Westcon Comstor
Delivering Results Together
powered by WestconGroup

Certified Information Privacy Manager
CIPM
iapp

International Association of Privacy Professionals (IAPP) CIPM

Course Length

2 days

Overview

Founded in 2000, the IAPP is the world's largest and most comprehensive privacy resource with a mission to define, support and improve the Privacy profession globally.

Every organization has data protection needs. Every day, we access, share and manage data across companies, continents and the globe. Knowing how to implement a privacy program is an invaluable skill that will help you protect your organization's data—and take your career to the next level.

Our Principles of Privacy Program Management training is the premier course on implementing a privacy program framework, managing the privacy program operational lifecycle and structuring a privacy team.

Course Objectives

Principles of Privacy Program Management is the how-to training on implementing a privacy program framework, managing the privacy program operational lifecycle and structuring a knowledgeable, high-performing privacy team. Those taking this course will learn the skills to manage privacy in an organization through process and technology—regardless of jurisdiction or industry.
The Principles of Privacy Program Management training is based on the body of knowledge for the IAPP's ANSI accredited Certified Information Privacy Manager (CIPM) certification program.

Target Student

- Data Protection Officers
- Data Protection Managers
- Auditors
- Legal Compliance Officers
- Security Manager
- Information Managers
- Anyone involved with data protection processes and programmes

Prerequisites: None

Book your place at academy.westconcomstor.com/be or sent e-mail to academy.be@westcon.com

Course Content

MODULE 1: Fundamentals of Information Privacy

Unit 1: Common Principles and Approaches to Privacy: This unit includes a brief discussion of the modern history of privacy, an introduction to types of information, an overview of information risk management and a summary of modern privacy principles.
Unit 2: Jurisdiction and Industries: This unit introduces the major privacy models employed around the globe and provides an overview of privacy and data protection regulation by jurisdictions and industry sectors.
Unit 3: Information Security: Safeguarding Personal Information This unit presents introductions to information security, including definitions, elements, standards and threats/ vulnerabilities, as well as introductions to information security management and governance, including frameworks, controls, cryptography and identity and access management (IAM).
Unit 4: Online Privacy: Using Personal Information on Websites and with Other Internet-related Technologies: This unit examines the web as a platform, as well as privacy considerations for sensitive online information, including policies and notices, access, security, authentication and data collection. Additional topics include children's online privacy, email, searches, online marketing and advertising, social media, online assurance, cloud computing and mobile devices.

MODULE 2: Privacy Program Management

This program is broken into two segments: the first illustrates important practices in managing privacy, and the second is an interactive format in which participants apply these practices to a real-world scenario.
Unit 1: Privacy Program Governance: This unit reveals how to create a privacy program at an organizational level, develop and implement a framework and establish metrics to measure program effectiveness. Topics include: creating a company vision for its privacy program; establishing a privacy program that aligns to the business; structuring the privacy team; developing organizational privacy policies, standards and guidelines; defining privacy program activities; and defining program metrics.
Unit 2: Privacy Operational Life Cycle: This substantial unit reviews privacy program practices employed throughout the privacy life cycle—assess, protect, sustain and respond. Topics include: documenting the privacy baseline of the organization; data processors and third-party vendor assessments; physical assessments; mergers, acquisitions and divestitures; privacy threshold analysis; privacy impact assessments; information security practices; Privacy by Design; integrating privacy requirements across the organization; auditing your privacy program; creating awareness of the organization's privacy program; compliance monitoring; handling information requests; and handling privacy incidents.