



# 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.pass4itsure.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**

An organization has determined that its previous waterfall approach to software development is not keeping pace with business demands. To adapt to the rapid changes required for product delivery, the organization has decided to move towards an Agile software development and release cycle. In order to ensure the success of the Agile methodology, who is MOST critical in creating acceptance tests or acceptance criteria for each release?

- A. Project managers
- B. Software developers
- C. Independent testers
- D. Business customers

Correct Answer: D

---

**QUESTION 2**

Which of the following is MOST appropriate to collect evidence of a zero-day attack?

- A. Firewall
- B. Honeypot
- C. Antispam
- D. Antivirus

Correct Answer: B

Honeypot is right

The rest of the options would not collect evidence until the real attack happens. That's what a Zero-day attack means nobody is aware of the attack including the vendor.

---

**QUESTION 3**

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 4**

Why is authentication by ownership stronger than authentication by knowledge?

- A. It is easier to change.
- B. It can be kept on the user's person.
- C. It is more difficult to duplicate.
- D. It is simpler to control.

Correct Answer: B

---

**QUESTION 5**

The existence of physical barriers, card and personal identification number (PIN) access systems, cameras, alarms, and security guards BEST describes this security approach?

- A. Security information and event management (SIEM)
- B. Security perimeter
- C. Defense-in-depth
- D. Access control

Correct Answer: B

---

**QUESTION 6**

Which reporting type requires a service organization to describe its system and define its control objectives and controls that are relevant to users internal control over financial reporting?

- A. Statement on Auditing Standards (SAS)70
- B. Service Organization Control 1 (SOC1)
- C. Service Organization Control 2 (SOC2)
- D. Service Organization Control 3 (SOC3)

Correct Answer: B

---

**QUESTION 7**

Two computers, each with a single connection on the same physical 10 gigabit Ethernet network segment, need to communicate with each other. The first machine has a single Internet Protocol (IP) Classless Inter-Domain Routing (CIDR) address of 192.168.1.3/30 and the second machine has an IP/CIDR address 192.168.1.6/30. Which of the following is correct?



- A. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network bridge in order to communicate.
- B. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network bridge in order to communicate.
- C. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network router in order to communicate.
- D. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network router in order to communicate.

Correct Answer: A

---

#### QUESTION 8

A software architect has been asked to build a platform to distribute music to thousands of users on a global scale. The architect has been reading about content delivery networks (CDN). Which of the following is a principal task to undertake?

- A. Establish a service-oriented architecture (SOA).
- B. Establish a media caching methodology.
- C. Establish relationships with hundreds of Internet service providers (ISP).
- D. Establish a low-latency wide area network (WAN).

Correct Answer: B

---

#### QUESTION 9

Which of the following is a MAJOR concern when there is a need to preserve or retain information for future retrieval?

- A. Laws and regulations may change in the interim, making it unnecessary to retain the information
- B. The expense of retaining the information could become untenable for the organization
- C. The organization may lose track of the information and not dispose of it securely
- D. The technology needed to retrieve the information may not be available in the future

Correct Answer: C

---

#### QUESTION 10

What is the MOST effective way to determine a mission critical asset in an organization?

- A. Vulnerability analysis



- B. business process analysis
- C. Threat analysis
- D. Business risk analysis

Correct Answer: B

---

#### QUESTION 11

Following a penetration test, what should an organization do FIRST?

- A. Review all security policies and procedures
- B. Ensure staff is trained in security
- C. Determine if you need to conduct a full security assessment
- D. Evaluate the problems identified in the test result

Correct Answer: D

---

#### QUESTION 12

What is the BEST approach to anonymizing personally identifiable information (PII) in a test environment?

- A. Randomizing data
- B. Swapping data
- C. Encrypting data
- D. Encoding data

Correct Answer: A

---

#### QUESTION 13

A scan report returned multiple vulnerabilities affecting several production servers that are mission critical. Attempts to apply the patches in the development environment have caused the servers to crash. What is the BEST course of action?

- A. Upgrade the software affected by the vulnerability.
- B. Inform management of possible risks.
- C. Mitigate the risks with compensating controls.
- D. Remove the affected software from the servers.



Correct Answer: C

---

#### QUESTION 14

A customer continues to experience attacks on their email, web, and File Transfer Protocol (FTP) servers. These attacks are impacting their business operations. Which of the following is the BEST recommendation to make?

- A. Configure an intrusion detection system (IDS).
- B. Create a demilitarized zone (DMZ).
- C. Deploy a bastion host.
- D. Setup a network firewall.

Correct Answer: C

---

#### QUESTION 15

Internet Protocol (IP) source address spoofing is used to defeat

- A. address-based authentication.
- B. Address Resolution Protocol (ARP).
- C. Reverse Address Resolution Protocol (RARP).
- D. Transmission Control Protocol (TCP) hijacking.

Correct Answer: A

[CISSP VCE Dumps](#)

[CISSP Study Guide](#)

[CISSP Braindumps](#)