Free Questions for CSSLP

Shared by Cortez on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Certification and Accreditation (C&A or CnA) is a process for implementing information security. Which of the following is the correct order of C&A phases in a DITSCAP assessment?

Options:

A- Verification, Definition, Validation, and Post Accreditation
B- Definition, Validation, Verification, and Post Accreditation
C- Definition, Verification, Validation, and Post Accreditation
D- Verification, Validation, Definition, and Post Accreditation

Answer:

C

Explanation:

C&A consists of four phases in a DITSCAP assessment. These phases are the same as NIACAP phases. The order of these phases is as

follows:

1.Definition: The definition phase is focused on understanding the IS business case, the mission, environment, and architecture. This

phase determines the security requirements and level of effort necessary to achieve Certification & Accreditation (C&A).

2.Verification: The second phase confirms the evolving or modified system's compliance with the information. The verification phase

ensures that the fully integrated system will be ready for certification testing.

3.Validation: The third phase confirms abidance of the fully integrated system with the security policy. This phase follows the

requirements slated in the SSAA. The objective of the validation phase is to show the required evidence to support the DAA in

accreditation process.

4.Post Accreditation: The Post Accreditation is the final phase of DITSCAP assessment and it starts after the system has been certified

and accredited for operations. This phase ensures secure system management, operation, and maintenance to save an acceptable

level of residual risk.

Question 2

Question Type: MultipleChoice

Which of the following models manages the software development process if the developers are limited to go back only one stage to rework?

Options:

A- Waterfall model
B- Spiral model
C- RAD model
D- Prototyping model

Answer:

A

Explanation:

In the waterfall model, software development can be managed if the developers are limited to go back only one stage to rework. If this

limitation is not imposed mainly on a large project with several team members, then any developer can be working on any phase at any time,

and the required rework might be accomplished several times.

Answer B is incorrect. The spiral model is a software development process combining elements of both design and prototyping-in-

stages, in an effort to combine advantages of top-down and bottom-up concepts. The basic principles of the spiral model are as follows:

The focus is on risk assessment and minimizing project risks by breaking a project into smaller segments and providing more ease-of-

change during the development process, as well as providing the opportunity to evaluate risks

and weigh consideration of project

continuation throughout the life cycle.

Each cycle involves a progression through the same sequence of steps, for each portion of the product and for each of its levels of

elaboration, from an overall concept-of-operation document down to the coding of each individual program.

Each trip around the spiral traverses the following four basic quadrants:

Determine objectives, alternatives, and constraints of the iteration.

Evaluate alternatives, and identify and resolve risks.

Develop and verify deliverables from the iteration.

Plan the next iteration.

Begin each cycle with an identification of stakeholders and their win conditions, and end each cycle with review and commitment.

Answer D is incorrect. The Prototyping model is a systems development method (SDM). In this model, a prototype is created, tested,

and then reworked as necessary until an adequate prototype is finally achieved from which the complete system or product can now be

developed.

Answer C is incorrect. Rapid Application Development (RAD) refers to a type of software development methodology that uses minimal

planning in favor of rapid prototyping.

Question 3

Question Type: MultipleChoice

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

Options:

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

Answer:

A, B, D, E, F

Explanation:

NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). 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 4

Question Type: MultipleChoice

Henry is the project manager of the QBG Project for his company. This project has a budget of $4,576,900 and is expected to last 18 months to complete. The CIO, a stakeholder in the project, has introduced a scope change request for additional deliverables as part of the project work.

What component of the change control system would review the proposed changes' impact on the features and functions of the project's product?

Options:

A- Configuration management system
B- Scope change control system
C- Cost change control system
D- Integrated change control

Answer:

A

Explanation:

The configuration management system ensures that proposed changes to the project's scope are reviewed and evaluated for their affect on

the project's product.

Configuration Management System is a subsystem of the overall project management system. It is a collection of formal documented

procedures used to identify and document the functional and physical characteristics of a product, result, service, or component of the project.

It also controls any changes to such characteristics, and records and reports each change and its implementation status. It includes the

documentation, tracking systems, and defined approval levels necessary for authorizing and controlling changes. Audits are performed as part

of configuration management to determine if the requirements have been met.

Answer B is incorrect. The scope change control system focuses on reviewing the actual changes to the project scope. When a change

to the project's scope is proposed, the configuration management system is also invoked.

Answer C is incorrect. The cost change control system is responsible for reviewing and controlling changes to the project costs.

Answer D is incorrect. Integrated change control examines the affect of a proposed change on the project as a whole.

Question 5

Question Type: MultipleChoice

Which of the following terms refers to the protection of data against unauthorized access?

Options:

A- Integrity
B- Recovery
C- Auditing
D- Confidentiality

Answer:

D

Explanation:

Confidentiality is a term that refers to the protection of data against unauthorized access. Administrators can provide confidentiality by

encrypting data. Symmetric encryption is a relatively fast encryption method. Hence, this method of encryption is best suited for encrypting

large amounts of data such as files on a computer.

Answer A is incorrect. Integrity ensures that no intentional or unintentional unauthorized modification is made to data.

Answer C is incorrect. Auditing is used to track user accounts for file and object access, logon attempts, system shutdown etc. This

enhances the security of the network. Before enabling auditing, the type of event to be audited should be specified in the Audit Policy in User

Manager for Domains.

Question 6

Question Type: MultipleChoice

Which of the following steps of the LeGrand Vulnerability-Oriented Risk Management method determines the necessary compliance offered by risk management practices and assessment of risk levels?

Options:

A- Assessment, monitoring, and assurance
B- Vulnerability management
C- Risk assessment
D- Adherence to security standards and policies for development and deployment

Answer:

A

Explanation:

Assessment, monitoring, and assurance determines the necessary compliance that are offered by risk management practices and assessment

of risk levels.