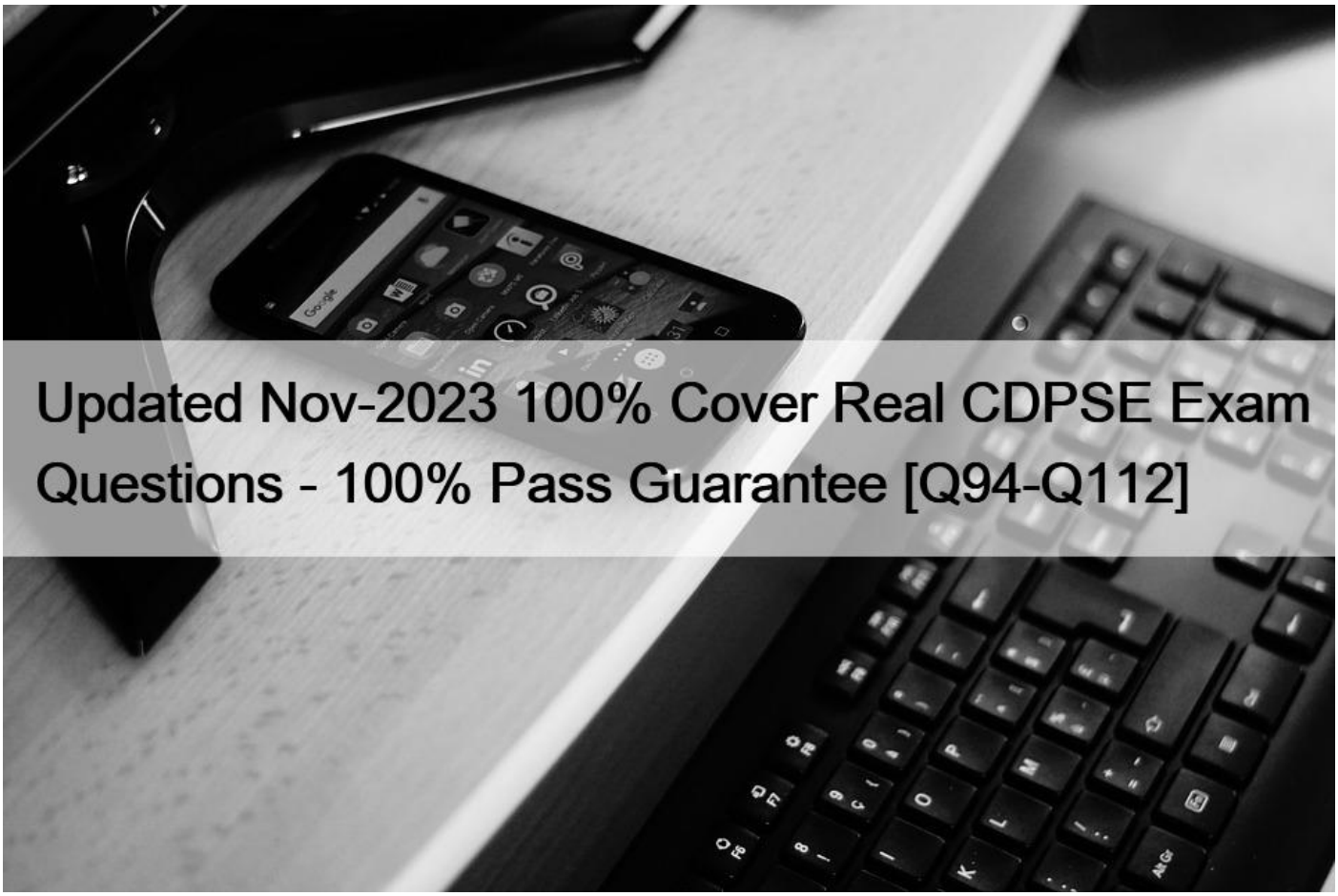
Updated Nov-2023 100% Cover Real CDPSE Exam Questions - 100% Pass Guarantee [Q94-Q112



Updated Nov-2023 100% Cover Real CDPSE Exam Questions - 100% Pass Guarantee
Use Real ISACA Dumps - 100% Free CDPSE Exam Dumps

One of the key benefits of the CDPSE certification is that it demonstrates a professional's understanding of global privacy regulations and their ability to develop and implement solutions that comply with these regulations. With the increasing number of privacy regulations around the world, including the GDPR, CCPA, and LGPD, the demand for professionals who can navigate these regulations and develop effective solutions is on the rise.

Isaca CDPSE Certification Exam - A quick overview

CDPSE Exam is a sought-after certification exam in the IT industry. It is also known as Certified Data Privacy Solutions Engineer. This certification exam is authorized by the International Society for Information Risk and Compliance (ISARC) and is offered by Isaca Training Institute. The exam is a certification exam that aims to validate the technical skills and knowledge it takes to assess, build and implement comprehensive privacy solutions. Implement cisco enterprise network solutions. The answers to these questions help to validate the candidate's skills and understanding of Privacy Solutions. **CDPSE Dumps** can help you pass this exam on your first attempt.
Candidates who pass the CDPSE Exam can fill the gap with technical privacy skills so that the organization has competent privacy

technologists to build and implement solutions that enhance efficiency and mitigate risk. Candidates who have passed the CDPSE Exam can be considered for employment opportunities in ISACA as a Professional in Risk Assurance and Information Security. The exam will certify the understanding and skills of a professional in information privacy. Understanding in hop redundancy protocols, logical security, and physical security. The majority of students are glad to decide to pursue this certification as it will help them to get a better job.

NEW QUESTION 94

Which of the following is the BEST way to ensure privacy considerations are included when working with vendors?
* Including privacy requirements in the request for proposal (RFP) process
* Monitoring privacy-related service level agreements (SLAS)
* Including privacy requirements in vendor c tracts
* Requiring vendors to complete privacy awareness training

Explanation

Including privacy requirements in vendor contracts is the best way to ensure privacy considerations are included when working with vendors because it establishes the obligations, expectations and responsibilities of both parties regarding the protection of personal data. It also provides a legal basis for enforcing compliance and resolving disputes. Including privacy requirements in the request for proposal (RFP) process, monitoring privacy-related service level agreements (SLAs) and requiring vendors to complete privacy awareness training are helpful measures, but they do not guarantee that vendors will adhere to the privacy requirements or that they will be held accountable for any violations.

References:

* CDPSE Review Manual (Digital Version), Domain 1: Privacy Governance, Task 1.7: Participate in the management and evaluation of contracts, service levels and practices of vendors and other external parties1

* CDPSE Certified Data Privacy Solutions Engineer All-in-One Exam Guide, Chapter 2: Privacy Governance, Section: Vendor Management2

NEW QUESTION 95

Which of the following should be the FIRST consideration when conducting a privacy impact assessment (PIA)?
* The applicable privacy legislation
* The quantity of information within the scope of the assessment
* The systems in which privacy-related data is stored
* The organizational security risk profile

NEW QUESTION 96

Which of the following would MOST effectively reduce the impact of a successful breach through a remote access solution?
* Compartmentalizing resource access
* Regular testing of system backups
* Monitoring and reviewing remote access logs
* Regular physical and remote testing of the incident response plan

NEW QUESTION 97

Which of the following is the MOST important consideration when using advanced data sanitization methods to ensure privacy data

will be unrecoverable?
* Subject matter expertise
* Type of media
* Regulatory compliance requirements
* Location of data

Explanation

Data sanitization is a process of permanently erasing or destroying data from a storage device or media to prevent unauthorized access or recovery of the data. Data sanitization methods can include physical destruction, degaussing, overwriting, encryption or cryptographic erasure. The most important consideration when using advanced data sanitization methods to ensure privacy data will be unrecoverable is the type of media on which the data is stored, as different media types may require different methods or techniques to achieve effective sanitization. For example, physical destruction may be suitable for optical disks or tapes, but not for solid state drives (SSDs) or flash memory devices. Degaussing may be effective for magnetic disks or tapes, but not for optical disks or SSDs. Overwriting may work for hard disk drives (HDDs) or SSDs, but not for tapes or optical disks. Encryption or cryptographic erasure may be applicable for any media type, but may require additional security measures to protect the encryption keys or certificates. The other options are not as important as the type of media when using advanced data sanitization methods. Subject matter expertise may be helpful, but not essential, as long as the appropriate method is selected and applied correctly. Regulatory compliance requirements may influence the choice of method, but not necessarily determine it, as different methods may meet different standards or criteria. Location of data may affect the feasibility or cost of applying a method, but not its effectiveness or suitability., p. 93-94 References: : CDPSE Review Manual (Digital Version)

NEW QUESTION 98

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

Explanation

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 is to identify controls to mitigate data privacy risks, such as data breaches, unauthorized access, misuse or loss of data. A PIA would help to evaluate the potential privacy impacts of using a new SaaS provider for CRM data processing activities, such as collecting, storing, analyzing or transferring customer data, and to implement appropriate controls to mitigate those impacts, such as encryption, access control, backup, audit trail or contractual clauses. A PIA would also help to ensure compliance with privacy principles, laws and regulations, and alignment with customer expectations and preferences. The other options are not primary objectives of performing a PIA prior to onboarding a new SaaS provider for CRM data processing activities. Classifying personal data according to the data classification scheme is an activity that may be part of a PIA process, but it is not an objective in itself. Assessing the risk associated with personal data usage is an activity that may be part of a PIA process, but it is not an objective in itself. Determining the service provider’s ability to maintain data protection controls is an activity that may be part of a PIA process, but it is not an objective in itself1, p. 67 References: 1: CDPSE Review Manual (Digital Version)

NEW QUESTION 99

What is the BES T way for an organization to maintain the effectiveness of its privacy breach incident response plan?

* Require security management to validate data privacy security practices.

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

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 tabletop exercise is a simulated scenario that tests the organization’s ability to respond to a privacy breach incident in a realistic and interactive way. A tabletop exercise can help the organization to evaluate the roles and responsibilities of the incident response team, identify the gaps and weaknesses in the plan, improve the communication and coordination among the stakeholders, and update the plan based on the lessons learned and best practices12. A tabletop exercise can also enhance the awareness and readiness of the organization to handle privacy breach incidents in a timely and effective manner3.
References:

* ISACA CDPSE Review Manual, Chapter 4, Section 4.3.2

* ISACA Journal, Volume 4, 2019, “Tabletop Exercises: Three Sample Scenarios”

* ISACA Journal, Volume 6, 2017, “Privacy Breach Response: Preparing for the Inevitable”

NEW QUESTION 100

Which of the following is the MOST important privacy consideration for video surveillance in high security areas?
* Video surveillance recordings may only be viewed by the organization.
* Those affected must be informed of the video surveillance_
* There is no limitation for retention of this data.
* Video surveillance data must be stored in encrypted format.

Explanation

One of the key principles of data protection is transparency, which means that individuals have the right to be informed about the collection and use of their personal data. This applies to video surveillance as well, especially in high security areas where the impact on privacy may be significant. Therefore, it is important to inform those affected by video surveillance about the purpose, scope, retention and access policies of the data collected.

References:

* ISACA Certified Data Privacy Solutions Engineer (CDPSE) Exam Content Outline, Domain 2: Privacy Architecture, Task 2.1: Design privacy controls based on privacy principles and legal requirements, Subtask 2.1.1: Identify applicable privacy principles and legal requirements.

* How can we comply with the data protection principles when using surveillance systems? | ICO

NEW QUESTION 101

Which of the following is the PRIMARY reason that organizations need to map the data flows of personal data?
* To assess privacy risks
* To evaluate effectiveness of data controls
* To determine data integration gaps
* To comply with regulations

Explanation

Data flow mapping is a technique to document how personal data flows within and outside an organization, including the sources, destinations, formats, purposes and legal bases of the data processing activities. Data flow mapping helps organizations to assess privacy risks, such as data breaches, unauthorized access, misuse or loss of data, and to implement appropriate controls to mitigate those risks. Data flow mapping may also help organizations to evaluate the effectiveness of data controls, determine data integration gaps and comply with regulations, but those are not the primary reasons for data flow mapping1, p. 69-70 References: 1:

CDPSE Review Manual (Digital Version)

NEW QUESTION 102

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.

NEW QUESTION 103

Which of the following poses the GREATEST privacy risk for client-side application processing?
* Failure of a firewall protecting the company network
* An employee loading personal information on a company laptop
* A remote employee placing communication software on a company server
* A distributed denial of service attack (DDoS) on the company network
Explanation

The greatest privacy risk for client-side application processing is an employee loading personal information on a company laptop. Client-side application processing refers to performing data processing operations on the user’s device or browser, rather than on a server or cloud. This can improve performance and user experience, but also pose privacy risks if the user’s device is lost, stolen, hacked, or infected with malware. An employee loading personal information on a company laptop is exposing that information to potential threats on the client-side, such as unauthorized access, use, disclosure, modification, or loss. Therefore, an organization should implement appropriate security measures to protect personal information on client-side devices, such as encryption, authentication, authorization, logging, monitoring, etc. References: : CDPSE Review Manual (Digital Version), page 153

NEW QUESTION 104

Which of the following activities would BEST enable an organization to identify gaps in its privacy posture?
* Retargeting employees for awareness training after a social engineering attack
* Conducting a simulation exercise that requires participants to respond to a privacy incident
* Providing an interactive session on privacy risks at an organization-wide meeting
* Requiring employees to review the organization’s privacy policy on an annual basis
Explanation

D) Requiring employees to review the organization’s privacy policy on an annual basis Short Explanation: Requiring employees to review the organization’s privacy policy on an annual basis is the best activity to enable an organization to identify gaps in its privacy posture because it can help to ensure that the employees are aware of the current privacy requirements, expectations, and practices of the organization. It can also help to identify any discrepancies, inconsistencies, or conflicts between the policy and the actual implementation of privacy controls and processes. By reviewing the policy regularly, the organization can also update and improve it as needed to reflect any changes in the privacy landscape, such as new laws, regulations, standards, or

threats.

References:

* Privacy Policy Review Checklist, PrivacySense

* How to Write a Privacy Policy for Your Website, TermsFeed

NEW QUESTION 105

Which of the following system architectures BEST supports anonymity for data transmission?
* Client-server
* Plug-in-based
* Front-end
* Peer-to-peer
Explanation

A peer-to-peer (P2P) system architecture is a network model where each node (peer) can act as both a client and a server, and communicate directly with other peers without relying on a centralized authority or intermediary. A P2P system architecture best supports anonymity for data transmission, by providing the following advantages:

* It can hide the identity and location of the peers, by using encryption, pseudonyms, proxies, or onion routing techniques, such as Tor1 or I2P2. These techniques can prevent eavesdropping, tracking, or censorship by third parties, such as Internet service providers, governments, or hackers.

* It can distribute the data across multiple peers, by using hashing, replication, or fragmentation techniques, such as BitTorrent3 or IPFS4. These techniques can reduce the risk of data loss, corruption,

* or tampering by malicious peers, and increase the availability and resilience of the data.

* It can enable the peers to control their own data, by using consensus, validation, or incentive mechanisms, such as blockchain5 or smart contracts. These mechanisms can ensure the integrity and authenticity of the data transactions, and enforce the privacy policies and preferences of the data owners.

NEW QUESTION 106

Which of the following system architectures BEST supports anonymity for data transmission?
* Client-server
* Plug-in-based
* Front-end
* Peer-to-peer

NEW QUESTION 107

Which of the following is the MOST effective way to support organizational privacy awareness objectives?
* Funding in-depth training and awareness education for data privacy staff
* Implementing an annual training certification process
* Including mandatory awareness training as part of performance evaluations
* Customizing awareness training by business unit function
Explanation

The most effective way to support organizational privacy awareness objectives is D. Customizing awareness training by business unit function.

A comprehensive explanation is:

Organizational privacy awareness objectives are the goals and expectations that an organization sets for its employees and stakeholders regarding the protection and management of personal data. Privacy awareness objectives may vary depending on the nature, scope, and purpose of the organization’s data processing activities, as well as the legal, regulatory, contractual, and ethical obligations and implications that apply to them.

One of the best practices to support organizational privacy awareness objectives is to customize awareness training by business unit function. This means that the organization should design and deliver privacy awareness training programs that are tailored to the specific roles, responsibilities, and needs of each business unit or department within the organization. Customizing awareness training by business unit function can have several benefits, such as:

* Enhancing the relevance and effectiveness of the training content and methods for each audience group, by addressing their specific privacy challenges, risks, and opportunities.

* Increasing the engagement and motivation of the trainees, by showing them how privacy relates to their daily tasks, goals, and performance.

* Improving the retention and application of the training knowledge and skills, by providing practical examples, scenarios, and exercises that reflect the real-world situations and problems that the trainees may encounter.

* Fostering a culture of privacy across the organization, by creating a common language and understanding of privacy concepts, principles, and practices among different business units or departments.

Some examples of how to customize awareness training by business unit function are:

* Providing different levels or modules of training based on the degree of access or exposure to personal data that each business unit or department has. For example, a basic level of training for all employees, an intermediate level of training for employees who handle personal data occasionally or incidentally, and an advanced level of training for employees who handle personal data regularly or extensively.

* Providing different topics or themes of training based on the type or category of personal data that each business unit or department processes. For example, a general topic of training for employees who process non-sensitive or non-personal data, a specific topic of training for employees who process sensitive or special data categories (such as health, biometric, financial, or political data), and a specialized topic of training for employees who process high-risk or high-value data (such as intellectual property, trade secrets, or customer loyalty data).

* Providing different formats or modes of training based on the preferences or constraints of each business unit or department. For example, a face-to-face format of training for employees who work in the same location or office, an online format of training for employees who work remotely or across different time zones, and a blended format of training for employees who work in a hybrid mode or have flexible schedules.

The other options are not as effective as option D.

Funding in-depth training and awareness education for data privacy staff (A) may improve the competence and confidence of the data privacy staff who are responsible for designing and implementing the privacy policies and practices of the organization, but it

does not necessarily support the organizational privacy awareness objectives for the rest of the employees and stakeholders.

Implementing an annual training certification process (B) may ensure that the employees and stakeholders are updated and refreshed on the privacy policies and practices of the organization on a regular basis, but it does not necessarily address their specific privacy needs and challenges based on their business unit function.

Including mandatory awareness training as part of performance evaluations may incentivize the employees and stakeholders to participate in and complete the privacy awareness training programs offered by the organization, but it does not necessarily enhance their understanding and application of privacy concepts and principles based on their business unit function.

References:

* The Benefits of Information Security and Privacy Awareness Training Programs1

* What Is Your Privacy and Data Protection Strategy?2

* What is Data Privacy Awareness?3

NEW QUESTION 108

When contracting with a Software as a Service (SaaS) provider, which of the following is the MOST important contractual requirement to ensure data privacy at service termination?
* Encryption of customer data
* Removal of customer data
* De-identification of customer data
* Destruction of customer data
Explanation

When contracting with a SaaS provider, it is important to ensure that the provider will remove all customer data from their systems and storage devices at the end of the service contract. This will prevent any unauthorized access, use, or disclosure of the customer data by the provider or third parties after the service termination. Removal of customer data means that the data are permanently erased and cannot be recovered or restored by any means.

References:

* ISACA, Data Privacy Audit/Assurance Program, Control Objective 9: Data Disposal, p. 16-171

* ISACA, CDPSE Review Manual 2021, Chapter 4: Privacy Incident Response, Section 4.2: Data Disposal and Destruction, p. 151-152.

NEW QUESTION 109

Which of the following is the BEST way for an organization to limit potential data exposure when implementing a new application?
* Implement a data loss prevention (DLP) system.
* Use only the data required by the application.
* Encrypt all data used by the application.
* Capture the application’s authentication logs.
Explanation

The principle of data minimization 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 using only the data required by the application, the organization can reduce the amount of data that is collected, stored, processed and potentially exposed. This can also help the organization comply with privacy laws and regulations that require data minimization, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

References:

* CDPSE Review Manual, 2021 Edition, ISACA, page 98

* [Data minimization], European Commission

NEW QUESTION 110

Which of the following is the PRIMARY objective of privacy incident response?
* To ensure data subjects impacted by privacy incidents are notified.
* To reduce privacy risk to the lowest possible level
* To mitigate the impact of privacy incidents
* To optimize the costs associated with privacy incidents

NEW QUESTION 111

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’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’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

NEW QUESTION 112

Which of the following is MOST important to include in a data use policy?
* The requirements for collecting and using personal data
* The method used to delete or destroy personal data
* The reason for collecting and using personal data
* The length of time personal data will be retained

Explanation

A data use policy is a document that defines the rules and guidelines for how personal data are collected, used, stored, shared and deleted by an organization. It is an important part of data governance and compliance, as it helps to ensure that personal data are handled in a lawful, fair and transparent manner, respecting the rights and preferences of data subjects. A data use policy should

include the requirements for collecting and using personal data, such as the legal basis, the purpose, the scope, the consent, the data minimization, the accuracy, the security and the accountability. These requirements help to establish the legitimacy and necessity of data processing activities, and to prevent unauthorized or excessive use of personal data.

References:

* ISACA Privacy Notice & Usage Disclosures, section 2.1: “We collect Personal Information from you when you provide it to us directly or through a third party who has assured us that they have obtained your consent.”

* Chapter Privacy Policy – Singapore Chapter – ISACA, section 2: “We will collect your personal data in accordance with the PDPA either directly from you or your authorized representatives, and/or through our third party service providers.”

* Data Minimization-A Practical Approach – ISACA, section 2: “Enterprises may only collect as much data as are necessary for the purposes defined at the time of collection, which may also be set out in a privacy notice (sometimes referred to as a privacy statement, a fair processing statement or a privacy policy).”

* Establishing Enterprise Roles for Data Protection – ISACA, section 3: “Data governance is typically implemented in organizations through policies, guidelines, tools and access controls.”