Vendor:ISC

Exam Code:CSSLP

Exam Name: Certified Secure Software Lifecycle Professional Practice Test

Version: Demo

QUESTION 1

Which of the following are the types of intellectual property? Each correct answer represents a complete solution. Choose all that apply.

A. Patent

B. Copyright

C. Standard

D. Trademark

Correct Answer: AB

Common types of intellectual property include copyrights, trademarks, patents, industrial design rights, and trade secrets. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. A trademark is a distinctive sign used by an individual, business organization, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities. A trademark is designated by the following symbols: : It is for an unregistered trade mark and it is used to promote or brand goods. : It is for an unregistered service mark and it is used to promote or brand services. : It is for a registered trademark. A patent is a set of exclusive rights granted by a state to an inventor or their assignee for a limited period of time in exchange for a public disclosure of an invention. Answer: C is incorrect. It is not a type of intellectual property.

QUESTION 2

Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle?

A. Phase 3, Validation

B. Phase 1, Definition

C. Phase 2, Verification

D. Phase 4, Post Accreditation Phase

Correct Answer: D

Phase 4, Post Accreditation Phase of the DITSCAP includes the activities, which are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle. Answer: B is incorrect. Phase 1, Definition, focuses on understanding the mission, the environment, and the architecture in order to determine the security requirements and level of effort necessary to achieve accreditation. Answer: C is incorrect. Phase 2, Verification, verifies the evolving or modified system\\'s compliance with the information agreed on in the System Security Authorization Agreement (SSAA). Answer: A is incorrect. Phase 3 validates the compliance of a fully integrated system with the information stated in the SSAA.

QUESTION 3

In which of the following types of tests are the disaster recovery checklists distributed to the members of disaster recovery team and asked to review the assigned checklist?

A. Parallel test

B. Simulation test

C. Full-interruption test

D. Checklist test

Correct Answer: D

A checklist test is a test in which the disaster recovery checklists are distributed to the members of the disaster recovery team. All members are asked to review the assigned checklist. The checklist test is a simple test and it is easy to conduct this test. It allows to accomplish the following three goals: It ensures that the employees are aware of their responsibilities and they have the refreshed knowledge. It provides an individual with an opportunity to review the checklists for obsolete information and update any items that require modification during the changes in the organization. It ensures that the assigned members of disaster recovery team are still working for the organization. Answer: B is incorrect. 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. 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. Answer: C 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.

QUESTION 4

Which of the following statements reflect the \\'Code of Ethics Canons\\' in the \\'(ISC)2 Code of Ethics\\'? Each correct answer represents a complete solution. Choose all that apply.

A. Act honorably, honestly, justly, responsibly, and legally.

B. Give guidance for resolving good versus good and bad versus bad dilemmas.

C. Provide diligent and competent service to principals.

D. Protect society, the commonwealth, and the infrastructure.

Correct Answer: ACD

The Code of Ethics Canons in (ISC)2 code of ethics are as follows: Protect society, the commonwealth, and the infrastructure. Act honorably, honestly, justly, responsibly, and legally. Provide diligent and competent service to principals. Advance and protect the profession.

QUESTION 5

Which of the following is a signature-based intrusion detection system (IDS) ?

A. RealSecure

B. StealthWatch

C. Tripwire

D. Snort

Correct Answer: D

Snort is a signature-based intrusion detection system. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as follows: Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console. Packet logger mode: It logs the packets to the disk. Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user-defined rule set. Answer: B is incorrect. StealthWatch is a behavior-based intrusion detection system. Answer: A is incorrect. RealSecure is a network-based IDS that monitors TCP, UDP and ICMP traffic and is configured to look for attack patterns. Answer: C is incorrect. Tripwire is a file integrity checker for UNIX/Linux that can be used for host-based intrusion detection.

QUESTION 6

Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one?

A. Configuration Identification

B. Configuration Verification and Auditing

C. Configuration Status Accounting

D. Configuration Item Costing

Correct Answer: D

Configuration item cost is not a valid activity for configuration management. Cost changes are managed by the cost change control system; configuration management is concerned with changes to the features and functions of the project deliverables.

QUESTION 7

John works as a security manager for SoftTech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?

A. Full-scale exercise

B. Walk-through drill

C. Structured walk-through test

D. Evacuation drill

Correct Answer: C

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: A is incorrect. In full-scale exercise, the critical systems run at an alternate site. Answer: B is incorrect. The emergency management group and response teams actually perform their emergency response functions by walking through the test, without actually initiating recovery procedures. But it is not much cost effective. Answer: D is incorrect. It is a test performed when personnel walks through the evacuation route to a designated area where procedures for accounting for the personnel are tested.

QUESTION 8

Frank is the project manager of the NHH Project. He is working with the project team to create a plan to document the procedures to manage risks throughout the project. This document will define how risks will be identified and quantified. It will also define how contingency plans will be implemented by the project team. What document is Frank and the NHH Project team creating in this scenario?

A. Risk management plan

B. Project plan

C. Project management plan

D. Resource management plan

Correct Answer: A

The risk management plan, part of the comprehensive management plan, defines how risks will be identified, analyzed, monitored and controlled, and even responded to. A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix. Risks are built in with any project, and project managers evaluate risks repeatedly and build plans to address them. The risk management plan consists of analysis of possible risks with both high and low impacts, and the mitigation strategies to facilitate the project and avoid being derailed through which the common problems arise. Risk management plans should be timely reviewed by the project team in order to avoid having the analysis become stale and not reflective of actual potential project risks. Most critically, risk management plans include a risk strategy for project execution. Answer: C is incorrect. The project management plan is a comprehensive plan that communicates the intent of the project for all project management knowledge areas. Answer: B is incorrect. The project plan is not an official PMBOK project management plan. Answer: D is incorrect. The resource management plan defines the management of project resources, such as project team members, facilities, equipment, and contractors.

QUESTION 9

The Phase 2 of DITSCAP CandA is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Certification analysis

B. Assessment of the Analysis Results

C. Configuring refinement of the SSAA

D. System development

E. Registration

Correct Answer: ABCD

The Phase 2 of DITSCAP CandA is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. This phase takes place between the signing of the initial version of the SSAA and the formal accreditation of the system. This phase verifies security requirements during system development. The process activities of this phase are as follows: Configuring refinement of the SSAA System development Certification analysis Assessment of the Analysis Results Answer: E is incorrect. Registration is a Phase 1 activity.

QUESTION 10

In which of the following architecture styles does a device receive input from connectors and generate transformed outputs?

A. N-tiered

B. Heterogeneous

C. Pipes and filters

D. Layered

Correct Answer: C

In the pipes and filters architecture style, a device receives input from connectors and generates transformed outputs. A pipeline has a series of processing elements in which the output of each element works as an input of the next element. A little amount of buffering is provided between the two successive elements.

QUESTION 11

Which of the following ISO standards provides guidelines for accreditation of an organization that is concerned with certification and registration related to ISMS?

A. ISO 27006

B. ISO 27005

C. ISO 27003

D. ISO 27004

Correct Answer: A

ISO 27006 is an information security standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information technology - Security techniques Requirements for bodies providing audit and certification of information security management systems". The ISO 27006 standard provides guidelines for accreditation of an organization which is concerned with certification and registration related to ISMS. The ISO 27006 standard contains the following elements: Scope Normative references Terms and definitions Principles General requirements Structural requirements Resource requirements Information requirements Process requirements Management system requirements for certification bodies Information security risk communication Information security risk monitoring and review Annex A. Defining the scope of process Annex B. Asset valuation and impact assessment Annex C. Examples of typical threats Annex D. Vulnerabilities and vulnerability assessment methods Annex E. Information security risk assessment (ISRA) approaches Answer: C is incorrect. The ISO 27003 standard provides guidelines for implementing an ISMS (Information Security Management System). Answer: D is incorrect. The ISO 27004 standard provides guidelines on specifications and use of measurement techniques for the assessment of the effectiveness of an implemented information security management system and controls. Answer: B is incorrect. The ISO 27005 standard provides guidelines for information security risk management.

QUESTION 12

Which of the following terms ensures that no intentional or unintentional unauthorized modification is made to data?

A. Non-repudiation

B. Integrity

C. Authentication

D. Confidentiality

Correct Answer: B

Integrity ensures that no intentional or unintentional unauthorized modification is made to data. Answer: D is incorrect. Confidentiality refers to the protection of data against unauthorized access. Administrators can provide confidentiality by encrypting data. Answer: A is incorrect. Non-repudiation is a mechanism to prove that the sender really sent this message. Answer: C is incorrect. Authentication is the process of verifying the identity of a person or network host.