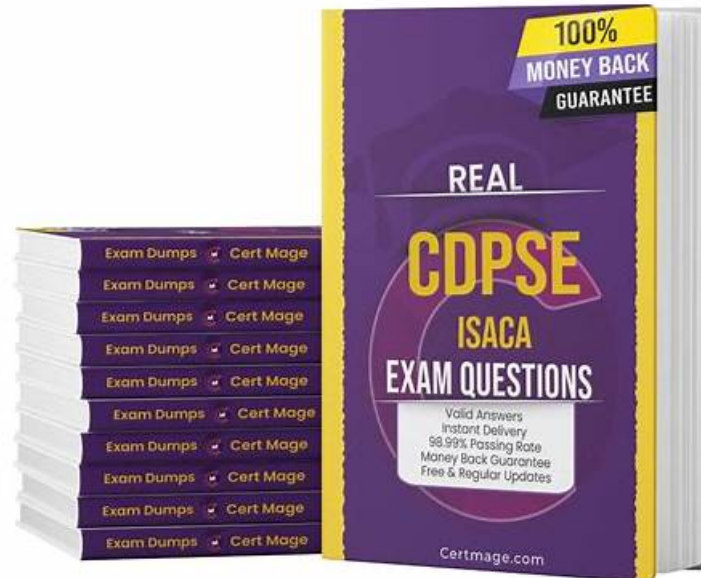


# CDPSE Exam Bootcamp, Examcollection CDPSE Free Dumps



P.S. Free 2026 ISACA CDPSE dumps are available on Google Drive shared by TestKingIT: [https://drive.google.com/open?id=1Gms\\_rsYBp9h6LVajLdFKw\\_YyYLcndaLc](https://drive.google.com/open?id=1Gms_rsYBp9h6LVajLdFKw_YyYLcndaLc)

As a top selling product in the market, our CDPSE study materials have many fans. They are keen to try our newest version products even if they have passed the CDPSE exam. They never give up learning new things. Every time they try our new version of the CDPSE Study Materials, they will write down their feelings and guidance. Also, they will exchange ideas with other customers. They give our CDPSE study materials strong support. So we are deeply moved by their persistence and trust.

ISACA CDPSE certification exam covers a wide range of topics related to data privacy solutions engineering. These topics include data privacy governance, data privacy program management, data privacy assessment, and data privacy solutions design and implementation. CDPSE Exam also covers the legal and regulatory requirements for data privacy and the impact of emerging technologies on data privacy.

>> CDPSE Exam Bootcamp <<

## Examcollection CDPSE Free Dumps | CDPSE Free Test Questions

The online version is open to any electronic equipment, at the same time, the online version of our CDPSE study materials can also be used in an offline state. You just need to use the online version at the first time when you are in an online state; you can have the right to use the version of our CDPSE Study Materials offline. And if you are willing to take our CDPSE study materials into more consideration, it must be very easy for you to pass your CDPSE exam in a short time.

ISACA CDPSE (Certified Data Privacy Solutions Engineer) exam is aimed at professionals who work in the field of data privacy and protection. Certified Data Privacy Solutions Engineer certification is designed to equip professionals with the knowledge and skills needed to effectively manage and protect sensitive data. The CDPSE Exam is a rigorous test of a candidate's ability to implement data privacy solutions, manage data access and control, and develop and implement privacy policies and procedures.

## ISACA Certified Data Privacy Solutions Engineer Sample Questions (Q167-Q172):

### NEW QUESTION # 167

Which of the following vulnerabilities would have the GREATEST impact on the privacy of information?

- A. Lack of password complexity
- B. Poor patch management
- C. Out-of-date antivirus signatures
- D. Private key exposure

**Answer: A**

### NEW QUESTION # 168

Which of the following is the BEST way to protect the privacy of data stored on a laptop in case of loss or theft?

- A. Remote wipe
- B. Endpoint encryption
- C. Strong authentication controls
- D. Regular backups

**Answer: B**

Explanation:

Endpoint encryption is a security practice that transforms the data stored on a laptop or other device into an unreadable format using a secret key or algorithm. Endpoint encryption protects the privacy of data in case of loss or theft, by ensuring that only authorized parties can access and use the data, while unauthorized parties cannot decipher or modify the data without the key or algorithm. Endpoint encryption also helps to comply with data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), which require data controllers and processors to implement appropriate technical and organizational measures to safeguard personal data.

The other options are less effective or irrelevant for protecting the privacy of data stored on a laptop in case of loss or theft. Strong authentication controls, such as passwords, biometrics or multifactor authentication, are important for verifying the identity and access rights of users, but they do not protect the data from being accessed by bypassing or breaking the authentication mechanisms. Remote wipe is a feature that allows users or administrators to erase the data on a lost or stolen device remotely, but it depends on the availability of network connection and device power, and it may not prevent data recovery by sophisticated tools. Regular backups are a process of creating copies of data for recovery purposes, such as in case of data loss or corruption, but they do not protect the data from being accessed by unauthorized parties who may obtain the backup media or files.

Reference:

An Ethical Approach to Data Privacy Protection - ISACA, section 2: "Encryption is one of the most effective security controls available to enterprises, but it can be challenging to deploy and maintain across a complex enterprise landscape." How to Protect and Secure Your Data in 10 Ways - TechRepublic, section 1: "Encrypt your hard drive Most work laptops use BitLocker to encrypt local files. That way, if the computer is stolen or hacked, the data it contains will be useless to the malicious actor."

10 Tips to Protect Your Files on PC and Cloud - microsoft.com, section 1: "Encrypt your hard drive Most work laptops use BitLocker to encrypt local files. That way, if the computer is stolen or hacked, the data it contains will be useless to the malicious actor."

11 practical ways to keep your IT systems safe and secure | ICO, section 1: "Use strong passwords and multi-factor authentication Make sure you use strong passwords on smartphones, laptops, tablets, email accounts and any other devices or accounts where personal information is stored."

### NEW QUESTION # 169

A software development organization with remote personnel has implemented a third-party virtualized workspace to allow the teams to collaborate. Which of the following should be of GREATEST concern?

- A. The third-party workspace is hosted in a highly regulated jurisdiction.
- B. There is a lack of privacy awareness and training among remote personnel.
- C. Personal data could potentially be exfiltrated through the virtual workspace.
- D. The organization's products are classified as intellectual property.

**Answer: C**

Explanation:

Explanation

The answer is B. Personal data could potentially be exfiltrated through the virtual workspace.

A comprehensive explanation is:

A virtualized workspace is a cloud-based service that provides remote access to a desktop environment, applications, and data. A virtualized workspace can enable software development teams to collaborate and work efficiently across different locations and devices. However, a virtualized workspace also poses significant privacy risks, especially when it is implemented by a third-party provider.

One of the greatest privacy concerns of using a third-party virtualized workspace is the potential for personal data to be exfiltrated through the virtual workspace. Personal data is any information that relates to an identified or identifiable individual, such as name, email, address, phone number, etc. Personal data can be collected, stored, processed, or transmitted by the software development organization or its clients, partners, or users. Personal data can also be generated or inferred by the software development activities or products.

Personal data can be exfiltrated through the virtual workspace by various means, such as:

**Data breaches:** A data breach is an unauthorized or unlawful access to or disclosure of personal data. A data breach can occur due to weak security measures, misconfiguration errors, human errors, malicious attacks, or insider threats. A data breach can expose personal data to hackers, competitors, regulators, or other parties who may use it for harmful purposes.

**Data leakage:** Data leakage is an unintentional or accidental transfer of personal data outside the intended boundaries of the organization or the virtual workspace. Data leakage can occur due to improper disposal of devices or media, insecure network connections, unencrypted data transfers, unauthorized file sharing, or careless user behavior. Data leakage can compromise personal data to third parties who may not have adequate privacy policies or practices.

**Data mining:** Data mining is the analysis of large and complex data sets to discover patterns, trends, or insights. Data mining can be performed by the third-party provider of the virtual workspace or by other authorized or unauthorized parties who have access to the virtual workspace. Data mining can reveal personal data that was not explicitly provided or intended by the organization or the individuals.

The exfiltration of personal data through the virtual workspace can have serious consequences for the software development organization and its stakeholders. It can result in:

**Legal liability:** The organization may face legal actions or penalties for violating the privacy laws, regulations, standards, or contracts that apply to the personal data in each jurisdiction where it operates or serves. For example, the General Data Protection Regulation (GDPR) in the European Union imposes strict obligations and sanctions for protecting personal data across borders.

**Reputational damage:** The organization may lose trust and credibility among its clients, partners, users, employees, investors, or regulators for failing to safeguard personal data. This can affect its brand image, customer loyalty, market share, revenue, or growth potential.

**Competitive disadvantage:** The organization may lose its competitive edge or intellectual property if its personal data is stolen or misused by its rivals or adversaries. This can affect its innovation capability, product quality, or market differentiation.

Therefore, it is essential for the software development organization to implement appropriate measures and controls to prevent or mitigate the exfiltration of personal data through the virtual workspace. Some of these measures and controls are:

**Data minimization:** The organization should collect and process only the minimum amount and type of personal data that is necessary and relevant for its legitimate purposes. It should also delete or anonymize personal data when it is no longer needed or required.

**Data encryption:** The organization should encrypt personal data at rest and in transit using strong and standardized algorithms and keys. It should also ensure that only authorized parties have access to the keys and that they are stored securely.

**Data segmentation:** The organization should segregate personal data into different categories based on their sensitivity and risk level. It should also apply different levels of protection and access control to each category of personal data.

**Data governance:** The organization should establish a clear and comprehensive policy and framework for managing personal data throughout its lifecycle. It should also assign roles and responsibilities for implementing and enforcing the policy and framework.

**Data audit:** The organization should monitor and review the activities and events related to personal data on a regular basis. It should also conduct periodic assessments and tests to evaluate the effectiveness and compliance of its privacy measures and controls.

**Data awareness:** The organization should educate and train its staff and users on the importance and best practices of protecting personal data. It should also communicate and inform its clients, partners, and regulators about its privacy policies and practices.

The other options are not as great of a concern as option B.

The third-party workspace being hosted in a highly regulated jurisdiction (A) may pose some challenges for complying with different privacy laws and regulations across borders. However it may also offer some benefits such as higher standards of privacy protection and enforcement.

The organization's products being classified as intellectual property may increase the value and attractiveness of the personal data related to the products, but it does not necessarily increase the risk of exfiltration of the personal data through the virtual workspace.

The lack of privacy awareness and training among remote personnel (D) may increase the likelihood of human errors or negligence that could lead to exfiltration of personal data through the virtual workspace. However it is not a direct cause or source of exfiltration, and it can be addressed by providing adequate education and training.

References:

8 Risks of Virtualization: Virtualization Security Issues<sup>1</sup>

Security & Privacy Risks of the Hybrid Work Environment<sup>2</sup>

The Risk of Virtualization - Concerns and Controls<sup>3</sup>

What is Virtualized Security?<sup>4</sup>

### NEW QUESTION # 170

An online retail company is trying to determine how to handle users' data if they unsubscribe from marketing emails generated from the website. Which of the following is the BEST approach for handling personal data that has been restricted?

- A. Flag users' email addresses to make sure they do not receive promotional information.
- B. Reference the privacy policy to see if the data is truly restricted.
- C. Encrypt users' information so it is inaccessible to the marketing department.
- D. Remove users' information and account from the system.

**Answer: A**

### NEW QUESTION # 171

An organization's data destruction guidelines should require hard drives containing personal data to go through which of the following processes prior to being crushed?

- A. Remote partitioning
- B. Hammer strike
- C. Low-level formatting
- D. Degaussing

**Answer: D**

Explanation:

Explanation

Degaussing is a hard drive sanitation method that uses a powerful magnetic field to erase or destroy the data stored on a magnetic disk or tape. Degaussing should be used to sanitize hard drives containing personal data prior to being crushed, as it provides an additional layer of assurance that data has been permanently erased and cannot be recovered by any means. Degaussing also damages the drive itself, making it unusable for future storage. The other options are not effective or necessary hard drive sanitation methods prior to being crushed.

Low-level formatting is a hard drive sanitation method that erases the data and the partition table on the drive, but it may leave some traces of data that can be recovered by forensic tools or software. Remote partitioning is a hard drive sanitation method that creates separate logical sections on the drive, but it does not erase or destroy the data on the drive. Hammer strike is a hard drive sanitation method that physically damages the drive by hitting it with a hammer, but it may not erase or destroy the data completely or prevent data recovery by advanced tools or techniques1, p. 93-94 References: 1: CDPSE Review Manual (Digital Version)

### NEW QUESTION # 172

.....

**Examcollection CDPSE Free Dumps:** <https://www.testkingit.com/ISACA/latest-CDPSE-exam-dumps.html>

- Reliable CDPSE Test Testking ☐ Reliable CDPSE Test Testking ☐ CDPSE Visual Cert Test ☐ Enter ➡ [www.testkingpass.com](http://www.testkingpass.com) ☐ and search for ☐ CDPSE ☐ to download for free ☐ Reliable CDPSE Test Testking
- Latest ISACA CDPSE Questions – Key To Success In First Try ☐ Download ☐ CDPSE ☐ for free by simply searching on > [www.pdfvce.com](http://www.pdfvce.com) < ☐ CDPSE Exam Actual Questions
- Reliable CDPSE Test Testking ☐ CDPSE Latest Cram Materials ☐ CDPSE Latest Cram Materials ☐ Open ➡ [www.exam4labs.com](http://www.exam4labs.com) ☐ enter **【 CDPSE 】** and obtain a free download ☐ Reliable CDPSE Test Testking
- Correct CDPSE Exam Bootcamp - Leader in Qualification Exams - Trustable CDPSE: Certified Data Privacy Solutions Engineer ☐ Search for 《 CDPSE 》 and easily obtain a free download on ☐ [www.pdfvce.com](http://www.pdfvce.com) ☐ ☐ CDPSE Certification Test Answers
- Valid CDPSE Test Materials ☐ CDPSE Valid Test Registration ☐ Reliable CDPSE Exam Book ☐ Download ➡ CDPSE ☐ for free by simply searching on ➡ [www.prepawayexam.com](http://www.prepawayexam.com) ☐ ☐ CDPSE Test Labs
- 2026 ISACA Authoritative CDPSE Exam Bootcamp ☐ Go to website ➡ [www.pdfvce.com](http://www.pdfvce.com) ☐ ☐ ☐ open and search for ⇒ CDPSE ⇐ to download for free ☐ New CDPSE Exam Question
- ISACA - CDPSE - Efficient Certified Data Privacy Solutions Engineer Exam Bootcamp ☐ Immediately open > [www.exam4labs.com](http://www.exam4labs.com) < and search for 《 CDPSE 》 to obtain a free download ☐ CDPSE Valid Test Registration
- New CDPSE Exam Question ☐ Reliable CDPSE Test Testking ☐ CDPSE Question Explanations ☐ Search for “ CDPSE ” and download it for free on ☐ [www.pdfvce.com](http://www.pdfvce.com) ☐ website ☐ CDPSE New Braindumps Questions

- What's more, part of that TestKingIT CDPSE dumps now are free: [https://drive.google.com/open?id=1Gms\\_rsYBp9h6LVajLdFKw\\_YyYLcndaLc](https://drive.google.com/open?id=1Gms_rsYBp9h6LVajLdFKw_YyYLcndaLc)

What's more, part of that TestKingIT CDPSE dumps now are free: [https://drive.google.com/open?id=1Gms\\_rsYBp9h6LVajLdFKw\\_YyYLcndaLc](https://drive.google.com/open?id=1Gms_rsYBp9h6LVajLdFKw_YyYLcndaLc)