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

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 technologies is used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices?

A. Hypervisor

B. Grid computing

C. Code signing

D. Digital rights management

Correct Answer: D

Digital rights management (DRM) is an access control technology used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices. It describes the technology that prevents the uses of digital content that were not desired or foreseen by the content provider. DRM does not refer to other forms of copy protection which can be circumvented without modifying the file or device, such as serial works or devices. Answer: C is incorrect. Code signing is the process of digitally signing executables and scripts in order to confirm the software author, and guarantee that the code has not been altered or corrupted since it is signed by use of a cryptographic hash. Answer: A is incorrect. A hypervisor is a virtualization technique that allows multiple operating systems (guests) to run concurrently on a host computer. It is also called the virtual machine monitor (VMM). The hypervisor provides a virtual operating platform to the guest operating systems and checks their execution process. It provides isolation to the host\\'s resources. The hypervisor is installed on server hardware. Answer: B is incorrect. Grid

computing refers to the combination of computer resources from multiple administrative domains to achieve a common goal.

QUESTION 3

Which of the following models manages the software development process if the developers are limited to go back only one stage to rework?

A. Waterfall model

B. Spiral model

C. RAD model

D. Prototyping model

Correct Answer: A

In the waterfall model, software development can be managed if the developers are limited to go back only one stage to rework. If this limitation is not imposed mainly on a large project with several team members, then any developer can be working on any phase at any time, and the required rework might be accomplished several times. Answer: B is incorrect. The spiral model is a software development process combining elements of both design and prototyping-in-stages, in an effort to combine advantages of top-down and bottom-up concepts. The basic principles of the spiral model are as follows: The focus is on risk assessment and minimizing project risks by breaking a project into smaller segments and providing more ease-of- change during the development process, as well as providing the opportunity to evaluate risks and weigh consideration of project continuation throughout the life cycle. Each cycle involves a progression through the same sequence of steps, for each portion of the product and for each of its levels of elaboration, from an overall concept-of-operation document down to the coding of each individual program. Each trip around the spiral traverses the following four basic quadrants: Determine objectives, alternatives, and constraints of the iteration. Evaluate alternatives, and identify and resolve risks. Develop and verify deliverables from the iteration. Plan the next iteration. Begin each cycle with an identification of stakeholders and their win conditions, and end each cycle with review and commitment. Answer: D is incorrect. The Prototyping model is a systems development method (SDM). In this model, a prototype is created, tested, and then reworked as necessary until an adequate prototype is finally achieved from which the complete system or product can now be developed. Answer: C is incorrect. Rapid Application Development (RAD) refers to a type of software development methodology that uses minimal planning in favor of rapid prototyping.

QUESTION 4

What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

A. Project Management Information System

B. Integrated Change Control

C. Configuration Management System

D. Scope Verification

Correct Answer: C

The change management system is comprised of several components that guide the change request through the

process. When a change request is made that will affect the project scope. The Configuration Management System evaluates the change request and documents the features and functions of the change on the project scope.

QUESTION 5

DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. What phases are identified by DIACAP? Each correct

answer represents a complete solution.

Choose all that apply.

A. System Definition

B. Validation

C. Identification

D. Accreditation

E. Verification

F. Re-Accreditation

Correct Answer: ABEF

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. DIACAP replaced the former process, known as DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process), in 2006. DoD Instruction (DoDI) 8510.01 establishes a standard DoD-wide process with a set of activities, general tasks, and a management structure to certify and accredit an Automated Information System (AIS) that will maintain the Information Assurance (IA) posture of the Defense Information Infrastructure (DII) throughout the system\\'s life cycle. DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. It identifies four phases: 1.System Definition 2.Verification 3.Validation 4.Re-Accreditation