# SSCP Q&As

System Security Certified Practitioner (SSCP)

## Pass ISC SSCP Exam with 100% Guarantee

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

**https://www.pass2lead.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 is the BEST way to detect software license violations?

A. Implementing a corporate policy on copyright infringements and software use.

B. Requiring that all PCs be diskless workstations.

C. Installing metering software on the LAN so applications can be accessed through the metered software.

D. Regularly scanning PCs in use to ensure that unauthorized copies of software have not been loaded on the PC.

Correct Answer: D

The best way to prevent and detect software license violations is to regularly scan used PCs, either from the LAN or directly, to ensure that unauthorized copies of software have not been loaded on the PC.

Other options are not detective.

A corporate policy is not necessarily enforced and followed by all employees.

Software can be installed from other means than floppies or CD-ROMs (from a LAN or even downloaded from the Internet) and software metering only concerns applications that are registered.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 108).

**QUESTION 2**

Which of the following steps is NOT one of the eight detailed steps of a Business Impact Assessment (BIA):

A. Notifying senior management of the start of the assessment.

B. Creating data gathering techniques.

C. Identifying critical business functions.

D. Calculating the risk for each different business function.

Correct Answer: A

Source: HARRIS, S., CISSP All- In-One uide, 3rd. Edition, 2005, Chapter 9, Page 701.

There have been much discussion about the steps of the BIA and I struggled with this before deciding to scrape the question about "the four steps," and re-write the question using the AIO for a reference. This question should be easy.... if you know all eight steps.

The eight detailed and granular steps of the BIA are:

1.

Select Individuals to interview for the data gathering.

2.

Create data gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).

3.

Identify the company\\'s critical business functions.

4.

Identify the resources that these functions depend upon.

5.

Calculate how long these functions can survive without these resources.

6.

Identify vulnerabilities and the threats to these functions.

7.

Calculate risk for each of the different business functions.

8.

Document findings and report them to management. Shon goes on to cover each step in Chapter 9.

**QUESTION 3**

Which of the following is not a disadvantage of symmetric cryptography when compared with Asymmetric Ciphers?

A. Provides Limited security services

B. Has no built in Key distribution

C. Speed

D. Large number of keys are needed

Correct Answer: C

Symmetric cryptography ciphers are generally fast and hard to break. So speed is one of the key advantage of Symmetric ciphers and NOT a disadvantage. Symmetric Ciphers uses simple encryption steps such as XOR, substitution, permutation, shifting columns, shifting rows, etc... Such steps does not required a large amount of processing power compare to the complex mathematical problem used within Asymmetric Ciphers.

Some of the weaknesses of Symmetric Ciphers are:

The lack of automated key distribution. Usually an Asymmetric cipher would be use to protect the symmetric key if it needs to be communicated to another entity securely over a public network. In the good old day this was done manually where it was distributed using the Floppy Net sometimes called the Sneaker Net (you run to someone\\'s office to give them the key).

As far as the total number of keys are required to communicate securely between a large group of users, it does not

scale very well. 10 users would require 45 keys for them to communicate securely with each other. If you have 1000 users then you would need almost half a million key to communicate secure. On Asymmetric ciphers there is only 2000 keys required for 1000 users. The formula to calculate the total number of keys required for a group of users who wishes to communicate securely with each others using Symmetric encryption is Total Number of Users (N) * Total Number of users minus one Divided by 2 or N (N-1)/2

Symmetric Ciphers are limited when it comes to security services, they cannot provide all of the security services provided by Asymmetric ciphers. Symmetric ciphers provides mostly confidentiality but can also provide integrity and authentication if a Message Authentication Code (MAC) is used and could also provide user authentication if Kerberos is used for example. Symmetric Ciphers cannot provide Digital Signature and Non-Repudiation.

Reference used for theis question:

WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 2).

**QUESTION 4**

Which access control model is best suited in an environment where a high security level is required and where it is desired that only the administrator grants access control?

A. DAC

B. MAC

C. Access control matrix

D. TACACS

Correct Answer: B

MAC provides high security by regulating access based on the clearance of individual users and sensitivity labels for each object. Clearance levels and sensitivity levels cannot be modified by individual users -- for example, user Joe (SECRET clearance) cannot reclassify the "Presidential Doughnut Recipe" from "SECRET" to "CONFIDENTIAL" so that his friend Jane (CONFIDENTIAL clearance) can read it. The administrator is ultimately responsible for configuring this protection in accordance with security policy and directives from the Data Owner.

DAC is incorrect. In DAC, the data owner is responsible for controlling access to the object.

Access control matrix is incorrect. The access control matrix is a way of thinking about the access control needed by a population of subjects to a population of objects. This access control can be applied using rules, ACL\\'s, capability tables, etc.

TACACS is incorrect. TACACS is a tool for performing user authentication.

References:

CBK, p. 187, Domain 2: Access Control.

AIO3, Chapter 4, Access Control.

**QUESTION 5**

Which of the following floors would be most appropriate to locate information processing facilities in a 6stories building?

A. Basement

B. Ground floor

C. Third floor

D. Sixth floor

Correct Answer: C

You data center should be located in the middle of the facility or the core of a building to provide protection from natural disasters or bombs and provide easier access to emergency crewmembers if necessary. By being at the core of the facility the external wall would act as a secondary layer of protection as well.

Information processing facilities should not be located on the top floors of buildings in case of a fire or flooding coming from the roof. Many crimes and theft have also been conducted by simply cutting a large hole on the roof.

They should not be in the basement because of flooding where water has a natural tendancy to flow down :-) Even a little amount of water would affect your operation considering the quantity of electrical cabling sitting directly on the cement floor under under your raise floor. The data center should not be located on the first floor due to the presence of the main entrance where people are coming in and out. You have a lot of high traffic areas such as the elevators, the loading docks, cafeteria, coffee shopt, etc.. Really a bad location for a data center.

So it was easy to come up with the answer by using the process of elimination where the top, the bottom, and the basement are all bad choices. That left you with only one possible answer which is the third floor.

Source: HARRIS, Shon, All-In-One CISSP Certification uide, 5th Edition, Page 425.