CSSLP$^{Q\&As}$

Certified Secure Software Lifecycle Professional Practice Test

Pass ISC CSSLP Exam with 100% Guarantee

Following Questions and Answers are all new published by ISC Official Exam Center

QUESTION 1

You work as a security engineer for BlueWell Inc. Which of the following documents will you use as a guide for the security certification and accreditation of Federal Information Systems?

A. NIST Special Publication 800-60

B. NIST Special Publication 800-53

C. NIST Special Publication 800-37

D. NIST Special Publication 800-59

Correct Answer: C

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.

QUESTION 2

Which of the following tiers addresses risks from an information system perspective?

A. Tier 0

B. Tier 3

C. Tier 2

D. Tier 1

Correct Answer: B

The information system level is the tier 3. It addresses risks from an information system perspective, and is guided by the risk decisions at tiers 1 and 2. Risk decisions at tiers 1 and 2 impact the ultimate selection and deployment of requisite safeguards. This also has an impact on the countermeasures at the information system level. The RMF primarily operates at tier3 but it can also have interactions at tiers 1 and 2. Answer: A is incorrect. It is an invalid Tier description. Answer: D is incorrect. The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. Answer: C is incorrect. The mission and business process level is the Tier 2, and it addresses risks from the mission and business process perspective.

QUESTION 3

You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You want to perform the following tasks: Develop a risk-driven enterprise information security architecture. Deliver security infrastructure solutions that support critical business initiatives. Which of the following methods will you use to accomplish these tasks?

A. Service-oriented modeling and architecture

B. Service-oriented modeling framework

C. Sherwood Applied Business Security Architecture

D. Service-oriented architecture

Correct Answer: C

SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. SABSA is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives. The primary characteristic of the SABSA model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited. Answer: B is incorrect. The service-oriented modeling framework (SOMF) is a service-oriented development life cycle methodology. It offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling. The service-oriented modeling framework illustrates the major elements that identify the "what to do" aspects of a service development scheme. Answer: A is incorrect. The service-oriented modeling and architecture (SOMA) includes an analysis and design method that extends traditional object-oriented and component-based analysis and design methods to include concerns relevant to and supporting SOA. Answer: D is incorrect. The service-oriented architecture (SOA) is a flexible set of design principles used during the phases of systems development and integration.

QUESTION 4

Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?

A. The custodian makes the initial information classification assignments, and the operations manager implements the scheme.

B. The data owner implements the information classification scheme after the initial assignment by the custodian.

C. The custodian implements the information classification scheme after the initial assignment by the operations manager.

D. The data custodian implements the information classification scheme after the initial assignment by the data owner.

Correct Answer: D

The data owner is responsible for ensuring that the appropriate security controls are in place, for assigning the initial classification to the data to be protected, for approving access requests from other parts of the organization, and for periodically reviewing the data classifications and access rights. Data owners are primarily responsible for determining the data\\'s sensitivity or classification levels, whereas the data custodian has the responsibility for backup, retention, and recovery of data. The data owner delegates these responsibilities to the custodian. Answer: B, A, and C are incorrect. These are not the valid answers.

QUESTION 5

Which of the following classification levels defines the information that, if disclosed to the unauthorized parties, could be reasonably expected to cause exceptionally grave damage to the national security?

A. Secret information

B. Unclassified information

C. Confidential information

D. Top Secret information

Correct Answer: D

Top Secret information is the highest level of classification of material on a national level. Such material would cause "exceptionally grave damage" to national security if publicly available. Answer: A is incorrect. Secret information is that, if disclosed to unauthorized parties, could be expected to cause serious damage to the national security, but it is not the best answer for the above question. Answer: C is incorrect. Such material would cause "damage" or be "prejudicial" to national security if publicly available. Answer: B is incorrect. Unclassified information, technically, is not a classification level, but is used for government documents that do not have a classification listed above. Such documents can sometimes be viewed by those without security clearance.