



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.pass4itsure.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**

RCA (root cause analysis) is an iterative and reactive method that identifies the root cause of various incidents, and the actions required to prevent these incidents from reoccurring. RCA is classified in various categories. Choose appropriate categories and drop them in front of their respective functions.

Drop Here	Function
Drop Here	It consists of plans from the health and safety areas.
Drop Here	It integrates quality control paradigms.
Drop Here	It integrates business processes.
Drop Here	It integrates failure analysis processes.
Drop Here	It integrates the methods from risk and systems analysis.

Safety-based RCA

Production-based RCA

Process-based RCA

Failure-based RCA

Systems-based RCA

Select and Place:

Drop Here	Function
Drop Here	It consists of plans from the health and safety areas.
Drop Here	It integrates quality control paradigms.
Drop Here	It integrates business processes.
Drop Here	It integrates failure analysis processes.
Drop Here	It integrates the methods from risk and systems analysis.

Safety-based RCA

Production-based RCA

Process-based RCA

Failure-based RCA

Systems-based RCA

Correct Answer:

Drop Here	Function
Safety-based RCA	It consists of plans from the health and safety areas.
Production-based RCA	It integrates quality control paradigms.
Process-based RCA	It integrates business processes.
Failure-based RCA	It integrates failure analysis processes.
Systems-based RCA	It integrates the methods from risk and systems analysis.



The various categories of root cause analysis (RCA) are as follows: Safety-based RCA. It consists of plans from the health and safety areas. Production-based RCA. It integrates quality control paradigms. Process-based RCA. It integrates business processes. Failure-based RCA. It integrates failure analysis processes as employed in engineering and maintenance. Systems-based RCA. It integrates the methods from risk and systems analysis.

QUESTION 2

Which of the following are the tasks performed by the owner in the information classification schemes? Each correct answer represents a part of the solution. Choose three.

- A. To make original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data.
- B. To review the classification assignments from time to time and make alterations as the business requirements alter.
- C. To perform data restoration from the backups whenever required.
- D. To delegate the responsibility of the data safeguard duties to the custodian.

Correct Answer: ABD

The different tasks performed by the owner are as follows: He makes the original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data. He reviews the classification assignments from time to time and makes alterations as the business needs change. He delegates the responsibility of the data safeguard duties to the custodian. He specifies controls to ensure confidentiality, integrity and availability. Answer: C is incorrect. This task is performed by the custodian and not by the owner.

QUESTION 3

Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

- A. Disaster recovery plan
- B. Business continuity plan
- C. Continuity of Operations Plan
- D. Contingency plan

Correct Answer: D

A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and triggers for initiating planned actions. Answer: A is incorrect. Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Answer: B is incorrect. It deals with the plans and procedures that identify and prioritize the critical business functions that must be preserved. Answer: C is incorrect. It includes the plans and procedures documented that ensure the continuity of critical operations during any period where normal operations are impossible.

**QUESTION 4**

Which of the following testing methods verifies the interfaces between components against a software design?

- A. Regression testing
- B. Integration testing
- C. Black-box testing
- D. Unit testing

Correct Answer: B

Integration testing is a software testing that seeks to verify the interfaces between components against a software design. Software components may be integrated in an iterative way or all together ("big bang"). Normally the former is considered a better practice since it allows interface issues to be localized more quickly and fixed. Integration testing works to expose defects in the interfaces and interaction between the integrated components (modules). Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system. Answer: A is incorrect. Regression testing focuses on finding defects after a major code change has occurred. Specifically, it seeks to uncover software regressions, or old bugs that have come back. Such regressions occur whenever software functionality that was previously working correctly stops working as intended. Typically, regressions occur as an unintended consequence of program changes, when the newly developed part of the software collides with the previously existing code. Answer: D is incorrect. Unit testing refers to tests that verify the functionality of a specific section of code, usually at the function level. In an object-oriented environment, this is usually at the class level, and the minimal unit tests include the constructors and destructors. These types of tests are usually written by developers as they work on code (white-box style), to ensure that the specific function is working as expected. One function might have multiple tests, to catch corner cases or other branches in the code. Unit testing alone cannot verify the functionality of a piece of software, but rather is used to assure that the building blocks the software uses work independently of each other. Answer: C is incorrect. The black-box testing uses external descriptions of the software, including specifications, requirements, and design to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects valid and invalid inputs and determines the correct output. There is no knowledge of the test object's internal structure. This method of test design is applicable to all levels of software testing: unit, integration, functional testing, system and acceptance. The higher the level, and hence the bigger and more complex the box, the more one is forced to use black box testing to simplify. While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested.

QUESTION 5

Which of the following security controls will you use for the deployment phase of the SDLC to build secure software? Each correct answer represents a complete solution. Choose all that apply.

- A. Change and Configuration Control
- B. Security Certification and Accreditation (CandA)
- C. Vulnerability Assessment and Penetration Testing
- D. Risk Adjustments

Correct Answer: BCD

The various security controls in the SDLC deployment phase are as follows: Secure Installation: While performing any software installation, it should kept in mind that the security configuration of the environment should never be reduced. If it is reduced then security issues and overall risks can affect the environment. Vulnerability Assessment and Penetration



Testing: Vulnerability assessments (VA) and penetration testing (PT) is used to determine the risk and attest to the strength of the software after it has been deployed. Security Certification and Accreditation (CandA): Security certification is the process used to ensure controls which are effectively implemented through established verification techniques and procedures, giving organization officials confidence that the appropriate safeguards and countermeasures are in place as means of protection. Accreditation is the provisioning of the necessary security authorization by a senior organization official to process, store, or transmit information. Risk Adjustments: Contingency plans and exceptions should be generated so that the residual risk be above the acceptable threshold.

[CSSLP PDF Dumps](#)[CSSLP VCE Dumps](#)[CSSLP Study Guide](#)