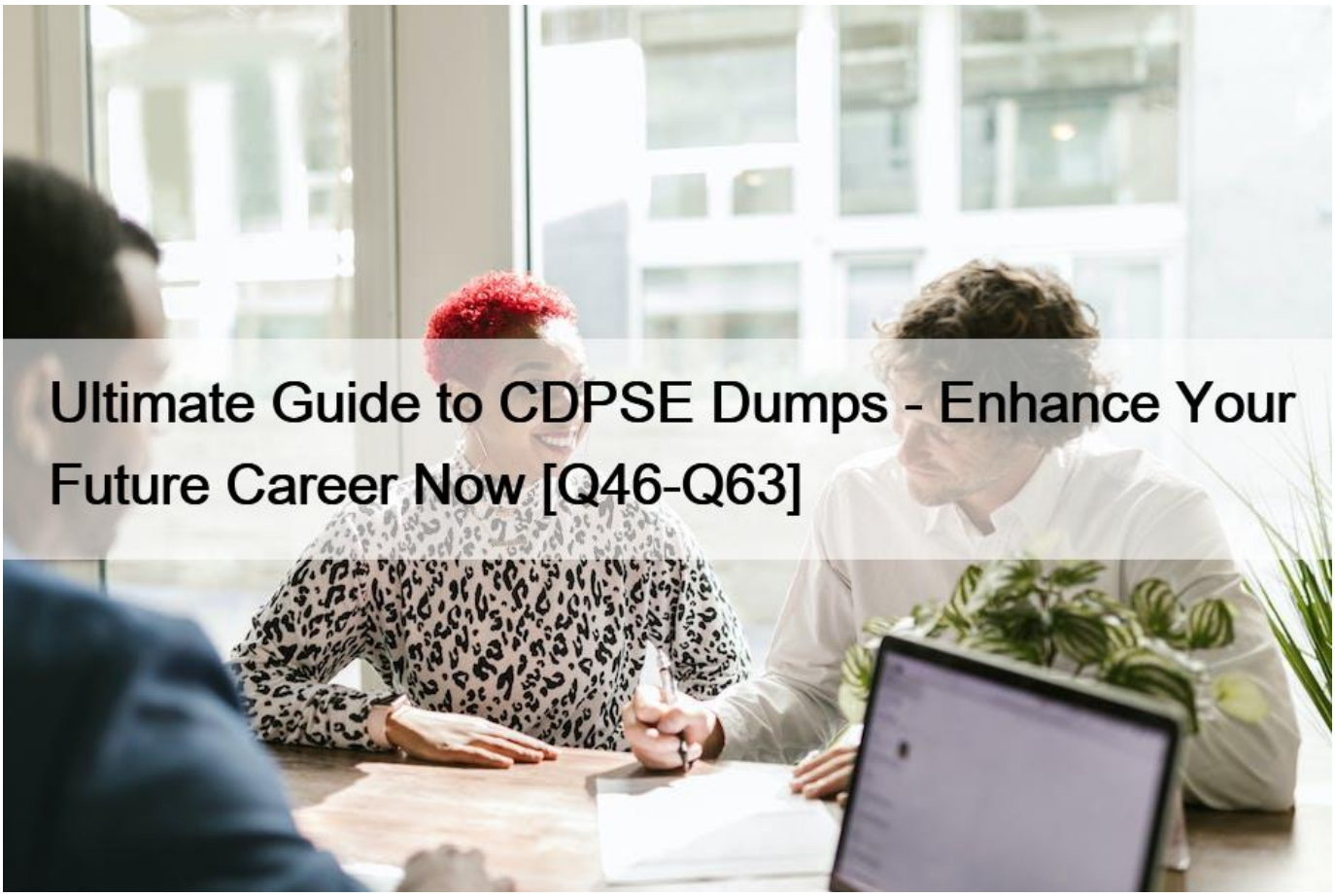
Ultimate Guide to CDPSE Dumps - Enhance Your Future Career Now [Q46-Q63



[Jul 17, 2023] ISACA Dumps - Learn How To Deal With The (CDPSE) Exam Anxiety
DEMO FREE BEFORE YOU BUY CDPSE DUMPS

Q46. Which of the following is the PRIMARY reason that a single cryptographic key should be used for only one purpose, such as encryption or authentication?
* It eliminates cryptographic key collision.
* It minimizes the risk if the cryptographic key is compromised.
* It is more practical and efficient to use a single cryptographic key.
* Each process can only be supported by its own unique key management process.

Q47. Which of the following is the BEST way to limit the organization’s potential exposure in the event of consumer data loss while maintaining the traceability of the data?
* De-identify the data.
* Require a digital signature.
* Use a unique hashing algorithm.
* Encrypt the data at rest.

Q48. Which party should data subject contact FIRST if they believe their personal information has been collected and used without

consent?
* Privacy rights advocate
* Outside privacy counsel
* Data protection authorities
* The organization’s chief privacy officer (CPO)

Q49. A multinational corporation is planning a big data initiative to help with critical business decisions. Which of the following is the BEST way to ensure personal data usage is standardized across the entire organization?
* De-identify all data.
* Develop a data dictionary.
* Encrypt all sensitive data.
* Perform data discovery.

Q50. Which of the following is the BEST way to manage different IT staff access permissions for personal data within an organization?
* Mandatory access control
* Network segmentation
* Dedicated access system
* Role-based access control

Q51. Which of the following is the BEST approach for a local office of a global organization faced with multiple privacy-related compliance requirements?
* Focus on developing a risk action plan based on audit reports.
* Focus on requirements with the highest organizational impact.
* Focus on global compliance before meeting local requirements.
* Focus on local standards before meeting global compliance.

Q52. Which of the following techniques mitigates design flaws in the application development process that may contribute to potential leakage of personal data?
* User acceptance testing (UAT)
* Patch management
* Software hardening
* Web application firewall (WAF)

Q53. Which of the following is the GREATEST benefit of adopting data minimization practices?
* Storage and encryption costs are reduced.
* Data retention efficiency is enhanced.
* The associated threat surface is reduced.
* Compliance requirements are met.

Unfortunately, the financial liability portion of retained personal information rarely shows up on an organization’s financial balance sheet. And yet it is indeed a liability: the impact on an organization when cybercriminals steal that information or when the information is misused is real, in the form of breach response costs, the costs related to reducing harm inflicted on affected parties (think of credit monitoring services, a frequent remedy for stolen credit card numbers), fines from governmental regulators, and the occasional class-action lawsuit.

Q54. When choosing data sources to be used within a big data architecture, which of the following data attributes MUST be considered to ensure data is not aggregated?
* Accuracy
* Granularity
* Consistency

* Reliability

Q55. Which of the following tracking technologies associated with unsolicited targeted advertisements presents the GREATEST privacy risk?
* Online behavioral tracking
* Radio frequency identification (RFID)
* Website cookies
* Beacon-based tracking

Q56. Which of the following hard drive sanitation methods provides an organization with the GREATEST level of assurance that data has been permanently erased?
* Degaussing the drive
* Factory resetting the drive
* Crypto-shredding the drive
* Reformatting the drive

Q57. 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.

Because many privacy incidents are also security incidents, the development of a privacy incident response plan should be performed in close cooperation with the security manager to avoid duplication of effort and to utilize existing response plan resources and practices.

Q58. When configuring information systems for the communication and transport of personal data, an organization should:
* adopt the default vendor specifications.
* review configuration settings for compliance.
* implement the least restrictive mode.
* enable essential capabilities only.

Q59. Which of the following is the BEST way to hide sensitive personal data that is in use in a data lake?
* Data masking
* Data truncation
* Data encryption
* Data minimization

Q60. Which of the following BEST represents privacy threat modeling methodology?
* Mitigating inherent risks and threats associated with privacy control weaknesses
* Systematically eliciting and mitigating privacy threats in a software architecture
* Reliably estimating a threat actor’s ability to exploit privacy vulnerabilities
* Replicating privacy scenarios that reflect representative software usage

Q61. Which of the following is MOST important when designing application programming interfaces (APIs) that enable mobile device applications to access personal data?
* The user’s ability to select, filter, and transform data before it is shared
* Umbrella consent for multiple applications by the same developer
* User consent to share personal data
* Unlimited retention of personal data by third parties

Q62. Which of the following is a PRIMARY objective of performing a privacy impact assessment (PIA) prior to onboarding a new Software as a Service (SaaS) provider for a customer relationship management (CRM) system?

* To identify controls to mitigate data privacy risks
* To classify personal data according to the data classification scheme
* To assess the risk associated with personal data usage
* To determine the service provider’s ability to maintain data protection controls

Q63. Which of the following protocols BEST protects end-to-end communication of personal data?

* Transmission Control Protocol (TCP)
* Transport Layer Security Protocol (TLS)
* Secure File Transfer Protocol (SFTP)
* Hypertext Transfer Protocol (HTTP)