Isaca CDPSE Mock Exam

Shared by Albert on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The purpose of consent tagging is to:

Options:

A- Ensure users have given consent to use cookies
B- Track and manage individuals' consent preferences
C- Log and track consent from a user visiting a website
D- Request consent from a user visiting a website

Answer:

B

Explanation:

Consent tagging is a metadata-driven process that associates consent preferences with an individual's data, enabling organizations to manage consent dynamically across systems. It is not limited to cookies (A), one-time logging (C), or initial requests (D).

''Consent tagging links an individual's data with their recorded consent choices for compliant processing.''

Question 2

Question Type: MultipleChoice

When is the BEST time during the secure development life cycle to perform privacy threat modeling?

Options:

A- When identifying business requirements
B- Early in the design phase
C- During functional verification testing
D- Prior to the production release

Answer:

B

Explanation:

The best time during the secure development life cycle to perform privacy threat modeling is early in the design phase, because this will help identify and mitigate the potential privacy risks and vulnerabilities of the system or application before they become costly or difficult to fix.Privacy threat modeling is a systematic process of analyzing the data flows, assets, actors, and scenarios of a system or application to identify and prioritize the privacy threats and countermeasures12. Performing privacy threat modeling early in the design phase will also help ensure that privacy is built into the system or application from the start, rather than as an afterthought.

CDPSE Exam Content Outline, Domain 2 -- Privacy Architecture (Privacy Architecture Implementation), Task 2: Implement privacy solutions3.

CDPSE Review Manual, Chapter 2 -- Privacy Architecture, Section 2.3 -- Privacy Architecture Implementation4.

Question 3

Question Type: MultipleChoice

Which of the following has the GREATEST impact on the treatment of data within the scope of an organization's privacy policy?

Options:

A- Data protection impact assessment (DPIA)
B- Data flow diagram
C- Data classification
D- Data processing agreement

Answer:

C

Explanation:

Data classification is the process of categorizing data according to its sensitivity, value, and criticality for the organization and the data subjects. Data classification has the greatest impact on the treatment of data within the scope of an organization's privacy policy, as it determines the appropriate level of protection, access, retention, and disposal for each type of dat

a. Data classification also helps to comply with the privacy principles and regulations, such as data minimization, purpose limitation, accuracy, security, and accountability.

Question 4

Question Type: MultipleChoice

Which of the following is the BEST way for senior management to verify the success of its commitment to privacy by design?

Options:

A- Review the findings of an industry benchmarking assessment
B- Identify trends in the organization's amount of compromised personal data
C- Review the findings of a third-party privacy control assessment
D- Identify trends in the organization's number of privacy incidents.

Answer:

C

Explanation:

A third-party privacy control assessment is an independent and objective evaluation of the design and effectiveness of the privacy controls implemented by an organization to protect personal data and comply with privacy laws and regulations. A third-party privacy control assessment can help senior management to verify the success of its commitment to privacy by design, by providing the following benefits:

It can measure the extent to which the organization has adopted and integrated the principles and practices of privacy by design throughout its products, services, processes and systems.

It can identify the strengths and weaknesses of the organization's privacy governance, policies, procedures, standards and guidelines, and provide recommendations for improvement.

It can validate the organization's compliance with the applicable privacy requirements and expectations of its customers, stakeholders, regulators and auditors.

It can enhance the organization's reputation and trustworthiness as a responsible and transparent data controller and processor.

The other options are less effective or irrelevant for verifying the success of the commitment to privacy by design. Reviewing the findings of an industry benchmarking assessment may provide some insights into how the organization compares with its peers or competitors in terms of privacy performance, but it may not reflect the specific privacy goals, risks and challenges of the organization. Identifying trends in the organization's amount of compromised personal data or number of privacy incidents may indicate some aspects of the organization's privacy maturity, but they are reactive and lagging indicators that do not capture the proactive and preventive nature of privacy by design. Moreover, these metrics may not account for other factors that may influence the occurrence or impact of data breaches or privacy violations, such as external threats, human errors or environmental changes.

Privacy by Design: How Far Have We Come? - ISACA, section 1: ''Privacy by design challenges conventional system thinking. It mandates that any system, process or infrastructure that uses personal data consider privacy throughout its development life cycle.''

Privacy Control Assessment - ISACA, section 1: ''A Privacy Control Assessment (PCA) is an independent evaluation performed by a qualified assessor to determine whether an entity's controls are suitably designed and operating effectively to meet its objectives related to protecting personal information.''

Privacy by Design: The New Competitive Advantage - ISACA, section 2: ''Privacy by design is a proactive approach to embedding privacy into the design specifications of various technologies, business practices and networked infrastructure.''

Question 5

Question Type: MultipleChoice

When capturing browsing and purchase data from consumers visiting a corporate website more than once, which of the following metadata-based technologies is typically used to identify a consumer?

Options:

A- Supercookie
B- HTTP cookie
C- Server cookie
D- Flash cookie

Answer:

B

Explanation:

HTTP cookies are the standard mechanism used by websites to recognize returning visitors by storing a small piece of metadata on the user's browser. Flash cookies (D) and supercookies (A) exist but are not as common or compliant. Server cookies (C) are not a distinct browser-side identifier. The CDPSE emphasizes cookies as central to tracking, profiling, and consent requirements.

''Cookies... small data stored on a browser to recognize repeat visits and enable tracking.''

Question 6

Question Type: MultipleChoice

Which data warehousing operating model masks data within a larger database to provide subset views to users?

Options:

A- Mandatory access control
B- Context-aware access control
C- Hierarchy-based user classification
D- Least privilege access control

Answer:

A

Question 7

Question Type: MultipleChoice

The MOST effective way to incorporate privacy by design principles into applications is to include privacy requirements in.

Options:

A- senior management approvals.
B- secure coding practices
C- software development practices.
D- software testing guidelines.

Answer:

C

Explanation:

The most effective way to incorporate privacy by design principles into applications is to include privacy requirements in software development practices, because this ensures that privacy is considered and integrated from the early stages of the design process and throughout the entire lifecycle of the application. Software development practices include activities such as defining the scope, objectives, and specifications of the application, identifying and analyzing the privacy risks and impacts, selecting and implementing the appropriate privacy-enhancing technologies and controls, testing and validating the privacy functionality and performance, and monitoring and reviewing the privacy compliance and effectiveness of the application. By including privacy requirements in software development practices, the organization can achieve a proactive, preventive, and embedded approach to privacy that aligns with the privacy by design principles.

CDPSE Review Manual, 2023 Edition, Domain 2: Privacy Architecture, Section 2.1.2: Privacy Requirements, p. 75

CDPSE Review Manual, 2023 Edition, Domain 2: Privacy Architecture, Section 2.2.1: Privacy by Design Methodology, p. 79-80

The 7 Principles of Privacy by Design | Blog | OneTrust1

Question 8

Question Type: MultipleChoice

Which option best protocols BEST protects end-to-end communication of personal data?

Options:

A- Transmission Control Protocol (TCP)
B- Transport Layer Security Protocol (TLS)

C- Secure File Transfer Protocol (SFTP)
D- Hypertext Transfer Protocol (HTTP)

Answer:

B

Explanation:

Transport Layer Security Protocol (TLS) is a cryptographic protocol that provides end-to-end communication security between two parties over a network, such as the internet. TLS protects the confidentiality, integrity and authenticity of the data exchanged between the parties, such as personal data, by using encryption, hashing and digital signatures. TLS is the best protocol to protect end-to-end communication of personal data, as it prevents unauthorized access, modification or tampering of the data by third parties or intermediaries. The other options are not as effective as TLS in protecting end-to-end communication of personal data. Transmission Control Protocol (TCP) is a network protocol that provides reliable and ordered delivery of data packets between two parties over a network, but it does not provide any security or encryption of the data. Secure File Transfer Protocol (SFTP) is a network protocol that provides secure and encrypted file transfer between two parties over a network, but it does not provide end-to-end communication security for other types of data or messages.Hypertext Transfer Protocol (HTTP) is a network protocol that defines how data is formatted and transmitted over the web, but it does not provide any security or encryption of the data1, p.90-91Reference:1: CDPSE Review Manual (Digital Version)

Question 9

Question Type: MultipleChoice

Which of the following should be done FIRST when performing a data quality assessment?

Options:

A- Identify the data owner.
B- Define data quality rules.
C- Establish business thresholds-
D- Assess completeness of the data inventory.

Answer:

D

Explanation:

The first step when performing a data quality assessment is to assess the completeness of the data inventory, which is a comprehensive list of all data assets within the organization. This will help identify the scope, sources, owners, and characteristics of the data to be assessed. The other options are possible actions that may be taken after the data inventory is complete, depending on the objectives and criteria of the assessment.

CDPSE Exam Content Outline, Domain 3 -- Data Lifecycle (Data Quality), Task 1: Perform a data quality assessment1.

CDPSE Review Manual, Chapter 3 -- Data Lifecycle, Section 3.2 -- Data Quality2.

Question 10

Question Type: MultipleChoice

An organization is considering whether to expand its operations into additional international jurisdictions. After performing a privacy risk assessment, the organization decides not to begin operating in those jurisdictions. Which option best BEST describes this type of risk response?

Options:

A- Risk avoidance
B- Risk reduction
C- Risk acceptance
D- Risk mitigation

Answer:

A

Explanation:

CDPSE/ISACA risk response taxonomy defines risk avoidance as deciding not to engage in the activity that gives rise to the risk. Reduction/mitigation (B/D) means proceed with controls; acceptance (C) means proceed without additional treatment. Not expanding is classic avoidance.

Key CDPSE-aligned phrasing (short extract): ''Risk avoidance: Discontinue or do not initiate

activities that create risk.''

Question 11

Question Type: MultipleChoice

An organization has a policy requiring the encryption of personal data if transmitted through email. Which of the following is the BEST control to ensure the effectiveness of this policy?

Options:

A- Provide periodic user awareness training on data encryption.
B- Implement a data loss prevention (DLP) tool.
C- Conduct regular control self-assessments (CSAs).
D- Enforce annual attestation to policy compliance.

Answer:

B

Explanation:

A data loss prevention (DLP) tool is a software solution that monitors, detects and prevents the unauthorized transmission or leakage of sensitive data, such as personal data, from an organization's network or devices. A DLP tool can help to ensure the effectiveness of a policy requiring the encryption of personal data if transmitted through email, by applying the following controls:

Scanning the content and attachments of outgoing emails for personal data, such as names, email addresses, biometric data, IP addresses, etc.

Blocking or quarantining emails that contain unencrypted personal data, and alerting the sender and/or the administrator of the policy violation.

Encrypting personal data automatically before sending them through email, using encryption standards and algorithms that are compliant with data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).

Generating audit logs and reports of email activities and incidents involving personal data, and providing visibility and accountability for policy compliance.

The other options are less effective or irrelevant to ensure the effectiveness of the policy.

Providing periodic user awareness training on data encryption is a good practice, but it does not guarantee that users will follow the policy or know how to encrypt personal data properly. Conducting regular control self-assessments (CSAs) is a useful method to evaluate the design and operation of the policy, but it does not prevent or detect policy violations in real time. Enforcing annual attestation to policy compliance is a formal way to demonstrate user commitment to the policy, but it does not verify or measure the actual level of compliance.

The Complexity Conundrum: Simplifying Data Security - ISACA, section 3: ''Data loss prevention (DLP) solutions can help prevent unauthorized access to sensitive information by monitoring network traffic for specific keywords or patterns.''

Guide to Securing Personal Data in Electronic Medium, section 3.2: ''Organisations should consider implementing DLP solutions to prevent unauthorised disclosure of personal data via email.''

Encryption in the Hands of End Users - ISACA, section 2: ''A key goal of encryption is to protect the file even when direct access is possible or the transfer is intercepted.''