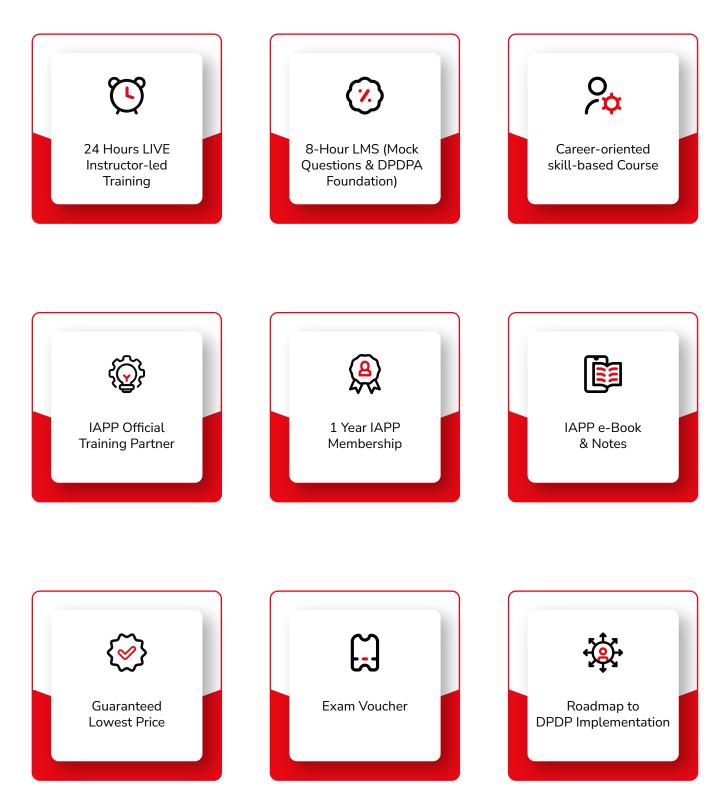# IAPP CIPM

Certification Training

Program Highlights

Certified Information Privacy Manager (CIPM) certification is developed by The **International Association of Privacy Professionals (IAPP)**. It uses a privacy program operational lifecycle, to demonstrate your comprehension and ability to use privacy and data protection practices in the construction, evaluation, and improvement of a privacy program. The CIPM program was created in response to the tremendous need for a collection and compilation of best practices for managing privacy operations. The CIPM certification training from InfosecTrain will provide you with the proper understanding of designing, building, and operating Data Privacy Management Programs.

INFOSECTRAIN

Course Highlights

24 Hours LIVE Instructor-led Training

8-Hour LMS (Mock Questions & DPDPA Foundation)

Career-oriented skill-based Course

IAPP Official Training Partner

1 Year IAPP Membership

IAPP e-Book & Notes

Guaranteed Lowest Price

Exam Voucher

Roadmap to DPDP Implementation

Target Audience

- Data Protection Officer
- Data Protection Lawyers
- IT Auditors
- Legal Compliance Officers
- Security Manager
- Information Officers
- Professionals responsible for integrating privacy requirements into day-to-day operations.

Pre-Requisites

There are no such prerequisites for CIPM certification.

Exam Information

Exam Format	Multiple Choice Questions
Number of Questions	90
Exam Duration	150 minutes
Passing Score	300 out of 500
Language	English, Chinese, French, German, Brazilian Portuguese

Course Objectives

At the end of the course, you will be able to:

- Manage, develop and implement a privacy program
- Perform data privacy and data protection assessment
- Implement privacy related policies
- Ensure data subject rights and develop and implement privacy training
- Protect personal information
- Respond to data security incident or breach
- Monitor, measure, analyze and audit performance of the privacy program

Course Content

- **Module 1: Introduction to privacy program management**
  Identifies privacy program management responsibilities and describes the role of accountability in privacy program management.
- **Module 2: Privacy governance**
  Examines considerations for developing and implementing a privacy program, including the position of the privacy function within the organization, role of the DPO, program scope and charter, privacy strategy, support and ongoing involvement of key functions and privacy frameworks.
- **Module 3: Applicable laws and regulations**
  Discusses the regulatory environment, common elements across jurisdictions and strategies for aligning compliance with organizational strategy.

Module 4: Data assessments

Relates practical processes for creating and using data inventories/maps, gap analysis, privacy assessments, privacy impact assessments/data protection impact assessments and vendor assessments.

Module 5: Policies

Describes common types of privacy-related policies, outlines components and offers strategies for implementation.

Module 6: Data subject rights

Discusses operational considerations for communicating and ensuring data subject rights, including privacy notice, choice and consent, access and rectification, data portability, and erasure.

Module 7: Training and awareness

Outlines strategies for developing and implementing privacy training and awareness programs.

Module 8: Protecting personal information

Examines a holistic approach to protecting personal information through privacy by design.

Module 9: Data breach incident plans

Provides guidance on planning for and responding to a data security incident or breach.

Module 10: Monitoring and auditing program performance

Relates common practices for monitoring, measuring, analyzing and auditing privacy program performance.

www.infosectrain.com | sales@infosectrain.com