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.pass2lead.com/csslp.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following processes describes the elements such as quantity, quality, coverage, timelines, and availability, and categorizes the different functions that the system will need to perform in order to gather the documented mission/ business needs?

A. Human factors

B. Functional requirements

C. Performance requirements

D. Operational scenarios

Correct Answer: B

The functional requirements categorize the different functions that the system will need to perform in order to gather the documented mission/business needs. The functional requirements describe the elements such as quantity, quality, coverage, timelines, and availability. Answer: C is incorrect. The performance requirements comprise of speed, throughput, accuracy, humidity tolerances, mechanical stresses such as vibrations or noises. Answer: A is incorrect. Human factor consists of factors, which affect the operation of the system or component, such as design space, eye movement, or ergonomics. Answer: D is incorrect. The operational scenarios provide assistance to the system designers and form the basis of major events in the acquisition phases, such as testing the products for system integration. The customer classifies and defines the operational scenarios, which indicate the range of anticipated uses of system products.

QUESTION 2

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 3

Which of the following are the levels of public or commercial data classification system? Each correct answer represents a complete solution. Choose all that apply.

A. Sensitive

B. Private

C. Unclassified

D. Confidential

E. Secret

F. Public

Correct Answer: ABDF

The public or commercial data classification is also built upon a four-level model, which are as follows: Public Sensitive Private Confidential Each level (top to bottom) represents an increasing level of sensitivity. The public level is similar to unclassified level military classification system. This level of data should not cause any damage if disclosed. Sensitive is a higher level of classification than public level data. This level of data requires a greater level of protection to maintain confidentiality. The Private level of data is intended for company use only. Disclosure of this level of data can damage the company. The Confidential level of data is considered very sensitive and is intended for internal use only. Disclosure of this level of data can cause serious damage to the company. Answer: C and E are incorrect. Unclassified and secret are the levels of military data classification.

QUESTION 4

Which of the following types of attacks occurs when an attacker successfully inserts an intermediary software or program between two communicating hosts?

A. Denial-of-service attack

B. Dictionary attack

C. Man-in-the-middle attack

D. Password guessing attack

Correct Answer: C

When an attacker successfully inserts an intermediary software or program between two

QUESTION 5

Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?

A. FITSAF

B. FIPS

C. TCSEC

D. SSAA

Correct Answer: C

Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information. It was replaced with the development of the Common Criteria international standard originally published in 2005. The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications. Answer: D is incorrect. System Security Authorization Agreement (SSAA) is an information security document used in the United States Department of Defense (DoD) to describe and accredit networks and systems. The SSAA is part of the Department of Defense Information Technology Security Certification and Accreditation Process, or DITSCAP (superseded by DIACAP). The DoD instruction (issues in December 1997, that describes DITSCAP and provides an outline for the SSAA document is DODI 5200.40. The DITSCAP application manual (DoD8510.1- M), published in July 2000, provides additional details. Answer: A is incorrect. FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. It provides an approach for federal agencies. It determines how federal agencies are meeting existing policy and establish goals. The main advantage of FITSAF is that it addresses the requirements of Office of Management and Budget (OMB). It also addresses the guidelines provided by the National Institute of Standards and Technology (NIsT). Answer: B is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.