



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

System Security Certified Practitioner (SSCP)

**Pass ISC SSCP Exam with 100% Guarantee**

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

<https://www.geekcert.com/sscp.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

Which of the following protects Kerberos against replay attacks?

- A. Tokens
- B. Passwords
- C. Cryptography
- D. Time stamps

Correct Answer: D

A replay attack refers to the recording and retransmission of packets on the network. Kerberos uses time stamps, which protect against this type of attack.

Source: HARRIS, Shon, All-In-One CISSP Certification guide, McGraw-Hill/Osborne, 2002, chapter

8: Cryptography (page 581).

---

### QUESTION 2

Who can best decide what are the adequate technical security controls in a computer-based application system in regards to the protection of the data being used, the criticality of the data, and its sensitivity level ?

- A. System Auditor
- B. Data or Information Owner
- C. System Manager
- D. Data or Information user

Correct Answer: B

The data or information owner also referred to as "Data Owner" would be the best person. That is the individual or officer who is ultimately responsible for the protection of the information and can therefore decide what are the adequate security controls according to the data sensitivity and data criticality. The auditor would be the best person to determine the adequacy of controls and whether or not they are working as expected by the owner.

The function of the auditor is to come around periodically and make sure you are doing what you are supposed to be doing. They ensure the correct controls are in place and are being maintained securely. The goal of the auditor is to make sure the organization complies with its own policies and the applicable laws and regulations.

Organizations can have internal auditors and/ or external auditors. The external auditors commonly work on behalf of a regulatory body to make sure compliance is being met. For example CobiT, which is a model that most information security auditors follow when evaluating a security program. While many security professionals fear and dread auditors, they can be valuable tools in ensuring the overall security of the organization. Their goal is to find the things you have missed and help you understand how to fix the problem. The Official ISC2 Guide (OIG) says:

IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements



placed on systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls and their effectiveness.

Example:

Bob is the head of payroll. He is therefore the individual with primary responsibility over the payroll database, and is therefore the information/data owner of the payroll database. In Bob's department, he has Sally and Richard working for him. Sally is responsible for making changes to the payroll database, for example if someone is hired or gets a raise. Richard is only responsible for printing paychecks. Given those roles, Sally requires both read and write access to the payroll database, but Richard requires only read access to it. Bob communicates these requirements to the system administrators (the "information/ data custodians") and they set the file permissions for Sally's and Richard's user accounts so that Sally has read/write access, while Richard has only read access.

So in short Bob will determine what controls are required, what is the sensitivity and criticality of the Data. Bob will communicate this to the custodians who will implement the requirements on the systems/DB. The auditor would assess if the controls are in fact providing the level of security the Data Owner expects within the systems/DB. The auditor does not determine the sensitivity of the data or the criticality of the data.

The other answers are not correct because:

A "system auditor" is never responsible for anything but auditing... not actually making control decisions but the auditor would be the best person to determine the adequacy of controls and then make recommendations. A "system manager" is really just another name for a system administrator, which is actually an information custodian as explained above.

A "Data or information user" is responsible for implementing security controls on a day-to-day basis as they utilize the information, but not for determining what the controls should be or if they are adequate.

References:

Official ISC2 Guide to the CISSP CBK, Third Edition , Page 477

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Information Security Governance and Risk Management ((ISC)2 Press) (Kindle Locations 294- 298). Auerbach Publications. Kindle Edition.

Harris, Shon (2012-10-25). CISSP All-in-One guide, 6th Edition (Kindle Locations 3108- 3114).

Information Security Glossary

Responsibility for use of information resources

---

### QUESTION 3

A one-way hash provides which of the following?

- A. Confidentiality
- B. Availability
- C. Integrity
- D. Authentication

Correct Answer: C



A one-way hash is a function that takes a variable-length string a message, and compresses and transforms it into a fixed length value referred to as a hash value. It provides integrity, but no confidentiality, availability or authentication.

Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 5).

---

#### QUESTION 4

Which of the following elements is NOT included in a Public Key Infrastructure (PKI)?

- A. Timestamping
- B. Repository
- C. Certificate revocation
- D. Internet Key Exchange (IKE)

Correct Answer: D

Other elements are included in a PKI.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 4: Cryptography (page 165).

---

#### QUESTION 5

Which of the following are NOT a countermeasure to traffic analysis?

- A. Padding messages.
- B. Eavesdropping.
- C. Sending noise.
- D. Faraday Cage

Correct Answer: B

Eavesdropping is not a countermeasure, it is a type of attack where you are collecting traffic and attempting to see what is being send between entities communicating with each other.

The following answers are incorrect:

Padding Messages. Is incorrect because it is considered a countermeasure you make messages uniform size, padding can be used to counter this kind of attack, in which decoy traffic is sent out over the network to disguise patterns and make it more difficult to uncover patterns.

Sending Noise. Is incorrect because it is considered a countermeasure, tansmitting non- informational data elements to disguise real data.

Faraday Cage Is incorrect because it is a tool used to prevent emanation of electromagnetic waves. It is a very effective tool to prevent traffic analysis.



VCE & PDF

GeekCert.com

<https://www.geekcert.com/sscp.html>

2024 Latest geekcert SSCP PDF and VCE dumps Download

---

[SSCP VCE Dumps](#)

[SSCP Exam Questions](#)

[SSCP Braindumps](#)