



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





QUESTION 1

Which of the following vulnerabilities occurs when an application directly uses or concatenates potentially hostile input with data file or stream functions?

- A. Insecure cryptographic storage
- B. Malicious file execution
- C. Insecure communication
- D. Injection flaw

Correct Answer: B

Malicious file execution is a vulnerability that occurs when an application directly uses or concatenates potentially hostile input with data file or stream functions. This leads to arbitrary remote and hostile data being included, processed, and invoked by the Web server. Malicious file execution can be prevented by using an indirect object reference map, input validation, or explicit taint checking mechanism. Answer: D is incorrect. Injection flaw occurs when data is sent to an interpreter as a part of command or query. Answer: A is incorrect. Insecure cryptographic storage occurs when applications have failed to encrypt data. Answer: C is incorrect. Insecure communication occurs when applications have failed to encrypt network traffic.

QUESTION 2

Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

- A. Authentication
- B. Integrity
- C. Non-repudiation
- D. Confidentiality

Correct Answer: D

The confidentiality service of a cryptographic system ensures that information will not be disclosed to any unauthorized person on a local network.

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

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 5

Which of the following components of configuration management involves periodic checks to determine the consistency and completeness of accounting information and to verify that all configuration management policies are being followed?

- A. Configuration Identification
- B. Configuration Auditing
- C. Configuration Control
- D. Configuration Status Accounting

Correct Answer: B

Configuration auditing is a component of configuration management, which involves periodic checks to establish the consistency and completeness of accounting information and to confirm that all configuration management policies are being followed. Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation. Answer: D is incorrect. The configuration status accounting procedure is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. It supports the functional and physical attributes of software at various points in time, and performs systematic control of accounting to the identified attributes for the purpose of maintaining software integrity and traceability throughout the software development life cycle. Answer: C is incorrect. Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Answer: A is incorrect. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed.

[CSSLP VCE Dumps](#)

[CSSLP Practice Test](#)

[CSSLP Exam Questions](#)