



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)

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

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

Answer: B

NEW QUESTION 2

- (Exam Topic 1)

Which of the following types of technologies would be the MOST cost-effective method to provide a reactive control for protecting personnel in public areas?

- A. Install mantraps at the building entrances
- B. Enclose the personnel entry area with polycarbonate plastic
- C. Supply a duress alarm for personnel exposed to the public
- D. Hire a guard to protect the public area

Answer: D

NEW QUESTION 3

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 4

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 5

- (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 6

- (Exam Topic 3)

The use of private and public encryption keys is fundamental in the implementation of which of the following?

- A. Diffie-Hellman algorithm
- B. Secure Sockets Layer (SSL)
- C. Advanced Encryption Standard (AES)
- D. Message Digest 5 (MD5)

Answer: A

NEW QUESTION 7

- (Exam Topic 3)

What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?

- A. Implementation Phase
- B. Initialization Phase
- C. Cancellation Phase
- D. Issued Phase

Answer: D

NEW QUESTION 8

- (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 9

- (Exam Topic 4)

In a Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which layer is responsible for negotiating and establishing a connection with another node?

- A. Transport layer
- B. Application layer
- C. Network layer
- D. Session layer

Answer: A

NEW QUESTION 10

- (Exam Topic 4)

Which of the following factors contributes to the weakness of Wired Equivalent Privacy (WEP) protocol?

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

Answer: A

NEW QUESTION 10

- (Exam Topic 5)

Which of the following BEST describes an access control method utilizing cryptographic keys derived from a smart card private key that is embedded within mobile devices?

- A. Derived credential
- B. Temporary security credential
- C. Mobile device credentialing service
- D. Digest authentication

Answer: A

NEW QUESTION 11

- (Exam Topic 6)

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

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

Answer: A

NEW QUESTION 12

- (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 14

- (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 16

- (Exam Topic 7)

What is the PRIMARY reason for implementing change management?

- A. Certify and approve releases to the environment
- B. Provide version rollbacks for system changes
- C. Ensure that all applications are approved
- D. Ensure accountability for changes to the environment

Answer: D

NEW QUESTION 20

- (Exam Topic 7)

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

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

Answer: C

NEW QUESTION 25

- (Exam Topic 8)

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

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

Answer: B

NEW QUESTION 28

- (Exam Topic 8)

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

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

Answer: C

NEW QUESTION 30

- (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 32

- (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 37

- (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 42

- (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 44

- (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 49

- (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 51

- (Exam Topic 9)

The key benefits of a signed and encrypted e-mail include

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

Answer: B

NEW QUESTION 54

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 57

- (Exam Topic 9)

Which layer of the Open Systems Interconnections (OSI) model implementation adds information concerning the logical connection between the sender and receiver?

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

Answer: C

NEW QUESTION 59

- (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 64

- (Exam Topic 9)

Which security action should be taken FIRST when computer personnel are terminated from their jobs?

- A. Remove their computer access
- B. Require them to turn in their badge
- C. Conduct an exit interview
- D. Reduce their physical access level to the facility

Answer: A

NEW QUESTION 68

- (Exam Topic 9)

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

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

Answer: B

NEW QUESTION 73

- (Exam Topic 9)

What security management control is MOST often broken by collusion?

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

Answer: B

NEW QUESTION 78

- (Exam Topic 9)

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

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

Answer: D

NEW QUESTION 80

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 82

- (Exam Topic 9)

The use of strong authentication, the encryption of Personally Identifiable Information (PII) on database servers, application security reviews, and the encryption of data transmitted across networks provide

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

Answer: B

NEW QUESTION 86

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 87

- (Exam Topic 9)

What principle requires that changes to the plaintext affect many parts of the ciphertext?

- A. Diffusion
- B. Encapsulation
- C. Obfuscation
- D. Permutation

Answer: A

NEW QUESTION 91

- (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 94

- (Exam Topic 9)

Which of the following is the FIRST step of a penetration test plan?

- A. Analyzing a network diagram of the target network
- B. Notifying the company's customers
- C. Obtaining the approval of the company's management
- D. Scheduling the penetration test during a period of least impact

Answer: C

NEW QUESTION 96

- (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 101

- (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 102

- (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 106

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 107

- (Exam Topic 9)

Why MUST a Kerberos server be well protected from unauthorized access?

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

Answer: A

NEW QUESTION 111

- (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 113

- (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 117

- (Exam Topic 9)

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

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

Answer: C

NEW QUESTION 122

- (Exam Topic 9)

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

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

Answer: A

NEW QUESTION 127

- (Exam Topic 9)

Which of the following BEST represents the principle of open design?

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

Answer: D

NEW QUESTION 132

- (Exam Topic 9)

Why must all users be positively identified prior to using multi-user computers?

- A. To provide access to system privileges
- B. To provide access to the operating system
- C. To ensure that unauthorized persons cannot access the computers
- D. To ensure that management knows what users are currently logged on

Answer: C

NEW QUESTION 134

- (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 137

- (Exam Topic 9)

Which Hyper Text Markup Language 5 (HTML5) option presents a security challenge for network data leakage prevention and/or monitoring?

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

Answer: B

NEW QUESTION 140

- (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 145

- (Exam Topic 9)

In Disaster Recovery (DR) and business continuity training, which BEST describes a functional drill?

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

Answer: B

NEW QUESTION 147

- (Exam Topic 10)

What 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 148

- (Exam Topic 10)

Which of the following violates identity and access management best practices?

- A. User accounts
- B. System accounts
- C. Generic accounts
- D. Privileged accounts

Answer: C

NEW QUESTION 151

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 156

- (Exam Topic 10)

Which of the following is the MOST beneficial to review when performing an IT audit?

- A. Audit policy
- B. Security log
- C. Security policies
- D. Configuration settings

Answer: C

NEW QUESTION 158

- (Exam Topic 10)

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

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

Answer: A

NEW QUESTION 160

- (Exam Topic 10)

What does secure authentication with logging provide?

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

Answer: B

NEW QUESTION 162

- (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 166

- (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 170

- (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 175

- (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 180

- (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
Systems	Systems	Authenticatio

NEW QUESTION 183

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 188

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 190

- (Exam Topic 10)

Which of the following is a critical factor for implementing a successful data classification program?

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

Answer: A

NEW QUESTION 195

- (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 197

- (Exam Topic 10)

Refer to the information below to answer the question.

A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns. In the plan, what is the BEST approach to mitigate future internal client-based attacks?

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

Answer: D

NEW QUESTION 200

- (Exam Topic 10)

When is security personnel involvement in the Systems Development Life Cycle (SDLC) process MOST beneficial?

- A. Testing phase
- B. Development phase
- C. Requirements definition phase
- D. Operations and maintenance phase

Answer: C

NEW QUESTION 204

- (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 209

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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

Answer: A

NEW QUESTION 212

- (Exam Topic 10)

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

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

Answer: B

NEW QUESTION 213

- (Exam Topic 10)

Refer to the information below to answer the question.

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

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

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

Answer: A

NEW QUESTION 218

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 222

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 224

- (Exam Topic 10)

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

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

Answer: C

NEW QUESTION 225

- (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 227

- (Exam Topic 10)

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

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

Answer: D

NEW QUESTION 229

- (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 233

- (Exam Topic 10)

Refer to the information below to answer the question.

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

Organizational policy requires the deletion of user data from Personal Digital Assistant (PDA) devices before disposal. It may not be possible to delete the user data if the device is malfunctioning. Which destruction method below provides the BEST assurance that the data has been removed?

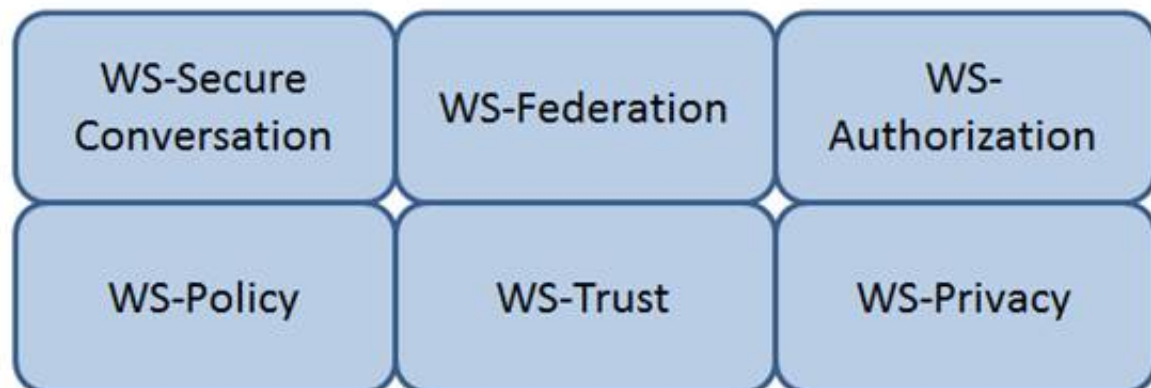
- A. Knurling
- B. Grinding
- C. Shredding
- D. Degaussing

Answer: C

NEW QUESTION 235

- (Exam Topic 11)

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

WS-Authorization

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

NEW QUESTION 238

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 241

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 242

- (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 246

- (Exam Topic 11)

A security professional has been asked to evaluate the options for the location of a new data center within a multifloor building. Concerns for the data center include emanations and physical access controls.

Which of the following is the BEST location?

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

Answer: C

NEW QUESTION 250

- (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 254

- (Exam Topic 11)

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

Step

Identify risks

Implement patch
deployment

Implement recurring
scanning schedule

Identify assets

Implement change
management

Order

1

2

3

4

5

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Step

Identify risks

Implement patch
deployment

Implement recurring
scanning schedule

Identify assets

Implement change
management

Order

1

2

3

4

5

NEW QUESTION 257

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 259

- (Exam Topic 11)

Which of the following PRIMARILY contributes to security incidents in web-based applications?

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

Answer: C

NEW QUESTION 261

- (Exam Topic 11)

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

- A. Supports Mandatory Access Control (MAC)

- B. Simplifies the management of access rights
- C. Relies on rotation of duties
- D. Requires two factor authentication

Answer: B

NEW QUESTION 266

- (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 270

- (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 273

- (Exam Topic 11)

What is the PRIMARY difference between security policies and security procedures?

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

Answer: D

NEW QUESTION 276

- (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 279

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 281

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 285

- (Exam Topic 11)

Which of the following is the PRIMARY security concern associated with the implementation of smart cards?

- A. The cards have limited memory
- B. Vendor application compatibility
- C. The cards can be misplaced
- D. Mobile code can be embedded in the card

Answer: C

NEW QUESTION 287

- (Exam Topic 11)

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

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

Answer: A

NEW QUESTION 292

- (Exam Topic 11)

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

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

Answer: D

NEW QUESTION 295

- (Exam Topic 11)

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

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

Answer: C

NEW QUESTION 298

- (Exam Topic 11)

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

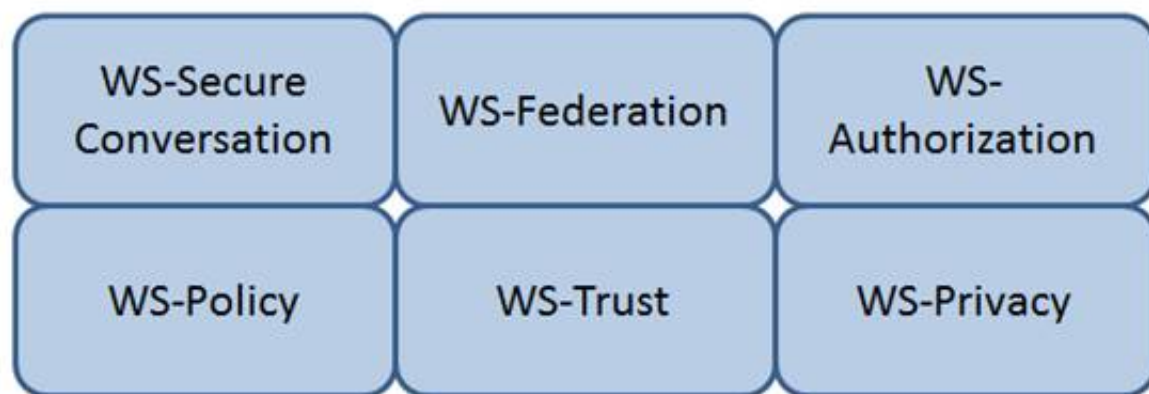
- A. Payload encryption and transport encryption
- B. Authentication Headers (AH)
- C. Keyed-Hashing for Message Authentication
- D. Point-to-Point Encryption (P2PE)

Answer: A

NEW QUESTION 303

- (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 306

- (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 311

- (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 315

- (Exam Topic 11)

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

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

Answer: B

NEW QUESTION 319

- (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 321

- (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 323

- (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 328

- (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 332

- (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 337

- (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 342

- (Exam Topic 11)

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

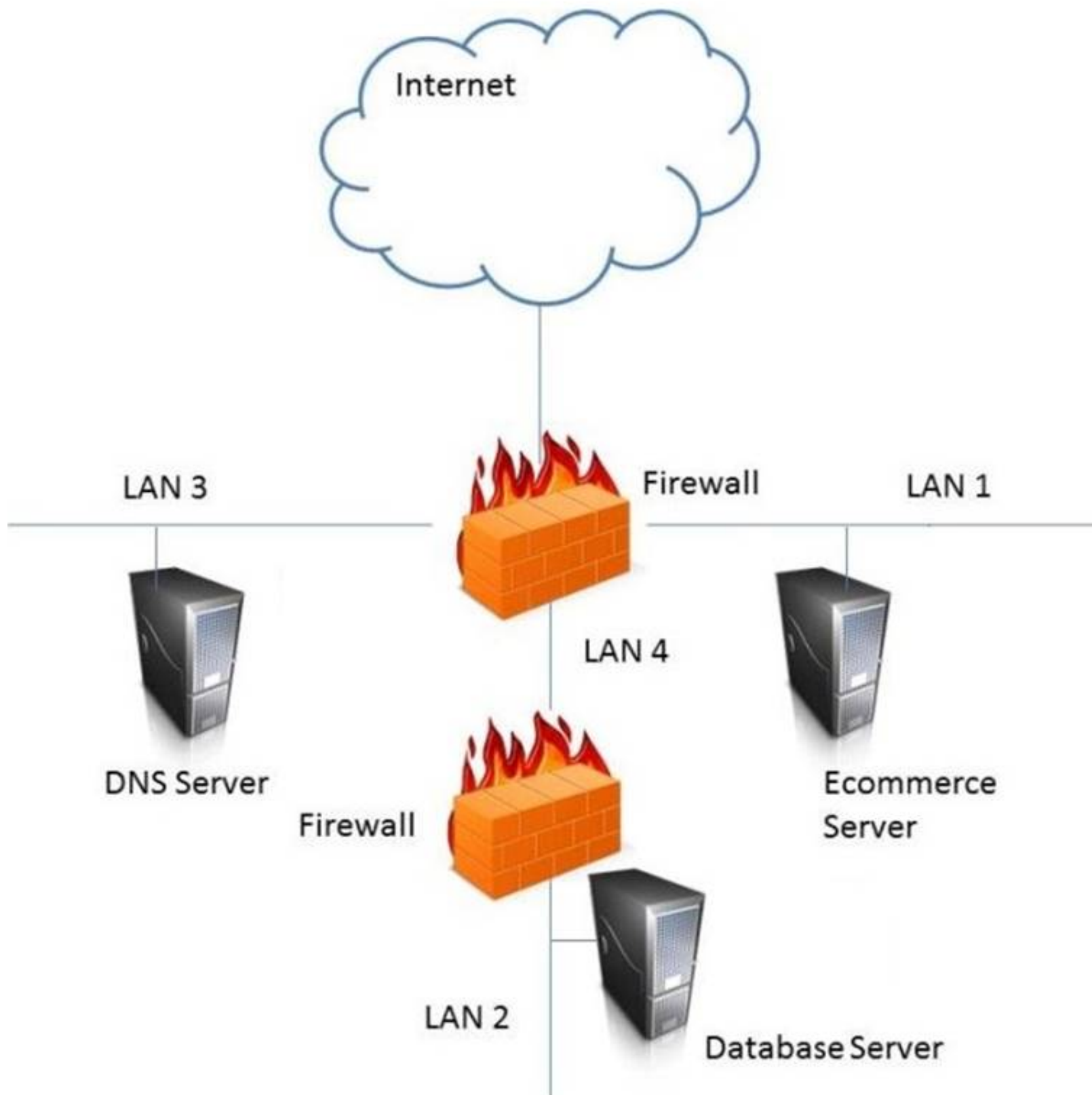
- A. Retention
- B. Reporting
- C. Recovery
- D. Remediation

Answer: A

NEW QUESTION 343

- (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 346

- (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 347

- (Exam Topic 12)

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

- A. Full name

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

Answer: B

NEW QUESTION 350

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 351

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 355

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 360

- (Exam Topic 12)

Which of the following sets of controls should allow an investigation if an attack is not blocked by preventive controls or detected by monitoring?

- A. Logging and audit trail controls to enable forensic analysis
- B. Security incident response lessons learned procedures
- C. Security event alert triage done by analysts using a Security Information and Event Management (SIEM) system
- D. Transactional controls focused on fraud prevention

Answer: C

NEW QUESTION 364

- (Exam Topic 12)

Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item?

- A. Property book
- B. Chain of custody form
- C. Search warrant return
- D. Evidence tag

Answer: D

NEW QUESTION 367

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 369

- (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 371

- (Exam Topic 12)

Which of the following BEST describes a chosen plaintext attack?

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

Answer: A

NEW QUESTION 372

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 375

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 379

- (Exam Topic 12)

An organization's information security strategic plan MUST be reviewed

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

Answer: C

NEW QUESTION 383

- (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 387

- (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 390

- (Exam Topic 12)

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

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

Answer: D

NEW QUESTION 395

- (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 400

- (Exam Topic 12)

Reciprocal backup site agreements are considered to be

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

Answer: B

NEW QUESTION 401

- (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 403

- (Exam Topic 12)

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

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

Answer: A

NEW QUESTION 408

- (Exam Topic 12)

What is a characteristic of Secure Socket Layer (SSL) and Transport Layer Security (TLS)?

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

Answer: A

NEW QUESTION 411

- (Exam Topic 13)

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

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

Answer:

C

NEW QUESTION 413

- (Exam Topic 13)

Which of the following is the MOST effective practice in managing user accounts when an employee is terminated?

- A. Implement processes for automated removal of access for terminated employees.
- B. Delete employee network and system IDs upon termination.
- C. Manually remove terminated employee user-access to all systems and applications.
- D. Disable terminated employee network ID to remove all access.

Answer: B

NEW QUESTION 416

- (Exam Topic 13)

Which one of the following is an advantage of an effective release control strategy from a configuration control standpoint?

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

Answer: C

NEW QUESTION 420

- (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 423

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 427

- (Exam Topic 13)

From a security perspective, which of the following assumptions MUST be made about input to an application?

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

Answer: D

NEW QUESTION 431

- (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 436

- (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 441

- (Exam Topic 13)

Unused space in a disk cluster is important in media analysis because it may contain which of the following?

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

Answer: A

NEW QUESTION 445

- (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 448

- (Exam Topic 13)

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

- A. The Data Protection Authority (DPA)
- B. The Cloud Service Provider (CSP)

- C. The application developers
- D. The data owner

Answer: B

NEW QUESTION 449

- (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 450

- (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 451

- (Exam Topic 13)

What does electronic vaulting accomplish?

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

Answer: A

Explanation:

Section: Security Operations

NEW QUESTION 455

- (Exam Topic 13)

What is the PRIMARY goal of fault tolerance?

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

Answer: A

NEW QUESTION 458

- (Exam Topic 13)

What is the second step in the identity and access provisioning lifecycle?

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

Answer: B

NEW QUESTION 462

- (Exam Topic 13)

Which of the following entails identification of data and links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

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

Answer: B

NEW QUESTION 465

- (Exam Topic 13)

When network management is outsourced to third parties, which of the following is the MOST effective method of protecting critical data assets?

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

Answer: D

NEW QUESTION 468

- (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 470

- (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 474

- (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 479

- (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 484

- (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 486

- (Exam Topic 13)

Who would be the BEST person to approve an organizations information security policy?

- A. Chief Information Officer (CIO)
- B. Chief Information Security Officer (CISO)
- C. Chief internal auditor
- D. Chief Executive Officer (CEO)

Answer:

B

Explanation:

Section: Security Operations

NEW QUESTION 490

- (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 492

- (Exam Topic 13)

In Disaster Recovery (DR) and Business Continuity (DC) training, which BEST describes a functional drill?

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

Answer: D

NEW QUESTION 497

- (Exam Topic 13)

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

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

Answer: A

NEW QUESTION 500

.....

Relate Links

100% Pass Your CISSP Exam with ExamBible Prep Materials

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

Contact us

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

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