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

SATISFACTION GUARANTEED • 100% • SATISFACTION GUARANTEED

QUESTION 1

In which of the following types of tests are the disaster recovery checklists distributed to the members of disaster recovery team and asked to review the assigned checklist?

A. Parallel test

B. Simulation test

C. Full-interruption test

D. Checklist test

Correct Answer: D

A checklist test is a test in which the disaster recovery checklists are distributed to the members of the disaster recovery team. All members are asked to review the assigned checklist. The checklist test is a simple test and it is easy to conduct this test. It allows to accomplish the following three goals: It ensures that the employees are aware of their responsibilities and they have the refreshed knowledge. It provides an individual with an opportunity to review the checklists for obsolete information and update any items that require modification during the changes in the organization. It ensures that the assigned members of disaster recovery team are still working for the organization. Answer: B is incorrect. A simulation test is a method used to test the disaster recovery plans. It operates just like a structured walk- through test. In the simulation test, the members of a disaster recovery team present with a disaster scenario and then, discuss on appropriate responses. These suggested responses are measured and some of them are taken by the team. The range of the simulation test should be defined carefully for avoiding excessive disruption of normal business activities. Answer: A is incorrect. A parallel test includes the next level in the testing procedure, and relocates the employees to an alternate recovery site and implements site activation procedures. These employees present with their disaster recovery responsibilities as they would for an actual disaster. The disaster recovery sites have full responsibilities to conduct the day-to-day organization\\'s business. Answer: C is incorrect. A full- interruption test includes the operations that shut down at the primary site and are shifted to the recovery site according to the disaster recovery plan. It operates just like a parallel test. The full- interruption test is very expensive and difficult to arrange. Sometimes, it causes a major disruption of operations if the test fails.

QUESTION 2

Which of the following policies can explain how the company interacts with partners, the company\\'s goals and mission, and a general reporting structure in different situations?

A. Informative

B. Advisory

C. Selective

D. Regulatory

Correct Answer: A

An informative policy informs employees about certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the company. The informative policy can explain how the company interacts with partners, the company\\'s goals and mission, and a general reporting structure in different situations. Answer: D is incorrect. A regulatory policy ensures that an organization follows the standards set by specific industry regulations. This type of policy is very detailed and specific to a type of industry. The regulatory policy is used in financial institutions, health care facilities, public utilities, and other government-regulated industries, e.g., TRAI. Answer: B is incorrect. An advisory policy strongly advises employees regarding which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. The advisory policy can be used to describe how to handle medical information, handle financial transactions, and process confidential information. Answer: C is incorrect. It is not a valid type of policy.

QUESTION 3

Which of the following NIST Special Publication documents provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives?

A. NIST SP 800-37

B. NIST SP 800-26

C. NIST SP 800-53A

D. NIST SP 800-59

E. NIST SP 800-53

F. NIST SP 800-60

Correct Answer: B

NIST SP 800-26 (Security Self-Assessment Guide for Information Technology Systems) provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives.

Answer: A, E, C, D, and F are incorrect. NIST has developed a suite of documents for conducting Certification and Accreditation (CandA). These documents are as follows:

NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53: This document provides a guideline for security controls for Federal

Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59:

This document is a guideline for identifying an information system as a National Security System. NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and

risk levels.

QUESTION 4

A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?

A. Exploit

B. Mitigation

C. Transference

D. Avoidance

Correct Answer: C

When you are hiring a third party to own risk, it is known as transference risk response. Transference is a strategy to mitigate negative risks or threats. In this strategy, consequences and the ownership of a risk is transferred to a third party. This strategy does not eliminate the risk but transfers responsibility of managing the risk to another party. Insurance is an example of transference. Answer: B is incorrect. The act of spending money to reduce a risk probability and impact is known as mitigation. Answer: A is incorrect. Exploit is a strategy that may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Answer: D is incorrect. When extra activities are introduced into the project to avoid the risk, this is an example of avoidance.

QUESTION 5

The Web resource collection is a security constraint element summarized in the Java Servlet Specification v2.4. Which of the following elements does it include? Each correct answer represents a complete solution. Choose two.

A. HTTP methods

B. Role names

C. Transport guarantees

D. URL patterns

Correct Answer: AD

Web resource collection is a set of URL patterns and HTTP operations that define all resources required to be protected. It is a security constraint element summarized in the Java Servlet Specification v2.4. The Web resource collection

includes the following elements: URL patterns HTTP methods Answer: B is incorrect. An authorization constraint includes role names. Answer:

C is incorrect. A user data constraint includes transport guarantees.

[CSSLP PDF Dumps](#) [CSSLP Practice Test](#) [CSSLP Exam Questions](#)