CISSP.exam.32q

Number: CISSP
Passing Score: 800
Time Limit: 120 min

CISSP

Certified Information Systems Security Professional

Sections

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management (IAM)
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

Exam A

QUESTION 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

Correct Answer: D

Section: Security and Risk Management

Explanation

Explanation/Reference:

QUESTION 2

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

Correct Answer: C
Section: Security and Risk Management
Explanation

Explanation/Reference:
Reference: https://www.giac.org/paper/gsec/3873/information-warfare-cyber-warfare-future-warfare/106165 (14)

QUESTION 3
Intellectual property rights are PRIMARY concerned with which of the following?

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

Correct Answer: D
Section: Security and Risk Management
Explanation

Explanation/Reference:

QUESTION 4
Which of the following is MOST important when assigning ownership of an asset to a department?

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

Correct Answer: B

Section: Asset Security
Explanation

Explanation/Reference:

QUESTION 5
Which one of the following affects the classification of data?

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

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:

QUESTION 6
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

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Reference: http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/asset-security/data-and-system-ownership/#gref

QUESTION 7
An organization has doubled in size due to a rapid market share increase. The size of the Information Technology (IT) staff has maintained pace with this growth. The organization hires several contractors whose onsite time is limited. The IT department has pushed its limits building servers and rolling out workstations and has a backlog of account management requests.
Which contract is BEST in offloading the task from the IT staff?

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

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:

QUESTION 8
When implementing a data classification program, why is it important to avoid too much granularity?

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

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:

Reference: http://www.ittoday.info/AIMS/DSM/82-02-55.pdf

QUESTION 9
In a data classification scheme, the data is owned by the

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

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:

QUESTION 10
Which of the following mobile code security models relies only on trust?
A. Code signing
B. Class authentication
C. Sandboxing
D. Type safety

Correct Answer: A
Section: Security Architecture and Engineering
Explanation

Explanation/Reference:
Reference: https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/t09.pdf (11)

QUESTION 11
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

Correct Answer: A
Section: Security Architecture and Engineering
Explanation

Explanation/Reference:

QUESTION 12
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

Correct Answer: D
Section: Security Architecture and Engineering
Explanation

Explanation/Reference:

QUESTION 13
Which component of the Security Content Automation Protocol (SCAP) specification contains the data required to estimate the severity of vulnerabilities identified automated vulnerability assessments?

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

Correct Answer: B
Section: Security Architecture and Engineering
Explanation

Explanation/Reference:

QUESTION 14
At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

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

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:

QUESTION 15
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

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:

QUESTION 16

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

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

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:

QUESTION 17

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

Correct Answer: A
Section: Identity and Access Management (IAM)
Explanation

Explanation/Reference:

QUESTION 18

Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee’s salary?

A. Limit access to predefined queries
B. Segregate the database into a small number of partitions each with a separate security level
C. Implement Role Based Access Control (RBAC)
D. Reduce the number of people who have access to the system for statistical purposes

Correct Answer: C
Section: Identity and Access Management (IAM)
Explanation

Explanation/Reference:

QUESTION 19
What is the BEST approach for controlling access to highly sensitive information when employees have the same level of security clearance?

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

Correct Answer: B
Section: Identity and Access Management (IAM)
Explanation

Explanation/Reference:
QUESTION 20
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

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:

QUESTION 21

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

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

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:

QUESTION 22

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

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:

QUESTION 23

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

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:

QUESTION 24
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

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:

QUESTION 25

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

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:

QUESTION 26

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

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

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:

Reference: http://www.manchester.gov.uk/info/200039/emergencies/6174/business_continuity_planning/5

QUESTION 27

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

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

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Reference: http://www.pearsonitcertification.com/articles/article.aspx?p=1329710&seqNum=3

QUESTION 28
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

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:

QUESTION 29
A continuous information security monitoring program can BEST reduce risk through which of the following?

A. Collecting security events and correlating them to identify anomalies
B. Facilitating system-wide visibility into the activities of critical user accounts
C. Encompassing people, process, and technology
D. Logging both scheduled and unscheduled system changes

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
QUESTION 30
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

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:

QUESTION 31
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

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:

QUESTION 32
Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

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

Correct Answer: D

Section: Software Development Security

Explanation Explanation/Reference: