

# CISSP<sup>Q&As</sup>

Certified Information Systems Security Professional

## Pass ISC CISSP Exam with 100% Guarantee

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

<https://www.pass2lead.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

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

Correct Answer: B

---

## QUESTION 2

Change management policies and procedures belong to which of the following types of controls?

- A. Directive
- B. Detective
- C. Corrective
- D. Preventative

Correct Answer: A

Reference: [https://books.google.com.pk/books?id=9gCn86CmsNQCandpg=PA570andlpg=PA570anddq=CISSP+Change+management+policies+and+procedures+belong+to+which+type+of+controlandsource=blandots=riGvVpUO4Handsig=ACfU3U0kRWWallj7gwqlovVku880wG5LOgandhl=enandsa=Xandved=2ahUKEwjA7cGL\\_anpAhULxoUKHc1ID3UQ6AEwCnoECBIQAQ#v=onepageandq=CISSP%20Change%20management%20policies%20and%20procedures%20belong%20to%20which%20type%20of%20controlandf=false](https://books.google.com.pk/books?id=9gCn86CmsNQCandpg=PA570andlpg=PA570anddq=CISSP+Change+management+policies+and+procedures+belong+to+which+type+of+controlandsource=blandots=riGvVpUO4Handsig=ACfU3U0kRWWallj7gwqlovVku880wG5LOgandhl=enandsa=Xandved=2ahUKEwjA7cGL_anpAhULxoUKHc1ID3UQ6AEwCnoECBIQAQ#v=onepageandq=CISSP%20Change%20management%20policies%20and%20procedures%20belong%20to%20which%20type%20of%20controlandf=false)

---

## QUESTION 3

During which of the following processes is least privilege implemented for a user account?

- A. Provision
- B. Approve
- C. Request
- D. Review

Correct Answer: A

---

## QUESTION 4

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

Correct Answer: C

---

## QUESTION 5

Which testing method requires very limited or no information about the network infrastructure?

- A. White box
- B. Static
- C. Black box
- D. Stress

Correct Answer: C

---

## QUESTION 6

Which of the following will accomplish Multi-Factor Authentication (MFA)?

- A. Issuing a smart card with a user-selected Personal Identification Number (PIN)
- B. Requiring users to enter a Personal Identification Number (PIN) and a password
- C. Performing a palm and retinal scan
- D. Issuing a smart card and a One Time Password (OTP) token

Correct Answer: A

---

## QUESTION 7

Refer to the information below to answer the question.

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

After magnetic drives were degaussed twice according to the product manufacturer's directions, what is the MOST LIKELY security issue with degaussing?

- A. Commercial products often have serious weaknesses of the magnetic force available in the degausser product.
- B. Degausser products may not be properly maintained and operated.
- C. The inability to turn the drive around in the chamber for the second pass due to human error.
- D. Inadequate record keeping when sanitizing media.

Correct Answer: B

---

#### QUESTION 8

A large corporation is looking for a solution to automate access based on where the request is coming from, who the user is, what device they are connecting with, and what and time of day they are attempting this access. What type of solution would suit their needs?

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

Correct Answer: B

---

#### QUESTION 9

What are the first two components of logical access control?

- A. Confidentiality and authentication
- B. Authentication and identification
- C. Identification and confidentiality
- D. Authentication and availability

Correct Answer: B

---

#### QUESTION 10

A large organization uses biometrics to allow access to its facilities. It adjusts the biometric value for incorrectly granting or denying access so that the two numbers are the same.

What is this value called?

- A. False Rejection Rate (FRR)
- B. Accuracy acceptance threshold

- C. Equal error rate
- D. False Acceptance Rate (FAR)

Correct Answer: C

---

#### QUESTION 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.

Correct Answer: B

---

#### QUESTION 12

Which of the following is the BEST method to assess the effectiveness of an organization's vulnerability management program?

- A. Review automated patch deployment reports
- B. Periodic third party vulnerability assessment
- C. Automated vulnerability scanning
- D. Perform vulnerability scan by security team

Correct Answer: B

---

#### QUESTION 13

By allowing storage communications to run on top of Transmission Control Protocol/Internet Protocol (TCP/IP) with a Storage Area Network (SAN), the

- A. confidentiality of the traffic is protected.
- B. opportunity to sniff network traffic exists.
- C. opportunity for device identity spoofing is eliminated.
- D. storage devices are protected against availability attacks.

Correct Answer: B

---

**QUESTION 14**

Which of the following techniques evaluates the secure design principles of network OF software architectures?

- A. Risk modeling
- B. Threat modeling
- C. Fuzzing
- D. Waterfall method

Correct Answer: B

---

**QUESTION 15**

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

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

Correct Answer: C

[CISSP PDF Dumps](#)

[CISSP Practice Test](#)

[CISSP Braindumps](#)