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.leads4pass.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

You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You have a disaster scenario and you want to discuss it with your team members for getting appropriate responses of the disaster. In which of the following disaster recovery tests can this task be performed?

A. Structured walk-through test

B. Full-interruption test

C. Parallel test

D. Simulation test

Correct Answer: D

A simulation test is a method used to test the disaster recovery plans. It operates just like a structured walk-through test. In the simulation test, the members of a disaster recovery team present with a disaster scenario and then, discuss on appropriate responses. These suggested responses are measured and some of them are taken by the team. The range of the simulation test should be defined carefully for avoiding excessive disruption of normal business activities. Answer: A is incorrect. The structured walk-through test is also known as the table-top exercise. In structured walk-through test, the team members walkthrough the plan to identify and correct weaknesses and how they will respond to the emergency scenarios by stepping in the course of the plan. It is the most effective and competent way to identify the areas of overlap in the plan before conducting more challenging training exercises. Answer: B is incorrect. A full-interruption test includes the operations that shut down at the primary site and are shifted to the recovery site according to the disaster recovery plan. It operates just like a parallel test. The full- interruption test is very expensive and difficult to arrange. Sometimes, it causes a major disruption of operations if the test fails. Answer: C is incorrect. A parallel test includes the next level in the testing procedure, and relocates the employees to an alternate recovery site and implements site activation procedures. These employees present with their disaster recovery responsibilities as they would for an actual disaster. The disaster recovery sites have full responsibilities to conduct the day-to-day organization\\'s business.

QUESTION 2

A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?

A. Exploit

B. Mitigation

C. Transference

D. Avoidance

Correct Answer: C

When you are hiring a third party to own risk, it is known as transference risk response. 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: B is incorrect. The act of spending money to reduce a risk probability and impact is known as mitigation. Answer: A is incorrect. Exploit is a strategy that may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Answer: D is incorrect. When

extra activities are introduced into the project to avoid the risk, this is an example of avoidance.

QUESTION 3

Which of the following is generally used in packages in order to determine the package or product tampering?

A. Tamper resistance

B. Tamper evident

C. Tamper data

D. Tamper proof

Correct Answer: A

Tamper resistance is resistance tampered by the users of a product, package, or system, or the users who can physically access it. It includes simple as well as complex devices. The complex device encrypts all the information between individual chips, or renders itself inoperable. Tamper resistance is generally used in packages in order to determine package or product tampering. Answer: B is incorrect. Tamper evident specifies a process or device that makes unauthorized access to the protected object easily detected. Answer: D is incorrect. Tamper proofing makes computers resistant to interference. Tamper proofing measures include automatic removal of sensitive information, automatic shutdown, and automatic physical locking. Answer: C is incorrect. Tamper data is used to view and modify the HTTP or HTTPS headers and post parameters.

QUESTION 4

Which of the following are the levels of public or commercial data classification system? Each correct answer represents a complete solution. Choose all that apply.

A. Sensitive

B. Private

C. Unclassified

D. Confidential

E. Secret

F. Public

Correct Answer: ABDF

The public or commercial data classification is also built upon a four-level model, which are as follows: Public Sensitive Private Confidential Each level (top to bottom) represents an increasing level of sensitivity. The public level is similar to unclassified level military classification system. This level of data should not cause any damage if disclosed. Sensitive is a higher level of classification than public level data. This level of data requires a greater level of protection to maintain confidentiality. The Private level of data is intended for company use only. Disclosure of this level of data can damage the company. The Confidential level of data is considered very sensitive and is intended for internal use only. Disclosure of this level of data can cause serious damage to the company. Answer: C and E are incorrect. Unclassified and secret are the levels of military data classification.

QUESTION 5

You work as a project manager for BlueWell Inc. You with your team are using a method or a (technical) process that conceives the risks even if all theoretically possible safety measures would be applied. One of your team member wants to know that what is a residual risk. What will you reply to your team member?

A. It is a risk that remains because no risk response is taken.

B. It is a risk that can not be addressed by a risk response.

C. It is a risk that will remain no matter what type of risk response is offered.

D. It is a risk that remains after planned risk responses are taken.

Correct Answer: D

Residual risks are generally smaller risks that remain in the project after larger risks have been addressed. The residual risk is the risk or danger of an action or an event, a method or a (technical) process that still conceives these dangers even if all theoretically possible safety measures would be applied. The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). Answer: B is incorrect. This is not a valid statement about residual risks. Answer: C is incorrect. This is not a valid statement about residual risks. Answer: A is incorrect. This is not a valid statement about residual risks.

QUESTION 6

Which of the following security models characterizes the rights of each subject with respect to every object in the computer system?

A. Clark-Wilson model

B. Bell-LaPadula model

C. Biba model

D. Access matrix

Correct Answer: D

The access matrix or access control matrix is an abstract, formal security model of protection state in computer systems that characterizes the rights of each subject with respect to every object in the system. It was first introduced by Butler W. Lampson in 1971. According to the access matrix model, the protection state of a computer system can be abstracted as a set of objects \\'O\\', that is the set of entities that needs to be protected (e.g. processes, files, memory pages) and a set of subjects \\'S\\' that consists of all active entities (e.g. users, processes). Further there exists a set of rights \\'R\\' of the form r(s,o), where s S, o O and r(s,o) R. A right thereby specifies the kind of access a subject is allowed to process with regard to an object. Answer: B is incorrect. The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g.,"Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public"). The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. Answer: A is incorrect. The Clark- Wilson model provides a foundation for specifying and analyzing an integrity policy for a computing system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. The

model\\'s enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. Answer: C is incorrect. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.

QUESTION 7

Joseph works as a Software Developer for WebTech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

A. Code Security law

B. Patent laws

C. Trademark laws

D. Copyright laws

Correct Answer: B

Patent laws are used to protect the duplication of software. Software patents cover the algorithms and techniques that are used in creating the software. It does not cover the entire program of the software. Patents give the author the right to make and sell his product. The time of the patent of a product is limited though, i.e., the author of the product has the right to use the patent for only a specific length of time. Answer: D is incorrect. Copyright laws protect original works or creations of authorship including literary, dramatic, musical, artistic, and certain other intellectual works.

QUESTION 8

Which of the following are Service Level Agreement (SLA) structures as defined by ITIL? Each correct answer represents a complete solution. Choose all that apply.

A. Component Based

B. Service Based

C. Segment Based

D. Customer Based

E. Multi-Level

Correct Answer: BDE

ITIL defines 3 types of Service Level Agreement (SLA) structures, which are as follows: 1.Customer Based: It covers all services used by an individual customer group. 2.Service Based: It is one service for all customers. 3.Multi-Level: Some examples of Multi-Level SLA are 3 Tier SLA encompassing Corporate and Customer and Service Layers. Answer: C and A are incorrect. There are no such SLA structures as Segment Based and Component Based.

QUESTION 9

Which of the following testing methods tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes?

A. Integration testing

B. Acceptance testing

C. Regression testing

Correct Answer:

Regression testing focuses on finding defects after a major code change has occurred. Specifically, it seeks to uncover software regressions, or old bugs that have come back. Such regressions occur whenever software functionality that was previously working correctly stops working as intended. Typically, regressions occur as an unintended consequence of program changes, when the newly developed part of the software collides with the previously existing code. Regression testing tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes. Answer: A is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit. Answer: C is incorrect. Acceptance testing is performed on the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for which it was made. Answer: B is incorrect. Integration testing is a software testing that seeks to verify the interfaces between components against a software design. Software components may be integrated in an iterative way or all together ("big bang"). Normally the former is considered a better practice since it allows interface issues to be localized more quickly and fixed. Integration testing works to expose defects in the interfaces and interaction between the integrated components (modules). Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system.

QUESTION 10

Which of the following processes does the decomposition and definition sequence of the Vee model include? Each correct answer represents a part of the solution. Choose all that apply.

A. Component integration and test

B. System security analysis

C. Security requirements allocation

D. High level software design

Correct Answer: BCD

Decomposition and definition sequence includes the following processes: System security analysis Security requirements allocation Software security requirements analysis High level software design Detailed software design Answer: A is incorrect. This process is included in the integration and verification sequence of the Vee model.

QUESTION 11

Security Test and Evaluation (STandE) is a component of risk assessment. It is useful in discovering system

vulnerabilities. For what purposes is STandE used? Each correct answer represents a complete solution. Choose all that apply.

A. To implement the design of system architecture

B. To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy

C. To assess the degree of consistency between the system documentation and its implementation

D. To uncover design, implementation, and operational flaws that may allow the violation of security policy

Correct Answer: BCD

Security Test and Evaluation (STandE) is a component of risk assessment. It is useful in discovering system vulnerabilities. According to NIST SP 800-42 (Guideline on Network Security Testing), STandE is used for the following purposes: To assess the degree of consistency between the system documentation and its implementation To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy To uncover design, implementation, and operational flaws that may allow the violation of security policy Answer: A is incorrect. STandE is not used for the implementation of the system architecture.

QUESTION 12

Which of the following governance bodies directs and coordinates implementations of the information security program?

A. Chief Information Security Officer

B. Information Security Steering Committee

C. Business Unit Manager

D. Senior Management

Correct Answer: A

Chief Information Security Officer directs and coordinates implementations of the information security program. The governance roles and responsibilities are mentioned below in the table:

Governance Body	Membership	Responsibilities
Information Security Steering Commitee	CFO, CEO, COO, CTO, VP Business units chaired by CISO	It establishes and supports security programs
Senior Management	C-level, unit VPs and senior VPs	It provides management, operational and technical controls to satisfy security requirements.
Chief Information Security Officer	CISO and staff	It directs and coordinates implementations of information security program.
Business Unit Managers	Department heads and supervisors	They Classify and establish requirements for safeguarding information assets.

QUESTION 13

Which of the following characteristics are described by the DIAP Information Readiness Assessment function? Each correct answer represents a complete solution. Choose all that apply.

A. It provides for entry and storage of individual system data.

B. It performs vulnerability/threat analysis assessment.

C. It provides data needed to accurately assess IA readiness.

D. It identifies and generates IA requirements.

Correct Answer: BCD

The characteristics of the DIAP Information Readiness Assessment function are as follows: It provides data needed to accurately assess IA readiness. It identifies and generates IA requirements. It performs vulnerability/threat analysis assessment. Answer: A is incorrect. It is a function performed by the ASSET system.

QUESTION 14

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 15

Which of the following are the goals of risk management? Each correct answer represents a complete solution. Choose three.

A. Identifying the risk

B. Assessing the impact of potential threats

C. Identifying the accused

D. Finding an economic balance between the impact of the risk and the cost of the countermeasure

Correct Answer: ABD

There are three goals of risk management as follows: Identifying the risk Assessing the impact of potential threats Finding an economic balance between the impact of the risk and the cost of the countermeasure Answer: C is incorrect. Identifying the accused does not come under the scope of risk management.