

CIPT

**CERTIFIED INFORMATION PRIVACY
TECHNOLOGIST**

PRACTICE EXAM QUESTIONS

SIMILAR EXAM QUESTIONS

*Are you **determined** to pass the exam?
then get the **full version** of this ebook!*



PREPARED BY CIPP/E, CISA, MSC EXPERTS
THIS IS NOT AN OFFICIAL IAPP MATERIAL

COPYRIGHT © CERTIFICATION EXAM TRAINER. ALL RIGHTS RESERVED

Introduction

Welcome to the CIPT Practice Exam Sample Book! This **sample** e-book is here to help you prepare for the Certified Information Privacy Technologist (CIPT) certification exam, which is administered by the International Association of Privacy Professionals (IAPP). Whether you're already working in privacy or just starting out, this book is designed to support you in getting ready for the exam.

The aim of this practice exam is not just to test whether you've memorized your study material, but also to assess your ability to apply it – a crucial aspect of passing the exam successfully.

Use this practice exam as a tool to gauge your understanding, identify areas of strength and weakness, and fine-tune your exam strategy. Remember, practice and application are key to success.

How to Take This Practice Exam

This e-book contains a brief subset of 11 questions from the CIPT Privacy Exam questions. The original book contains 151 questions, distributed between direct questions and 12 scenarios. The target to aim for is an 80% score, meaning you should aim to around 30 mistakes or fewer in order to be confident in your readiness for the exam. If you score 80% or higher, you can consider yourself well-prepared for exam day.

- **Gather Your Materials:** Get a piece of paper, a pencil, and a timer.
- **Set a Timer:** Set a timer for 2.5 hours and aim to resolve 90 questions (as the actual exam). This will simulate the time constraint of the actual exam.
- **Answering Questions:** Write down the number of each question and the answer you believe is correct. If you're unsure about an answer or want to review it later, mark it with a question mark. This helps you flag questions for review without wasting time.
- **Flagging for Review:** Mark the question you want to review later. This technique can be helpful during the actual exam as well.
- **Refer to Answer Key:** After completing the exam or when the timer runs out, refer to the answer key provided in this e-book to determine your score.

- **Understanding the Logic:** Take time to understand the reasoning behind each question and answer. This is crucial for learning and improving your understanding of the material.
- **Reviewing Explanations:** In the last section, explanations are provided for each question. Use these explanations to deepen your understanding of the concepts tested.

By following these steps, you'll not only assess your readiness for the exam but also enhance your knowledge and test-taking skills.

About This Book

Unlike the current practice exams available, which are often out-of-date, expensive, and too easy, this practice exam offers a more challenging and realistic experience. With brief explanations provided, you'll gain insight into question phrasing and learn how to select the best answer.

Note: This is not an official CIPT sample exam, nor does it contain real exam questions. However, it provides similar questions and degree of difficulty as the real exam.

By using this e-book alongside your regular study material, you'll not only enhance your speed and accuracy but also have ample time to review flagged questions. The variety of question types in this practice exam mirrors the actual exam, ensuring a balanced approach to testing your knowledge.

For those seeking to further test their privacy and technology skills, this book is perfect for you! This resource focuses specifically on scenario-based questions, which are often the most difficult part of the exam, providing an additional challenge to assess your understanding of Privacy and Technology.

Best of luck in your preparations!

Note: This e-book is protected by copyright law. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. Unauthorized copying, distribution, or resale of this eBook is strictly prohibited. Legal action will be taken against individuals or entities found to be in violation of these restrictions.

Table of Contents

Introduction	1
How to Take This Practice Exam.....	1
About This Book.....	2
CIPT Practice Exam Questions	4
CIPT Practice Exam Answers & Explanations	7

CIPT Practice Exam Questions

1. What is the main reason the Do Not Track (DNT) header is not acknowledged by more companies?

- A. Most web browsers incorporate the DNT feature.
- B. The financial penalties for violating DNT guidelines are too high.
- C. There is a lack of consensus about what the DNT header should mean.
- D. It has been difficult to solve the technological challenges surrounding DNT.

2. Why is first-party web tracking very difficult to prevent?

- A. The available tools to block tracking would break most sites' functionality.
- B. Consumers enjoy the many benefits they receive from targeted advertising.
- C. Regulatory frameworks are not concerned with web tracking.
- D. Most browsers do not support automatic blocking.

3. During a transport layer security (TLS) session, what happens immediately after the web browser creates a random PreMasterSecret?

- A. The server decrypts the PremasterSecret.
- B. The web browser opens a TLS connection to the PremasterSecret.
- C. The web browser encrypts the PremasterSecret with the server's public key.
- D. The server and client use the same algorithm to convert the PremasterSecret into an encryption key.

4. What is the main benefit of using a private cloud?

- A. The ability to use a backup system for personal files.
- B. The ability to outsource data support to a third party.
- C. The ability to restrict data access to employees and contractors.
- D. The ability to cut costs for storing, maintaining, and accessing data.

5. SCENARIO

Please use the following scenario to answer the following questions:

You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.

Ancillary's operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving. However, the company now sells

online through retail sites designated for industries and demographics, sites such as "My Cool Ride" for automobile-related products or "Zoomer" for gear aimed toward young adults. The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards.

Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols. You have been asked to lead three important new projects at Ancillary:

The first is the personal data management and security component of a multi-faceted initiative to unify the company's culture. For this project, you are considering using a series of third- party servers to provide company data and approved applications to employees.

The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.

Finally, you are charged with developing privacy protections for a single web store housing all the company's product lines as well as products from affiliates. This new omnibus site will be known, aptly, as "Under the Sun." The Director of Marketing wants the site not only to sell Ancillary's products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.

If you are asked to advise on privacy concerns regarding paid advertisements, which is the most important aspect to cover?

- A. Unseen web beacons that combine information on multiple users.
- B. Latent keys that trigger malware when an advertisement is selected.
- C. Personal information collected by cookies linked to the advertising network.
- D. Sensitive information from Structured Query Language (SQL) commands that may be exposed.

6. SCENARIO

What technology is under consideration in the first project in this scenario?

- A. Server driven controls.
- B. Cloud computing
- C. Data on demand
- D. MAC filtering

7. SCENARIO

Which should be used to allow the home sales force to accept payments using smartphones?

- A. Field transfer protocol.
- B. Cross-current translation.

- C. Near-field communication
 - D. Radio Frequency Identification
- 8. What is the best way to protect privacy on a geographic information system (GIS)?**
- A. Limiting the data provided to the system.
 - B. Using a wireless encryption protocol.
 - C. Scrambling location information.
 - D. Using a firewall.
- 9. In the realm of artificial intelligence, how has deep learning enabled greater implementation of machine learning?**
- A. By using hand-coded classifiers like edge detection filters so that a program can identify where an object starts and stops.
 - B. By increasing the size of neural networks and running massive amounts of data through the network to train it.
 - C. By using algorithmic approaches such as decision tree learning and inductive logic programming.
 - D. By hand coding software routines with a specific set of instructions to accomplish a task.
- 10. Which of the following is an example of the privacy risks associated with the Internet of Things (IoT)?**
- A. A group of hackers infiltrate a power grid and cause a major blackout.
 - B. An insurance company raises a person's rates based on driving habits gathered from a connected car.
 - C. A website stores a cookie on a user's hard drive so the website can recognize the user on subsequent visits.
 - D. A water district fines an individual after a meter reading reveals excess water use during drought conditions.
- 11. How can a hacker gain control of a smartphone to perform remote audio and video surveillance?**
- A. By performing cross-site scripting.
 - B. By installing a roving bug on the phone.
 - C. By manipulating geographic information systems.
 - D. By accessing a phone's global positioning system satellite signal.

Interested in more similar exam questions? Then obtain the full e-book with more than 150 similar exam questions and answers!

Our exams are reviewed and curated by certified privacy experts.

CIPT Practice Exam Answers & Explanations

1. C. There is a lack of consensus about what the DNT header should mean.

Explanation: The main reason the Do Not Track (DNT) header is not acknowledged by more companies is the lack of consensus about what it should mean and how it should be implemented. Without clear standards, companies are hesitant to adopt it.

2. A. The available tools to block tracking would break most sites' functionality.

Explanation: First-party web tracking is difficult to prevent because the tools designed to block tracking can disrupt the functionality of many websites, making them difficult to use or access.

3. C. The web browser encrypts the PreMasterSecret with the server's public key.

Explanation: In a TLS session, after the web browser creates a random PreMasterSecret, it encrypts this PreMasterSecret with the server's public key and sends it to the server.

4. C. The ability to restrict data access to employees and contractors.

Explanation: The main benefit of using a private cloud is the ability to restrict data access to employees and contractors, thereby enhancing security and control over data.

5. C. Personal information collected by cookies linked to the advertising network.

Explanation: When advising on privacy concerns regarding paid advertisements, the most important aspect to cover is the personal information collected by cookies linked to the advertising network, as this can significantly impact user privacy.

6. B. Cloud computing

Explanation: The first project involves using a series of third-party servers to provide company data and approved applications to employees, indicating the use of cloud computing.

7. C. Near-field communication

Explanation: The best technology to allow the home sales force to accept payments using smartphones is Near-field communication (NFC), which enables secure contactless transactions.

8. A. Limiting the data provided to the system.

Explanation: The best way to protect privacy on a geographic information system (GIS) is by limiting the data provided to the system, thereby minimizing the amount of potentially sensitive information that can be exposed.

9. B. By increasing the size of neural networks and running massive amounts of data through the network to train it.

Explanation: Deep learning has enabled greater implementation of machine learning by increasing the size of neural networks and running massive amounts of data through them for training, which improves the accuracy and capabilities of AI models.

10. B. An insurance company raises a person's rates based on driving habits gathered from a connected car.

Explanation: An example of the privacy risks associated with the Internet of Things (IoT) is an insurance company raising a person's rates based on driving habits gathered from a connected car. This use of personal data can have significant privacy implications.

11. B. By installing a roving bug on the phone.

Explanation: A hacker can gain control of a smartphone to perform remote audio and video surveillance by installing a roving bug on the phone, which allows the hacker to activate the device's microphone and camera without the user's knowledge.

