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 phases of the DITSCAP CandA process is used to define the CandA level of effort, to identify the main CandA roles and responsibilities, and to create an agreement on the method for implementing the security requirements?

A. Phase 1

B. Phase 4

C. Phase 2

D. Phase 3

Correct Answer: A

The Phase 1 of the DITSCAP CandA process is known as Definition Phase. The goal of this phase is to define the CandA level of effort, identify the main CandA roles and responsibilities, and create an agreement on the method for implementing the security requirements. Answer: C is incorrect. The Phase 2 of the DITSCAP CandA process is known as Verification. Answer: D is incorrect. The Phase 3 of the DITSCAP CandA process is known as Validation. Answer: B is incorrect. The Phase 4 of the DITSCAP CandA process is known as Post Accreditation.

QUESTION 2

Which of the following are the initial steps required to perform a risk analysis process? Each correct answer represents a part of the solution. Choose three.

A. Valuations of the critical assets in hard costs.

B. Evaluate potential threats to the assets.

C. Estimate the potential losses to assets by determining their value.

D. Establish the threats likelihood and regularity.

Correct Answer: BCD

The main steps of performing risk analysis are as follows: Estimate the potential losses to the assets by determining their value. Evaluate the potential threats to the assets. Establish the threats probability and regularity. Answer: A is incorrect. Valuations of the critical assets in hard costs is one of the final steps taken after performing the risk analysis.

QUESTION 3

You are the project manager of the GHY project for your organization. You are about to start the qualitative risk analysis process for the project and you need to determine the roles and responsibilities for conducting risk management. Where can you find this information?

A. Risk register

B. Staffing management plan

C. Risk management plan

D. Enterprise environmental factors

Correct Answer: C

The risk management plan defines the roles and responsibilities for conducting risk management. A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix. Risks are built in with any project, and project managers evaluate risks repeatedly and build plans to address them. The risk management plan consists of analysis of possible risks with both high and low impacts, and the mitigation strategies to facilitate the project and avoid being derailed through which the common problems arise. Risk management plans should be timely reviewed by the project team in order to avoid having the analysis become stale and not reflective of actual potential project risks. Most critically, risk management plans include a risk strategy for project execution. Answer: A is incorrect. The risk register does not define the risk management roles and responsibilities. Answer: D is incorrect. Enterprise environmental factors may define the roles that risk management officials or departments play in the project, but the best answer for all projects is the risk management plan. Answer: B is incorrect. The staffing management plan does not define the risk management roles and responsibilities.

QUESTION 4

Which of the following security design principles supports comprehensive and simple design and implementation of protection mechanisms, so that an unintended access path does not exist or can be readily identified and eliminated?

A. Least privilege

B. Economy of mechanism

C. Psychological acceptability

D. Separation of duties

Correct Answer: B

The economy of mechanism is a security design principle, which supports simple and comprehensive design and implementation of protection mechanisms, so that an unintended access path does not exist or can be readily identified and eliminated. Answer: D is incorrect. Separation of duties defines that the completion of a specific sensitivity activity or access to sensitive object depends on the satisfaction of multiple conditions. Answer: C is incorrect. Psychological acceptability defines the ease of use and intuitiveness of the user interface that controls and interacts with the access control mechanisms. Answer: A is incorrect. Least privilege maintains that an individual, process, or other type of entity should be given the minimum privileges and resources for the minimum period of time required to complete a task.

QUESTION 5

You work as a security engineer for BlueWell Inc. You want to use some techniques and procedures to verify the effectiveness of security controls in Federal Information System. Which of the following NIST documents will guide you?

A. NIST Special Publication 800-53

B. NIST Special Publication 800-59

C. NIST Special Publication 800-53A

D. NIST Special Publication 800-37

Correct Answer: C

NIST has developed a suite of documents for conducting Certification and Accreditation (CandA). These documents are as follows: 1.NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. 2.NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. 3.NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. 4.NIST Special Publication 800-59: This document provides a guideline for identifying an information system as a National Security System. 5.NIST Special Publication 800

60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.