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.certbus.com/cipt.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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.

What measures can protect client information stored at GFDC?

A. De-linking of data into client-specific packets.

B. Cloud-based applications.

C. Server-side controls.

D. Data pruning

Correct Answer: A

QUESTION 2

What has been identified as a significant privacy concern with chatbots?

A. Most chatbot providers do not agree to code audits

B. Chatbots can easily verify the identity of the contact.

C. Users\\' conversations with chatbots are not encrypted in transit.

D. Chatbot technology providers may be able to read chatbot conversations with users.

Correct Answer: D

Reference: https://resources.infosecinstitute.com/privacy-concerns-emotional-chatbots/

QUESTION 3

What would be an example of an organization transferring the risks associated with a data breach?

A. Using a third-party service to process credit card transactions.

B. Encrypting sensitive personal data during collection and storage

C. Purchasing insurance to cover the organization in case of a breach.

D. Applying industry standard data handling practices to the organization\\' practices.

Correct Answer: C

Reference: http://www.hpso.com/Documents/pdfs/newsletters/firm09-rehabv1.pdf

Purchasing insurance to cover the organization in case of a breach. By purchasing insurance, the organization can transfer the financial risks associated with a data breach to an insurance provider. This is a risk management strategy that can help an organization mitigate the financial impact of a breach.

Transferring risk means shifting some or all of the potential losses or liabilities associated with a risk to another party2. Purchasing insurance is one way of transferring risk, as it allows the organization to share the financial burden of a data breach with an insurer. The other options do not involve transferring risk, but rather reducing, avoiding or accepting it.

QUESTION 4

Granting data subjects the right to have data corrected, amended, or deleted describes?

A. Use limitation.

B. Accountability.

C. A security safeguard

D. Individual participation

Correct Answer: D

Reference: https://www.ncbi.nlm.nih.gov/books/NBK236546/

Granting data subjects the right to have data corrected, amended, or deleted describes individual participation1. As explained above, the individual participation principle gives individuals certain rights over their personal data held by a data controller1. One of these rights is to challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed or amended1. The other options are not principles that describe granting data subjects this right.

QUESTION 5

Which is likely to reduce the types of access controls needed within an organization?

A. Decentralization of data.

B. Regular data inventories.

C. Standardization of technology.

D. Increased number of remote employees.

Correct Answer: C

QUESTION 6

An organization is considering launching enhancements to improve security and authentication mechanisms in their products. To better identify the user and reduce friction from the authentication process, they plan to track physical attributes of an individual. A privacy technologist assessing privacy implications would be most interested in which of the following?

A. The purpose of the data tracking.

B. That the individual is aware tracking is occurring.

C. The authentication mechanism proposed.

D. The encryption of individual physical attributes.

Correct Answer: A

a privacy technologist assessing privacy implications would be most interested in the purpose of the data tracking.

QUESTION 7

An organization is deciding between building a solution in-house versus purchasing a solution for a new customer facing application. When security threat are taken into consideration, a key advantage of purchasing a solution would be the availability of?

A. Outsourcing.

B. Persistent VPN.

C. Patching and updates.

D. Digital Rights Management.

Correct Answer: C

when security threats are taken into consideration, a key advantage of purchasing a solution would be the availability of patching and updates.

QUESTION 8

In terms of data extraction, which of the following should NOT be considered by a privacy technologist in relation to data portability?

A. The size of the data.

B. The format of the data.

C. The range of the data.

D. The medium of the data.

Correct Answer: D

The medium of the data. Data portability refers to an individual\\'s right to receive their personal data in a structured and commonly used format so that they can transfer it to another service provider. The size (A), format (B), and range ?of the data are all relevant considerations when extracting data for portability purposes. However, the medium of the data is not relevant in this context.

QUESTION 9

When deploying a consumer gadget that incorporates speech recognition, where is the speech generally best processed, from a privacy by design perspective?

A. Within the subject\\'s jurisdiction

B. On the remote server

C. On the local device

D. In the cloud

Correct Answer: C

QUESTION 10

When should code audits be concluded?

A. At code check-in time.

B. At engineering design time.

C. While code is being sent to production.

D. Before launch after all code for a feature is complete.

Correct Answer: A

QUESTION 11

Which of the following CANNOT be effectively determined during a code audit?

A. Whether access control logic is recommended in all cases.

B. Whether data is being incorrectly shared with a third-party.

C. Whether consent is durably recorded in the case of a server crash.

D. Whether the differential privacy implementation correctly anonymizes data.

Correct Answer: D

QUESTION 12

Which of the following statements is true regarding software notifications and agreements?

A. Website visitors must view the site\\'s privacy statement before downloading software.

B. Software agreements are designed to be brief, while notifications provide more details.

C. It is a good practice to provide users with information about privacy prior to software installation.

D. "Just in time" software agreement notifications provide users with a final opportunity to modify the agreement.

Correct Answer: C

QUESTION 13

One difference between privacy threat modeling and information security threat modeling is?

A. Privacy threat modeling looks at threats to the individual while security threat modeling looks at threats to the organization.

B. Security threat modeling is required by regulations such as the HIPAA Privacy Rule, but privacy threat modeling is not.

C. Privacy threat modeling does not consider technical defects such as software vulnerabilities.

D. Privacy threat modeling must consider insider threats, but security threat modeling does not.

Correct Answer: A

QUESTION 14

How does k-anonymity help to protect privacy in micro data sets?

A. By ensuring that every record in a set is part of a group of "k" records having similar identifying information.

B. By switching values between records in order to preserve most statistics while still maintaining privacy.

C. By adding sufficient noise to the data in order to hide the impact of any one individual.

D. By top-coding all age data above a value of "k."

Correct Answer: A

Reference: https://www.researchgate.net/publication/284332229_k- Anonymity_A_Model_for_Protecting_Privacy

QUESTION 15

SCENARIO

Carol was a U.S.-based glassmaker who sold her work at art festivals. She kept things simple by only accepting cash and personal checks.

As business grew, Carol couldn\\'t keep up with demand, and traveling to festivals became burdensome. Carol opened a small boutique and hired Sam to run it while she worked in the studio. Sam was a natural salesperson, and business doubled. Carol told Sam, "I don\\'t know what you are doing, but keep doing it!"

But months later, the gift shop was in chaos. Carol realized that Sam needed help so she hired Jane, who had business expertise and could handle the back-office tasks. Sam would continue to focus on sales. Carol gave Jane a few weeks to get acquainted with the artisan craft business, and then scheduled a meeting for the three of them to discuss Jane\\'s first impressions.

At the meeting, Carol could not wait to hear Jane\\'s thoughts, but she was unprepared for what Jane had to say. "Carol, I know that he doesn\\'t realize it, but some of Sam\\'s efforts to increase sales have put you in a vulnerable position. You are not protecting customers\\' personal information like you should."

Sam said, "I am protecting our information. I keep it in the safe with our bank deposit. It\\'s only a list of customers\\' names, addresses and phone numbers that I get from their checks before I deposit them. I contact them when you finish a piece that I think they would like. That\\'s the only information I have! The only other thing I do is post photos and information about your work on the photo sharing site that I use with family and friends. I provide my email address and people send me their information if they want to see more of your work. Posting online really helps sales, Carol. In fact, the only complaint I hear is about having to come into the shop to make a purchase."

Carol replied, "Jane, that doesn\\'t sound so bad. Could you just fix things and help us to post even more online?"

`I can," said Jane. "But it\\'s not quite that simple. I need to set up a new program to make sure that we follow the best practices in data management. And I am concerned for our customers. They should be able to manage how we use their personal information. We also should develop a social media strategy."

Sam and Jane worked hard during the following year. One of the decisions they made was to contract with an outside vendor to manage online sales. At the end of the year, Carol shared some exciting news. "Sam and Jane, you have done such a great job that one of the biggest names in the glass business wants to buy us out! And Jane, they want to talk to you about merging all of our customer and vendor information with theirs beforehand."

Which regulator has jurisdiction over the shop\\'s data management practices?

A. The Federal Trade Commission.

B. The Department of Commerce.

C. The Data Protection Authority.

D. The Federal Communications Commission.

Correct Answer: C

The Data Protection Authority is a regulatory body responsible for enforcing data protection laws and ensuring that

organizations comply with their obligations to protect personal data. The Federal Trade Commission (FTC) is an independent agency of the United States government whose primary mission is to promote consumer protection and prevent anti-competitive business practices.