SSCP$^{Q\&As}$

System Security Certified Practitioner (SSCP)

Pass ISC SSCP Exam with 100% Guarantee

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

QUESTION 1

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 it\\'s 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 sensitivily 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 crititicality 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 uide, 6th Edition (Kindle Locations 3108- 3114).

Information Security Glossary

Responsibility for use of information resources

QUESTION 2

The Logical Link Control sub-layer is a part of which of the following?

A. The ISO/OSI Data Link layer

B. The Reference monitor

C. The Transport layer of the TCP/IP stack model

D. Change management control

Correct Answer: A

The OSI/ISO Data Link layer is made up of two sub-layers; (1) the Media Access Control layer refers downward to lower layer hardware functions and (2) the Logical Link Control refers upward to higher layer software functions. Other choices are distracters. Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

QUESTION 3

Which of the following was designed to support multiple network types over the same serial link?

A. Ethernet

B. SLIP

C. PPP

D. PPTP

Correct Answer: C

The Point-to-Point Protocol (PPP) was designed to support multiple network types over the same serial

link, just as Ethernet supports multiple network types over the same LAN. PPP replaces the earlier Serial

Line Internet Protocol (SLIP) that only supports IP over a serial link. PPTP is a tunneling protocol.

Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 3:

TCP/IP from a Security Viewpoint.

QUESTION 4

Related to information security, integrity is the opposite of which of the following?

A. abstraction

B. alteration

C. accreditation

D. application

Correct Answer: B

Integrity is the opposite of "alteration."

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 59.

QUESTION 5

Which conceptual approach to intrusion detection system is the most common?

A. Behavior-based intrusion detection

B. Knowledge-based intrusion detection

C. Statistical anomaly-based intrusion detection

D. Host-based intrusion detection

Correct Answer: B

There are two conceptual approaches to intrusion detection. Knowledge-based intrusion detection uses a database of known vulnerabilities to look for current attempts to exploit them on a system and trigger an alarm if an attempt is found. The other approach, not as common, is called behaviour-based or statistical analysis-based. A host-based intrusion detection system is a common implementation of intrusion detection, not a conceptual approach.

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 3: Telecommunications and Network Security (page 63).

Also: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 193-194).