Free Questions for CSSLP by dumpshq

Shared by Anthony on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: FillInTheBlank

Fill in the blank with an appropriate phrase The is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity.

Answer:

Explanation:

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 2

Question Type: MultipleChoice

Which of the following are the phases of the Certification and Accreditation (C&A) process?

Each correct answer represents a complete solution. Choose two.

Options:

A- Continuous Monitoring

B- Auditing

C- Detection

D- Initiation

Answer:

A, D

Explanation:

The Certification and Accreditation (C&A) process consists of four distinct phases:

1.Initiation

2.Security Certification

3.Security Accreditation

4.Continuous Monitoring

The C&A activities can be applied to an information system at appropriate phases in the system development life cycle by selectively tailoring

the various tasks and subtasks.

Answer B and C are incorrect. Auditing and detection are not phases of the Certification and Accreditation process.

Question 3

Question Type: **MultipleChoice**

You work as an analyst for Tech Perfect Inc. You want to prevent information flow that may cause a conflict of interest in your organization representing competing clients. Which of the following security models will you use?

Options:

A- Bell-LaPadula model

B- Chinese Wall model

C- Clark-Wilson model

D- Biba model

Answer:

B

Explanation:

The Chinese Wall Model is the basic security model developed by Brewer and Nash. This model prevents information flow that may cause a

conflict of interest in an organization representing competing clients. The Chinese Wall Model provides both privacy and integrity for data.

Answer D 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.

Answer C 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 A 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.

Question 4

Question Type: MultipleChoice

You work as a project manager for BlueWell Inc. You are preparing to plan risk responses for your project with your team. How many risk response types are available for a negative risk event in the project?

Options:

A- Three

B- Seven

C- One

D- Four

Answer:

D

Explanation:

There are four risk responses available for a negative risk event.

The risk response strategies for negative risks are:

Avoid: It involves altering the project management plan to remove the threats completely.

Transfer: It requires shifting some or all of the negative effects of a threat including the ownership of response, to a third party.

Mitigate: It implies a drop in the probability and impact of an unfavorable risk event to be within suitable threshold limits.

Accept: It delineates that the project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk occurs. It is used for both negative and positive risks.

Answer C is incorrect. There are four responses for negative risk events.

Answer A is incorrect. There are four, not three, responses for negative risk events. Do not forget that acceptance can be used for negative risk events.

Answer B is incorrect. There are seven total risk responses, four of which can be used for negative risk events.

Question 5

Question Type: **MultipleChoice**

You are the project manager of the GHY project for your organization. You are about to start the qualitative risk analysis process for the project and you need to determine the roles and responsibilities for conducting risk management. Where can you find this information?

Options:

A- Risk register

B- Staffing management plan

C- Risk management plan

D- Enterprise environmental factors

Answer:

C

Explanation:

The risk management plan defines the roles and responsibilities for conducting risk management.

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 A is incorrect. The risk register does not define the risk management roles and responsibilities.

Answer D is incorrect. Enterprise environmental factors may define the roles that risk management officials or departments play in the

project, but the best answer for all projects is the risk management plan.

Answer B is incorrect. The staffing management plan does not define the risk management roles and responsibilities.

Question 6

Question Type: **MultipleChoice**

Who amongst the following makes the final accreditation decision?

Options:

A- ISSE

B- CRO

C- DAA

D- ISSO

Answer:

C

Explanation:

The DAA, also known as Authorizing Official, makes the final accreditation decision. The Designated Approving Authority (DAA), in the United

States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level

of risk. The DAA is responsible for implementing system security. The DAA can grant the accreditation and can determine that the system's

risks are not at an acceptable level and the system is not ready to be operational.

Answer D is incorrect. An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information

System Security Officer (ISSO) are as follows:

Manages the security of the information system that is slated for Certification & Accreditation (C&A).

Insures the information systems configuration with the agency's information security policy.

Supports the information system owner/information owner for the completion of security-related responsibilities.

Takes part in the formal configuration management process.

Prepares Certification & Accreditation (C&A) packages.

Answer A is incorrect. An Information System Security Engineer (ISSE) plays the role of an advisor. The responsibilities of an

Information System Security Engineer are as follows:

Provides view on the continuous monitoring of the information system.

Provides advice on the impacts of system changes.

Takes part in the configuration management process.

Takes part in the development activities that are required to implement system changes.

Follows approved system changes.

Answer B is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief

Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks,

and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational,

financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk

and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management

(ERM) approach.

Question 7

Question Type: MultipleChoice

Which of the following statements about a host-based intrusion prevention system (HIPS) are true?

Each correct answer represents a complete solution. Choose two.

Options:

A- It can detect events scattered over the network.

B- It is a technique that allows multiple computers to share one or more IP addresses.

C- It can handle encrypted and unencrypted traffic equally.

D- It cannot detect events scattered over the network.

Answer:

C, D

Explanation:

A host-based intrusion prevention system (HIPS) is an application usually employed on a single computer. It complements traditional finger-

print-based and heuristic antivirus detection methods, since it does not need continuous updates to stay ahead of new malware. When a

malicious code needs to modify the system or other software residing on the machine, a HIPS system will notice some of the resulting changes

and prevent the action by default or notify the user for permission. It can handle encrypted and unencrypted traffic equally and cannot detect

events scattered over the network.

Answer B is incorrect. Network address translation (NAT) is a technique that allows multiple computers to share one or more IP

addresses. NAT is configured at the server between a private network and the Internet. It allows the computers in a private network to share

a global, ISP assigned address. NAT modifies the headers of packets traversing the server. For packets outbound to the Internet, it translates

the source addresses from private to public, whereas for packets inbound from the Internet, it translates the destination addresses from

public to private.

Answer A is incorrect. Network intrusion prevention system (NIPS) is a hardware/software platform that is designed to analyze, detect,

and report on security related events. NIPS is designed to inspect traffic and based on its configuration or security policy, it can drop malicious

traffic. NIPS is able to detect events scattered over the network and can react.

Question 8

Question Type: MultipleChoice

In which of the following deployment models of cloud is the cloud infrastructure administered by the organizations or a third party? Each correct answer represents a complete solution. Choose two.

Options:

A- Private cloud

B- Public cloud

C- Hybrid cloud

D- Community cloud

Answer:

A, D

Explanation:

In private cloud, the cloud infrastructure is operated exclusively for an organization. The private cloud infrastructure is administered by the

organization or a third party, and exists on premise and off premise.

In community cloud, the cloud infrastructure is shared by a number of organizations and supports a particular community. The community cloud

infrastructure is administered by the organizations or a third party and exists on premise or off premise.

Answer B is incorrect. In public cloud, the cloud infrastructure is administered by an organization that sells cloud services.

Answer C is incorrect. In hybrid cloud, the cloud infrastructure is administered by both, i.e., an organization and a third party.

Question 9

Question Type: **MultipleChoice**

Which of the following disaster recovery tests includes the operations that shut down at the primary site, and are shifted to the recovery site according to the disaster recovery plan?

Options:

A- Structured walk-through test

B- Full-interruption test

C- Parallel test

D- Simulation test

Answer:

B

Explanation:

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 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 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.

Answer D 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.

Question 10

Question Type: MultipleChoice

The NIST ITL Cloud Research Team defines some primary and secondary technologies as the fundamental elements of cloud computing in its "Effectively and Securely Using the Cloud Computing Paradigm" presentation. Which of the following technologies are included in the primary technologies?

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

Options:

A- Web application framework

B- Free and open source software

C- SOA

D- Virtualization

Answer:

B, C, D

Explanation:

The primary technologies defined by the NIST ITL Cloud Research Team in its 'Effectively and Securely Using the Cloud Computing Paradigm'

presentation are as follows:

Virtualization

Grid technology

SOA (Service Oriented Architecture)

Distributed computing

Broadband network

Browser as a platform

Free and open source software

Answer A is incorrect. It is defined as the secondary technology.

Question 11

Question Type: **MultipleChoice**

Which of the following components of configuration management involves periodic checks to determine the consistency and completeness of accounting information and to verify that all configuration management policies are being followed?

Options:

A- Configuration Identification

B- Configuration Auditing

C- Configuration Control

D- Configuration Status Accounting

Answer:

B

Explanation:

Configuration auditing is a component of configuration management, which involves periodic checks to establish the consistency and

completeness of accounting information and to confirm that all configuration management policies are being followed. Configuration audits are

broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional

configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration

audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.

Answer D is incorrect. The configuration status accounting procedure is the ability to record and report on the configuration baselines

associated with each configuration item at any moment of time. It supports the functional and physical attributes of software at various points

in time, and performs systematic control of accounting to the identified attributes for the purpose of maintaining software integrity and

traceability throughout the software development life cycle.

Answer C is incorrect. Configuration control is a procedure of the Configuration management. Configuration control is a set of

processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the

functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes.

Answer A is incorrect. Configuration identification is the process of identifying the attributes that define every aspect of a configuration

item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in

configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the

event that these attributes are changed.

Question 12

Question Type: MultipleChoice

A service provider guarantees for end-to-end network traffic performance to a customer. Which of the following types of agreement is this?

Options:

A- SLA

B- VPN

C- NDA

D- LA

Answer:

A

Explanation:

This is a type of service-level agreement.

A service-level agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. It records a common understanding about services, priorities, responsibilities, guarantees, and warranties. Each area of service scope should have the 'level of service' defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service, such as billing.

Answer C is incorrect. Non-disclosure agreements (NDAs) are often used to protect the confidentiality of an invention as it is being evaluated by potential licensees.

Answer D is incorrect. License agreements (LA) describe the rights and responsibilities of a party related to the use and exploitation of intellectual property.

Answer B is incorrect. There is no such type of agreement as VPN.