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

QUESTION 1

Which of the following documents were developed by NIST for conducting Certification and Accreditation (CandA)? Each correct answer represents a complete solution. Choose all that apply.

A. NIST Special Publication 800-60

B. NIST Special Publication 800-53

C. NIST Special Publication 800-37A

D. NIST Special Publication 800-59

E. NIST Special Publication 800-37

F. NIST Special Publication 800-53A

Correct Answer: ABDEF

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. Answer: C is incorrect. There is no such type of NIST document.

QUESTION 2

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 3

Which of the following are the important areas addressed by a software system\\'s security policy? Each correct answer represents a complete solution. Choose all that apply.

A. Identification and authentication

B. Punctuality

C. Data protection

D. Accountability

E. Scalability

F. Access control

Correct Answer: ACDF

The security policy of a software system addresses the following important areas:

Access control Data protection Confidentiality Integrity Identification and authentication Communication security Accountability Answer: E and B are incorrect. Scalability and punctuality are not addressed by a software system\\'s security

policy.

QUESTION 4

A number of security patterns for Web applications under the DARPA contract have been developed by Kienzle, Elder, Tyree, and Edwards-Hewitt. Which of the following patterns are applicable to aspects of authentication in Web applications?b Each correct answer represents a complete solution. Choose all that apply.

A. Authenticated session

B. Secure assertion

C. Partitioned application

D. Password authentication

E. Account lockout

F. Password propagation

Correct Answer: ADEF

The various patterns applicable to aspects of authentication in the Web applications are as follows: Account lockout: It implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks. Authenticated session: It 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. Password authentication: It provides protection against weak passwords, automated password-guessing attacks, and mishandling of passwords. Password propagation: It offers a choice by requiring that a user\\'s authentication credentials be verified by the database before providing access to that user\\'s data. Answer: B and C are incorrect. Secure assertion and partitioned application patterns are applicable to software assurance in general.

QUESTION 5

The DARPA paper defines various procedural patterns to perform secure system development practices. Which of the following patterns does it include? Each correct answer represents a complete solution. Choose three.

A. Hidden implementation

B. Document the server configuration

C. Patch proactively

D. Red team the design

E. Password propagation

Correct Answer: BCD

The following procedural patterns are defined by the DARPA paper in order to perform secure software development practices: Build the server from the ground up: It includes the following features: Build the server from the ground up. Identify the default installation of the operating system and applications. Support hardening procedures to remove unnecessary services. Identify a vulnerable service for ongoing risk management. Choose the right stuff: It defines guidelines to select right commercial off-the-shelf (COTS) components and decide whether to use and build custom components. Document the server configuration: It supports the creation of an initial configuration baseline and tracks all modifications made to servers and application configurations. Patch proactively: It supports in applying patches as soon as they are available rather than waiting until the systems cooperate. Red team the design: It supports an independent security assessment from the perspective of an attacker in the quality assurance or testing stage. An independent security assessment is helpful in addressing a security issue before it occurs. Answer: A is incorrect. Hidden implementation pattern is not defined in the DARPA paper. This pattern is applicable to software assurance in general. Hidden implementation limits the ability of an attacker to distinguish the internal workings of an application. Answer: E is incorrect. Password propagation is not defined in the DARPA paper. This pattern is applicable to aspects of authentication in a Web application. 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.