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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

Billy is the project manager of the HAR Project and is in month six of the project. The project is scheduled to last for 18 months. Management asks Billy how often the project team is participating in risk reassessment in this project. What should Billy tell management if he\\'s following the best practices for risk management?

A. Project risk management happens at every milestone.

B. Project risk management has been concluded with the project planning.

C. Project risk management is scheduled for every month in the 18-month project.

D. At every status meeting the project team project risk management is an agenda item.

Correct Answer: D

Risk management is an ongoing project activity. It should be an agenda item at every project status meeting. Answer: A is incorrect. Milestones are good times to do reviews, but risk management should happen frequently. Answer: C is incorrect. This answer would only be correct if the project has a status meeting just once per month in the project. Answer: B is management happens throughout the project as does project planning.

QUESTION 2

Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?

A. FITSAF

B. FIPS

C. TCSEC

D. SSAA

Correct Answer: C

Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information. It was replaced with the development of the Common Criteria international standard originally published in 2005. The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications. Answer: D is incorrect. System Security Authorization Agreement (SSAA) is an information security document used in the United States Department of Defense (DoD) to describe and accredit networks and systems. The SSAA is part of the Department of Defense Information Technology Security Certification and Accreditation Process, or DITSCAP (superseded by DIACAP). The DoD instruction (issues in December 1997, that describes DITSCAP and provides an outline for the SSAA document is DODI 5200.40. The DITSCAP application manual (DoD8510.1- M), published in July 2000, provides additional details. Answer: A is incorrect. FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. It provides an approach for federal agencies. It determines how federal agencies are meeting existing policy and establish goals. The main advantage of FITSAF is that it addresses the requirements of Office of Management and Budget (OMB). It also addresses the guidelines provided by the National Institute of Standards and Technology (NIsT). Answer: B is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all non-military

government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.

QUESTION 3

Which of the following testing methods tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes?

A. Integration testing

B. Acceptance testing

C. Regression testing

Correct Answer:

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. Regression testing tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes. Answer: A is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit. Answer: C is incorrect. Acceptance testing is performed on the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for which it was made. Answer: B is incorrect. 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.

QUESTION 4

The service-oriented modeling framework (SOMF) introduces five major life cycle modeling activities that drive a service evolution during design-time and run-time. Which of the following activities integrates SOA software assets and establishes SOA logical environment dependencies?

A. Service-oriented discovery and analysis modeling

B. Service-oriented business integration modeling

C. Service-oriented logical architecture modeling

D. Service-oriented logical design modeling

Correct Answer: C

The service-oriented logical architecture modeling integrates SOA software assets and establishes SOA logical environment dependencies. It also offers foster service reuse, loose coupling and consolidation. Answer: A is incorrect. The service-oriented discovery and analysis modeling discovers and analyzes services for granularity, reusability, interoperability, loose- coupling, and identifies consolidation opportunities. Answer: B is incorrect. The service-oriented business integration modeling identifies service integration and alignment opportunities with business domains\\' processes. Answer: D is incorrect. The service-oriented logical design modeling establishes service relationships and message exchange paths.

QUESTION 5

You work as a Security Manager for Tech Perfect Inc. You find that some applications have failed to encrypt network traffic while ensuring secure communications in the organization. Which of the following will you use to resolve the issue?

A. SCP

B. TLS

C. IPSec

D. HTTPS

Correct Answer: B

In order to resolve the issue, you should use TLS (Transport Layer Security). Transport Layer Security (TLS) is a cryptographic protocol that provides security and data integrity for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end. Several versions of the protocols are in wide-spread use in applications like web browsing, electronic mail, Internet faxing, instant messaging, and voiceover-IP (VoIP). The TLS protocol, an application layer protocol, allows client/server applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography. Answer: C is incorrect. Internet Protocol Security (IPSec) is a method of securing data. It secures traffic by using encryption and digital signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender verification that ensures the certainty of the datagram\\'s origin to the receiver. Answer: D is incorrect. Hypertext Transfer Protocol Secure (HTTPS) protocol is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure site. If a site has been made secure by using the Secure Sockets Layer (SSL) then HTTPS, instead of HTTP protocol, should be used as a protocol type in the URL. Answer: A is incorrect. The SCP (secure copy) protocol is a network protocol that supports file transfers. The SCP protocol, which runs on port 22, is based on the BSD RCP protocol which is tunneled through the Secure Shell (SSH) protocol to provide encryption and authentication. SCP might not even be considered a protocol itself, but merely a combination of RCP and SSH. The RCP protocol performs the file transfer and the SSH protocol performs authentication and encryption. SCP protects the authenticity and confidentiality of the data in transit. It hinders the ability for packet sniffers to extract usable information from the data packets.

Latest CSSLP Dumps CSSLP PDF Dumps CSSLP VCE Dumps