

Answer: C

NEW QUESTION 143

- (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 147

- (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 149

- (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 150

- (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 153

- (Exam Topic 9)

Which of the following is a security limitation of File Transfer Protocol (FTP)?

- A. Passive FTP is not compatible with web browsers.
- B. Anonymous access is allowed.
- C. FTP uses Transmission Control Protocol (TCP) ports 20 and 21.
- D. Authentication is not encrypted.

Answer: D

NEW QUESTION 157

- (Exam Topic 9)

In Business Continuity Planning (BCP), what is the importance of documenting business processes?

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

Answer: D

NEW QUESTION 158

- (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 159

- (Exam Topic 9)

The birthday attack is MOST effective against which one of the following cipher technologies?

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

Answer: C

NEW QUESTION 161

- (Exam Topic 9)

A disadvantage of an application filtering firewall is that it can lead to

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

Answer: B

NEW QUESTION 165

- (Exam Topic 9)

Which one of the following is a fundamental objective in handling an incident?

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

Answer: A

NEW QUESTION 170

- (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 172

- (Exam Topic 9)

Which of the following would be the **FIRST** step to take when implementing a patch management program?

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

Answer: D

NEW QUESTION 176

- (Exam Topic 9)

In a basic SYN flood attack, what is the attacker attempting to achieve?

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

Answer: A

NEW QUESTION 178

- (Exam Topic 9)

Which of the following is an appropriate source for test data?

- A. Production data that is secured and maintained only in the production environment.
- B. Test data that has no similarities to production data.
- C. Test data that is mirrored and kept up-to-date with production data.
- D. Production data that has been sanitized before loading into a test environment.

Answer: D

NEW QUESTION 179

- (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 184

- (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 185

- (Exam Topic 9)

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

- A. Trusted path
- B. Malicious logic

- C. Social engineering
- D. Passive misuse

Answer: C

NEW QUESTION 187

- (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 191

- (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 195

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 199

- (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 200

- (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 204

- (Exam Topic 9)

Passive Infrared Sensors (PIR) used in a non-climate controlled environment should

- A. reduce the detected object temperature in relation to the background temperature.
- B. increase the detected object temperature in relation to the background temperature.
- C. automatically compensate for variance in background temperature.
- D. detect objects of a specific temperature independent of the background temperature.

Answer: C

NEW QUESTION 205

- (Exam Topic 9)

When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?

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

Answer: B

NEW QUESTION 207

- (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 209

- (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 212

- (Exam Topic 9)

The goal of software assurance in application development is to

- A. enable the development of High Availability (HA) systems.
- B. facilitate the creation of Trusted Computing Base (TCB) systems.
- C. prevent the creation of vulnerable applications.
- D. encourage the development of open source applications.

Answer: C

NEW QUESTION 213

- (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 220

- (Exam Topic 9)

Which of the following Disaster Recovery (DR) sites is the MOST difficult to test?

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

Answer: B

NEW QUESTION 221

- (Exam Topic 9)

Which of the following statements is TRUE of black box testing?

- A. Only the functional specifications are known to the test planner.
- B. Only the source code and the design documents are known to the test planner.
- C. Only the source code and functional specifications are known to the test planner.
- D. Only the design documents and the functional specifications are known to the test planner.

Answer: A

NEW QUESTION 225

- (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 10)

What is the MAIN feature that onion routing networks offer?

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

Answer: C

NEW QUESTION 229

- (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 231

- (Exam Topic 10)

What do Capability Maturity Models (CMM) serve as a benchmark for in an organization?

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

Answer: D

NEW QUESTION 234

- (Exam Topic 10)

Refer to the information below to answer the question.

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

Which of the following solutions would have MOST likely detected the use of peer-to-peer programs when the computer was connected to the office network?

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

Answer: B

NEW QUESTION 238

- (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 240

- (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 245

- (Exam Topic 10)

Refer to the information below to answer the question.

In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

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

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

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

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

Answer: C

NEW QUESTION 247

- (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 250

- (Exam Topic 10)

An online retail company has formulated a record retention schedule for customer transactions. Which of the following is a valid reason a customer transaction is kept beyond the retention schedule?

- A. Pending legal hold
- B. Long term data mining needs
- C. Customer makes request to retain
- D. Useful for future business initiatives

Answer: A

NEW QUESTION 252

- (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 253

- (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 255

- (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 257

- (Exam Topic 10)

Which of the following is required to determine classification and ownership?

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

Answer: A

NEW QUESTION 262

- (Exam Topic 10)

Refer to the information below to answer the question.

A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.

The third party needs to have

- A. processes that are identical to that of the organization doing the outsourcing.
- B. access to the original personnel that were on staff at the organization.
- C. the ability to maintain all of the applications in languages they are familiar with.
- D. access to the skill sets consistent with the programming languages used by the organization.

Answer: D

NEW QUESTION 263

- (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 265

- (Exam Topic 10)

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

<u>Area</u>		<u>Technolog</u>
Facilities	<input type="text"/>	Encryption
Devices	<input type="text"/>	Window
Information	<input type="text"/>	Firewall
Systems	<input type="text"/>	Authenticatio

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 269

- (Exam Topic 10)

What is the MOST critical factor to achieve the goals of a security program?

- A. Capabilities of security resources
- B. Executive management support
- C. Effectiveness of security management
- D. Budget approved for security resources

Answer: B

NEW QUESTION 271

- (Exam Topic 10)

What is the BEST first step for determining if the appropriate security controls are in place for protecting data at rest?

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

Answer: B

NEW QUESTION 274

- (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 277

- (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 282

- (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 284

- (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 288

- (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 292

- (Exam Topic 10)

Which of the following actions MUST be taken if a vulnerability is discovered during the maintenance stage in a System Development Life Cycle (SDLC)?

- A. Make changes following principle and design guidelines.
- B. Stop the application until the vulnerability is fixed.
- C. Report the vulnerability to product owner.
- D. Monitor the application and review code.

Answer: C

NEW QUESTION 296

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.

Which of the following will indicate where the IT budget is BEST allocated during this time?

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

Answer: C

NEW QUESTION 297

- (Exam Topic 10)

Which of the following is the MOST effective attack against cryptographic hardware modules?

- A. Plaintext
- B. Brute force
- C. Power analysis
- D. Man-in-the-middle (MITM)

Answer: C

NEW QUESTION 298

- (Exam Topic 10)

Refer to the information below to answer the question.

In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

Table A

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

Table B

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

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

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

Answer: D

NEW QUESTION 303

- (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 308

- (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 311

- (Exam Topic 10)

Refer to the information below to answer the question.

A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.

Following best practice, where should the permitted access for each department and job classification combination be specified?

- A. Security procedures
- B. Security standards
- C. Human resource policy
- D. Human resource standards

Answer: B

NEW QUESTION 316

- (Exam Topic 10)

Which of the following **MUST** system and database administrators be aware of and apply when configuring systems used for storing personal employee data?

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

Answer: B

NEW QUESTION 317

- (Exam Topic 10)

Refer to the information below to answer the question.

A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.

Which of the following **BEST** describes the access control methodology used?

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

Answer: C

NEW QUESTION 318

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 323

- (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 328

- (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 333

- (Exam Topic 10)

The amount of data that will be collected during an audit is PRIMARILY determined by the

- A. audit scope.
- B. auditor's experience level.
- C. availability of the data.
- D. integrity of the data.

Answer: A

NEW QUESTION 338

- (Exam Topic 10)

Refer to the information below to answer the question.

Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.

After magnetic drives were degaussed twice according to the product manufacturer's directions, what is the MOST LIKELY security issue with degaussing?

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

Answer: B

NEW QUESTION 341

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 342

- (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 345

- (Exam Topic 10)

Without proper signal protection, embedded systems may be prone to which type of attack?

- A. Brute force
- B. Tampering
- C. Information disclosure
- D. Denial of Service (DoS)

Answer: C

NEW QUESTION 347

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.

When determining appropriate resource allocation, which of the following is MOST important to monitor?

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

Answer: B

NEW QUESTION 352

- (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 355

- (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 356

- (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 357

- (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 358

- (Exam Topic 10)

Which of the following is the BEST countermeasure to brute force login attacks?

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

Answer: D

NEW QUESTION 363

- (Exam Topic 10)

Which of the following is critical for establishing an initial baseline for software components in the operation and maintenance of applications?

- A. Application monitoring procedures
- B. Configuration control procedures
- C. Security audit procedures
- D. Software patching procedures

Answer: B

NEW QUESTION 366

- (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 371

- (Exam Topic 11)

What is the process called when impact values are assigned to the security objectives for information types?

- A. Qualitative analysis
- B. Quantitative analysis
- C. Remediation
- D. System security categorization

Answer: D

NEW QUESTION 376

- (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 381

- (Exam Topic 11)

A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

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

Answer: A

NEW QUESTION 384

- (Exam Topic 11)

Which of the following is generally indicative of a replay attack when dealing with biometric authentication?

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

Answer: D

NEW QUESTION 387

- (Exam Topic 11)

Which of the following is a function of Security Assertion Markup Language (SAML)?

- A. File allocation
- B. Redundancy check
- C. Extended validation
- D. Policy enforcement

Answer: D

NEW QUESTION 390

- (Exam Topic 11)

Data remanence refers to which of the following?

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

Answer: D

NEW QUESTION 395

- (Exam Topic 11)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step		Order
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 398

- (Exam Topic 11)

Which of the following is the MOST important element of change management documentation?

- A. List of components involved
- B. Number of changes being made
- C. Business case justification
- D. A stakeholder communication

Answer: C

NEW QUESTION 402

- (Exam Topic 11)

Which of the following is a reason to use manual patch installation instead of automated patch management?

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

Answer: C

NEW QUESTION 406

- (Exam Topic 11)

If compromised, which of the following would lead to the exploitation of multiple virtual machines?

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

Answer: B

NEW QUESTION 411

- (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)

A mobile device application that restricts the storage of user information to just that which is needed to accomplish lawful business goals adheres to what privacy principle?

- A. Onward transfer
- B. Collection Limitation
- C. Collector Accountability
- D. Individual Participation

Answer: B

NEW QUESTION 414

- (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 417

- (Exam Topic 11)

Which of the following is the BEST method to assess the effectiveness of an organization's vulnerability management program?

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

Answer: B

NEW QUESTION 421

- (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 424

- (Exam Topic 11)

What is an important characteristic of Role Based Access Control (RBAC)?

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

Answer: B

NEW QUESTION 427

- (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 428

- (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 433

- (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 436

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 441

- (Exam Topic 11)

How does Encapsulating Security Payload (ESP) in transport mode affect the Internet Protocol (IP)?

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

Answer: B

NEW QUESTION 446

- (Exam Topic 11)

Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

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

Answer: A

NEW QUESTION 447

- (Exam Topic 11)

Which of the following is the PRIMARY concern when using an Internet browser to access a cloud-based service?

- A. Insecure implementation of Application Programming Interfaces (API)
- B. Improper use and storage of management keys
- C. Misconfiguration of infrastructure allowing for unauthorized access
- D. Vulnerabilities within protocols that can expose confidential data

Answer: D

NEW QUESTION 449

- (Exam Topic 11)

Which of the following is an essential step before performing Structured Query Language (SQL) penetration tests on a production system?

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

Answer: C

NEW QUESTION 452

- (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 455

- (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 459

- (Exam Topic 11)

For privacy protected data, which of the following roles has the highest authority for establishing dissemination rules for the data?

- A. Information Systems Security Officer
- B. Data Owner
- C. System Security Architect
- D. Security Requirements Analyst

Answer: B

NEW QUESTION 464

- (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 466

- (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 471

- (Exam Topic 11)

The PRIMARY security concern for handheld devices is the

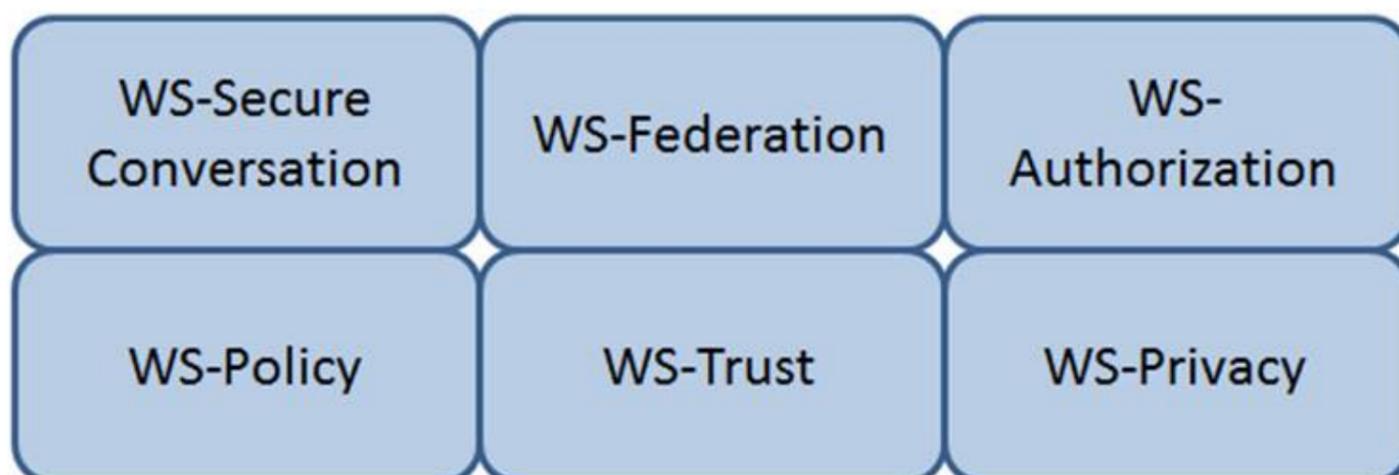
- A. strength of the encryption algorithm.
- B. spread of malware during synchronization.
- C. ability to bypass the authentication mechanism.
- D. strength of the Personal Identification Number (PIN).

Answer: C

NEW QUESTION 475

- (Exam Topic 11)

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

WS-Trust

The protocol used for issuing security tokens is based on WS-Trust. WS-Trust is a Web service specification that builds on WS-Security. It describes a protocol used for issuance, exchange, and validation of security tokens. WS-Trust provides a solution for interoperability by defining a protocol for issuing and exchanging security tokens, based on token format, namespace, or trust boundaries.

Reference: <https://msdn.microsoft.com/en-us/library/ff650503.aspx>

NEW QUESTION 478

- (Exam Topic 11)

Sensitive customer data is going to be added to a database. What is the MOST effective implementation for ensuring data privacy?

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

Answer: B

NEW QUESTION 480

- (Exam Topic 11)

What does an organization FIRST review to assure compliance with privacy requirements?

- A. Best practices
- B. Business objectives
- C. Legal and regulatory mandates
- D. Employee's compliance to policies and standards

Answer: C

NEW QUESTION 484

- (Exam Topic 11)

Discretionary Access Control (DAC) is based on which of the following?

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

Answer: B

NEW QUESTION 487

- (Exam Topic 11)

For an organization considering two-factor authentication for secure network access, which of the following is MOST secure?

- A. Challenge response and private key
- B. Digital certificates and Single Sign-On (SSO)
- C. Tokens and passphrase
- D. Smart card and biometrics

Answer: D

NEW QUESTION 489

- (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 491

- (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 494

- (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 496

- (Exam Topic 11)

Which of the following BEST describes the purpose of the security functional requirements of Common Criteria?

- A. Level of assurance of the Target of Evaluation (TOE) in intended operational environment
- B. Selection to meet the security objectives stated in test documents
- C. Security behavior expected of a TOE
- D. Definition of the roles and responsibilities

Answer: C

NEW QUESTION 500

- (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 505

- (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 510

- (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 514

- (Exam Topic 11)

In the Open System Interconnection (OSI) model, which layer is responsible for the transmission of binary data over a communications network?

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

Answer: B

NEW QUESTION 516

- (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 519

- (Exam Topic 11)

While investigating a malicious event, only six days of audit logs from the last month were available. What policy should be updated to address this problem?

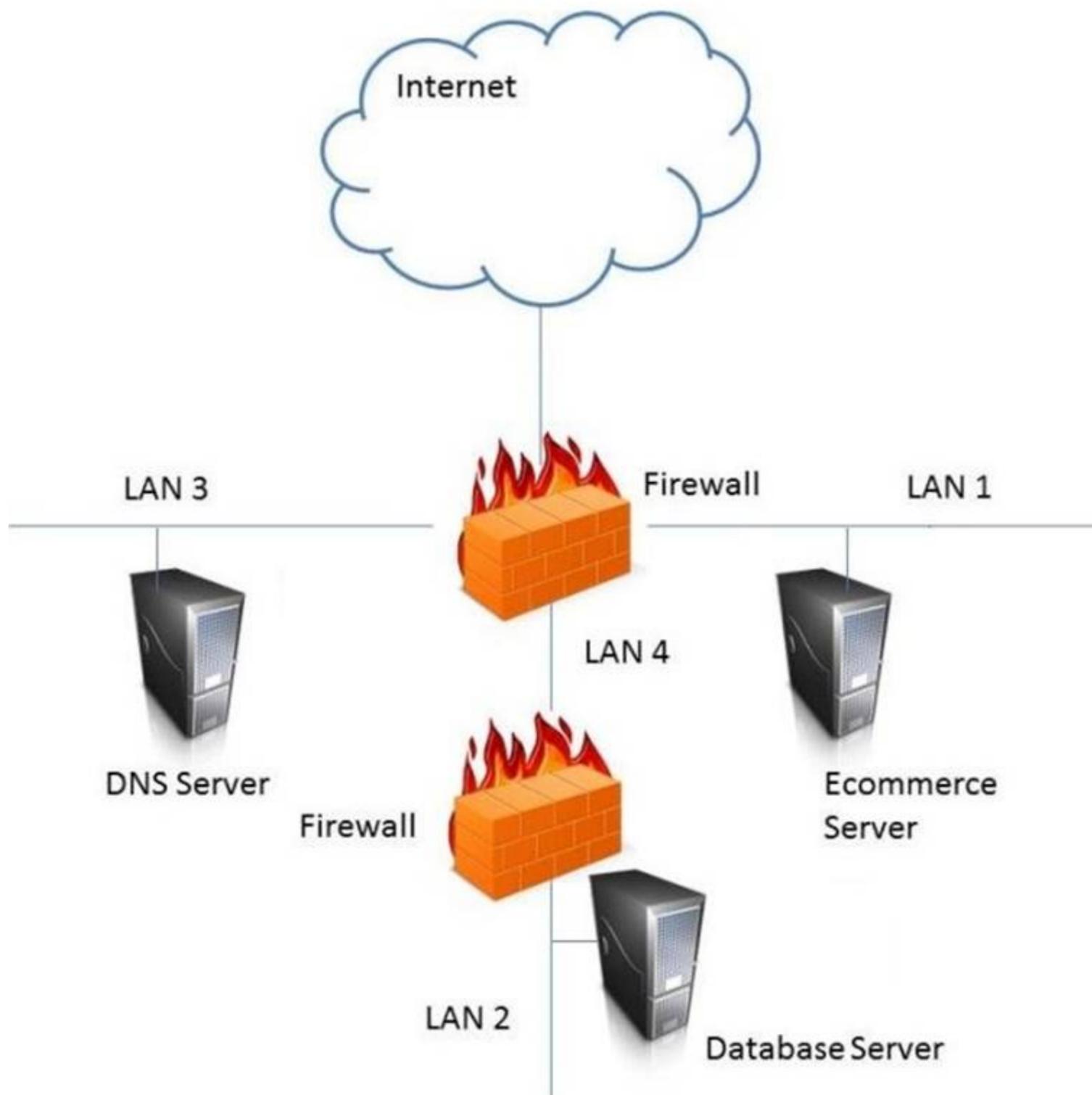
- A. Retention
- B. Reporting
- C. Recovery
- D. Remediation

Answer: A

NEW QUESTION 521

- (Exam Topic 11)

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
LAN 4

NEW QUESTION 526

- (Exam Topic 11)

Which of the following is the MOST important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?

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

Answer: D

NEW QUESTION 530

- (Exam Topic 11)

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

Answer: D

NEW QUESTION 535

- (Exam Topic 11)

Which of the following is the PRIMARY benefit of implementing data-in-use controls?

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

Answer: C

NEW QUESTION 539

- (Exam Topic 11)

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

- A. Document the system as high risk
- B. Perform a vulnerability assessment
- C. Perform a quantitative threat assessment
- D. Notate the information and move on

Answer: B

NEW QUESTION 542

- (Exam Topic 11)

The BEST method to mitigate the risk of a dictionary attack on a system is to

- A. use a hardware token.
- B. use complex passphrases.
- C. implement password history.
- D. encrypt the access control list (ACL).

Answer: A

NEW QUESTION 544

- (Exam Topic 11)

A global organization wants to implement hardware tokens as part of a multifactor authentication solution for remote access. The PRIMARY advantage of this implementation is

- A. the scalability of token enrollment.
- B. increased accountability of end users.
- C. it protects against unauthorized access.
- D. it simplifies user access administration.

Answer: C

NEW QUESTION 548

- (Exam Topic 11)

Which of the following provides the minimum set of privileges required to perform a job function and restricts the user to a domain with the required privileges?

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

Answer: B

NEW QUESTION 550

- (Exam Topic 11)

In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Mandatory Access Control – End user cannot set controls

Discretionary Access Control (DAC) – Subject has total control over objects

Role Based Access Control (RBAC) – Dynamically assigns roles permissions to particular duties based on job function

Rule Based access control – Dynamically assigns roles to subjects based on criteria assigned by a custodian.

NEW QUESTION 558

- (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 561

- (Exam Topic 12)

Which of the following is the BEST method to reduce the effectiveness of phishing attacks?

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

Answer: A

NEW QUESTION 563

- (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 565

- (Exam Topic 12)

Which of the following adds end-to-end security inside a Layer 2 Tunneling Protocol (L2TP) Internet Protocol Security (IPSec) connection?

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

Answer: B

NEW QUESTION 566

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 567

- (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 570

- (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 574

- (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 579

- (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 581

- (Exam Topic 12)

Which of the following restricts the ability of an individual to carry out all the steps of a particular process?

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

Answer: B

NEW QUESTION 585

- (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 586

- (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 589

- (Exam Topic 12)

The PRIMARY purpose of accreditation is to:

- A. comply with applicable laws and regulations.
- B. allow senior management to make an informed decision regarding whether to accept the risk of operating the system.
- C. protect an organization's sensitive data.
- D. verify that all security controls have been implemented properly and are operating in the correct manner.

Answer: B

NEW QUESTION 592

- (Exam Topic 12)

Which of the following media sanitization techniques is MOST likely to be effective for an organization using public cloud services?

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

Answer: B

NEW QUESTION 593

- (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 594

- (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 597

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 601

- (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 602

- (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 604

- (Exam Topic 12)

Which of the following would BEST describe the role directly responsible for data within an organization?

- A. Data custodian
- B. Information owner
- C. Database administrator
- D. Quality control

Answer: A

NEW QUESTION 608

- (Exam Topic 12)

At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

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

Answer: C

NEW QUESTION 609

- (Exam Topic 12)

How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

- A. Examines log messages or other indications on the system.
- B. Monitors alarms sent to the system administrator
- C. Matches traffic patterns to virus signature files
- D. Examines the Access Control List (ACL)

Answer: C

NEW QUESTION 612

- (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 615

- (Exam Topic 12)

An employee of a retail company has been granted an extended leave of absence by Human Resources (HR). This information has been formally communicated to the access provisioning team. Which of the following is the BEST action to take?

- A. Revoke access temporarily.
- B. Block user access and delete user account after six months.
- C. Block access to the offices immediately.
- D. Monitor account usage temporarily.

Answer: D

NEW QUESTION 619

- (Exam Topic 12)

Which of the following is the PRIMARY benefit of a formalized information classification program?

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

Answer: B

NEW QUESTION 620

- (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 624

- (Exam Topic 12)

Which of the following approaches is the MOST effective way to dispose of data on multiple hard drives?

- A. Delete every file on each drive.
- B. Destroy the partition table for each drive using the command line.
- C. Degauss each drive individually.
- D. Perform multiple passes on each drive using approved formatting methods.

Answer: D

NEW QUESTION 627

- (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 632

- (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 636

- (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 637

- (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 639

- (Exam Topic 12)

When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?

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

Answer: D

NEW QUESTION 640

- (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 641

- (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 646

- (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 651

- (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 655

- (Exam Topic 12)

Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?

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

Answer: C

NEW QUESTION 658

- (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 661

- (Exam Topic 12)

Which of the following is the PRIMARY reason to perform regular vulnerability scanning of an organization network?

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

Answer: B

NEW QUESTION 662

- (Exam Topic 13)

Which one of the following data integrity models assumes a lattice of integrity levels?

- A. Take-Grant
- B. Biba
- C. Harrison-Ruzzo

D. Bell-LaPadula

Answer: B

NEW QUESTION 664

- (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 665

- (Exam Topic 13)

Which of the following steps should be performed FIRST when purchasing Commercial Off-The-Shelf (COTS) software?

- A. undergo a security assessment as part of authorization process
- B. establish a risk management strategy
- C. harden the hosting server, and perform hosting and application vulnerability scans
- D. establish policies and procedures on system and services acquisition

Answer: D

NEW QUESTION 667

- (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 670

- (Exam Topic 13)

Which of the following is the MOST important security goal when performing application interface testing?

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

Answer: B

NEW QUESTION 674

- (Exam Topic 13)

An organization's security policy delegates to the data owner the ability to assign which user roles have access to a particular resource. What type of authorization mechanism is being used?

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

Answer: A

NEW QUESTION 679

- (Exam Topic 13)

Due to system constraints, a group of system administrators must share a high-level access set of credentials. Which of the following would be MOST appropriate to implement?

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

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 680

- (Exam Topic 13)

Who is responsible for the protection of information when it is shared with or provided to other organizations?

- A. Systems owner
- B. Authorizing Official (AO)
- C. Information owner
- D. Security officer

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 685

- (Exam Topic 13)

What protocol is often used between gateway hosts on the Internet?

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

Answer: B

NEW QUESTION 686

- (Exam Topic 13)

As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

- A. Use a web scanner to scan for vulnerabilities within the website.
- B. Perform a code review to ensure that the database references are properly addressed.
- C. Establish a secure connection to the web server to validate that only the approved ports are open.
- D. Enter only numbers in the web form and verify that the website prompts the user to enter a valid input.

Answer: D

NEW QUESTION 687

- (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 688

- (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 693

- (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 698

- (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 701

- (Exam Topic 13)

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

<u>Security Engineering Term</u>	<u>Definition</u>
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment	The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment	The method used to identify feasible security risk mitigation options and plans.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

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

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

NEW QUESTION 706

- (Exam Topic 13)

Which of the following could be considered the MOST significant security challenge when adopting DevOps practices compared to a more traditional control framework?

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

Answer: B

NEW QUESTION 710

- (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 712

- (Exam Topic 13)

Which factors **MUST** be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?

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

Answer: A

NEW QUESTION 713

- (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 718

- (Exam Topic 13)

A security practitioner is tasked with securing the organization's Wireless Access Points (WAP). Which of these is the **MOST** effective way of restricting this environment to authorized users?

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

Answer: D

NEW QUESTION 721

- (Exam Topic 13)

What is the **MAIN** purpose of a change management policy?

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

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 725

- (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 730

- (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 733

- (Exam Topic 13)

Which of the following methods of suppressing a fire is environmentally friendly and the **MOST** appropriate for a data center?

- A. Inert gas fire suppression system

- B. Halon gas fire suppression system
- C. Dry-pipe sprinklers
- D. Wet-pipe sprinklers

Answer: C

NEW QUESTION 735

- (Exam Topic 13)

What are the steps of a risk assessment?

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

Answer: A

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 737

- (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 740

- (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 741

- (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 744

- (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 749

- (Exam Topic 13)

Which of the following is considered a secure coding practice?

- A. Use concurrent access for shared variables and resources
- B. Use checksums to verify the integrity of libraries
- C. Use new code for common tasks
- D. Use dynamic execution functions to pass user supplied data

Answer: B

NEW QUESTION 751

- (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 754

- (Exam Topic 13)

Match the functional roles in an external audit to their responsibilities. Drag each role on the left to its corresponding responsibility on the right. Select and Place:

<u>Role</u>		<u>Responsibility</u>
Executive management	<input type="text"/>	Approve audit budget and resource allocation.
Audit committee	<input type="text"/>	Provide audit oversight.
Compliance officer	<input type="text"/>	Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor	<input type="text"/>	Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<u>Role</u>		<u>Responsibility</u>
Executive management	Executive management	Approve audit budget and resource allocation.
Audit committee	Audit committee	Provide audit oversight.
Compliance officer	External auditor	Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor	Compliance officer	Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

NEW QUESTION 755

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 759

- (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 763

- (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 764

- (Exam Topic 13)

An Information Technology (IT) professional attends a cybersecurity seminar on current incident response methodologies. What code of ethics canon is being observed?

- A. Provide diligent and competent service to principals
- B. Protect society, the commonwealth, and the infrastructure
- C. Advance and protect the profession
- D. Act honorable, honesty, justly, responsibly, and legally

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 769

- (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 772

- (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 776

- (Exam Topic 13)

A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report. In which phase of the assessment was this error **MOST** likely made?

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

Answer: A

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 780

- (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 783

- (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 788

- (Exam Topic 13)

An organization adopts a new firewall hardening standard. How can the security professional verify that the technical staff correct implemented the new standard?

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

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 790

- (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 791

- (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 792

- (Exam Topic 13)

Which of the following alarm systems is recommended to detect intrusions through windows in a high-noise, occupied environment?

- A. Acoustic sensor
- B. Motion sensor
- C. Shock sensor
- D. Photoelectric sensor

Answer: C

NEW QUESTION 795

- (Exam Topic 13)

Which of the following is the MOST important part of an awareness and training plan to prepare employees for emergency situations?

- A. Having emergency contacts established for the general employee population to get information
- B. Conducting business continuity and disaster recovery training for those who have a direct role in the recovery
- C. Designing business continuity and disaster recovery training programs for different audiences
- D. Publishing a corporate business continuity and disaster recovery plan on the corporate website

Answer: C

NEW QUESTION 800

- (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.

Actions

- Define the perimeter.
- Identify the vulnerability.
- Assess the risk.
- Determine the actions.

Steps

- Step 1
- Step 2
- Step 3
- Step 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

- Define the perimeter.
- Identify the vulnerability.
- Assess the risk.
- Determine the actions.

Steps

- Identify the vulnerability.
- Define the perimeter.
- Assess the risk.
- Determine the actions.
- Step 1
- Step 2
- Step 3
- Step 4

NEW QUESTION 802

- (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 807

- (Exam Topic 13)

Which of the following is the BEST metric to obtain when gaining support for an Identify and Access Management (IAM) solution?

- A. Application connection successes resulting in data leakage
- B. Administrative costs for restoring systems after connection failure
- C. Employee system timeouts from implementing wrong limits
- D. Help desk costs required to support password reset requests

Answer: D

NEW QUESTION 809

- (Exam Topic 13)

Which of the following management process allows ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

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

Answer: A

NEW QUESTION 810

- (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 811

- (Exam Topic 13)

Which one of the following considerations has the LEAST impact when considering transmission security?

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

Answer: C

NEW QUESTION 816

- (Exam Topic 13)

Which of the following techniques is known to be effective in spotting resource exhaustion problems, especially with resources such as processes, memory, and connections?

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

Answer: A

NEW QUESTION 821

.....

Relate Links

100% Pass Your CISSP Exam with Exambible Prep Materials

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

Contact us

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

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