Pass2Lead

https://Pass2Lead.com

CIPT^{Q&As}

Certified Information Privacy Technologist (CIPT)

Pass IAPP CIPT Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/cipt.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

Which of the following would be the best method of ensuring that Information Technology projects follow Privacy by Design (PbD) principles?

A. Develop a technical privacy framework that integrates with the development lifecycle.

B. Utilize Privacy Enhancing Technologies (PETs) as a part of product risk assessment and management.

C. Identify the privacy requirements as a part of the Privacy Impact Assessment (PIA) process during development and evaluation stages.

D. Develop training programs that aid the developers in understanding how to turn privacy requirements into actionable code and design level specifications.

Correct Answer: D

QUESTION 2

Which of the following is a stage in the data life cycle?

A. Data classification.

B. Data inventory.

C. Data masking.

D. Data retention.

Correct Answer: D

The stages in a typical data lifecycle include creation/collection, processing, storage/retention, usage/access/sharing/distribution, archival/preservation and destruction/deletion/disposition 3. Among these options provided here only "Data retention" is a stage in this cycle.

QUESTION 3

You are a wine collector who uses the web to do research about your hobby. You navigate to a news site and an ad for wine pops up. What kind of advertising is this?

A. Remnant.

B. Behavioral.

C. Contextual.

D. Demographic.

Correct Answer: B

Reference: https://neilpatel.com/blog/behavioral-advertising/

QUESTION 4

What is a mistake organizations make when establishing privacy settings during the development of applications?

A. Providing a user with too many choices.

B. Failing to use "Do Not Track" technology.

C. Providing a user with too much third-party information.

D. Failing to get explicit consent from a user on the use of cookies.

Correct Answer: D

Failing to get explicit consent from a user on the use of cookies is a mistake organizations make when establishing privacy settings during the development of applications2. Cookies are small files that store information about users\\' preferences and behavior on websites2 . They can be used for various purposes such as authentication, personalization, analytics, advertising etc.2 However, they can also pose privacy risks as they may collect sensitive or personal information without users\\' knowledge or consent2. Therefore, organizations should inform users about how they use cookies and obtain their explicit consent before placing cookies on their devices2. This is also required by some laws such as EU\\'s General Data Protection Regulation (GDPR) and ePrivacy Directive2. The other options are not mistakes organizations make when establishing privacy settings during the development of applications.

QUESTION 5

SCENARIO

It should be the most secure location housing data in all of Europe, if not the world. The Global Finance Data Collective (GFDC) stores financial information and other types of client data from large banks, insurance companies, multinational corporations and governmental agencies. After a long climb on a mountain road that leads only to the facility, you arrive at the security booth. Your credentials are checked and checked again by the guard to visually verify that you are the person pictured on your passport and national identification card. You are led down a long corridor with server rooms on each side, secured by combination locks built into the doors. You climb a flight of stairs and are led into an office that is lighted brilliantly by skylights where the GFDC Director of Security, Dr. Monique Batch, greets you. On the far wall you notice a bank of video screens showing different rooms in the facility. At the far end, several screens show different sections of the road up the mountain

Dr. Batch explains once again your mission. As a data security auditor and consultant, it is a dream assignment: The GFDC does not want simply adequate controls, but the best and most effective security that current technologies allow.

"We were hacked twice last year," Dr. Batch says, "and although only a small number of records were stolen, the bad press impacted our business. Our clients count on us to provide security that is nothing short of impenetrable and to do so quietly. We hope to never make the news again." She notes that it is also essential that the facility is in compliance with all relevant security regulations and standards.

You have been asked to verify compliance as well as to evaluate all current security controls and security measures, including data encryption methods, authentication controls and the safest methods for transferring data into and out of the facility. As you prepare to begin your analysis, you find yourself considering an intriguing question: Can these people be sure that I am who I say I am?

You are shown to the office made available to you and are provided with system login information, including the name of the wireless network and a wireless key. Still pondering, you attempt to pull up the facility\\'s wireless network, but no networks appear in the wireless list. When you search for the wireless network by name, however it is readily found.

![Pass2Lead](https://Pass2Lead.com)
Why would you recommend that GFC use record encryption rather than disk, file or table encryption?

A. Record encryption is asymmetric, a stronger control measure.

B. Record encryption is granular, limiting the damage of potential breaches.

C. Record encryption involves tag masking, so its metadata cannot be decrypted

D. Record encryption allows for encryption of personal data only.

Correct Answer: B

Record encryption is granular, limiting the damage of potential breaches. Record encryption encrypts data at the record level, providing a more granular level of protection than disk, file or table encryption. This means that even if a breach were to occur, only the specific records that were accessed would be compromised.

[CIPT Study Guide](#)   [CIPT Exam Questions](#)   [CIPT Braindumps](#)