ISC.Premium.CISSP.by.VCEplus.62q

Number: CISSP VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 1.3

Exam Code: CISSP 2018
Exam Name: Certified Information Systems Security Professional 2018
Certification Provider: ISC
Corresponding Certification: CISSP
Website: www.vceplus.com
Free Exam: https://vceplus.com/exam-cissp-2018/
Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in CISSP exam products and you get latest questions. We strive to deliver the best CISSP exam product for top grades in your first attempt.

Website: https://vceplus.com
VCE to PDF Converter: https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus

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

QUESTION 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

Correct Answer: B
Section: Security and Risk Management
Explanation

Explanation/Reference:
Section: Security and Risk Management

QUESTION 2
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

Correct Answer: D
Section: Security and Risk Management
Explanation

Explanation/Reference:
Section: Security and Risk Management

QUESTION 3
Which of the following represents the GREATEST risk to data confidentiality?

A. Network redundancies are not implemented

B. Security awareness training is not completed
C. Backup tapes are generated unencrypted
D. Users have administrative privileges

Correct Answer: C
Section: Security and Risk Management
Explanation

Explanation/Reference:
Section: Security and Risk Management

QUESTION 4
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

Correct Answer: C
Section: Security and Risk Management
Explanation

Explanation/Reference:
Section: Security and Risk Management

QUESTION 5
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

Correct Answer: C
Section: Security and Risk Management
Explanation

Explanation/Reference:
Section: Security and Risk Management

Reference: https://www.colocationamerica.com/data-center/tier-standards-overview.htm

QUESTION 6
When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined?

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

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Section: Security and Risk Management

QUESTION 7
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:
Section: Security and Risk Management

QUESTION 8
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:
Section: Security and Risk Management

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

QUESTION 9
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:
Section: Security and Risk Management

QUESTION 10
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:
Section: Asset Security

QUESTION 11
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:
Section: Asset Security

QUESTION 12
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:
Section: Asset Security

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

QUESTION 13
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:
Section: Asset Security

QUESTION 14
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:
Section: Asset Security

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

QUESTION 15
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:
Section: Asset Security

QUESTION 16
Which of the following is an initial consideration when developing an information security management system?

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

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Section: Asset Security

QUESTION 17
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

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Section: Asset Security

QUESTION 18
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

Correct Answer: A
Section: Security Architecture and Engineering
Explanation

Explanation/Reference:
Section: Security Architecture and Engineering

QUESTION 19
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:
Section: Security Architecture and Engineering

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 20
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:
Section: Security Architecture and Engineering

QUESTION 21
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:
Section: Security Architecture and Engineering

QUESTION 22
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:
Section: Security Architecture and Engineering

QUESTION 23
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)

Correct Answer: A
Section: Security Architecture and Engineering
Explanation

Explanation/Reference:
Section: Security Architecture and Engineering

QUESTION 24
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)

Correct Answer: A
Section: Security Architecture and Engineering
Explanation

Explanation/Reference:
Section: Security Architecture and Engineering

QUESTION 25
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

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Section: Communication and Network Security

QUESTION 26
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:
Section: Communication and Network Security

QUESTION 27
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:
Section: Communication and Network Security

QUESTION 28
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:
Section: Communication and Network Security

QUESTION 29
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

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Section: Communication and Network Security

Reference: https://www.sans.org/reading-room/whitepapers/protocols/applying-osi-layer-network-model-information-security-1309 (10)

QUESTION 30
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

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Section: Communication and Network Security

QUESTION 31
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

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Section: Communication and Network Security

QUESTION 32
Which of the following is the BEST network defense against unknown types of attacks or stealth attacks in progress?

A. Intrusion Prevention Systems (IPS)
B. Intrusion Detection Systems (IDS)
C. Stateful firewalls
D. Network Behavior Analysis (NBA) tools

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Section: Communication and Network Security

QUESTION 33
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)

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Section: Communication and Network Security
Reference: http://www.dummies.com/programming/networking/understanding-wep-weaknesses/

QUESTION 34
A manufacturing organization wants to establish a Federated Identity Management (FIM) system with its 20 different supplier companies. Which of the following is the BEST solution for the manufacturing organization?

A. Trusted third-party certification
B. Lightweight Directory Access Protocol (LDAP)
C. Security Assertion Markup language (SAML)
D. Cross-certification

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

Explanation/Reference:
Section: Identity and Access Management (IAM)