Explore ISACA CDPSE Exam Questions with Our Free Demo Download
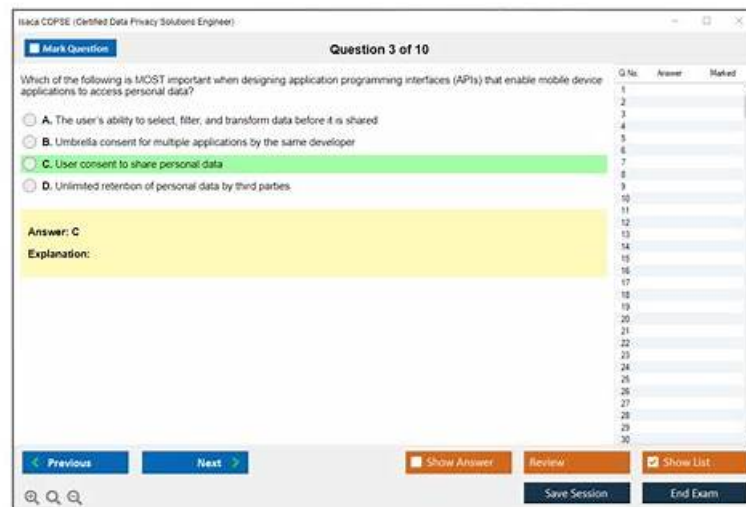

DOWNLOAD the newest ExamCost CDPSE PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1z5I0NeqeyAPzI7kZ8QNFQnn29mSGhszK

First and foremost, we have high class operation system so we can assure you that you can start to prepare for the CDPSE exam with our study materials only 5 to 10 minutes after payment. Second, once we have compiled a new version of the CDPSE test question, we will send the latest version of our CDPSE Training Materials to our customers for free during the whole year after purchasing. Last but not least, our worldwide after sale staffs will provide the most considerate after sale service for you in twenty four hours a day, seven days a week.

ISACA CDPSE (Certified Data Privacy Solutions Engineer) Exam is a certification program that equips professionals with the knowledge and skills necessary to design and implement data privacy solutions. Certified Data Privacy Solutions Engineer certification is globally recognized and signifies that the holder is capable of driving effective data privacy solutions in organizations. The CDPSE Exam covers topics such as data privacy governance, data protection, data retention, and data disposal. CDPSE exam is designed to test the candidate's ability to analyze and mitigate privacy risks, create and implement privacy policies and procedures, and monitor and report on privacy compliance.

>> Trusted CDPSE Exam Resource <<

CDPSE Latest Cram Materials, Latest CDPSE Questions

We have authoritative production team made up by thousands of experts helping you get hang of our CDPSE study question and enjoy the high quality study experience. We will update the content of CDPSE test guide from time to time according to recent changes of examination outline and current policies. Besides, our CDPSE Exam Questions can help you optimize your learning method by simplifying obscure concepts so that you can master better. One more to mention, with our CDPSE test guide, there is no doubt that you can cut down your preparing time in 20-30 hours of practice before you take the exam.

The CDPSE Certification is ideal for professionals who want to advance their careers in the field of data privacy. Certified Data Privacy Solutions Engineer certification is recognized globally and is highly valued by employers, demonstrating that you have the knowledge and expertise to manage data privacy risks and protect sensitive data. Certified Data Privacy Solutions Engineer certification can help professionals advance their careers and increase their earning potential.

ISACA Certified Data Privacy Solutions Engineer Sample Questions (Q198-Q203):

NEW QUESTION # 198
Which of the following practices BEST indicates an organization follows the data minimization principle?

- A. Data is encrypted before storage.
- B. Data is pseudonymized when being backed up.
- C. Data is regularly reviewed tor its relevance
- D. Data is only accessible on a need-to-know basis.

Answer: C

Explanation:
The practice that best indicates an organization follows the data minimization principle is that data is regularly reviewed for its relevance. The data minimization principle is one of the core principles of data protection under various laws and regulations, such as the GDPR or the CCP A) It states that personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. By regularly reviewing the data they hold, organizations can ensure that they do not collect or retain excessive or unnecessary data that may pose privacy risks or violate data subject rights.
Data is pseudonymized when being backed up, data is encrypted before storage, or data is only accessible on a need-to-know basis are also good practices for data protection, but they do not directly indicate that the organization follows the data minimization principle. Pseudonymization is a process of replacing identifying information in data with artificial identifiers or pseudonyms. Pseudonymization can help enhance the privacy of data by reducing the linkability between data and data subjects, but it does not prevent re-identification or inference attacks. Encryption is a process of transforming data into an unreadable form using a secret key or algorithm. Encryption can help protect the confidentiality, integrity, and availability of data by preventing unauthorized access, disclosure, or modification. Access control is a process of restricting who can access, modify, or delete data based on their roles, permissions, or credentials. Access control can help prevent unauthorized or inappropriate use of data by limiting the scope of access.

NEW QUESTION # 199
Which of the following hard drive sanitation methods provides an organization with the GREATEST level of assurance that data has been permanently erased?

- A. Reformatting the drive
- B. Factory resetting the drive
- C. Degaussing the drive
- D. Crypto-shredding the drive

Answer: C

Explanation:
Reference:
Degaussing is a hard drive sanitation method that uses a powerful magnetic field to erase or destroy the data stored on a magnetic disk or tape. Degaussing provides an organization with the greatest level of assurance that data has been permanently erased, as it renders the data unrecoverable by any means and also damages the drive itself, making it unusable for future storage. The other options are not as effective as degaussing in ensuring permanent data erasure. Factory resetting is a hard drive sanitation method that restores the drive to its original settings and deletes the user data, but it may leave some traces of data that can be recovered by forensic tools or software. Crypto-shredding is a hard drive sanitation method that encrypts the data on the drive and then deletes the encryption key, making the data inaccessible, but it may not erase the data completely or prevent unauthorized access if the key is compromised or recovered. Reformatting is a hard drive sanitation method that changes the file system or structure of the drive and deletes the data, but it may not overwrite the data entirely or prevent data recovery by advanced tools or techniques1, p. 93-94
Reference: 1: CDPSE Review Manual (Digital Version)

NEW QUESTION # 200
Which of the following should be the FIRST consideration when conducting a privacy impact assessment (PIA)?

- A. The applicable privacy legislation
- B. The organizational security risk profile
- C. The quantity of information within the scope of the assessment
- D. The systems in which privacy-related data is stored

Answer: A

Explanation:
Explanation

The first consideration when conducting a privacy impact assessment (PIA) is the applicable privacy legislation that governs the collection, processing, storage, transfer, and disposal of personal data within the scope of the assessment. The applicable privacy legislation may vary depending on the jurisdiction, sector, or purpose of the data processing activity. The PIA should identify and comply with the relevant legal requirements and obligations for data protection and privacy, such as obtaining consent, providing notice, ensuring data quality and security, respecting data subject rights, and reporting data breaches. The applicable privacy legislation also determines the criteria, methodology, and documentation for conducting the PIA.
References:
* ISACA, Performing an Information Security and Privacy Risk Assessment1
* ISACA, Best Practices for Privacy Audits2
* ISACA, GDPR Data Protection Impact Assessments3
* ISACA, GDPR Data Protection Impact Assessment Template4

NEW QUESTION # 201
Which of the following is the BEST way to protect the privacy of data stored on a laptop in case of loss or theft?

- A. Strong authentication controls
- B. Endpoint encryption
- C. Regular backups
- D. Remote wipe

Answer: B

Explanation:
Explanation
Endpoint encryption is a security practice that transforms the data stored on a laptop or other device into an unreadable format using a secret key or algorithm. Endpoint encryption protects the privacy of data in case of loss or theft, by ensuring that only authorized parties can access and use the data, while unauthorized parties cannot decipher or modify the data without the key or algorithm. Endpoint encryption also helps to comply with data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), which require data controllers and processors to implement appropriate technical and organizational measures to safeguard personal data.
The other options are less effective or irrelevant for protecting the privacy of data stored on a laptop in case of loss or theft. Strong authentication controls, such as passwords, biometrics or multifactor authentication, are important for verifying the identity and access rights of users, but they do not protect the data from being accessed by bypassing or breaking the authentication mechanisms. Remote wipe is a feature that allows users or administrators to erase the data on a lost or stolen device remotely, but it depends on the availability of network connection and device power, and it may not prevent data recovery by sophisticated tools. Regular backups are a process of creating copies of data for recovery purposes, such as in case of data loss or corruption, but they do not protect the data from being accessed by unauthorized parties who may obtain the backup media or files.
References:
* An Ethical Approach to Data Privacy Protection - ISACA, section 2: "Encryption is one of the most effective security controls available to enterprises, but it can be challenging to deploy and maintain across a complex enterprise landscape."
* How to Protect and Secure Your Data in 10 Ways - TechRepublic, section 1: "Encrypt your hard drive Most work laptops use BitLocker to encrypt local files. That way, if the computer is stolen or hacked, the data it contains will be useless to the malicious actor."
* 10 Tips to Protect Your Files on PC and Cloud - microsoft.com, section 1: "Encrypt your hard drive Most work laptops use BitLocker to encrypt local files. That way, if the computer is stolen or hacked, the data it contains will be useless to the malicious actor."
* 11 practical ways to keep your IT systems safe and secure | ICO, section 1: "Use strong passwords and multi-factor authentication Make sure you use strong passwords on smartphones, laptops, tablets, email accounts and any other devices or accounts where personal information is stored."

NEW QUESTION # 202
An organization must de-identify its data before it is transferred to a third party Which of the following should be done FIRST?

- A. Encrypt the data at rest and in motion
- B. Ensure logging is turned on for the database
- C. Determine the categories of personal data collected
- D. Remove the identifiers during the data transfer

Answer: C

Explanation:
Explanation
Before de-identifying data, it is important to determine the categories of personal data collected, such as names, addresses, phone numbers, email addresses, social security numbers, health information, and so on.
This will help to identify which data elements are considered identifiers or quasi-identifiers, and which de-identification techniques are appropriate for each category. For example, some data elements may need to be removed completely, while others may be masked, generalized, or perturbed.
References:
* Anonymize and De-identify | Research Data Management
* Data De-identification: An Overview of Basic Terms - ed

NEW QUESTION # 203

......