Free Questions for CSSLP

Shared by Suarez on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following DITSCAP phases validates that the preceding work has produced an IS that operates in a specified computing environment?

Options:

A- Phase 2

B- Phase 4

C- Phase 1

D- Phase 3

Answer:

D

Explanation:

The Phase 3 of DITSCAP C&A is known as Validation. The goal of Phase 3 is to validate that the preceding work has produced an IS that

operates in a specified computing environment.

Answer C is incorrect. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and

create an agreement on the method for implementing the security requirements.

Answer A is incorrect. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation.

Answer B is incorrect. This phase ensures that it will maintain an acceptable level of residual risk.

Question 2

Question Type: MultipleChoice

Which of the following is a chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event?

Options:

A- Corrective controls

B- Audit trail

C- Security audit

D- Detective controls

Answer:

B

Explanation:

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from

the execution of a business process or system function. Audit records typically result from activities such as transactions or communications by

individual people, systems, accounts, or other entities. The process that creates audit trail should always run in a privileged mode, so it could

access and supervise all actions from all users, and normal user could not stop/change it. Furthermore, for the same reason, trail file or

database table with a trail should not be accessible to normal users.

Answer C is incorrect. A computer security audit is a manual or systematic measurable technical assessment of a system or application.

Manual assessments include interviewing staff, performing security vulnerability scans, reviewing application and operating system access controls, and analyzing physical access to the systems. Automated assessments, or CAAT's, include system generated audit reports or using software to monitor and report changes to files and settings on a system. Systems can include personal computers, servers, mainframes, network routers, and switches.

Answer D is incorrect. Detective controls are the audit controls that are not needed to be restricted. Any control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a Detective control. If the organization in question has not properly followed the rules, a diligent auditor should be able to detect the deficiency which indicates that some control somewhere has failed.

Answer A is incorrect. Reactive or corrective controls typically work in response to a detective control, responding in such a way as to alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself, based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or Reactive control.

Question 3

Question Type: **MultipleChoice**

Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

Options:

A- Discretionary Access Control

B- Mandatory Access Control

C- Policy Access Control

D- Role-Based Access Control

Answer:

D

Explanation:

Role-based access control (RBAC) is an access control model. In this model, a user can access resources according to his role in the

organization. For example, a backup administrator is responsible for taking backups of important data. Therefore, he is only authorized to

access this data for backing it up. However, sometimes users with different roles need to access the same resources. This situation can also

be handled using the RBAC model.

Answer B is incorrect. Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the

system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an

object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as 'secret', he cannot grant

permission to other users to see this object unless they have the appropriate permission.

Answer A is incorrect. DAC is an access control model. In this model, the data owner has the right to decide who can access the data.

This model is commonly used in PC environment. The basis of this model is the use of Access Control List (ACL).

Answer C is incorrect. There is no such access control model as Policy Access Control.

Question 4

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 5

Question Type: MultipleChoice

You are the project manager for a construction project. The project involves casting of a column in a very narrow space. Because of lack of space, casting it is highly dangerous. High technical skill will be required for casting that column. You decide to hire a local expert team for casting that column. Which of the following types of risk response are you following?

Options:

A- Avoidance

B- Acceptance

C- Mitigation

D- Transference

Answer:

D

Explanation:

According to the question, you are hiring a local expert team for casting the column. As you have transferred your risk to a third party, this is

the transference risk response that you have adopted. Transference is a strategy to mitigate negative risks or threats. In this strategy,

consequences and the ownership of a risk is transferred to a third party. This strategy does not eliminate the risk but transfers responsibility

of managing the risk to another party. Insurance is an example of transference.

Answer C is incorrect. Mitigation is a risk response planning technique associated with threats that seeks to reduce the probability of

occurrence or impact of a risk to below an acceptable threshold. Risk mitigation involves taking early action to reduce the probability and impact of a risk occurring on the project. Adopting less complex processes, conducting more tests, or choosing a more stable supplier are

examples of mitigation actions.

Answer A is incorrect. Avoidance involves changing the project management plan to eliminate the threat entirely.

Answer B is incorrect. Acceptance response is a part of Risk Response planning process. Acceptance response delineates that the

project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk does occur. Acceptance

response to a risk event is a strategy that can be used for risks that pose either threats or opportunities. Acceptance response can be of two

types:

Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk.

Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur.

Acceptance is the only response for both threats and opportunities.

Question 6

Question Type: **MultipleChoice**

Which of the following are the responsibilities of the owner with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

Options:

A- Reviewing the classification assignments at regular time intervals and making changes as the business needs change.

B- Running regular backups and routinely testing the validity of the backup data.

C- Delegating the responsibility of the data protection duties to a custodian.

D- Determining what level of classification the information requires.

Answer:

A, C, D

Explanation:

The following are the responsibilities of the owner with regard to data in an information classification program:

Determining what level of classification the information requires.

Reviewing the classification assignments at regular time intervals and making changes as the business needs change.

Delegating the responsibility of the data protection duties to a custodian.

An information owner can be an executive or a manager of an organization. He will be responsible for the asset of information that must be

protected.

Answer B is incorrect. Running regular backups and routinely testing the validity of the backup data is the responsibility of a custodian.