# 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.leads4pass.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**

To help review or design security controls, they can be classified by several criteria. One of these criteria is based on time. According to this criteria, which of the following controls are intended to prevent an incident from occurring?

A. Corrective controls

B. Adaptive controls

C. Detective controls

D. Preventive controls

Correct Answer: D

Preventive controls are the security controls that are intended to prevent an incident from occurring, e.g., by locking out unauthorized intruders. Answer: C is incorrect. Detective controls are intended to identify and characterize an incident in progress, e.g., by sounding the intruder alarm and alerting the security guards or police. Answer: A is incorrect. Corrective controls are intended to limit the extent of any damage caused by the incident, e.g., by recovering the organization to normal working status as efficiently as possible. Answer: B is incorrect. There is no such categorization of controls based on time.

**QUESTION 2**

Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle?

A. Phase 2, Verification

B. Phase 3, Validation

C. Phase 1, Definition

D. Phase 4, Post Accreditation Phase

Correct Answer: D

Phase 4, Post Accreditation Phase, of the DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle. Answer: C is incorrect. Phase 1, Definition, focuses on understanding the mission, the environment, and the architecture in order to determine the security requirements and level of effort necessary to achieve accreditation. Answer: A is incorrect. Phase 2, Verification, verifies the evolving or modified system\\'s compliance with the information agreed on in the System Security Authorization Agreement (SSAA). Answer: B is incorrect. Phase 3 validates the compliance of a fully integrated system with the information stated in the SSAA.

**QUESTION 3**

Which of the following activities are performed by the \\'Do\\' cycle component of PDCA (plan- do- check-act)? Each correct answer represents a complete solution. Choose all that apply.

A. It detects and responds to incidents properly.

B. It determines controls and their objectives.

C. It manages resources that are required to achieve a goal.

D. It performs security awareness training.

E. It operates the selected controls.

Correct Answer: ACDE

The \\'Do\\' cycle component performs the following activities: It operates the selected controls. It detects and responds to incidents properly. It performs security awareness training. It manages resources that are required to achieve a goal. Answer: B is incorrect. This activity is performed by the \\'Plan\\' cycle component of PDCA.

**QUESTION 4**

Which of the following methods offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling?

A. Service-oriented modeling framework (SOMF)

B. Service-oriented architecture (SOA)

C. Sherwood Applied Business Security Architecture (SABSA)

D. Service-oriented modeling and architecture (SOMA)

Correct Answer: A

The service-oriented modeling framework (SOMF) has been proposed by author Michael Bell as a service-oriented modeling language for software development that employs disciplines and a holistic language to provide strategic solutions to enterprise problems. The service-oriented modeling framework (SOMF) is a service-oriented development life cycle methodology. It offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling. The service-oriented modeling framework illustrates the major elements that identify the "what to do" aspects of a service development scheme. Answer: B is incorrect. The service-oriented architecture (SOA) is a flexible set of design principles used during the phases of systems development and integration. Answer: D is incorrect. The service-oriented modeling and architecture (SOMA) includes an analysis and design method that extends traditional object-oriented and component-based analysis and design methods to include concerns relevant to and supporting SOA. Answer: C is incorrect. SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. It is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives.

**QUESTION 5**

Which of the following documents were developed by NIST for conducting Certification and Accreditation (CandA)? Each correct answer represents a complete solution. Choose all that apply.

A. NIST Special Publication 800-60

B. NIST Special Publication 800-53

C. NIST Special Publication 800-37A

D. NIST Special Publication 800-59

E. NIST Special Publication 800-37

F. NIST Special Publication 800-53A

Correct Answer: ABDEF

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. Answer: C is incorrect. There is no such type of NIST document.