Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

ISACA-CDPSE MCQs
ISACA-CDPSE TestPrep
ISACA-CDPSE Study Guide
ISACA-CDPSE Practice Test
ISACA-CDPSE Exam Questions

killexams.com

ISACA

ISACA-CDPSE

Certified Data Privacy Solutions Engineer (CDPSE) - 202

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/CDPSE

Question: 662

What is the primary benefit of employing Transport Layer Security (TLS) over its predecessor, Secure Sockets Layer (SSL)?

A. TLS is easier to implement
B. TLS is more widely supported by legacy systems
C. TLS provides stronger encryption and security features
D. TLS requires less computing power

Answer: C

Explanation: TLS provides stronger encryption and enhanced security features compared to SSL, making it the preferred choice for securing data in transit.

Question: 663

In the context of data subject rights under the GDPR, which of the following statements is true regarding the right to data portability?

A. It allows data subjects to request data in any format they prefer
B. It permits data subjects to transfer their data directly between service providers
C. It only applies to data collected by public authorities
D. It requires organizations to delete personal data upon request

Answer: B

Explanation: The right to data portability enables data subjects to request their personal data be transferred directly from one service provider to another, enhancing user control.

Question: 664

Which of the following is a potential consequence of failing to implement adequate monitoring and logging practices?

A. Increased system performance
B. Inability to detect security incidents
C. Reduced operational costs
D. Enhanced user productivity

Answer: B

Explanation: Without proper monitoring and logging, organizations may struggle to detect and respond to security incidents promptly, which could lead to severe data breaches and losses.

Question: 665

During an audit, it was found that an organization failed to document the legal basis for processing personal data as required by GDPR. Which of the following artifacts would best demonstrate compliance moving forward?

A. A newly created data processing policy
B. Employee training materials on data protection
C. Updated records of processing activities
D. Reports on previous data breaches

Answer: C

Explanation: Updated records of processing activities (RoPA) that clearly document the legal basis for data processing would best demonstrate compliance with GDPR moving forward.

Question: 666

A company employing big data analytics must navigate various privacy considerations. What should be the primary focus when developing data handling procedures for this type of data?

A. Maximizing data collection for broader insights.
B. Limiting data access to senior management only.
C. Ensuring that data anonymization techniques are robust and effective.
D. Conducting data analysis without any oversight.

Answer: C

Explanation: Ensuring robust anonymization techniques is critical when handling big data to protect individual privacy while still deriving valuable insights.

Question: 667

In the selection of communication and transport protocols for protecting sensitive data in transit, which of the following protocols provides the most robust encryption to ensure data privacy?

A. HTTP
B. FTP
C. Telnet
D. HTTPS

Answer: D

Explanation: HTTPS uses SSL/TLS to encrypt data in transit, ensuring that sensitive information is protected from eavesdropping and tampering, thus maintaining data privacy.

Question: 668

Which of the following is a recommended practice for ensuring effective communication of privacy policies to employees?

A. Providing static documents without updates
B. Relying solely on verbal communication
C. Utilizing multiple channels, including digital platforms and in-person meetings
D. Limiting access to policy documents

Answer: C

Explanation: Utilizing multiple channels for communication, including digital platforms and in-person meetings, ensures that employees receive and understand privacy policies effectively.

Question: 669

When assessing the effectiveness of privacy-enhancing technologies (PETs) implemented in an organization, which of the following metrics would provide the most relevant insights into their performance?

A. The total cost of implementing the PETs over time.
B. The percentage of data processed by PETs compared to total data.
C. Employee satisfaction with the PETs used in daily operations.
D. The number of data breaches reported before and after implementation.

Answer: D

Explanation: The number of data breaches reported before and after implementation directly indicates the effectiveness of PETs in enhancing privacy protection.

Question: 670

An organization is planning to implement a new policy for data retention and destruction. Which of the following steps should be taken first in developing this policy?

A. Roll out the policy organization-wide immediately
B. Draft the policy without stakeholder input
C. Consult legal and compliance teams to ensure adherence to laws
D. Focus on training employees on data handling

Answer: C

Explanation: Consulting legal and compliance teams first ensures that the policy adheres to applicable laws and regulations, laying a solid foundation for the organization’s data retention and destruction practices.

Question: 671

A company is preparing to launch a new product that will collect biometric data from users. Which of the following privacy regulations requires explicit consent from users before collecting such sensitive data?

A. HIPAA
B. CCPA
C. GDPR
D. ePrivacy Directive

Answer: C

Explanation: GDPR requires explicit consent from users before collecting sensitive data, such as biometric data, ensuring that individuals have control over their personal information.

Question: 672

In an effort to comply with GDPR's accountability principle, a company decides to implement a data governance program. What is the most crucial component of this program to ensure it meets GDPR requirements?

A. Regular employee surveys on data handling
B. Detailed documentation of data processing activities
C. Comprehensive data retention policies
D. A designated Data Protection Officer (DPO)

Answer: B

Explanation: Detailed documentation of data processing activities is crucial for demonstrating accountability under GDPR, providing transparency and evidence of compliance.

Question: 673

Which of the following is the MOST effective method for ensuring user awareness about data privacy during transfers?

A. Mandatory training sessions
B. Regular policy updates
C. Automated email reminders
D. Simplified privacy notices

Answer: A

Explanation: Mandatory training sessions are the most effective method, as they actively engage users and ensure they understand data privacy requirements and best practices.

Question: 674

A healthcare organization is required by law to protect patient data rigorously. As part of its privacy-related security controls, it plans to implement a data encryption strategy. Which of the following factors should be prioritized when selecting an encryption method?

A. Encryption speed over security strength
B. Compatibility with legacy systems
C. Compliance with industry standards and regulations
D. User preferences for ease of use

Answer: C

Explanation: Compliance with industry standards and regulations is paramount when selecting an encryption method, particularly in healthcare, to ensure that sensitive patient data is adequately protected.

Question: 675
An organization is developing a new mobile application that requires access to users' location data. What is the most important step to take during the risk management process?

A. Ignoring location data collection if it enhances user experience
B. Conducting a comprehensive risk assessment focusing on location data
C. Ensuring that users can opt-out of location tracking
D. Collecting location data without user consent

Answer: B

Explanation: Conducting a comprehensive risk assessment focusing on location data is essential to identify potential risks and ensure compliance with privacy regulations.

Question: 676

An organization is planning to conduct a privacy impact assessment (PIA) for a new project involving personal data processing. What is the first step that should be taken in this process?

A. Identify stakeholders affected by the data processing
B. Analyze existing data protection measures
C. Define the scope and objectives of the PIA
D. Draft a report of potential privacy risks

Answer: C

Explanation: Defining the scope and objectives of the PIA is the first step, as it sets the foundation for the assessment and identifies what areas need to be evaluated.

Question: 677

In the context of API security, what does the term "SSO" (Single Sign-On) refer to?

A. A method of encrypting API requests
B. A way to create multiple API keys for different users
C. A technique for generating secure tokens
D. A mechanism that allows users to authenticate once to access multiple applications

Answer: D

Explanation: Single Sign-On (SSO) enables users to authenticate once and gain access to multiple applications, simplifying user management while enhancing security through centralized authentication.

Question: 678
A company faces a data breach due to malware that exploited a known vulnerability. What should the organization focus on to prevent future incidents?

A. Enhancing employee awareness of malware
B. Regularly updating software and systems to patch vulnerabilities
C. Implementing strict access controls for all employees
D. Reviewing the incident response plan

Answer: B

Explanation: Regularly updating software and systems to patch known vulnerabilities is a critical preventive measure against malware and other cyber threats.

Question: 679

When deploying machine learning models that handle personal data, what is the most effective way to ensure compliance with data protection regulations?

A. Use historical data without any modifications.
B. Ensure that data is anonymized or pseudonymized before use.
C. Focus solely on the accuracy of the model outputs.
D. Collect data from as many users as possible to improve model performance.

Answer: B

Explanation: Ensuring that data is anonymized or pseudonymized before use is the most effective way to comply with data protection regulations when deploying machine learning models.

Question: 680

In a scenario where a company is found to have inadequate security measures resulting in a data breach, which evidence would be most critical in demonstrating that the organization had a functioning privacy

program in place prior to the incident?

A. Data breach response plan
B. Documentation of employee training sessions
C. Records of privacy impact assessments
D. Risk assessment reports

Answer: C

Explanation: Records of privacy impact assessments demonstrate proactive measures to identify and mitigate privacy risks, providing critical evidence of a functioning privacy program prior to the incident.

Question: 681

Which of the following practices is most effective in mitigating the risk of unauthorized access to sensitive personal data stored in a data warehouse?

A. Using complex passwords for all user accounts
B. Storing sensitive data in less accessible locations
C. Relying on perimeter defenses like firewalls
D. Conducting regular security audits and access reviews

Answer: D

Explanation: Conducting regular security audits and access reviews is the most effective practice for mitigating unauthorized access risks, as it helps identify vulnerabilities and ensures appropriate access controls are maintained.

Question: 682

When assessing the effectiveness of a privacy program, which of the following would be the most relevant metric to track?

A. Number of data breaches reported
B. Percentage of employees completing privacy training
C. Employee turnover rate
D. Number of new data processing activities initiated

Answer: B

Explanation: The percentage of employees completing privacy training is a direct indicator of awareness and preparedness regarding privacy practices, making it an important metric for assessing program effectiveness.

Question: 683

What is the PRIMARY benefit of using encryption for data transfers involving personal information?

A. Faster data transfer speeds
B. Enhanced user experience
C. Protection against unauthorized access
D. Simplified compliance processes

Answer: C

Explanation: Encryption provides protection against unauthorized access during data transfers, ensuring that personal information remains confidential even if intercepted.

Question: 684

What is the purpose of implementing HMAC (Hash-based Message Authentication Code) in API requests?

A. To encrypt the data being sent
B. To simplify the authentication process
C. To ensure the integrity and authenticity of the message
D. To reduce API response times

Answer: C

Explanation: HMAC is used to ensure both the integrity and authenticity of a message, verifying that the message has not been altered and confirming the sender's identity.

Question: 685
A data privacy compliance team is evaluating the effectiveness of its privacy training program. Which of the following methods would provide the most reliable data on the program's impact on employee behavior?

A. Surveys distributed after each training session
B. Tracking the number of training materials distributed
C. Collecting feedback from training facilitators
D. Monitoring employee compliance with data handling protocols

Answer: D

Explanation: Monitoring employee compliance with data handling protocols provides direct evidence of behavior change and the program's real-world effectiveness.

Question: 686

An organization is implementing a new data governance framework that includes measures for personal information management. Which of the following practices would best support the promotion of fairness

and accountability throughout the data lifecycle?

A. Implementing a one-size-fits-all policy for data handling across all departments.
B. Assigning data stewardship roles to senior management only.
C. Limiting data access to IT personnel exclusively.
D. Conducting regular audits of data usage and handling practices.

Answer: D

Explanation: Regular audits of data usage and handling ensure accountability and fairness by identifying and addressing any deviations from established data governance practices.

Question: 687

A retail company has identified that 25% of customer complaints stem from data privacy issues. To address this, which metric should the company prioritize in its program monitoring to effectively track improvements in customer satisfaction related to privacy?

A. Number of privacy incidents reported
B. Average response time to privacy complaints
C. Frequency of data protection training sessions
D. Customer satisfaction scores post-incident

Answer: D

Explanation: Customer satisfaction scores post-incident provide direct feedback on how effectively the company is addressing data privacy issues and improving customer perception, making it a key metric to monitor.

Question: 688

What is the primary goal of patch management in maintaining data privacy?

A. To enhance user interface design
B. To mitigate vulnerabilities in software
C. To ensure compliance with regulations
D. To improve system performance

Answer: B

Explanation: The main focus of patch management is to identify and apply updates to software that fix vulnerabilities, thereby reducing the risk of data breaches and enhancing overall security posture.

Question: 689

In a scenario where a company handles sensitive financial data, what is the most critical component of its

patch management policy to maintain compliance and security?

A. Regularly scheduled patch updates
B. Manual patch application by IT staff
C. Ignoring non-critical patches
D. Allowing users to decide on patching schedules

Answer: A

Explanation: Regularly scheduled patch updates are critical to maintaining compliance and security, ensuring that vulnerabilities are addressed promptly to protect sensitive financial data.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.