CSSLP^{Q&As}

Certified Secure Software Lifecycle Professional Practice Test

Pass ISC CSSLP Exam with 100% Guarantee

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

https://www.geekcert.com/csslp.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 monitors the hard disks of its employees\\' computers from time to time. Which policy does this pertain to?

A. Backup policy

B. User password policy

C. Privacy policy

D. Network security policy

Correct Answer: C

Monitoring the computer hard disks or e-mails of employees pertains to the privacy policy of an organization. Answer: A is incorrect. The backup policy of a company is related to the backup of its data. Answer: D is incorrect. The network security policy is related to the security of a company\\'s network. Answer: B is incorrect. The user password policy is related to passwords that users provide to log on to the network.

QUESTION 2

Which of the following are the basic characteristics of declarative security? Each correct answer represents a complete solution. Choose all that apply.

A. It is a container-managed security.

B. It has a runtime environment.

C. All security constraints are stated in the configuration files.

D. The security policies are applied at the deployment time.

Correct Answer: ABC

The following are the basic characteristics of declarative security: In declarative security, programming is not required. All security constraints are stated in the configuration files. It is a container-managed security. The application server manages the enforcing process of security constraints. It has a runtime environment. The security policies for runtime environment are represented by the deployment descriptor. It can support different environments, such as development, testing, and production. Answer: D is incorrect. It is the characteristic of programmatic security.

QUESTION 3

Which of the following test methods has the objective to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes?

A. Security Test and Evaluation (STandE)

B. Penetration testing

C. Automated vulnerability scanning tool

D. On-site interviews

Correct Answer: B

The goal of penetration testing is to examine the IT system from the perspective of a threat-source, and to identify potential failures in the IT system protection schemes. Penetration testing, when performed in the risk assessment process, is used to assess an IT system\'s capability to survive with the intended attempts to thwart system security. Answer: A is incorrect. The objective of STandE is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization\'s security policy or meet industry standards.

QUESTION 4

John works as a security manager for SoftTech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?

A. Full-scale exercise

B. Walk-through drill

C. Structured walk-through test

D. Evacuation drill

Correct Answer: C

The structured walk-through test is also known as the table-top exercise. In structured walk-through test, the team members walkthrough the plan to identify and correct weaknesses and how they will respond to the emergency scenarios by stepping in the course of the plan. It is the most effective and competent way to identify the areas of overlap in the plan before conducting more challenging training exercises. Answer: A is incorrect. In full-scale exercise, the critical systems run at an alternate site. Answer: B is incorrect. The emergency management group and response teams actually perform their emergency response functions by walking through the test, without actually initiating recovery procedures. But it is not much cost effective. Answer: D is incorrect. It is a test performed when personnel walks through the evacuation route to a designated area where procedures for accounting for the personnel are tested.

QUESTION 5

Which of the following individuals inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company\'s stated security objectives?

A. Information system security professional

B. Data owner

C. Senior management

D. Information system auditor

Correct Answer: D

An information system auditor is an individual who inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company\'s stated security objectives. He is responsible for reporting the senior management about the value of security controls by performing regular and independent audits. Answer: B is incorrect. A data owner determines the sensitivity or classification levels of data. Answer: A is incorrect. An informational systems security professional is an individual who designs, implements, manages, and reviews the security policies, standards, guidelines, and procedures of the organization. He is responsible to implement and maintain security by the senior-level management. Answer: C is incorrect. A senior management assigns overall responsibilities to other individuals.