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

In 2003, NIST developed a new Certification and Accreditation (CandA) guideline known as FIPS 199. What levels of potential impact are defined by FIPS 199? Each correct answer represents a complete solution. Choose all that apply.

A. Moderate

B. Medium

C. High

D. Low

Correct Answer: BCD

In 2003, NIST developed a new Certification and Accreditation (CandA) guideline known as FIPS 199. FIPS 199 is a standard for security categorization of Federal Information and Information Systems. It defines three levels of potential impact: Low: It causes a limited adverse effect. Medium: It causes a serious adverse effect. High: It causes a severe adverse effect.

QUESTION 2

Della works as a security engineer for BlueWell Inc. She wants to establish configuration management and control procedures that will document proposed or actual changes to the information system. Which of the following phases of NIST SP 800-37 CandA methodology will define the above task?

A. Initiation

B. Security Certification

C. Continuous Monitoring

D. Security Accreditation

Correct Answer: C

The various phases of NIST SP 800-37 CandA are as follows:

Phase 1: Initiation- This phase includes preparation, notification and resource identification. It performs the security plan analysis, update, and acceptance. Phase 2: Security Certification- The Security certification phase evaluates the controls

and documentation. Phase 3: Security Accreditation- The security accreditation phase examines the residual risk for acceptability, and prepares the final security accreditation package. Phase 4: Continuous Monitoring-This phase monitors

the configuration management and control, ongoing security control verification, and status reporting and documentation.

QUESTION 3

The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. Which of the following participants are required in a NIACAP security assessment? Each correct answer represents a part of the solution. Choose all that apply.

A. Certification agent

B. Designated Approving Authority

C. IS program manager

D. Information Assurance Manager

E. User representative

Correct Answer: ABCE

The NIACAP roles are nearly the same as the DITSCAP roles. Four minimum participants (roles) are required to perform a NIACAP security assessment: IS program manager: The IS program manager is the primary authorization advocate. He is responsible for the Information Systems (IS) throughout the life cycle of the system development. Designated Approving Authority (DAA): The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. Certification agent: The certification agent is also referred to as the certifier. He provides the technical expertise to conduct the certification throughout the system life cycle. User representative: The user representative focuses on system availability, access, integrity, functionality, performance, and confidentiality in a Certification and Accreditation (CandA) process. Answer: D is incorrect. Information Assurance Manager (IAM) is one of the key participants in the DIACAP process.

QUESTION 4

Elizabeth is a project manager for her organization and she finds risk management to be very difficult for her to manage. She asks you, a lead project manager, at what stage in the project will risk management become easier. What answer best resolves the difficulty of risk management practices and the effort required?

A. Risk management only becomes easier when the project moves into project execution.

B. Risk management only becomes easier when the project is closed.

C. Risk management is an iterative process and never becomes easier.

D. Risk management only becomes easier the more often it is practiced.

Correct Answer: B

According to the PMBOK, "Like many things in project management, the more it is done the easier the practice becomes." Answer: B is incorrect. This answer is not the best choice for the project. Answer: A is incorrect. Risk management likely becomes more difficult in project execution that in other stages of the project. Answer: C is incorrect. Risk management does become easier the more often it is done.

QUESTION 5

Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces

throughout its life cycle?

A. Phase 3, Validation

B. Phase 1, Definition

C. Phase 2, Verification

D. Phase 4, Post Accreditation Phase

Correct Answer: D

Phase 4, Post Accreditation Phase of the DITSCAP includes the activities, which are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle. Answer: B is incorrect. Phase 1, Definition, focuses on understanding the mission, the environment, and the architecture in order to determine the security requirements and level of effort necessary to achieve accreditation. Answer: C is incorrect. Phase 2, Verification, verifies the evolving or modified system\\'s compliance with the information agreed on in the System Security Authorization Agreement (SSAA). Answer: A is incorrect. Phase 3 validates the compliance of a fully integrated system with the information stated in the SSAA.

Latest CSSLP Dumps CSSLP Practice Test CSSLP Exam Questions