# Certified Information Privacy Manager (CIPM) Training

Course: **00050**
Filter: **Beginner**
Duration: **20 hours**
Category:: **Gouvernance, Risk and Compliance**
Price: **1500,00 €**

## About Course

The Certified Information Privacy Manager (CIPM) course is the “how-to” of privacy training. The CIPM is the world’s first and only certification in privacy program management. This course covers implementing a privacy program framework, managing the privacy program operational lifecycle and structuring a knowledgeable, high-performing privacy team regardless of jurisdiction or industry. The Certified Information Privacy Manager (CIPM) Training is based on the body of knowledge for the IAPP’s ANSI-accredited Certified Information Privacy Professional/ U.S. (CIPM/US) certification program. The content is based on the Body of Knowledge for the globally recognized Certified Information Privacy Professional/Management (CIPM) credential.

## What you'll learn

- Create a company vision around data privacy
- Structure the privacy team
- Develop and implement a privacy program framework
- Communicate to stakeholders
- Measure performance

## Pre-requisites

- No prerequisites, but we recommend all potential test takers to read the IAPP Privacy Certification Handbook 2018 prior to attending.

## Curriculum

### Module 1: Introduction to privacy program management

- Identify privacy program management responsibilities and describes the role of accountability in privacy program management.

### Module 2: Privacy Governance

- Examine considerations for developing and implementing a privacy program, including the position of the privacy function within the organization, role of the DPO

### Module 3: Applicable laws and regulations

- Discuss the regulatory environment, common elements across jurisdictions and strategies for aligning compliance with organizational strategy

### Module 4: Data assessments

- Relate practical processes for creating and using data inventories/maps, gap analyses, privacy assessments, privacy impact assessments/data protection impact assessments and vendor assessments

### Module 5: Policies

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

### Module 6: Data subject rights

- Discuss operational considerations for communicating and ensuring data subject rights, including privacy notice, choice and consent, access and rectification, data portability, and erasure and the right to be forgotten

### Module 7: Training and awareness

- Outline strategies for developing and implementing privacy training and awareness programs.

**Module 8: Protecting personal information**

- Examine a holistic approach to protecting personal information through Privacy by Design.

**Module 9: Data breach incident plans**

- Provide guidance on planning for and responding to a data security incident or breach

**Module 10: Measuring monitoring and auditing program performance**

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