CDPSE Fragenkatalog, CDPSE Zertifikatsdemo

Übrigens, Sie können die vollständige Version der ZertPruefung CDPSE Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=14FT5hSbruy9EHy-VXn3pctbOuE51b5z2

Wir alle wissen, dass im Zeitalter des Internets ist es ganz einfach, die Informationen zu bekommen. Aber was fehlt ist nämlich, Qualität und Anwendbarkeit. Viele Leute suchen im Internet die Schulungsunterlagen zur ISACA CDPSE Zertifizierungsprüfung. Und Sie wissen einfach nicht, ob sie zuverlässig sind. Hier empfehle ich Ihnen die Schulungsunterlagen zur ISACA CDPSE Zertifizierungsprüfung von ZertPruefung. Sie haben im Internet die höchste Kauf-Rate und einen guten Ruf. Sie können im Internet Teil der Prüfungsfragen und Antworten zur ISACA CDPSE Zertifizierungsprüfung von ZertPruefung kostenlos herunterladen. Dann können Sie entscheiden, ZertPruefung zu kaufen oder nicht. Und Sie können auch die Echtheit von ZertPruefung kriegen.

Um für die CDPSE-Prüfung zugelassen zu werden, sollten Kandidaten mindestens fünf Jahre Erfahrung im Bereich Datenschutz haben, einschließlich mindestens drei Jahren Erfahrung in der Entwicklung und Implementierung von Datenschutzlösungen. Sie sollten auch einen Bachelor-Abschluss oder höher von einer akkreditierten Institution oder eine gleichwertige Arbeitserfahrung haben. Die CDPSE-Prüfung besteht aus 150 Multiple-Choice-Fragen, die innerhalb von vier Stunden beantwortet werden müssen.

ISACA CDPSE Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Participate in the development of data lifecycle procedures that align with privacy policies and business needs • Develop and • or implement a prioritization process for privacy practices
Thema 2	• Implement procedures related to data lifecycle that align with privacy policies • Coordinate and • or perform privacy impact assessments (PIA) and other privacy-focused assessments
Thema 3	• Evaluate advancements in privacy-enhancing technologies and changes in the regulatory landscape • Identify, validate, and • or implement appropriate privacy and security controls according to data classification procedures
Thema 4	• Identify, validate, and • or implement appropriate privacy and security controls according to data classification procedures • Participate in the development of privacy control procedures that align with privacy policies and business needs
Thema 5	• Identify the internal and external privacy requirements relating to the organization's data lifecycle practices • Participate in privacy training and promote awareness of privacy practices

>> CDPSE Fragenkatalog <<

bestehen Sie CDPSE Ihre Prüfung mit unserem Prep CDPSE Ausbildung Material & kostenloser Dowload Torrent

Wenn Sie ISACA CDPSE Zertifizierungsprüfung ablegen, ist es nötig für Sie, die richtigen ISACA CDPSE Prüfungsunterlagen zu benutzen. Wenn Sie irgendwo die Unterlagen suchen, stoppen Sie jetzt bitte. Wenn Sie keine richtigen Unterlagen haben, probieren Sie bitte ISACA CDPSE Dumps von ZertPruefung. Die Hitrate der Dumps ist so hoch, dass sie Ihnen den einmaligen Erfolg garantieren. Im Verglich zu anderen Prüfungsunterlagen können diese Dumps die Prüfungsinhalte ganz richtig greifen. Damit können Sie Ihre Lerneffektivität erhöhen und sich besser auf ISACA CDPSE Zertifizierungsprüfung vorbereiten.

ISACA Certified Data Privacy Solutions Engineer CDPSE Prüfungsfragen mit Lösungen (Q158-Q163):

158. Frage
Which of the following is a foundational goal of data privacy laws?

- A. Privacy laws are designed to give people rights over the collection of personal data
- B. Privacy laws are designed to protect companies' collection of personal data
- C. Privacy laws are designed to prevent the collection of personal data
- D. Privacy laws are designed to provide transparency for the collection of personal data

Antwort: A

Begründung:
Explanation
One of the foundational goals of data privacy laws is to give people rights over the collection of personal data, such as the right to access, correct, delete, or object to the processing of their data. Privacy laws also aim to protect people's dignity, autonomy, and self-determination in relation to their personal data. The other options are not accurate or complete descriptions of the purpose of data privacy laws.
References:
* CDPSE Review Manual, Chapter 1 - Privacy Governance, Section 1.1 - Privacy Principles1.
* CDPSE Certified Data Privacy Solutions Engineer All-in-One Exam Guide, Chapter 1 - Privacy Governance, Section 1.2 - Data Privacy Laws and Regulations2.

159. Frage
An organization is developing a wellness smartwatch application and is considering what information should be collected from the application users. Which of the following is the MOST legitimate information to collect for business reasons in this situation?

- A. Sleep schedule and calorie intake
- B. Education and profession
- C. Height, weight, and activities
- D. Race, age, and gender

Antwort: C

Begründung:
Explanation
Height, weight, and activities are the most legitimate information to collect for business reasons in this situation, as they are directly related to the purpose and functionality of a wellness smartwatch application that aims to monitor and improve the health and fitness of its users. Collecting height, weight, and activities would also comply with the data minimization principle that requires limiting the collection, storage and processing of personal data to what is necessary and relevant for the intended purposes. The other options are not legitimate information to collect for business reasons in this situation, as they are not related to the purpose and functionality of a wellness smartwatch application and may violate the privacy rights and preferences of its users. Collecting sleep schedule and calorie intake may be useful for some users who want to track their sleep quality and nutrition intake, but they are not essential for a wellness smartwatch application and may require additional consent or justification from the users. Collecting education and profession may be irrelevant for a wellness smartwatch application and may be used for other purposes, such as marketing or profiling, without the consent or knowledge of the users. Collecting race, age, and gender may be sensitive for some users who do not want to disclose their personal characteristics or identity, and may require additional safeguards or measures to protect their privacy1, p. 75-76 References: 1: CDPSE Review Manual (Digital Version)

160. Frage
Which of the following deployed at an enterprise level will MOST effectively block malicious tracking of user Internet browsing?

- A. Website URL blacklisting
- B. Web application firewall (WAF)
- C. Desktop antivirus software
- D. Domain name system (DNS) sinkhole

Antwort: D

Begründung:
Domain name system (DNS) sinkhole is a technology that redirects malicious or unwanted domain names to alternative destinations, such as a fake or harmless website, a warning page, or a null address. DNS sinkhole is the most effective technology deployed at an enterprise level to block malicious tracking of user internet browsing, as it would prevent users from accessing websites that use tracking technologies, such as cookies, web beacons, or fingerprinting, to collect and analyze user behavior or preferences. DNS sinkhole would also protect users from other malicious activities, such as malware distribution, phishing attempts, or botnet command and control. The other options are not as effective as DNS sinkhole in blocking malicious tracking of user internet browsing at an enterprise level. Web application firewall (WAF) is a technology that monitors and filters incoming and outgoing web traffic to protect web applications from attacks, such as cross-site scripting (XSS), SQL injection, or denial-of-service (DoS), but it does not block malicious tracking of user internet browsing. Website URL blacklisting is a method of blocking access to websites that are known or suspected to be malicious or harmful, but it does not block malicious tracking of user internet browsing from unknown or legitimate websites that use tracking technologies. Desktop antivirus software is a technology that scans and removes viruses, malware, spyware, or other threats from desktop computers or devices, but it does not block malicious tracking of user internet browsing from websites that use tracking technologies1, p. 92 Reference: 1: CDPSE Review Manual (Digital Version)

161. Frage
Which of the following is the BEST way for an organization to gain visibility into Its exposure to privacy-related vulnerabilities?

- A. Review historical privacy incidents in the organization.
- B. Implement a data loss prevention (DLP) solution.
- C. Perform an analysis of known threats.
- D. Monitor inbound and outbound communications.

Antwort: C

Begründung:
An analysis of known threats is the best way for an organization to gain visibility into its exposure to privacy-related vulnerabilities because it helps identify the sources, methods and impacts of potential privacy breaches and assess the effectiveness of existing controls. A data loss prevention (DLP) solution, a review of historical privacy incidents and a monitoring of inbound and outbound communications are useful tools for detecting and preventing privacy violations, but they do not provide a comprehensive view of the organization's privacy risk posture.
Reference:
CDPSE Review Manual (Digital Version), Domain 1: Privacy Governance, Task 1.4: Coordinate and/or perform privacy impact assessments (PIA) and other privacy-focused assessments1 CDPSE Certified Data Privacy Solutions Engineer All-in-One Exam Guide, Chapter 2: Privacy Governance, Section: Privacy Risk Assessment2

162. Frage
As part of a major data discovery initiative to identify personal data across the organization, the project team has identified the proliferation of personal data held as unstructured data as a major risk. What should be done FIRST to address this situation?

- A. Identify sensitive unstructured data at the point of creation.
- B. Assign an owner to sensitive unstructured data.
- C. Classify sensitive unstructured data.
- D. Identify who has access to sensitive unstructured data.

Antwort: C

Begründung:

Classifying sensitive unstructured data should be done first to address the situation of the proliferation of personal data held as unstructured data, as it helps to identify the types, locations, and owners of the data, and to apply the appropriate privacy controls and measures based on the data classification level. Classifying sensitive unstructured data also facilitates the data discovery, data minimization, data retention, and data disposal processes. Reference: 2 Domain 3, Task 2; 5 Page 9

163. Frage
......

Warum wählen viele Leute die Schulungsunterlagen zur ISACA CDPSE Zertifizierungsprüfung von ZertPruefung? Es gibt auch andere Websites, die Schulungsressourcen zur CDPSE Zertifizierungsprüfung bietet. Unser ZertPruefung stellt Ihnen die echten Prüfungsmaterialien zur Verfügung. Unser Eliteteam, Zertifizierungsexperten, Techniker und berühmte Linguisten bearbeiten die neueste ISACA CDPSE Zertifizierungsprüfung. Deshalb klicken Sie ZertPruefung Website, wenn Sie die ISACA CDPSE Zertifizierungsprüfung bestehen wollen. Mit ZertPruefung können Sie Ihren Traum Schritt für Schritt verwirklichen.