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.passapply.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

Which of the following refers to a process that is used for implementing information security?

A. Classic information security model

B. Five Pillars model

C. Certification and Accreditation (CandA)

D. Information Assurance (IA)

Correct Answer: C

Certification and Accreditation (CandA or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The CandA process is used extensively in the U.S. Federal Government. Some CandA processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Answer: D is incorrect. Information Assurance (IA) is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of information security, which in turn grew out of practices and procedures of computersecurity. Answer: A is incorrect. The classic information security model is used in the practice of Information Assurance (IA) to define assurance requirements. The classic information security model, also called the CIA Triad, addresses three attributes of information and information systems, confidentiality, integrity, and availability. This C-I-A model is extremely useful for teaching introductory and basic concepts of information security and assurance; the initials are an easy mnemonic to remember, and when properly understood, can prompt systems designers and users to address the most pressing aspects of assurance. Answer: B is incorrect. The Five Pillars model is used in the practice of Information Assurance (IA) to define assurance requirements. It was promulgated by the U.S. Department of Defense (DoD) in a variety of publications, beginning with the National Information Assurance Glossary, Committee on National Security Systems Instruction CNSSI-4009. Here is the definition from that publication: "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." The Five Pillars model is sometimes criticized because authentication and non-repudiation are not attributes of information or systems; rather, they are procedures or methods useful to assure the integrity and authenticity of information, and to protect the confidentiality of the same.

QUESTION 2

The Phase 1 of DITSCAP CandA is known as Definition Phase. The goal of this phase is to define the CandA level of effort, identify the main CandA roles and responsibilities, and create an agreement on the method for implementing the security requirements. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Negotiation

B. Registration

C. Document mission need

D. Initial Certification Analysis

Correct Answer: ABC

The Phase 1 of DITSCAP CandA is known as Definition Phase. The goal of this phase is to define the CandA level of effort, identify the main CandA roles and responsibilities, and create an agreement on the method for implementing the security requirements. The Phase 1 starts with the input of the mission need. This phase comprises three process activities: Document mission need

QUESTION 3

Which of the following are the principle duties performed by the BIOS during POST (power-on- self-test)? Each correct answer represents a part of the solution. Choose all that apply.

A. It provides a user interface for system\\'s configuration.

B. It identifies, organizes, and selects boot devices.

C. It delegates control to other BIOS, if it is required.

D. It discovers size and verifies system memory.

E. It verifies the integrity of the BIOS code itself.

F. It interrupts the execution of all running programs.

Correct Answer: ABCDE

The principle duties performed by the BIOS during POST (power-on-self-test) are as follows: It verifies the integrity of the BIOS code itself. It discovers size and verifies system memory. It discovers, initializes, and catalogs all system hardware. It delegates control to other BIOS if it is required. It provides a user interface for system\\'s configuration. It identifies, organizes, and selects boot devices. It executes the bootstrap program. Answer: F is incorrect. The BIOS does not interrupt the execution of all running programs.

QUESTION 4

You work as a security manager for BlueWell Inc. You are going through the NIST SP 800-37 CandA methodology, which is based on four well defined phases. In which of the following phases of NIST SP 800-37 CandA methodology does the security categorization occur?

A. Security Accreditation

B. Security Certification

C. Continuous Monitoring

D. Initiation

Correct Answer: D

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 5

What are the subordinate tasks of the Initiate and Plan IA CandA phase of the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

A. Initiate IA implementation plan

B. Develop DIACAP strategy

C. Assign IA controls.

D. Assemble DIACAP team

E. Register system with DoD Component IA Program.

F. Conduct validation activity.

Correct Answer: ABCDE

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.

The subordinate tasks of the Initiate and Plan IA CandA phase are as follows: Register system with DoD Component IA Program. Assign IA controls. Assemble DIACAP team. Develop DIACAP strategy. Initiate IA implementation plan. Answer:

F is incorrect. Validation activities are conducted in the second phase of the DIACAP process, i.e., Implement and Validate Assigned IA