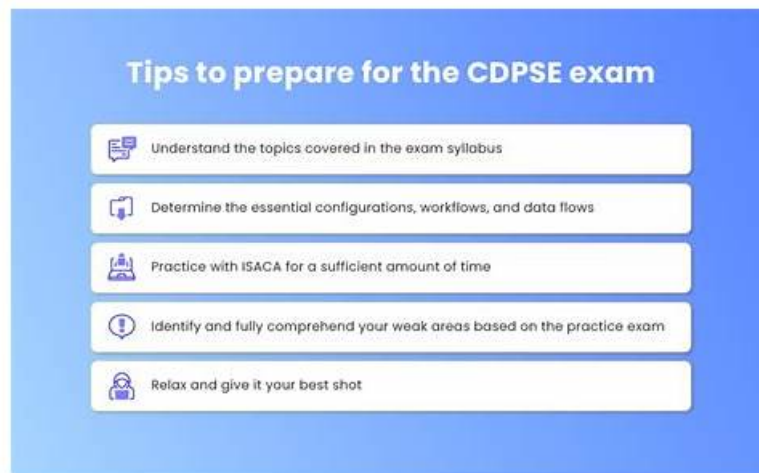


ISACA CDPSE Reliable Test Tips | Reliable CDPSE Exam Cost



DOWNLOAD the newest Getcertkey CDPSE PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1V3pD_27Ufn3B74gFkYGNjOSDtXWMmsij

If you prefer to practice CDPSE questions and answers on paper, then our CDPSE exam dumps are your best choice. CDPSE PDF version is printable, and you can print them into a hard one and take notes on them, and you can take them with you. CDPSE exam bootcamp offers you free demo for you to have a try before buying, so that you can have a better understanding of what you are going to buy. CDPSE Exam Materials contain both questions and answers, and you can have a convenient check after practicing.

Professionals interested in taking the CDPSE exam must have at least five years of experience in data privacy or related fields. A combination of education and experience may also be considered. In addition to meeting the eligibility requirements, candidates must also adhere to ISACA's Code of Professional Ethics and Continuing Professional Education (CPE) policy. This ensures that they are committed to upholding the highest ethical standards and staying up-to-date with the latest developments in the field.

The world is becoming increasingly digital, with advancements in technology transforming the way we live and work. As we continue to rely on technology for daily tasks, there is a growing concern for the privacy and security of personal data. This is where the ISACA CDPSE Certification comes in, providing individuals with the knowledge and skills necessary to implement data privacy solutions in their organizations.

>> ISACA CDPSE Reliable Test Tips <<

CDPSE Reliable Test Tips & Leading Offer in Qualification Exams & Reliable CDPSE Exam Cost

We all know that the importance of the Certified Data Privacy Solutions Engineer (CDPSE) certification exam has increased. Many people remain unsuccessful in its CDPSE exam because of using invalid CDPSE Practice Test material. If you want to avoid failure and loss of money and time, download actual CDPSE Questions of Getcertkey.

ISACA Certified Data Privacy Solutions Engineer Sample Questions (Q198-Q203):

NEW QUESTION # 198

Which of the following provides the BEST assurance that a potential vendor is able to comply with privacy regulations and the organization's data privacy policy?

- A. Obtaining self-attestations from all candidate vendors
- **B. Conducting a risk assessment of all candidate vendors**
- C. Requiring candidate vendors to provide documentation of privacy processes

- D. Including mandatory compliance language in the request for proposal (RFP)

Answer: B

Explanation:

Conducting a risk assessment of all candidate vendors is the best way to provide assurance that a potential vendor is able to comply with privacy regulations and the organization's data privacy policy, because it allows the organization to evaluate the vendor's privacy practices, controls, and performance against a set of criteria and standards. A risk assessment can also help to identify any gaps, weaknesses, or threats that may pose a risk to the organization's data privacy objectives and obligations. A risk assessment can be based on various sources of information, such as self-attestations, documentation, audits, or independent verification. A risk assessment can also help to prioritize the vendors based on their level of risk and impact, and to determine the appropriate mitigation or monitoring actions.

Reference:

8 Steps to Manage Vendor Data Privacy Compliance, DocuSign
Supplier Security and Privacy Assurance (SSPA) program, Microsoft Learn

NEW QUESTION # 199

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 of the following BEST describes this type of risk response?

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

Answer: D

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."

NEW QUESTION # 200

Which of the following is the BEST way to address threats to mobile device privacy when using beacons as a tracking technology?

- **A. Disable Bluetooth services.**
- B. Disable location services.
- C. Enable antivirus for mobile devices.
- D. Enable Trojan scanners.

Answer: A

Explanation:

Beacons use Bluetooth low-energy (BLE) wireless technology to transmit information to nearby devices that have Bluetooth enabled. By disabling Bluetooth services on the mobile device, the user can prevent beacons from detecting and tracking their location and sending them unwanted messages or advertisements. This can help protect the user's privacy and avoid potential security risks from malicious beacons. Disabling location services, enabling Trojan scanners, or enabling antivirus for mobile devices are not effective ways to address threats to mobile device privacy when using beacons as a tracking technology, because they do not prevent the communication between beacons and the mobile device.

Reference:

Beacon Technology: What It Is and How It Impacts You1
What Does It All Mean: Beacon Technology, GPS and Geofencing2

NEW QUESTION # 201

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?

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

Answer: D

Explanation:

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.

References:

- * 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."

NEW QUESTION # 202

Which of the following is a PRIMARY element of application and software hardening?

- **A. Code review**
- B. Software repository
- C. Vulnerability analysis
- D. Database configuration

Answer: A

Explanation:

Code review is a primary element of application and software hardening. Code review is a process of examining the source code of an application or software to identify and fix errors, vulnerabilities, or inefficiencies that may compromise its functionality, security, or performance. Code review can help prevent common security risks such as buffer overflows, SQL injections, cross-site scripting, or logic flaws. Code review can also help improve the quality, readability, maintainability, and usability of the code. Code review can be done manually by developers or peers, or automatically by tools such as static code analyzers or code quality checkers.

Vulnerability analysis, database configuration, and software repository are also important for application and software hardening, but they are not primary elements. Vulnerability analysis is a process of identifying and assessing the weaknesses or flaws in an application or software that may expose it to attacks or exploitation. Vulnerability analysis can be done by tools such as vulnerability scanners or penetration testers. Database configuration is a process of setting up and managing the parameters, options, or features of a database system that stores or processes data for an application or software. Database configuration can include aspects such as access control, encryption, backup, recovery, performance tuning, or replication. Software repository is a location where the source code, binaries, or documentation of an application or software are stored and managed. Software repository can facilitate version control, collaboration, distribution, or deployment of the application or software.

• • • • •

Reliable CDPSE Exam Cost: https://www.getcertkey.com/CDPSE_braindumps.html

- What's more, part of that Getcertkey CDPSE dumps now are free: https://drive.google.com/open?id=1V3pD_27Ufm3B74gFkYGNjOSDtXWMmsij

id=1V3pD_27Ufm3B74gFkYGNjOSDtXWMmsj