# Free Questions for CDPSE by certsinside

## Shared by Cobb on 29-01-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

Which of the following principles is MOST important to apply when granting access to an enterprise resource planning (ERP) system that contains a significant amount of personal data?

## Options:

**A-** Read-only access

**B-** Least privilege

**C-** Segregation of duties

**D-** Data minimization

## Answer:

B

## Explanation:

The principle of least privilege is the most important principle to apply when granting access to an ERP system that contains a significant amount of personal dat

a. The principle of least privilege states that users should only have the minimum level of access and permissions necessary to perform their legitimate tasks and functions, and no more. Applying the principle of least privilege helps to protect the privacy and security of the personal data in the ERP system, as it reduces the risk of unauthorized or inappropriate access, disclosure, modification, or deletion of the data. It also helps to comply with the privacy laws and regulations, such as the GDPR, that require data controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

# Question 2

**Question Type:** MultipleChoice

Who is ULTIMATELY accountable for the protection of personal data collected by an organization?

## Options:

**A-** Data processor

**B-** Data owner

**C-** Data custodian

**D-** Data protection officer

### Answer:

B

### Explanation:

The data owner is the person or entity who has the ultimate authority and responsibility for the protection of personal data collected by an organization. The data owner defines the purpose, scope, classification, and retention of the personal data, as well as the rights and obligations of the data subjects and other parties involved in the data processing. The data owner also ensures that the personal data is handled in compliance with the applicable privacy laws and regulations, as well as the organization's privacy policies and standards. The data owner may delegate some of the operational tasks to the data processor, data custodian, or data protection officer, but the accountability remains with the data owner.

## Question 3

**Question Type:** MultipleChoice

Which of the following BEST illustrates privacy by design in the development of a consumer mobile application?

## Options:

**A-** The application only stores data locally.

**B-** The application shares personal information upon request.

**C-** The application only stores data for 24 hours.

**D-** The application requires consent before sharing locations.

## Answer:

D

## Explanation:

Privacy by design is an approach that embeds privacy principles and considerations into the design and development of products, services, systems, and processes that involve personal dat

a. Privacy by design aims to protect the privacy and security of the data subjects, as well as to comply with the applicable privacy laws and regulations. One of the key principles of privacy by design is to obtain the consent and choice of the data subjects regarding the collection, use, and disclosure of their personal data. Therefore, the best example of privacy by design in the development of a consumer mobile application is to require consent before sharing locations, as this gives the data subjects control and transparency over their personal data. The other options are not as effective or sufficient as requiring consent before sharing locations, as they do not address the principle of consent and choice, or they may violate other privacy principles or requirements.

# Question 4

**Question Type:** MultipleChoice

An increase in threats originating from endpoints is an indication that:

## Options:

**A-** network audit frequency should increase.

**B-** network protection should be maintained remotely.

**C-** extended detection and response should be installed.

**D-** credential management should be implemented.

## Answer:

C

## Explanation:

Extended detection and response (XDR) is a security solution that collects and analyzes data from multiple sources, such as endpoints, networks, servers, cloud, and applications, to detect and respond to threats in real time. XDR should be installed to address the increase in threats originating from endpoints, as it provides a holistic and integrated view of the threat landscape, as well as automated and coordinated actions to contain and remediate the threats. XDR also helps to improve the visibility, efficiency, and effectiveness of the security operations, as well as to reduce the complexity and costs of managing multiple security tools.

# Question 5

**Question Type:** MultipleChoice

Which of the following is the BEST way to ensure that application hardening is included throughout the software development life cycle (SDLC)?

## Options:

**A-** Require an annual internal audit of SDLC processes.

**B-** Include qualified application security personnel as part of the process.

**C-** Ensure comprehensive application security testing immediately prior to release.

**D-** Require an annual third-party audit of new client software solutions.

## Answer:

B

## Explanation:

The best way to ensure that application hardening is included throughout the software development life cycle (SDLC) is to include qualified application security personnel as part of the process. Application hardening is the process of applying security measures and techniques to an application to reduce its attack surface, vulnerabilities, and risks. Application hardening should be integrated into every stage of the SDLC, from planning and design to development and testing to deployment and maintenance. Including qualified application security personnel as part of the process helps to ensure that application hardening is performed effectively and consistently, as well as to provide guidance, feedback, and support to the developers, testers, and project managers. The other options are not as effective or sufficient as including qualified application security personnel as part of the process, as they do not address the root cause of the lack of application hardening, which is the gap in skills and knowledge among the SDLC participants.

# Question 6

**Question Type:** MultipleChoice

Which of the following is the MOST important consideration for determining the operational life of an encryption key?

## Options:

**A-** Number of entities involved in communication

**B-** Number of digitally signed documents in force

**C-** Volume and sensitivity of data protected

**D-** Length of key and complexity of algorithm

## Answer:

C

## Explanation:

The most important consideration for determining the operational life of an encryption key is the volume and sensitivity of data protected by the key. The operational life of an encryption key is the period of time during which the key can be used securely and effectively to encrypt and decrypt data. The operational life of an encryption key depends on various factors, such as the length and complexity of the key, the strength and speed of the encryption algorithm, the number and frequency of encryption operations, the number of entities involved in communication, and the number of digitally signed documents in force. However, among these factors, the volume and sensitivity of data protected by the key is the most critical, as it affects the risk and impact of a potential compromise or exposure of the key. The higher the volume and sensitivity of data protected by the key, the shorter the operational life of the key should be, as this reduces the window of opportunity for an attacker to access or misuse the data.

# Question 7

**Question Type:** MultipleChoice

An organization plans to implement a new cloud-based human resources (HR) solution with a mobile application interface. Which of the following is the BEST control to prevent data leakage?

## Options:

**A-** Download of data to the mobile devices is disabled.

**B-** Single sign-on is enabled for the mobile application.

**C-** Data stored in the cloud-based solution is encrypted.

**D-** Separate credentials are used for the mobile application.

## Answer:

A

## Explanation:

The best control to prevent data leakage for a cloud-based HR solution with a mobile application interface is to disable the download of data to the mobile devices. This is because downloading data to the mobile devices increases the risk of data loss, theft, or unauthorized

access, especially if the devices are lost, stolen, or compromised. Disabling the download of data to the mobile devices ensures that the data remains in the cloud-based solution, where it can be protected by encryption, access control, and other security measures. The other options are not as effective or sufficient as disabling the download of data to the mobile devices, as they do not address the root cause of the data leakage risk, which is the exposure of data outside the cloud-based solution.

# Question 8

**Question Type:** MultipleChoice

Which of the following helps define data retention time in a stream-fed data lake that includes personal data?

## Options:

**A-** Privacy impact assessments (PIAs)

**B-** Data lake configuration

**C-** Data privacy standards

**D-** Information security assessments

## Answer:

C

### Explanation:

Data privacy standards are the set of rules, guidelines, and best practices that define the requirements and expectations for the collection, processing, storage, sharing, and disposal of personal dat

a. Data privacy standards help to ensure that personal data is treated in a fair, lawful, transparent, and secure manner, as well as to comply with the applicable privacy laws and regulations. Data privacy standards also help to define the data retention time in a stream-fed data lake that includes personal data, as they specify the criteria and conditions for how long personal data can be kept in the data lake, based on factors such as the purpose, necessity, relevance, and quality of the data. Data retention time is an important aspect of data privacy, as it affects the risk of data breaches, unauthorized access, or misuse of personal data.

## Question 9

**Question Type:** MultipleChoice

Which cloud deployment model is BEST for an organization whose main objectives are to logically isolate personal data from other tenants and adopt custom privacy controls for the data?

## Options:

**A-** Community cloud

**B-** Private cloud

**C-** Hybrid cloud

**D-** Public cloud

## Answer:

B

## Explanation:

A private cloud is a cloud deployment model that provides exclusive access and control to a single organization or a specific group of users within the organization. A private cloud is best for an organization whose main objectives are to logically isolate personal data from other tenants and adopt custom privacy controls for the data, as it offers the highest level of security, privacy, and customization among the cloud deployment models. A private cloud allows the organization to implement its own privacy policies, standards, and procedures for the personal data, as well as to configure the cloud infrastructure, services, and applications according to its specific needs and preferences. A private cloud also reduces the risk of data breaches, unauthorized access, or co-mingling of data from other tenants, as the personal data is stored and processed in a dedicated and isolated environment.