



ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

- (Exam Topic 1)

An important principle of defense in depth is that achieving information security requires a balanced focus on which PRIMARY elements?

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

Answer: C

NEW QUESTION 2

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 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)

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 5

- (Exam Topic 3)

Which of the following mobile code security models relies only on trust?

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

Answer: A

NEW QUESTION 6

- (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 7

- (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 8

- (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 9

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 10

- (Exam Topic 4)

An input validation and exception handling vulnerability has been discovered on a critical web-based system. Which of the following is MOST suited to quickly implement a control?

- A. Add a new rule to the application layer firewall
- B. Block access to the service
- C. Install an Intrusion Detection System (IDS)
- D. Patch the application source code

Answer: A

NEW QUESTION 10

- (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 14

- (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 16

- (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 17

- (Exam Topic 6)

Which of the following is a PRIMARY benefit of using a formalized security testing report format and structure?

- A. Executive audiences will understand the outcomes of testing and most appropriate next steps for corrective actions to be taken

- B. Technical teams will understand the testing objectives, testing strategies applied, and business risk associated with each vulnerability
- C. Management teams will understand the testing objectives and reputational risk to the organization
- D. Technical and management teams will better understand the testing objectives, results of each test phase, and potential impact levels

Answer: D

NEW QUESTION 18

- (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 20

- (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 23

- (Exam Topic 7)

Which of the following is a PRIMARY advantage of using a third-party identity service?

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

Answer: D

NEW QUESTION 25

- (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 29

- (Exam Topic 7)

An organization is found lacking the ability to properly establish performance indicators for its Web hosting solution during an audit. What would be the MOST probable cause?

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

Answer: D

NEW QUESTION 30

- (Exam Topic 7)

Which of the following types of business continuity tests includes assessment of resilience to internal and external risks without endangering live operations?

- A. Walkthrough
- B. Simulation
- C. Parallel
- D. White box

Answer: B

NEW QUESTION 35

- (Exam Topic 7)

Which of the following is the FIRST step in the incident response process?

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

Answer: D

NEW QUESTION 38

- (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 39

- (Exam Topic 8)

A Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. The program is not working as expected. What is the MOST probable security feature of Java preventing the program from operating as intended?

- A. Least privilege
- B. Privilege escalation
- C. Defense in depth
- D. Privilege bracketing

Answer: A

NEW QUESTION 40

- (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 44

- (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 48

- (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 53

- (Exam Topic 9)

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

- A. Immediately document the finding and report to senior management.
- B. Use system privileges to alter the permissions to secure the server

- C. Continue the testing to its completion and then inform IT management
- D. Terminate the penetration test and pass the finding to the server management team

Answer: A

NEW QUESTION 57

- (Exam Topic 9)

Which of the following **MUST** be part of a contract to support electronic discovery of data stored in a cloud environment?

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

Answer: D

NEW QUESTION 61

- (Exam Topic 9)

Which of the following is a limitation of the Common Vulnerability Scoring System (CVSS) as it relates to conducting code review?

- A. It has normalized severity ratings.
- B. It has many worksheets and practices to implement.
- C. It aims to calculate the risk of published vulnerabilities.
- D. It requires a robust risk management framework to be put in place.

Answer: C

NEW QUESTION 63

- (Exam Topic 9)

A vulnerability test on an Information System (IS) is conducted to

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

Answer: C

NEW QUESTION 66

- (Exam Topic 9)

In the area of disaster planning and recovery, what strategy entails the presentation of information about the plan?

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

Answer: A

NEW QUESTION 70

- (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 71

- (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 76

- (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 80

- (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 82

- (Exam Topic 9)

Which of the following is an authentication protocol in which a new random number is generated uniquely for each login session?

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

Answer: A

NEW QUESTION 84

- (Exam Topic 9)

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 85

- (Exam Topic 9)

In a financial institution, who has the responsibility for assigning the classification to a piece of information?

- A. Chief Financial Officer (CFO)
- B. Chief Information Security Officer (CISO)
- C. Originator or nominated owner of the information
- D. Department head responsible for ensuring the protection of the information

Answer: C

NEW QUESTION 90

- (Exam Topic 9)

When building a data center, site location and construction factors that increase the level of vulnerability to physical threats include

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

Answer: D

NEW QUESTION 93

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 94

- (Exam Topic 9)

The PRIMARY purpose of a security awareness program is to

- A. ensure that everyone understands the organization's policies and procedures.
- B. communicate that access to information will be granted on a need-to-know basis.
- C. warn all users that access to all systems will be monitored on a daily basis.
- D. comply with regulations related to data and information protection.

Answer: A

NEW QUESTION 95

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 98

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 100

- (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 105

- (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 108

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 112

- (Exam Topic 9)

The FIRST step in building a firewall is to

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

Answer: D

NEW QUESTION 116

- (Exam Topic 9)

Which one of the following describes granularity?

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

Answer: D

NEW QUESTION 118

- (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 123

- (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 127

- (Exam Topic 9)

A security consultant has been asked to research an organization's legal obligations to protect privacy-related information. What kind of reading material is MOST relevant to this project?

- A. The organization's current security policies concerning privacy issues
- B. Privacy-related regulations enforced by governing bodies applicable to the organization
- C. Privacy best practices published by recognized security standards organizations
- D. Organizational procedures designed to protect privacy information

Answer: B

NEW QUESTION 129

- (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 134

- (Exam Topic 9)

Which type of control recognizes that a transaction amount is excessive in accordance with corporate policy?

- A. Detection
- B. Prevention
- C. Investigation
- D. Correction

Answer: A

NEW QUESTION 139

- (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 140

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 144

- (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 146

- (Exam Topic 9)

What is the ultimate objective of information classification?

- A. To assign responsibility for mitigating the risk to vulnerable systems
- B. To ensure that information assets receive an appropriate level of protection
- C. To recognize that the value of any item of information may change over time
- D. To recognize the optimal number of classification categories and the benefits to be gained from their use

Answer: B

NEW QUESTION 149

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 150

- (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 154

- (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 157

- (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 160

- (Exam Topic 9)

Who must approve modifications to an organization's production infrastructure configuration?

- A. Technical management
- B. Change control board
- C. System operations
- D. System users

Answer: B

NEW QUESTION 161

- (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 164

- (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 166

- (Exam Topic 9)

Which one of the following affects the classification of data?

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

Answer: A

NEW QUESTION 169

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 171

- (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 173

- (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 176

- (Exam Topic 9)

At a MINIMUM, a formal review of any Disaster Recovery Plan (DRP) should be conducted

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

Answer: C

NEW QUESTION 179

- (Exam Topic 10)

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

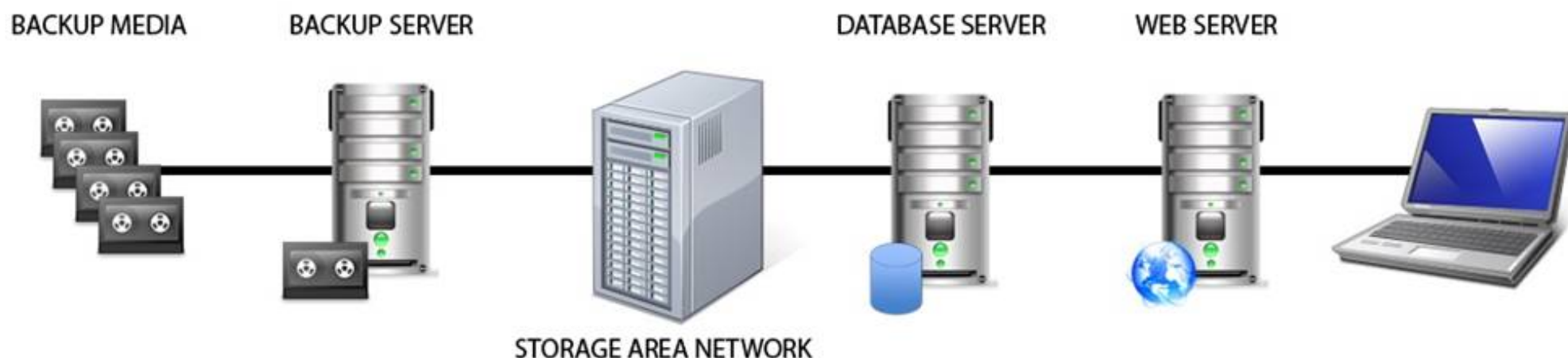
- A. Experience in the industry
- B. Definition of security profiles
- C. Human resource planning efforts
- D. Procedures in systems development

Answer: D

NEW QUESTION 180

- (Exam Topic 10)

Identify the component that MOST likely lacks digital accountability related to information access. Click on the correct device in the image below.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Backup Media

Reference: Official (ISC)2 Guide to the CISSP CBK, Third Edition page 1029

NEW QUESTION 185

- (Exam Topic 10)

Which of the following is the BEST reason to review audit logs periodically?

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

Answer: C

NEW QUESTION 190

- (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 193

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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 195

- (Exam Topic 10)

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

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

Answer: A

NEW QUESTION 197

- (Exam Topic 10)

What physical characteristic does a retinal scan biometric device measure?

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

Answer: C

NEW QUESTION 200

- (Exam Topic 10)

Refer to the information below to answer the question.

An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration

functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.

Which of the following will be the PRIMARY security concern as staff is released from the organization?

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

Answer: B

NEW QUESTION 204

- (Exam Topic 10)

If an attacker in a SYN flood attack uses someone else's valid host address as the source address, the system under attack will send a large number of Synchronize/Acknowledge (SYN/ACK) packets to the

- A. default gateway.
- B. attacker's address.
- C. local interface being attacked.
- D. specified source address.

Answer: D

NEW QUESTION 207

- (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 210

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 211

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 215

- (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 220

- (Exam Topic 10)

Multi-Factor Authentication (MFA) is necessary in many systems given common types of password attacks. Which of the following is a correct list of password attacks?

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

Answer: B

NEW QUESTION 221

- (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 224

- (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 227

- (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 232

- (Exam Topic 10)

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

Area		Technolog
Facilities		Encryption
Devices		Window
Information		Firewall
Systems		Authenticatio

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Area		Technolog
Facilities	Information	Encryption
Devices	Facilities	Window
Information	Devices	Firewall
Svstems	Systems	Authenticatio

NEW QUESTION 234

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

Answer: A

NEW QUESTION 239

- (Exam Topic 10)

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

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

D. SAML tokens contain user information.

Answer: A

NEW QUESTION 242

- (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 245

- (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 250

- (Exam Topic 10)

During the procurement of a new information system, it was determined that some of the security requirements were not addressed in the system specification.

Which of the following is the MOST likely reason for this?

- A. The procurement officer lacks technical knowledge.
- B. The security requirements have changed during the procurement process.
- C. There were no security professionals in the vendor's bidding team.
- D. The description of the security requirements was insufficient.

Answer: D

NEW QUESTION 254

- (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 257

- (Exam Topic 10)

Which of the following is the MOST crucial for a successful audit plan?

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

Answer: A

NEW QUESTION 262

- (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 MOST likely allow the organization to keep risk at an acceptable level?

- A. Increasing the amount of audits performed by third parties
- B. Removing privileged accounts from operational staff
- C. Assigning privileged functions to appropriate staff
- D. Separating the security function into distinct roles

Answer: C

NEW QUESTION 265

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 270

- (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 273

- (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 278

- (Exam Topic 10)

The use of proximity card to gain access to a building is an example of what type of security control?

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

Answer: C

NEW QUESTION 283

- (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 is the BEST reason for the organization to pursue a plan to mitigate client-based attacks?

- A. Client privilege administration is inherently weaker than server privilege administration.
- B. Client hardening and management is easier on clients than on servers.
- C. Client-based attacks are more common and easier to exploit than server and network based attacks.
- D. Client-based attacks have higher financial impact.

Answer: C

NEW QUESTION 287

- (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. In addition to authentication at the start of the user session, best practice would require re-authentication

- A. periodically during a session.
- B. for each business process.
- C. at system sign-off.
- D. after a period of inactivity.

Answer: D

NEW QUESTION 288

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

In a Bell-LaPadula system, which user has the MOST restrictions when writing data to any of the four files?

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

Answer: D

NEW QUESTION 289

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

Answer: D

NEW QUESTION 292

- (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 295

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 300

- (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 305

- (Exam Topic 10)

What is the PRIMARY reason for ethics awareness and related policy implementation?

- A. It affects the workflow of an organization.
- B. It affects the reputation of an organization.
- C. It affects the retention rate of employees.
- D. It affects the morale of the employees.

Answer: B

NEW QUESTION 308

- (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 312

- (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 313

- (Exam Topic 10)

Refer to the information below to answer the question.

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

Aside from the potential records which may have been viewed, which of the following should be the PRIMARY concern regarding the database information?

- A. Unauthorized database changes
- B. Integrity of security logs
- C. Availability of the database
- D. Confidentiality of the incident

Answer: A

NEW QUESTION 314

- (Exam Topic 11)

Which of the following BEST describes the purpose of performing security certification?

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

Answer: B

NEW QUESTION 317

- (Exam Topic 11)

If an identification process using a biometric system detects a 100% match between a presented template and a stored template, what is the interpretation of this

result?

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

Answer: B

NEW QUESTION 318

- (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 323

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 328

- (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 333

- (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 338

- (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 342

- (Exam Topic 11)

Regarding asset security and appropriate retention, which of the following INITIAL top three areas are important to focus on?

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

Answer: A

NEW QUESTION 346

- (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 350

- (Exam Topic 11)

Which of the following is most helpful in applying the principle of LEAST privilege?

- A. Establishing a sandboxing environment
- B. Setting up a Virtual Private Network (VPN) tunnel
- C. Monitoring and reviewing privileged sessions
- D. Introducing a job rotation program

Answer: A

NEW QUESTION 352

- (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 356

- (Exam Topic 11)

Which of the following roles has the obligation to ensure that a third party provider is capable of processing and handling data in a secure manner and meeting the standards set by the organization?

- A. Data Custodian
- B. Data Owner
- C. Data Creator
- D. Data User

Answer: B

NEW QUESTION 358

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 363

- (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 366

- (Exam Topic 11)

An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?

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

Answer: A

NEW QUESTION 369

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 371

- (Exam Topic 11)

Retaining system logs for six months or longer can be valuable for what activities?

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

Answer: B

NEW QUESTION 374

- (Exam Topic 11)

The BEST example of the concept of "something that a user has" when providing an authorized user access to a computing system is

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

Answer: B

NEW QUESTION 376

- (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?

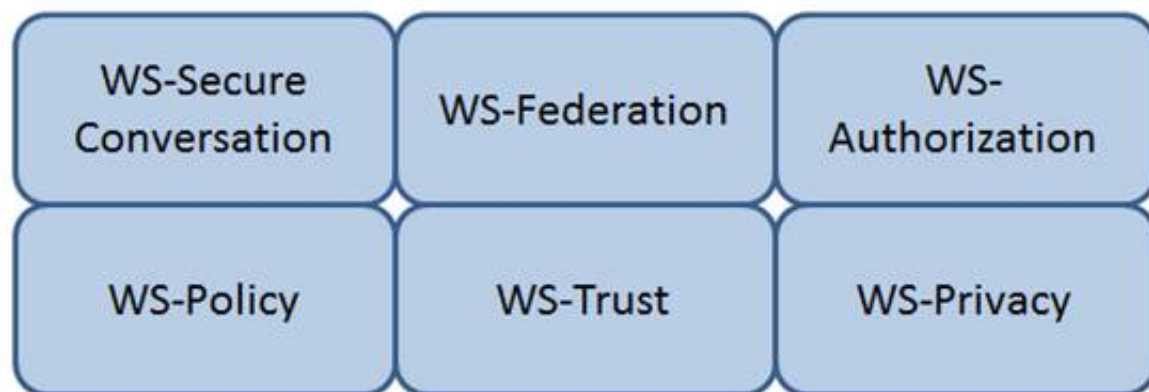
- A. Acceptance of risk by the authorizing official
- B. Remediation of vulnerabilities
- C. Adoption of standardized policies and procedures
- D. Approval of the System Security Plan (SSP)

Answer: A

NEW QUESTION 381

- (Exam Topic 11)

Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

WS-Federation

Reference: Java Web Services: Up and Running" By Martin Kalin page 228

NEW QUESTION 386

- (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 387

- (Exam Topic 11)

Which methodology is recommended for penetration testing to be effective in the development phase of the life-cycle process?

- A. White-box testing
- B. Software fuzz testing
- C. Black-box testing
- D. Visual testing

Answer: A

NEW QUESTION 388

- (Exam Topic 11)

The PRIMARY characteristic of a Distributed Denial of Service (DDoS) attack is that it

- A. exploits weak authentication to penetrate networks.
- B. can be detected with signature analysis.
- C. looks like normal network activity.
- D. is commonly confused with viruses or worms.

Answer: C

NEW QUESTION 391

- (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 396

- (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 399

- (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 401

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 405

- (Exam Topic 11)

Which of the following controls is the FIRST step in protecting privacy in an information system?

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

Answer: B

NEW QUESTION 407

- (Exam Topic 11)

Software Code signing is used as a method of verifying what security concept?

- A. Integrity
- B. Confidentiality
- C. Availability
- D. Access Control

Answer: A

NEW QUESTION 410

- (Exam Topic 11)

Data leakage of sensitive information is MOST often concealed by which of the following?

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

Answer: A

NEW QUESTION 415

- (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 419

- (Exam Topic 11)

An organization has decided to contract with a cloud-based service provider to leverage their identity as a service offering. They will use Open Authentication (OAuth) 2.0 to authenticate external users to the organization's services.

As part of the authentication process, which of the following must the end user provide?

- A. An access token
- B. A username and password
- C. A username
- D. A password

Answer: A

NEW QUESTION 422

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 423

- (Exam Topic 11)

Which of the following is the MOST effective method of mitigating data theft from an active user workstation?

- A. Implement full-disk encryption
- B. Enable multifactor authentication
- C. Deploy file integrity checkers
- D. Disable use of portable devices

Answer: D

NEW QUESTION 426

- (Exam Topic 11)

Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic media.

Sequence		Method
1		Overwriting
2		Degaussing
3		Destruction
4		Deleting

A. Mastered

B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 430

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 433

- (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 434

- (Exam Topic 11)

What type of test assesses a Disaster Recovery (DR) plan using realistic disaster scenarios while maintaining minimal impact to business operations?

- A. Parallel
- B. Walkthrough
- C. Simulation
- D. Tabletop

Answer: C

NEW QUESTION 439

- (Exam Topic 11)

A network scan found 50% of the systems with one or more critical vulnerabilities. Which of the following represents the BEST action?

- A. Assess vulnerability risk and program effectiveness.
- B. Assess vulnerability risk and business impact.
- C. Disconnect all systems with critical vulnerabilities.
- D. Disconnect systems with the most number of vulnerabilities.

Answer: B

NEW QUESTION 441

- (Exam Topic 11)

Which of the following questions can be answered using user and group entitlement reporting?

- A. When a particular file was last accessed by a user
- B. Change control activities for a particular group of users
- C. The number of failed login attempts for a particular user
- D. Where does a particular user have access within the network

Answer: D

NEW QUESTION 443

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 447

- (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 452

- (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 454

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 457

- (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 459

- (Exam Topic 11)

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

- A. They should be recycled to save energy.
- B. They should be recycled according to NIST SP 800-88.

- C. They should be inspected and sanitized following the organizational policy.
- D. They should be inspected and categorized properly to sell them for reuse.

Answer: C

NEW QUESTION 463

- (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 464

- (Exam Topic 11)

The 802.1x standard provides a framework for what?

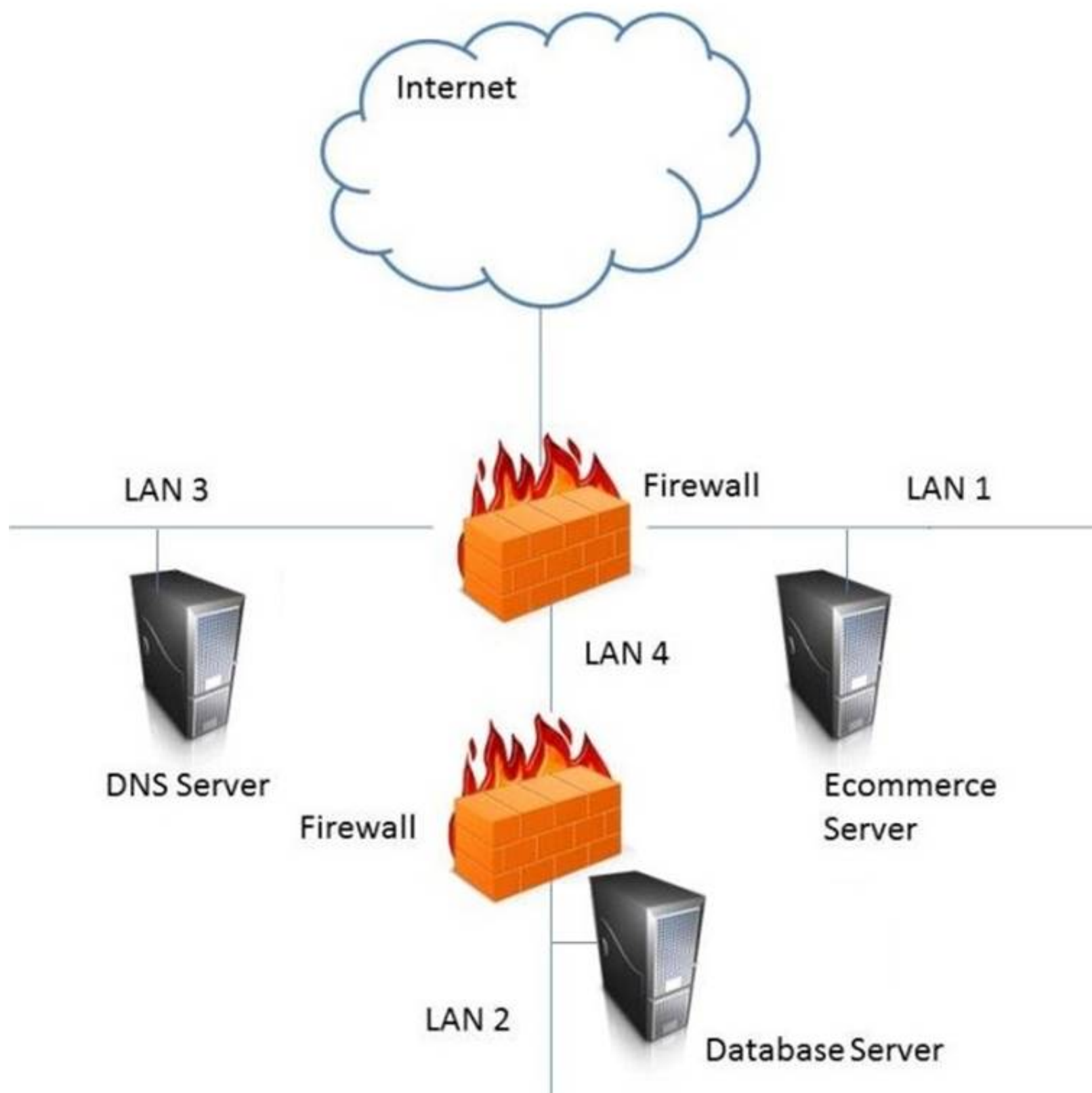
- A. Network authentication for only wireless networks
- B. Network authentication for wired and wireless networks
- C. Wireless encryption using the Advanced Encryption Standard (AES)
- D. Wireless network encryption using Secure Sockets Layer (SSL)

Answer: B

NEW QUESTION 469

- (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 473

- (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 477

- (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 480

- (Exam Topic 11)

By carefully aligning the pins in the lock, which of the following defines the opening of a mechanical lock without the proper key?

- A. Lock pinging
- B. Lock picking
- C. Lock bumping
- D. Lock bricking

Answer: B

NEW QUESTION 484

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 486

- (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 491

- (Exam Topic 12)

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

- A. Transport
- B. Data link

- C. Network
- D. Application

Answer: D

NEW QUESTION 493

- (Exam Topic 12)
As a best practice, the Security Assessment Report (SAR) should include which of the following sections?

- A. Data classification policy
- B. Software and hardware inventory
- C. Remediation recommendations
- D. Names of participants

Answer: B

NEW QUESTION 498

- (Exam Topic 12)
What is the difference between media marking and media labeling?

- A. Media marking refers to the use of human-readable security attributes, while media labeling refers to the use of security attributes in internal data structures.
- B. Media labeling refers to the use of human-readable security attributes, while media marking refers to the use of security attributes in internal data structures.
- C. Media labeling refers to security attributes required by public policy/law, while media marking refers to security required by internal organizational policy.
- D. Media marking refers to security attributes required by public policy/law, while media labeling refers to security attributes required by internal organizational policy.

Answer: D

NEW QUESTION 503

- (Exam Topic 12)
Which of the following is a remote access protocol that uses a static authentication?

- A. Point-to-Point Tunneling Protocol (PPTP)
- B. Routing Information Protocol (RIP)
- C. Password Authentication Protocol (PAP)
- D. Challenge Handshake Authentication Protocol (CHAP)

Answer: C

NEW QUESTION 504

- (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 508

- (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 513

- (Exam Topic 12)

Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

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

Answer: A

NEW QUESTION 516

- (Exam Topic 12)

A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

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

Answer: A

NEW QUESTION 519

- (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 520

- (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 521

- (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 523

- (Exam Topic 12)

Match the types of e-authentication tokens to their description.

Drag each e-authentication token on the left to its corresponding description on the right.

E-Authentication Token		Description
Memorized Secret Token		A physical or electronic token that stores a set of secrets between the claimant and the credential service provider
Out-of-Band Token		A physical token that is uniquely addressable and can receive a verifier-selected secret for one-time use
Look-up Secret Token		A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process
Pre-registered Knowledge Token		A secret shared between the subscriber and credential service provider that is typically character strings

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

Out-of-Band Token - A physical token that is uniquely addressable and can receive a verifier-selected secret for one-time use

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

Memorized Secret Token - A secret shared between the subscriber and credential service provider that is typically character strings

NEW QUESTION 527

- (Exam Topic 12)

What type of wireless network attack BEST describes an Electromagnetic Pulse (EMP) attack?

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

Answer: B

NEW QUESTION 532

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 537

- (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 540

- (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 545

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 546

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 549

- (Exam Topic 12)

In general, servers that are facing the Internet should be placed in a demilitarized zone (DMZ). What is MAIN purpose of the DMZ?

- A. Reduced risk to internal systems.
- B. Prepare the server for potential attacks.
- C. Mitigate the risk associated with the exposed server.
- D. Bypass the need for a firewall.

Answer: A

NEW QUESTION 553

- (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 556

- (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 558

- (Exam Topic 12)

What is the BEST way to encrypt web application communications?

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

Answer: D

NEW QUESTION 562

- (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 563

- (Exam Topic 12)

Which of the following BEST represents the concept of least privilege?

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

Answer: A

NEW QUESTION 568

- (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 571

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 572

- (Exam Topic 12)

What is an advantage of Elliptic Curve Cryptography (ECC)?

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

Answer: C

NEW QUESTION 574

- (Exam Topic 12)

Which of the following is the MOST important consideration when developing a Disaster Recovery Plan (DRP)?

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

Answer: C

NEW QUESTION 577

- (Exam Topic 12)

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

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

Answer: C

NEW QUESTION 581

- (Exam Topic 12)

A security architect plans to reference a Mandatory Access Control (MAC) model for implementation. This indicates that which of the following properties are being prioritized?

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

Answer: C

NEW QUESTION 583

- (Exam Topic 12)

Which of the following is a characteristic of the initialization vector when using Data Encryption Standard (DES)?

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

Answer: B

NEW QUESTION 587

- (Exam Topic 12)

From a cryptographic perspective, the service of non-repudiation includes which of the following features?

- A. Validity of digital certificates
- B. Validity of the authorization rules
- C. Proof of authenticity of the message
- D. Proof of integrity of the message

Answer: C

NEW QUESTION 588

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 589

- (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 594

- (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 598

- (Exam Topic 12)

During the Security Assessment and Authorization process, what is the PRIMARY purpose for conducting a hardware and software inventory?

- A. Calculate the value of assets being accredited.
- B. Create a list to include in the Security Assessment and Authorization package.
- C. Identify obsolete hardware and software.
- D. Define the boundaries of the information system.

Answer: A

NEW QUESTION 602

- (Exam Topic 12)

Which of the following countermeasures is the MOST effective in defending against a social engineering attack?

- A. Mandating security policy acceptance
- B. Changing individual behavior
- C. Evaluating security awareness training
- D. Filtering malicious e-mail content

Answer: C

NEW QUESTION 604

- (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 605

- (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 607

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 609

- (Exam Topic 13)

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

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

Answer: B

NEW QUESTION 612

- (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 615

- (Exam Topic 13)

What is the MAIN goal of information security awareness and training?

- A. To inform users of the latest malware threats
- B. To inform users of information assurance responsibilities
- C. To comply with the organization information security policy

D. To prepare students for certification

Answer: B

NEW QUESTION 618

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 620

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 623

- (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 626

- (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 631

- (Exam Topic 13)

An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject's data?

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

Answer: C

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 633

- (Exam Topic 13)

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

Security Engineering Term

Definition

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 637

- (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 642

- (Exam Topic 13)

Which of the following is the MOST efficient mechanism to account for all staff during a speedy nonemergency evacuation from a large security facility?

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

Answer: B

Explanation:

Section: Security Operations

NEW QUESTION 646

- (Exam Topic 13)

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

- A. An internal audit is typically shorter in duration than an external audit.

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

Answer: D

NEW QUESTION 647

- (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 651

- (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 656

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 659

- (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 661

- (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 664

- (Exam Topic 13)

Which of the following is a responsibility of the information owner?

- A. Ensure that users and personnel complete the required security training to access the Information System (IS)
- B. Defining proper access to the Information System (IS), including privileges or access rights
- C. Managing identification, implementation, and assessment of common security controls

D. Ensuring the Information System (IS) is operated according to agreed upon security requirements

Answer: C

NEW QUESTION 665

- (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 668

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 669

- (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 673

- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 677

- (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 680

- (Exam Topic 13)

After following the processes defined within the change management plan, a super user has upgraded a device within an Information system. What step would be taken to ensure that the upgrade did NOT affect the network security posture?

- A. Conduct an Assessment and Authorization (A&A)
- B. Conduct a security impact analysis
- C. Review the results of the most recent vulnerability scan

D. Conduct a gap analysis with the baseline configuration

Answer: B

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 682

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 685

- (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 688

- (Exam Topic 13)

What does a Synchronous (SYN) flood attack do?

- A. Forces Transmission Control Protocol /Internet Protocol (TCP/IP) connections into a reset state
- B. Establishes many new Transmission Control Protocol / Internet Protocol (TCP/IP) connections
- C. Empties the queue of pending Transmission Control Protocol /Internet Protocol (TCP/IP) requests
- D. Exceeds the limits for new Transmission Control Protocol /Internet Protocol (TCP/IP) connections

Answer: B

NEW QUESTION 689

- (Exam Topic 13)

Who has the PRIMARY responsibility to ensure that security objectives are aligned with organization goals?

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

Answer: C

NEW QUESTION 694

- (Exam Topic 13)

An organization has discovered that users are visiting unauthorized websites using anonymous proxies. Which of the following is the BEST way to prevent future occurrences?

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

Answer: C

NEW QUESTION 695

- (Exam Topic 13)

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

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

Answer: C

NEW QUESTION 696

- (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 698

- (Exam Topic 13)

Which of the following is the GREATEST benefit of implementing a Role Based Access Control (RBAC) system?

- A. Integration using Lightweight Directory Access Protocol (LDAP)
- B. Form-based user registration process
- C. Integration with the organizations Human Resources (HR) system
- D. A considerably simpler provisioning process

Answer: D

NEW QUESTION 703

- (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 704

- (Exam Topic 13)

A company receives an email threat informing of an Imminent Distributed Denial of Service (DDoS) attack targeting its web application, unless ransom is paid. Which of the following techniques BEST addresses that threat?

- A. Deploying load balancers to distribute inbound traffic across multiple data centers
- B. Set Up Web Application Firewalls (WAFs) to filter out malicious traffic
- C. Implementing reverse web-proxies to validate each new inbound connection
- D. Coordinate with and utilize capabilities within Internet Service Provider (ISP)

Answer: D

NEW QUESTION 707

- (Exam Topic 13)

Attack trees are MOST useful for which of the following?

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

Answer: A

NEW QUESTION 708

- (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 713

- (Exam Topic 13)

The MAIN use of Layer 2 Tunneling Protocol (L2TP) is to tunnel data

- A. through a firewall at the Session layer
- B. through a firewall at the Transport layer
- C. in the Point-to-Point Protocol (PPP)
- D. in the Payload Compression Protocol (PCP)

Answer: C

NEW QUESTION 714

- (Exam Topic 13)

Which of the following is BEST achieved through the use of eXtensible Access Markup Language (XACML)?

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

Answer: D

NEW QUESTION 717

- (Exam Topic 13)

Which of the following provides the MOST comprehensive filtering of Peer-to-Peer (P2P) traffic?

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

Answer: A

NEW QUESTION 721

- (Exam Topic 13)

A post-implementation review has identified that the Voice Over Internet Protocol (VoIP) system was designed to have gratuitous Address Resolution Protocol (ARP) disabled.

Why did the network architect likely design the VoIP system with gratuitous ARP disabled?

- A. Gratuitous ARP requires the use of Virtual Local Area Network (VLAN) 1.
- B. Gratuitous ARP requires the use of insecure layer 3 protocols.
- C. Gratuitous ARP requires the likelihood of a successful brute-force attack on the phone.
- D. Gratuitous ARP requires the risk of a Man-in-the-Middle (MITM) attack.

Answer: D

NEW QUESTION 725

- (Exam Topic 13)

Access to which of the following is required to validate web session management?

- A. Log timestamp
- B. Live session traffic
- C. Session state variables
- D. Test scripts

Answer: C

NEW QUESTION 728

.....

Relate Links

100% Pass Your CISSP Exam with Examible 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/>