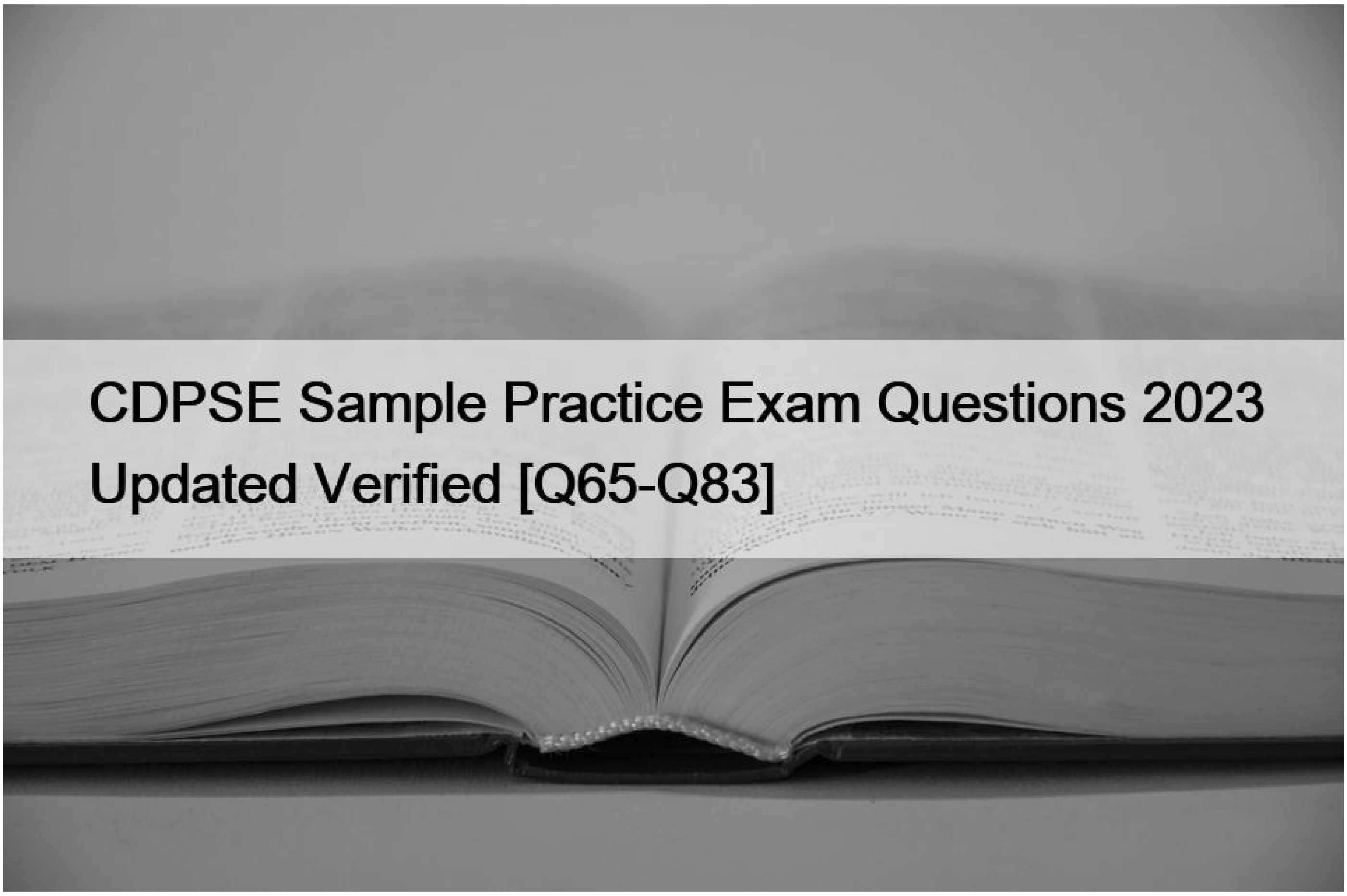
CDPSE Sample Practice Exam Questions 2023 Updated Verified [Q65-Q83



CDPSE Sample Practice Exam Questions 2023 Updated Verified Exam Study Guide Free Practice Test LAST UPDATED CDPSE

The Certified Data Privacy Solutions Engineer (CDPSE) certification is a globally recognized credential offered by the Information Systems Audit and Control Association (ISACA). The CDPSE certification exam is designed to assess an individual's knowledge and expertise in data privacy and protection, as well as their ability to implement effective data privacy solutions in their organizations.

The CDPSE certification exam is focused on the latest data privacy technologies, policies, and practices, making it an ideal qualification for individuals looking to specialize in data privacy engineering. CDPSE exam is designed to test the knowledge and skills of professionals in the field, ensuring that they have a deep understanding of data privacy regulations and the ability to implement solutions that are compliant with these regulations. CDPSE exam covers a range of topics, including privacy governance, data protection, data management, and data privacy regulations.

NO.65 An organization&#8217;s work-from-home policy allows employees to access corporate IT assets remotely Which of the

following controls is MOST important to mitigate the risk of potential personal data compromise?
* Encryption of network traffic
* Intrusion prevention system (IPS)
* Firewall rules review
* Intrusion detection system (IOS)
Explanation

Encryption of network traffic is the most important control to mitigate the risk of potential personal data compromise when employees access corporate IT assets remotely. Encryption is a process that transforms data into an unreadable form, making it difficult for unauthorized parties to intercept, modify, or steal it.

Encryption of network traffic ensures that the data transmitted between the remote employees and the corporate network is protected from eavesdropping, tampering, or leakage.

Intrusion prevention system (IPS), firewall rules review, and intrusion detection system (IDS) are also useful controls for network security, but they are not as effective as encryption for protecting personal data in transit.

IPS and IDS can monitor and block malicious or suspicious network traffic, but they cannot prevent data exposure if the traffic is intercepted by a third party. Firewall rules review can help optimize and secure the firewall configuration, but it cannot guarantee that the firewall will not be bypassed or compromised by an attacker. Therefore, encryption of network traffic is the best option among the choices given.

NO.66 Which of the following scenarios should trigger the completion of a privacy impact assessment (PIA)?
* Updates to data quality standards
* New inter-organizational data flows
* New data retention and backup policies
* Updates to the enterprise data policy
Explanation

A privacy impact assessment (PIA) is a process of analyzing the potential privacy risks and impacts of collecting, using, and disclosing personal data. A PIA should be conducted when there is a change in the data processing activities that may affect the privacy of individuals or the compliance with data protection laws and regulations. One of the scenarios that should trigger the completion of a PIA is when there are new inter-organizational data flows, which means that personal data is shared or transferred between different entities or jurisdictions. This may introduce new privacy risks, such as unauthorized access, misuse, or breach of data, as well as new legal obligations, such as obtaining consent, ensuring adequate safeguards, or notifying authorities.

References:

* PIA Triggers &#8211; International Association of Privacy Professionals

* Privacy Impact Assessment &#8211; International Association of Privacy Professionals

* GDPR Privacy Impact Assessment

* Data Protection Impact Assessment triggers: Clarity or confusion?

NO.67 Which of the following should be done FIRST to address privacy risk when migrating customer relationship management (CRM) data to a new system?
* Develop a data migration plan.
* Conduct a legitimate interest analysis (LIA).

* Perform a privacy impact assessment (PIA).
* Obtain consent from data subjects.

NO.68 An organization Wishes to deploy strong encryption to its most critical and sensitive databases. Which of the following is the BEST way to safeguard the encryption keys?
* Ensure key management responsibility is assigned to the privacy officer.
* Ensure the keys are stored in a remote server.
* Ensure the keys are stored in a cryptographic vault.
* Ensure all access to the keys is under dual control_
Explanation

The best way to safeguard the encryption keys is to ensure that they are stored in a cryptographic vault. A cryptographic vault is a secure hardware or software module that provides cryptographic services and protects the keys from unauthorized access, modification, or disclosure. A cryptographic vault can also provide other functions, such as key generation, key backup, key rotation, key destruction, and key auditing. A cryptographic vault can enhance the security and privacy of the encrypted data by preventing key compromise, leakage, or misuse. A cryptographic vault can also comply with the security standards and best practices for key management, such as the ISO/IEC 27002, NIST SP 800-57, or PCI DSS. References:

* [ISACA Glossary of Terms]

* [ISACA CDPSE Review Manual, Chapter 3, Section 3.3.3]

* [ISACA Journal, Volume 4, 2019, &#8220;Key Management in the Multi-Cloud Environment&#8221;]

* [ISACA CDPSE Review Manual, Chapter 3, Section 3.3.4]

NO.69 Which of the following is an IT privacy practitioner&#8217;s BEST recommendation to reduce privacy risk before an organization provides personal data to a third party?
* Tokenization
* Aggregation
* Anonymization
* Encryption

NO.70 An organization is concerned with authorized individuals accessing sensitive personal customer information to use for unauthorized purposes. Which of the following technologies is the BEST choice to mitigate this risk?
* Email filtering system
* Intrusion monitoring
* Mobile device management (MDM)
* User behavior analytics

NO.71 Which of the following processes BEST enables an organization to maintain the quality of personal data?
* Implementing routine automatic validation
* Maintaining hashes to detect changes in data
* Encrypting personal data at rest
* Updating the data quality standard through periodic review
Explanation

The best way to maintain the quality of personal data is to implement routine automatic validation, which is a process of checking the accuracy, completeness, consistency, and timeliness of the data using automated tools or scripts. Routine automatic validation can help identify and correct any errors, anomalies, or discrepancies in the data, as well as ensure that the data meets the specified quality standards and requirements. Routine automatic validation can also help improve the efficiency and reliability of the data processing and analysis12.

References:

* CDPSE Exam Content Outline, Domain 3 &#8211; Data Lifecycle (Data Quality), Task 2: Implement data quality measures3.

* CDPSE Review Manual, Chapter 3 &#8211; Data Lifecycle, Section 3.2 &#8211; Data Quality4.

NO.72 Which of the following is the MOST effective remote access model for reducing the likelihood of attacks originating from connecting devices?
* Thick client desktop with virtual private network (VPN) connection
* Remote wide area network (WAN) links
* Thin Client remote desktop protocol (RDP)
* Site-to-site virtual private network (VPN)
Explanation

A thin client remote desktop protocol (RDP) is the most effective remote access model for reducing the likelihood of attacks originating from connecting devices, because it minimizes the amount of data and processing that occurs on the remote device. A thin client RDP only sends keyboard, mouse and display information between the remote device and the server, while the actual processing and storage of data happens on the server. This reduces the exposure of sensitive data and applications to potential attackers who may compromise the remote device.

References:

* CDPSE Review Manual, Chapter 2 &#8211; Privacy Architecture, Section 2.3 &#8211; Privacy Architecture Implementation1.

* CDPSE Certified Data Privacy Solutions Engineer All-in-One Exam Guide, Chapter 2 &#8211; Privacy Architecture, Section 2.4 &#8211; Remote Access2.

NO.73 Which of the following describes a user&#8217;s &#8220;right to be forgotten&#8221;?
* The data is being used to comply with legal obligations or the public interest.
* The data is no longer required for the purpose originally collected.
* The individual objects despite legitimate grounds for processing.
* The individual&#8217;s legal residence status has recently changed.
Explanation

The right to be forgotten is a privacy right that allows individuals to request the deletion or removal of their personal data from a data controller&#8217;s records or systems under certain conditions. One of these conditions is when the data is no longer required for the purpose originally collected, meaning that the data has become obsolete, irrelevant or excessive for fulfilling the initial purpose for which it was obtained or processed by the data controller. The other options are not valid conditions for exercising the right to be forgotten. The data is being used to comply with legal obligations or public interest is an exception that may prevent the data controller from deleting or removing the data upon request, as there may be overriding legitimate grounds for retaining the data for legal compliance or public interest reasons. The individual objects despite legitimate grounds for processing is a condition for exercising the right to object, not the right to be forgotten, which allows individuals to oppose the processing of their personal data based on their particular situation or for direct marketing purposes. The individual&#8217;s legal residence status has recently changed is not a relevant factor for exercising the right to be forgotten, as it does not affect the necessity or relevance of the data for its original purpose1, p. 107-108 References: 1: CDPSE Review Manual (Digital Version)

NO.74 Which of the following BEST enables an organization to ensure consumer credit card numbers are accurately captured?

* Input reference controls
* Access controls
* Input validation controls
* Reconciliation controls
Explanation

Input validation controls are the best way to ensure consumer credit card numbers are accurately captured.

Input validation controls are methods that check the format, type, range, and length of the input data before accepting, processing, or storing it. Input validation controls can help prevent errors, fraud, or data loss by rejecting invalid, incomplete, or malicious input. For example, input validation controls can verify that a credit card number follows the Luhn algorithm1, has the correct number of digits2, and matches the card issuer&#8217;s prefix3. Input validation controls can also prevent SQL injection attacks4 or cross-site scripting attacks5 that may compromise the security and privacy of the data.

Input reference controls, access controls, and reconciliation controls are also important for data quality and security, but they do not directly ensure the accuracy of consumer credit card numbers. Input reference controls are methods that compare the input data with a predefined list of values or a reference table to ensure consistency and validity. For example, input reference controls can check if a country name or a postal code is valid by looking up a database of valid values. Access controls are methods that restrict who can access, modify, or delete the data based on their roles, permissions, or credentials. For example, access controls can prevent unauthorized users from accessing or tampering with consumer credit card numbers. Reconciliation controls are methods that compare the data from different sources or systems to ensure completeness and accuracy. For example, reconciliation controls can check if the transactions recorded in the accounting system match the transactions processed by the payment gateway.

References: Luhn algorithm, Credit card number, Bank card number, SQL injection, Cross-site scripting

NO.75 When using anonymization techniques to prevent unauthorized access to personal data, which of the following is the MOST important consideration to ensure the data is adequately protected?
* The key must be kept separate and distinct from the data it protects.
* The data must be protected by multi-factor authentication.
* The key must be a combination of alpha and numeric characters.
* The data must be stored in locations protected by data loss prevention (DLP) technology.
Explanation

Anonymization is a technique that removes or modifies personal data in such a way that it can no longer be attributed to a specific data subject. Anonymization can be achieved by various methods, such as encryption, pseudonymization, aggregation, generalization, etc. When using anonymization techniques to prevent unauthorized access to personal data, the most important consideration to ensure the data is adequately protected is that the key must be kept separate and distinct from the data it protects. The key is a piece of information that is used to reverse the anonymization process and restore the original personal data. The key must be stored and managed in a secure location that is different from where the anonymized data is stored and processed. This way, even if the anonymized data is compromised, the key cannot be accessed or used to re-identify the data subjects. References: : CDPSE Review Manual (Digital Version), page 29

NO.76 Which of the following should be done FIRST to establish privacy to design when developing a contact-tracing application?
* Conduct a privacy impact assessment (PIA).
* Conduct a development environment review.
* Identify privacy controls for the application.
* Identify differential privacy techniques.

NO.77 An organization is planning a new implementation for tracking consumer web browser activity. Which of the following should be done FIRST?

* Seek approval from regulatory authorities.
* Conduct a privacy impact assessment (PIA).
* Obtain consent from the organization&#8217;s clients.
* Review and update the cookie policy.

Explanation

A privacy impact assessment (PIA) is a systematic process to identify and evaluate the potential privacy impacts of a system, project, program or initiative that involves the collection, use, disclosure or retention of personal data. A PIA should be done first when planning a new implementation for tracking consumer web browser activity, as it would help to ensure that privacy risks are identified and mitigated before the implementation is executed. A PIA would also help to ensure compliance with privacy principles, laws and regulations, and alignment with consumer expectations and preferences. The other options are not as important as conducting a PIA when planning a new implementation for tracking consumer web browser activity.

Seeking approval from regulatory authorities may be required or advisable for some types of personal data or data processing activities, but it may not be necessary or sufficient for tracking consumer web browser activity, depending on the context and jurisdiction. Obtaining consent from the organization&#8217;s clients may be required or advisable for some types of personal data or data processing activities, but it may not be necessary or sufficient for tracking consumer web browser activity, depending on the context and jurisdiction. Reviewing and updating the cookie policy may be required or advisable for some types of personal data or data processing activities, but it may not be necessary or sufficient for tracking consumer web browser activity, depending on the context and jurisdiction1, p. 67 References: 1: CDPSE Review Manual (Digital Version)

NO.78 Which of the following BEST ensures data confidentiality across databases?

* Logical data model
* Data normalization
* Data catalog vocabulary
* Data anonymization

NO.79 Which of the following MOST effectively protects against the use of a network sniffer?

* Network segmentation
* Transport layer encryption
* An intrusion detection system (IDS)
* A honeypot environment

NO.80 Which of the following BEST supports an organization&#8217;s efforts to create and maintain desired privacy protection practices among employees?

* Skills training programs
* Awareness campaigns
* Performance evaluations
* Code of conduct principles

NO.81 What is the BEST way for an organization to maintain the effectiveness of its privacy breach incident response plan?

* Require security management to validate data privacy security practices.
* Involve the privacy office in an organizational review of the incident response plan.
* Hire a third party to perform a review of data privacy processes.
* Conduct annual data privacy tabletop exercises.

Explanation

The best way for an organization to maintain the effectiveness of its privacy breach incident response plan is to conduct annual data privacy tabletop exercises. A data privacy tabletop exercise is a simulated scenario that tests the organization&#8217;s ability to respond to a privacy breach incident, such as a data breach, leak, or misuse.

A data privacy tabletop exercise involves key stakeholders, such as the privacy office, the information security team, the legal counsel, the public relations team, etc., who role-play their actions and decisions based on the scenario. A data privacy tabletop exercise helps to evaluate and improve the organization&#8217;s privacy breach incident response plan, such as identifying gaps or weaknesses, validating roles and responsibilities, verifying procedures and protocols, assessing communication and coordination, etc. References: : CDPSE Review Manual (Digital Version), page 83

NO.82 An organization is concerned with authorized individuals accessing sensitive personal customer information to use for unauthorized purposes. Which of the following technologies is the BEST choice to mitigate this risk?
* Email filtering system
* Intrusion monitoring
* Mobile device management (MDM)
* User behavior analytics
Explanation

User behavior analytics is a technology that uses data analysis and machine learning to monitor, detect and respond to anomalous or malicious user activities, such as accessing sensitive personal customer information to use for unauthorized purposes. User behavior analytics is the best choice to mitigate this risk, as it would help to identify and prevent insider threats, data breaches, fraud or misuse of data by authorized individuals.

User behavior analytics can also help to enforce policies and controls, such as access control, audit trail or data loss prevention. The other options are not as effective as user behavior analytics in mitigating this risk. Email filtering system is a technology that scans and blocks incoming or outgoing emails that contain spam, malware or phishing attempts, but it does not address the issue of authorized individuals accessing sensitive personal customer information to use for unauthorized purposes. Intrusion monitoring is a technology that monitors and alerts on unauthorized or malicious attempts to access a system or network, but it does not address the issue of authorized individuals accessing sensitive personal customer information to use for unauthorized purposes. Mobile device management (MDM) is a technology that manages and secures mobile devices that are used to access or store organizational data, but it does not address the issue of authorized individuals accessing sensitive personal customer information to use for unauthorized purposes1, p. 92 References: 1:

CDPSE Review Manual (Digital Version)

NO.83 When a government&#8217;s health division established the complete privacy regulation for only the health market, which privacy protection reference model is being used?
* Comprehensive
* Sectoral
* Self-regulatory
* Co-regulatory

What are the requirements to take the Isaca CDPSE Certification Exam?

The candidate must have three or more years of experience in information security and privacy. Happy customer reviews and testimonials are important.

The New CDPSE 2023 Updated Verified Study Guides & Best Courses: https://www.braindumpsit.com/CDPSE_real-exam.html
]