Free Questions for Cybersecurity-Audit-Certificate by actualtestdumps

Shared by Weaver on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The risk of an evil twin attack on mobile devices is PRIMARILY due to:

Options:

A- tokens stored as plain text in many mobile device applications.

B- use of data transmission that is not always encrypted.

C- generic names that mobile devices will accept without verification.

D- weak authentication protocols in wireless networks.

Answer:

C

Explanation:

The risk of an evil twin attack on mobile devices is PRIMARILY due to theuse of generic names that mobile devices will accept without verification. An evil twin attack is a type of wireless network attack where an attacker sets up a rogue access point that mimics a legitimate one. The attacker can then lure unsuspecting users to connect to the rogue access point and intercept their data or launch

further attacks. Mobile devices are vulnerable to evil twin attacks because they often use generic names for their wireless networks, such as "Free WiFi" or "Public Hotspot". These names can be easily spoofed by an attacker and accepted by mobile devices without verifying the identity or security of the access point.

Question 2

Question Type: MultipleChoice

Which of the following cloud characteristics refers to resource utilization that can be optimized by leveraging charge-per-use capabilities?

Options:

A- On demand self-service

B- Elasticity

C- Measured service

D- Resource pooling

Answer:

C

Explanation:

The cloud characteristic that refers to resource utilization that can be optimized by leveraging charge-per-use capabilities is measured service. This is because measured service is a characteristic of cloud computing that involves monitoring, controlling, and reporting on the usage and consumption of cloud resources by cloud providers and consumers. Measured service helps to optimize resource utilization by leveraging charge-per-use capabilities, which means that cloud consumers only pay for the amount of resources that they actually use or consume, rather than paying for fixed or predetermined amounts of resources. The other options are not cloud characteristics that refer to resource utilization that can be optimized by leveraging charge-per-use capabilities, but rather different characteristics of cloud computing that describe other aspects or benefits of cloud services, such as on demand self-service (A), elasticity (B), or resource pooling (D).

Question 3

Question Type: MultipleChoice

Which of the following is the GREATEST drawback when using the AICPA/CICA Trust Sen/ices to evaluate a cloud service provider?

Options:

A- Incompatibility with cloud service business model

B- Lack of specificity m the principles

C- Omission of confidentiality in the criteria

D- Inability to issue SOC 2 or SOC 3 reports

Answer:

B

Explanation:

The GREATEST drawback when using the AICPA/CICA Trust Services to evaluate a cloud service provider is the lack of specificity in the principles. This is because the AICPA/CICA Trust Services are a set of principles and criteria that provide guidance for evaluating and reporting on controls over information systems and services. However, the principles and criteria are very broad and generic, and do not address the specific risks and challenges that are associated with cloud services, such as data sovereignty, multi-tenancy, portability, etc. The other options are not drawbacks when using the AICPA/CICA Trust Services to evaluate a cloud service provider, but rather different aspects or benefits of using the AICPA/CICA Trust Services to evaluate a cloud service provider, such as compatibility (A), confidentiality , or reporting (D).

Question 4

Question Type: MultipleChoice

Which of the following BEST characterizes security mechanisms for mobile devices?

Options:

A- Easy to control through mobile device management

B- Comparatively weak relative to workstations

C- Inadequate for organizational use

D- Configurable and reliable across device types

Answer:

A

Explanation:

The BEST characteristic that describes security mechanisms for mobile devices is easy to control through mobile device management. This is because mobile device management is a technique that allows organizations to centrally manage and secure mobile devices, such as smartphones, tablets, laptops, etc., that are used by their employees or customers. Mobile device management helps to enforce security policies, configure settings, install applications, monitor usage, wipe data, etc., on mobile devices remotely and efficiently. The other options are not characteristics that describe security mechanisms for mobile devices, but rather different aspects or factors that affect security mechanisms for mobile devices, such as weakness (B), inadequacy , or reliability (D).

Question 5

Question Type: MultipleChoice

Which of the following should an IS auditor do FIRST to ensure cyber security-related legal and regulatory requirements are followed by an organization?

Options:

A- Determine if the cybersecurity program is mapped to relevant legal and regulatory requirements.

B- Review the most recent legal and regulatory audit report conducted by an independent party.

C- Determine if there is a formal process to review changes in legal and regulatory requirements.

D- Obtain a list of relevant legal and regulatory requirements.

Answer:

A

Explanation:

The FIRST thing that an IS auditor should do to ensure cyber security-related legal and regulatory requirements are followed by an organization is to determine if the cybersecurity program is mapped to relevant legal and regulatory requirements. This is because mapping the cybersecurity program to relevant legal and regulatory requirements helps to ensure that the organization has identified and addressed all the applicable laws and regulations that affect its cybersecurity posture, such as data protection, privacy, breach notification, etc. Mapping the cybersecurity program to relevant legal and regulatory requirements also helps to evaluate the alignment and compliance of the organization's cybersecurity policies, procedures, controls, and practices with the legal and regulatory requirements. The other options are not the first thing that an IS auditor should do to ensure cyber security-related legal and regulatory requirements are followed by an organization, but rather follow after determining if the cybersecurity program is mapped to relevant legal and regulatory requirements, such as reviewing the most recent legal and regulatory audit report (B), determining if there is a formal process to review changes in legal and regulatory requirements , or obtaining a list of relevant legal and regulatory requirements (D).

Question 6

Question Type: **MultipleChoice**

In cloud computing, which type of hosting is MOST appropriate for a large organization that wants greater control over the environment?

Options:

A- Private hosting

B- Public hosting

C- Shared hosting

D- Hybrid hosting

Answer:

A

Explanation:

In cloud computing, the type of hosting that is MOST appropriate for a large organization that wants greater control over the environment isprivate hosting. Private hosting is a type of cloud service model where the cloud infrastructure is dedicated to a single organization and hosted either on-premise or off-premise by a third-party provider. Private hosting offers more control over the security, performance, customization, and compliance of the cloud environment than other types of hosting.