CISSP Q&As

Certified Information Systems Security Professional

Pass ISC CISSP Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/cissp.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A cybersecurity engineer has been tasked to research and implement an ultra-secure communications channel to protect the organization\\'s most valuable intellectual property (IP). The primary directive in this initiative is to ensure there Is no possible way the communications can be intercepted without detection. Which of the following Is the only way to ensure this outcome?

A. Diffie-Hellman key exchange

B. Symmetric key cryptography

C. [Public key infrastructure (PKI)

D. Quantum Key Distribution

Correct Answer: C

QUESTION 2

An organization\\'s retail website provides its only source of revenue, so the disaster recovery plan (DRP) must document an estimated time for each step in the plan.

Which of the following steps in the DRP will list the GREATEST duration of time for the service to be fully operational?

A. Update the Network Address Translation (NAT) table.

B. Update Domain Name System (DNS) server addresses with domain registrar.

C. Update the Border Gateway Protocol (BGP) autonomous system number.

D. Update the web server network adapter configuration.

Correct Answer: B

QUESTION 3

Which of the following would qualify as an exception to the "right to be forgotten" of the General Data Protection Regulation\\'s (GDPR)?

A. For the establishment, exercise, or defense of legal claims

B. The personal data has been lawfully processed and collected

C. The personal data remains necessary to the purpose for which it was collected

D. For the reasons of private interest

Correct Answer: C

QUESTION 4

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

A. Transport

B. Data link

C. Network

D. Application

Correct Answer: D

QUESTION 5

Refer to the information below to answer the question.

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

The effectiveness of the security program can PRIMARILY be measured through

A. audit findings.

B. risk elimination.

C. audit requirements.

D. customer satisfaction.

Correct Answer: A

QUESTION 6

Which of the following is the BEST defense against password guessing?

A. Limit external connections to the network

B. Disable the account after a limited number of unsuccessful attempts

C. Force the password to be changed after an invalid password has been entered

D. Require a combination of letters, numbers, and special characters in the password

Correct Answer: B

QUESTION 7

Which of the following is the MOST appropriate action when reusing media that contains sensitive data?

A. Erase

B. Sanitize

C. Encrypt

D. Degauss

Correct Answer: B

QUESTION 8

A company hired an external vendor to perform a penetration test ofa new payroll system. The company\\'s internal test team had already performed an in-depth application and security test of the system and determined that it met security requirements. However, the external vendor uncovered significant security weaknesses where sensitive personal data was being sent unencrypted to the tax processing systems. What is the MOST likely cause of the security issues?

A. Failure to perform interface testing

B. Failure to perform negative testing

C. Inadequate performance testing

D. Inadequate application level testing

Correct Answer: A

QUESTION 9

A breach investigation found a website was exploited through an open source component. What is the FIRST step in the process that could have prevented this breach?

A. Application whitelisting

B. Vulnerability remediation

C. Web application firewall (WAF)

D. Software inventory

Correct Answer: C

QUESTION 10

An information security consultant is asked to make recommendations for a small business to protect the access to information, stored on network drives. The small business supports several government agencies that manage highly sensitive information. Which of the following recommendations is BEST to achieve this objective?

A. Develop and implement a security information and event monitoring system.

B. Develop and implement access management policies and procedures.

C. Develop and implement data center access policies and procedures.

D. Develop and implement a security operations center (SOC) for access monitoring.

Correct Answer: B

Reference: https://www.techtarget.com/searchsecurity/post/5-steps-to-ensure-a-successful-access-management-strategy

QUESTION 11

Continuity of operations is BEST supported by which of the following?

A. Confidentiality, availability, and reliability

B. Connectivity, reliability, and redundancy

C. Connectivity, reliability, and recovery

D. Confidentiality, integrity, and availability

Correct Answer: B

QUESTION 12

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

QUESTION 13

What is the benefit of using Network Admission Control (NAC)?

A. Operating system (OS) versions can be validated prior to allowing network access.

B. NAC supports validation of the endpoint\\'s security posture prior to allowing the session to go into an authorized state.

C. NAC can require the use of certificates, passwords, or a combination of both before allowing network admission.

D. NAC only supports Windows operating systems (OS).

Correct Answer: B

QUESTION 14

Checking routing information on e-mail to determine it is in a valid format and contains valid information is an example of which of the following anti-spam approaches?

A. Simple Mail Transfer Protocol (SMTP) blacklist

B. Reverse Domain Name System (DNS) lookup

C. Hashing algorithm

D. Header analysis

Correct Answer: D

QUESTION 15

What is the term commonly used to refer to a technique of authenticating one machine to another by forging packets from a trusted source?

A. Man-in-the-Middle (MITM) attack

B. Smurfing

C. Session redirect

D. Spoofing

Correct Answer: D