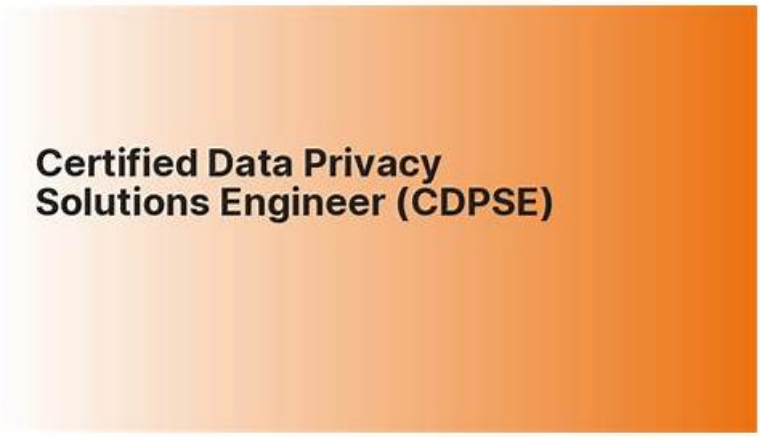
CDPSE Testengine, CDPSE Echte Fragen



P.S. Kostenlose und neue CDPSE Prüfungsfragen sind auf Google Drive freigegeben von DeutschPrüfung verfügbar: https://drive.google.com/open?id=1byp28k3DCNITEPdBipBxNal_9O2UIQqo

Wenn Sie DeutschPrüfung wählen, können Sie 100% die Prüfung bestehen. Nach den Veränderungen der Prüfungsthemen der ISACA CDPSE aktualisieren wir auch ständig unsere Schulungsunterlagen und bieten neue Prüfungsinhalte. DeutschPrüfung bietet Ihnen rund um die Uhr kostenlosen Online-Service. Falls Sie in der ISACA CDPSE Zertifizierungsprüfung durchfallen, zahlen wir Ihnen die gesammte Summe zurück.

Um in der IT-Branche große Fortschritte zu machen, entscheiden sich viele ambitionierte IT-Profis dafür, die ISACA CDPSE Zertifizierungsprüfung abzulegen und somit das IT-Zertifikat zu bekommen. Wegen des schwierigkeitsgrades der ISACA CDPSE Zertifizierungsprüfung ist die Erfolgsquote sehr niedrig. Aber es ist doch eine weise Wahl, an der ISACA CDPSE Zertifizierungsprüfung teilzunehmen, denn in der heutigen konkurrenzfähigen IT-Branche muss man sich immer noch verbessern. Und Sie können auch viele Methoden wählen, die Ihnen beim Bestehen der Prüfung helfen.

>> CDPSE Testengine <<

Certified Data Privacy Solutions Engineer cexamkiller Praxis Dumps & CDPSE Test Training Überprüfungen

DeutschPrüfung ist professionell und geschaffen für die breiten Kandidaten. Es ist nicht nur von hoher Qualität und guter Dienstleistungen, sondern auch ganz billig. Wenn Sie über DeutschPrüfung verfügen, brauchen Sie keine Sorge um dieISACA CDPSE Zertifizerungsprüfungen machen. DeutschPrüfung wird Ihnen in kürzester Zeit helfen, die ISACA CDPSE Prüfungen zu bestehen. Mit diesen Lernhilfe werden Sie näher von einem IT-Spezialisten sind.

Das Erzählen der CDPSE -Zertifizierung zeigt ein starkes Engagement für die Datenschutz und die Fähigkeit, effektive Datenschutzlösungen zu verwalten und umzusetzen. Es ist eine zunehmend wertvolle Zertifizierung im heutigen digitalen Zeitalter, in dem Datenschutz für Organisationen aller Größen und Branchen ein entscheidendes Problem darstellt. Durch die Abgabe der CDPSE -Prüfung können Kandidaten ihre berufliche Glaubwürdigkeit verbessern und ihre Karrieren in den Bereichen IT und Sicherheit vorantreiben.

ISACA Certified Data Privacy Solutions Engineer CDPSE Prüfungsfragen mit Lösungen (Q108-Q113):

108. Frage
Which of the following is an example of data anonymization as a means to protect personal data when sharing a database?

- A. Names and addresses are removed but the rest of the data is left untouched.
- B. Key fields are hidden and unmasking is required to access to the data.
- C. The data is transformed such that re-identification is impossible.
- D. The data is encrypted and a key is required to re-identify the data.

Antwort: C

Begründung:
Explanation
Data anonymization is a method of protecting personal data by modifying or removing any information that can be used to identify an individual, either directly or indirectly, in a data set. Data anonymization aims to prevent the re-identification of the data subjects, even by the data controller or processor, or by using additional data sources or techniques. Data anonymization 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 respect the privacy rights and preferences of the data subjects.
The data is transformed such that re-identification is impossible is an example of data anonymization, as it involves applying irreversible techniques, such as aggregation, generalization, perturbation, or synthesis, to alter the original data in a way that preserves their utility and meaning, but eliminates their identifiability. For example, a database of customer transactions can be anonymized by replacing the names and addresses of the customers with random codes, and by adding noise or rounding to the amounts and dates of the transactions.
The other options are not examples of data anonymization, but of other methods of protecting personal data that do not guarantee the impossibility of re-identification. The data is encrypted and a key is required to re-identify the data is an example of data pseudonymization, which is a method of replacing direct identifiers with pseudonyms, such as codes or tokens, that can be linked back to the original data with a key or algorithm.
Data pseudonymization does not prevent re-identification by authorized parties who have access to the key or algorithm, or by unauthorized parties who can break or bypass the encryption. Key fields are hidden and unmasking is required to access to the data is an example of data masking, which is a method of concealing or obscuring sensitive data elements, such as names or credit card numbers, with characters, symbols or blanks.
Data masking does not prevent re-identification by authorized parties who have permission to unmask the data, or by unauthorized parties who can infer or guess the hidden data from other sources or clues. Names and addresses are removed but the rest of the data is left untouched is an example of data deletion, which is a method of removing direct identifiers from a data set. Data deletion does not prevent re-identification by using indirect identifiers, such as age, gender, occupation or location, that can be combined or matched with other data sources to re-establish the identity of the data subjects.
References:
Big Data Deidentification, Reidentification and Anonymization - ISACA, section 2: "Anonymization is the ability for the data controller to anonymize the data in a way that it is impossible for anyone to establish the identity of the data." Data Anonymization - Overview, Techniques, Advantages, section 1: "Data anonymization is a method of ensuring that the company understands and enforces its duty to secure sensitive, personal, and confidential data in a world of highly complex data protection mandates that can vary depending on where the business and the customers are based."

109. Frage
Which of the following is the BEST way to distinguish between a privacy risk and compliance risk?

- A. Conduct a privacy risk remediation exercise.
- B. Perform a privacy risk audit.
- C. Validate a privacy risk attestation.
- D. Conduct a privacy risk assessment.

Antwort: D

Begründung:
A privacy risk assessment is a process of identifying, analyzing and evaluating the privacy risks associated with the collection, use, disclosure or retention of personal data. A privacy risk assessment is the best way to distinguish between a privacy risk and compliance risk, as it would help to determine the likelihood and impact of privacy incidents or breaches that could affect the rights and interests of the data subjects, as well as the legal obligations and responsibilities of the organization. A privacy risk assessment would also help to identify and implement appropriate controls and measures to mitigate or reduce the privacy risks and ensure compliance with privacy principles, laws and regulations. The other options are not as effective as conducting a privacy risk assessment in distinguishing between a privacy risk and compliance risk. Performing a privacy risk audit is a process of verifying and validating the effectiveness and adequacy of the privacy controls and measures implemented by the organization, but it does not necessarily identify or evaluate the privacy risks or compliance risks. Validating a privacy risk attestation is a process of confirming and certifying the accuracy and completeness of the privacy information or statements provided by the organization, but it does not necessarily identify or evaluate the privacy risks or compliance risks. Conducting a privacy risk remediation exercise is a process of implementing corrective actions or improvements to address the identified or reported privacy risks or compliance risks, but it does not necessarily distinguish between them1, p. 66-67 Reference: 1: CDPSE Review Manual (Digital Version)

110. Frage
Which of the following would MOST effectively reduce the impact of a successful breach through a remote access solution?

- A. Monitoring and reviewing remote access logs
- B. Compartmentalizing resource access
- C. Regular testing of system backups
- D. Regular physical and remote testing of the incident response plan

Antwort: D

111. Frage
An organization must de-identify its data before it is transferred to a third party Which of the following should be done FIRST?

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

Antwort: C

Begründung:
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

112. Frage
Which of the following helps to ensure the identities of individuals in a two-way communication are verified?

- A. Virtual private network (VPN)
- B. Secure Shell (SSH)
- C. Transport Layer Security (TLS)
- D. Mutual certificate authentication

Antwort: D

Begründung:
The best answer is D. Mutual certificate authentication.
A comprehensive explanation is:
Mutual certificate authentication is a method of mutual authentication that uses public key certificates to verify the identities of both parties in a two-way communication. A public key certificate is a digital document that contains information about the identity of the certificate holder, such as their name, organization, domain name, etc., as well as their public key, which is used for encryption and digital signature. A public key certificate is issued and signed by a trusted authority, called a certificate authority (CA), that vouches for the validity of the certificate.
Mutual certificate authentication works as follows:
Both parties have a public key certificate issued by a CA that they trust.
When they initiate a communication, they exchange their certificates with each other.
They verify the signatures on the certificates using the CA's public key, which they already have or can obtain from a trusted source.
They check that the certificates are not expired, revoked, or tampered with.
They extract the public keys from the certificates and use them to encrypt and decrypt messages or to generate and verify digital signatures.
They confirm that the identities in the certificates match their expectations and intentions.
By using mutual certificate authentication, both parties can be confident that they are communicating with the intended and legitimate party, and that their communication is secure and confidential.

Mutual certificate authentication is often used in conjunction with Transport Layer Security (TLS), a protocol that provides encryption and authentication for network communications. TLS supports both one-way and two-way authentication. In one-way authentication, only the server presents a certificate to the client, and the client verifies it. In two-way authentication, also known as mutual TLS or mTLS, both the server and the client present certificates to each other, and they both verify them. Mutual TLS is commonly used for secure web services, such as APIs or webhooks, that require both parties to authenticate each other.
Virtual private network (VPN), Secure Shell (SSH), and Transport Layer Security (TLS) are all technologies that can help to ensure the identities of individuals in a two-way communication are verified, but they are not methods of mutual authentication by themselves. They can use mutual certificate authentication as one of their options, but they can also use other methods, such as username and password, pre-shared keys, or tokens. Therefore, they are not as specific or accurate as mutual certificate authentication.
Reference:
What is mutual authentication? | Two-way authentication1
How to prove and verify someone's identity2
Identity verification - Information Security & Policy3

113. Frage
.....