Free Questions for CSSLP by certsinside

Shared by Woodard on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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.

Options:

A- Component integration and test

B- System security analysis

C- Security requirements allocation

D- High level software design

Answer:

B, C, D

Explanation:

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 2

Question Type: MultipleChoice

To help review or design security controls, they can be classified by several criteria. One of these criteria is based on time. According to this criteria, which of the following controls are intended to prevent an incident from occurring?

Options:

A- Corrective controls

B- Adaptive controls

C- Detective controls

D- Preventive controls

Answer:

D

Explanation:

Preventive controls are the security controls that are intended to prevent an incident from occurring, e.g., by locking out unauthorized intruders.

Answer C is incorrect. Detective controls are intended to identify and characterize an incident in progress, e.g., by sounding the intruder alarm and alerting the security guards or police.

Answer A is incorrect. Corrective controls are intended to limit the extent of any damage caused by the incident, e.g., by recovering the organization to normal working status as efficiently as possible.

Answer B is incorrect. There is no such categorization of controls based on time.

Question 3

Question Type: MultipleChoice

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?

Options:

A- Phase 2, Verification

B- Phase 3, Validation

C- Phase 1, Definition

D- Phase 4, Post Accreditation Phase

Answer:

D

Explanation:

Phase 4, Post Accreditation Phase, of the 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.

Answer C 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 A 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 B is incorrect. Phase 3 validates the compliance of a fully integrated system with the information stated in the SSAA.

Question 4

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 5

Question Type: MultipleChoice

The rights of an author or a corporation to make profit from the creation of their products (such as software, music, etc.) are protected by the Intellectual Property law. Which of the following are the components of the Intellectual Property law?

Each correct answer represents a part of the solution. Choose two.

Options:

A- Trademark law

B- Industrial Property law

C- Copyright law

D- Patent law

Answer:

B, C

Explanation:

The Industrial Property law and the Copyright law are the components of the Intellectual Property law.

Question 6

Question Type: MultipleChoice

You work as a Security Manager for Tech Perfect Inc. You find that some applications have failed to encrypt network traffic while ensuring secure communications in the organization. Which of the following will you use to resolve the issue?

Options:

A- SCP

B- TLS

C- IPSec

D- HTTPS

Answer:

B

Explanation:

In order to resolve the issue, you should use TLS (Transport Layer Security). Transport Layer Security (TLS) is a cryptographic protocol that

provides security and data integrity for communications over networks such as the Internet. TLS and SSL encrypt the segments of network

connections at the Transport Layer end-to-end. Several versions of the protocols are in wide-spread use in applications like web browsing,

electronic mail, Internet faxing, instant messaging, and voice-over-IP (VoIP). The TLS protocol, an application layer protocol, allows

client/server applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery.

TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography.

Answer C is incorrect. Internet Protocol Security (IPSec) is a method of securing data. It secures traffic by using encryption and digital

signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender verification

that ensures the certainty of the datagram's origin to the receiver.

Answer D is incorrect. Hypertext Transfer Protocol Secure (HTTPS) protocol is a protocol used in the Universal Resource Locater (URL)

address line to connect to a secure site. If a site has been made secure by using the Secure Sockets Layer (SSL) then HTTPS, instead of HTTP

protocol, should be used as a protocol type in the URL.

Answer A is incorrect. The SCP (secure copy) protocol is a network protocol that supports file transfers. The SCP protocol, which runs on

port 22, is based on the BSD RCP protocol which is tunneled through the Secure Shell (SSH) protocol to provide encryption and authentication.

SCP might not even be considered a protocol itself, but merely a combination of RCP and SSH. The RCP protocol performs the file transfer and

the SSH protocol performs authentication and encryption. SCP protects the authenticity and confidentiality of the data in transit. It hinders the

ability for packet sniffers to extract usable information from the data packets.

Question 7

Question Type: MultipleChoice

Security controls are safeguards or countermeasures to avoid, counteract, or minimize security risks. Which of the following are types of security controls?

Each correct answer represents a complete solution. Choose all that apply.

Options:

A- Common controls

B- Hybrid controls

C- Storage controls

D- System-specific controls

Answer:

A, B, D

Explanation:

Security controls are safeguards or countermeasures to avoid, counteract, or minimize security risks. The following are the types of security

controls for information systems, that can be employed by an organization:

1.System-specific controls: These types of security controls provide security capability for a particular information system only.

2.Common controls: These types of security controls provide security capability for multiple information systems.

3.Hybrid controls: These types of security controls have features of both system-specific and common controls.

Answer C is incorrect. It is an invalid control.

Question 8

Question Type: MultipleChoice

In which of the following phases of the SDLC does the software and other components of the system faithfully incorporate the design specifications and provide proper documentation and training?

Options:

A- Design

B- Evaluation and acceptance

C- Programming and training

D- Initiation

Answer:

C

Explanation:

In the programming and training phase of the SDLC, the software and other components of the system faithfully incorporate the design specifications, and proper documentation and training are provided.

Answer D is incorrect. During the initiation phase, the need for a system is expressed and the purpose of the system is documented.

Answer A is incorrect. During the design phase, systems requirements are incorporated into design. This phase specifies to include

controls that support the auditing of the system.

Answer B is incorrect. During the evaluation and acceptance phase, the system and data are validated, all the control requirements and the user requirements are met by the system.

Question 9

Question Type: MultipleChoice

Which of the following are the types of intellectual property?

Each correct answer represents a complete solution. Choose all that apply.

Options:

A- Patent

B- Copyright

C- Standard

D- Trademark

Answer:

A, B, D

Explanation:

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 10

Question Type: MultipleChoice

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies?

Each correct answer represents a complete solution. Choose all that apply.

Options:

A- Advisory

B- Systematic

C- Informative

D- Regulatory

Answer:

A, C, D

Explanation:

Following are the different types of policies:

Regulatory: This type of policy ensures that the organization is following standards set by specific industry regulations. This policy type is very detailed and specific to a type of industry. This is used in financial institutions, health care facilities, public utilities, and other government-regulated industries, e.g., TRAI.

Advisory: This type of policy strongly advises employees regarding which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and

activities. This policy type can be used, for example, to describe how to handle medical information, handle financial transactions, or process confidential information.

Informative: This type of policy informs employees of certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the company. It could explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations.

Answer B is incorrect. No such type of policy exists.

Question 11

Question Type: MultipleChoice

In which of the following IDS evasion attacks does an attacker send a data packet such that IDS accepts the data packet but the host computer rejects it?

Options:

A- Evasion attack

B- Fragmentation overlap attack

C- Fragmentation overwrite attack

D- Insertion attack

Answer:

D

Explanation:

In an insertion attack, an IDS accepts a packet and assumes that the host computer will also accept it. But in reality, when a host system

rejects the packet, the IDS accepts the attacking string that will exploit vulnerabilities in the IDS. Such attacks can badly infect IDS signatures

and IDS signature analysis.

Answer B is incorrect. In this approach, an attacker sends packets in such a manner that one packet fragment overlaps data from a

previous fragment. The information is organized in the packets in such a manner that when the victim's computer reassembles the packets, an

attack string is executed on the victim's computer. Since the attacking string is in fragmented form, IDS is unable to detect it.

Answer C is incorrect. In this approach, an attacker sends packets in such a manner that one packet fragment overwrites data from a

previous fragment. The information is organized into the packets in such a manner that when the victim's computer reassembles the packets,

an attack string is executed on the victim's computer. Since the attacking string is in fragmented form, IDS becomes unable to detect it.

Answer A is incorrect. An evasion attack is one in which an IDS rejects a malicious packet but the host computer accepts it. Since an IDS

has rejected it, it does not check the contents of the packet. Hence, using this technique, an attacker can exploit the host computer. In many

cases, it is quite simple for an attacker to send such data packets that can easily perform evasion attacks on an IDSs.

Question 12

Question Type: **MultipleChoice**

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?

Options:

A- Service-oriented modeling and architecture

B- Service-oriented modeling framework

C- Sherwood Applied Business Security Architecture

D- Service-oriented architecture

Answer:

C

Explanation:

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.