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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

A. Level 2

B. Level 3

C. Level 5

D. Level 1

E. Level 4

Correct Answer: B

The following are the five levels of FITSAF based on SEI\\'s Capability Maturity Model (CMM):

Level 1: The first level reflects that an asset has documented a security policy. Level 2: The second level shows that the asset has documented procedures and controls to implement the policy. Level 3: The third level indicates that these

procedures and controls have been implemented. Level 4: The fourth level shows that the procedures and controls are tested and reviewed. Level 5: The fifth level is the final level and shows that the asset has procedures and controls fully

integrated into a comprehensive program.

QUESTION 2

Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies?

A. OMB

B. NIST

C. NSA/CSS

D. DCAA

Correct Answer: A

The Office of Management and Budget (OMB) is a Cabinet-level office, and is the largest office within the Executive Office of the President (EOP) of the United States. The current OMB Director is Peter Orszag and was appointed by President Barack Obama. The OMB\\'s predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President\\'s spending plans, the OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. The OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President\\'s Budget and with Administration policies. Answer: D is incorrect. The DCAA has the aim to monitor contractor costs and perform contractor audits. Answer: C is incorrect. The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis. NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence. The Central Security Service is a co-located agency created to coordinate intelligence activities and co- operation between NSA and U.S. military cryptanalysis agencies. NSA\\'s work is limited to communications intelligence. It does not perform field or human intelligence activities. Answer: B is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute\\'s official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

QUESTION 3

The Software Configuration Management (SCM) process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. What are the procedures that must be defined for each software project to ensure that a sound SCM process is implemented? Each correct answer represents a complete solution. Choose all that apply.

A. Configuration status accounting

B. Configuration change control

C. Configuration identification

D. Configuration audits

E. Configuration implementation

F. Configuration deployment

Correct Answer: ABCD

The SCM process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. It identifies four procedures that must be defined for each software project to ensure that a sound SCM process is implemented. They are as follows: 1.Configuration identification: 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. 2.Configuration change control: Configuration change control is a set of processes and approval stages required to change a configuration item\\'s attributes and to re-baseline them. 3.Configuration status accounting: Configuration status accounting is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. 4.Configuration audits: 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.

QUESTION 4

Which of the following security design patterns provides an alternative by requiring that a user\\'s authentication credentials be verified by the database before providing access to that user\\'s data?

A. Secure assertion

B. Authenticated session

C. Password propagation

D. Account lockout

Correct Answer: C

Password propagation provides an alternative by requiring that a user\\'s authentication credentials be verified by the database before providing access to that user\\'s data. Answer: D is incorrect. Account lockout implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks. Answer: B is incorrect. Authenticated session allows a user to access more than one access-restricted Web page without re-authenticating every page. It also integrates user authentication into the basic session model. Answer: A is incorrect. Secure assertion distributes application-specific sanity checks throughout the system.

QUESTION 5

Which of the following NIST Special Publication documents provides a guideline on network security testing?

A. NIST SP 800-42

B. NIST SP 800-53A

C. NIST SP 800-60

D. NIST SP 800-53

E. NIST SP 800-37

F. NIST SP 800-59

Correct Answer: A

NIST SP 800-42 provides a guideline on network security testing. Answer: E, D, B, F, and C 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.

CSSLP PDF Dumps CSSLP Practice Test CSSLP Exam Questions