INFOSECTRAIN

IAPP
OFFICIAL
TRAINING
PARTNER

IAPP CIPM

CERTIFIED INFORMATION PRIVACY MANAGER

TRAINING AND CERTIFICATION

INFOSECTRAIN

Course Highlights

- 32 hrs of instructor-led training
- IAPP Training Partner
- 1 Year IAPP Membership*
- Post Training support
- Exam Voucher
- IAPP e-book & notes

COURSE DESCRIPTION

The Certified Information Privacy Manager (CIPM) certificate validates your expertise in privacy program management and your capability to create, operate, and manage a privacy program throughout all its lifecycle stages. To become certified, you must master all the ideas and subjects listed in the CIPM body of knowledge. CIPM training teaches a process for conceptualizing, designing, building and operating a data privacy management program It also gives professionals the skills to operationalize privacy and minimize risks to reputation from improper handling of personal data.

WHY CIPM CERTIFICATION TRAINING WITH INFOSECTRAIN?

InfosecTrain is a proficient technology and security training and consulting organization across the globe, specializing in various IT security courses and services. Our Certified Information Privacy Manager (CIPM) certification training aims to explain to you all about the privacy program. You can leverage the following benefits with InfosecTrain:

- We can help you present your qualifications and work experience for the designated profile.
- We provide a flexible training schedule.
- We provide post-training assistance.
- We also create groups for discussion.
- We also provide a certificate of participation to each candidate.

IAPP
OFFICIAL
TRAINING
PARTNER

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 Details

EXAM PATTERN	MULTIPLE CHOICE QUESTIONS
NO. OF QUESTIONS	90 QUESTIONS OUT OF WHICH 70 QUESTIONS ARE SCORED
EXAM DURATION	150 MINUTES
PASSING SCORE	300 OUT OF 500
EXAM LANGUAGE	ENGLISH, FRENCH, GERMAN, BRAZILIAN PORTUGUESE

Course Content

Developing a Privacy Program

1. Create a company vision

> Acquire knowledge on privacy approaches

> Evaluate the intended objective

> Gain executive sponsor approval for this vision

2. Establish a Data Governance model

> Centralized

> Distributed

> Hybrid

3. Establish a privacy program

> Define program scope and charter

> Identify the source, types, and uses of personal information (PI) within the organization and the applicable laws

> Develop a privacy strategy

4. Structure the privacy team

> Establish the organizational model, responsibilities and reporting structure appropriate to the size of the organization

> Designate a point of contact for privacy issues

> Establish/endorse the measurement of professional competency

5. Communicate

> Awareness

Privacy Program Framework

1. Develop the Privacy Program Framework

> Develop organizational privacy policies, standards, and/or guidelines

> Define privacy program activities

2. Implement the Privacy Program Framework

> Communicate the framework to internal and external stakeholders

> Ensure continuous alignment to applicable laws and regulations to support the development of an organizational privacy program framework

3. Develop Appropriate Metrics

> Identify intended audience for metrics

> Define reporting resources

> Define privacy metrics for oversight and governance per audience

> Identify systems/application collection points

3. Develop Appropriate Metrics

> Identify intended audience for metrics

> Define reporting resources

> Define privacy metrics for oversight and governance per audience

> Identify systems/application collection points

Privacy Operational Life Cycle: Assess

1. Document current baseline of your privacy program

> Education and awareness
> Monitoring and responding to the regulatory environment
> Internal policy compliance
> Data, systems and process assessment
> Risk assessment (PIAs, etc.)
> Incident response
> Remediation
> Determine desired state and perform gap analysis against an accepted standard or law (including GDPR)
> Program assurance, including audits

2. Processors and third-party vendor assessment

> Evaluate processors and third-party vendors, insourcing and outsourcing privacy risks, including rules of international data transfer
> Understand and leverage the different types of relationships
> Risk assessment
> Contractual requirements
> Ongoing monitoring and auditing

3. Physical assessments

> Identify operational risk

4. Mergers, acquisitions and divestitures

> Due diligence
> Risk assessment

5. Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs)

> Privacy Threshold Analysis (PTAs) on systems, applications and processes

> Privacy Impact Assessments (PIAs)

Privacy Operational Life Cycle: Protect

1. Information security practices

> Access controls for physical and virtual systems

> Technical security controls

> Implement appropriate administrative safeguards

2. Privacy by Design

> Integrate privacy throughout the system development life cycle (SDLC)

> Establish privacy gates as part of the system development framework

3. Integrate privacy requirements and representation into functional areas across the organization

> Information security

> IT operations and development

> Business continuity and disaster recovery planning

> Mergers, acquisitions and divestitures

> Human resources

> Compliance and ethics

> Audit

> Marketing/business development

> Public relations

> Procurement/sourcing

> Legal and contracts

> Security/emergency services

> Finance

> Others

4. Other organizational measures

> Quantify the costs of technical controls
> Manage data retention with respect to the organization's policies
> Define the methods for physical and electronic data destruction
> Define roles and responsibilities for managing the sharing and disclosure of data for internal and external use

Privacy Operational Life Cycle: Protect

1. Monitor

> Environment (e.g., systems, applications) monitoring
> Monitor compliance with established privacy policies
> Monitor regulatory and legislative changes
> Compliance monitoring (e.g. collection, use and retention)

2. Audit

> Align privacy operations to an internal and external compliance audit program
> Audit compliance with privacy policies and standards
> Audit data integrity and quality and communicate audit findings with stakeholders
> Audit information access, modification and disclosure accounting
> Targeted employee, management and contractor training

Privacy Operational Life Cycle: Respond

1. Data-subject information requests and privacy rights

- Access
- Redress
- Correction
- Managing data integrity
- Right of Erasure
- Right to be informed
- Control over use of data

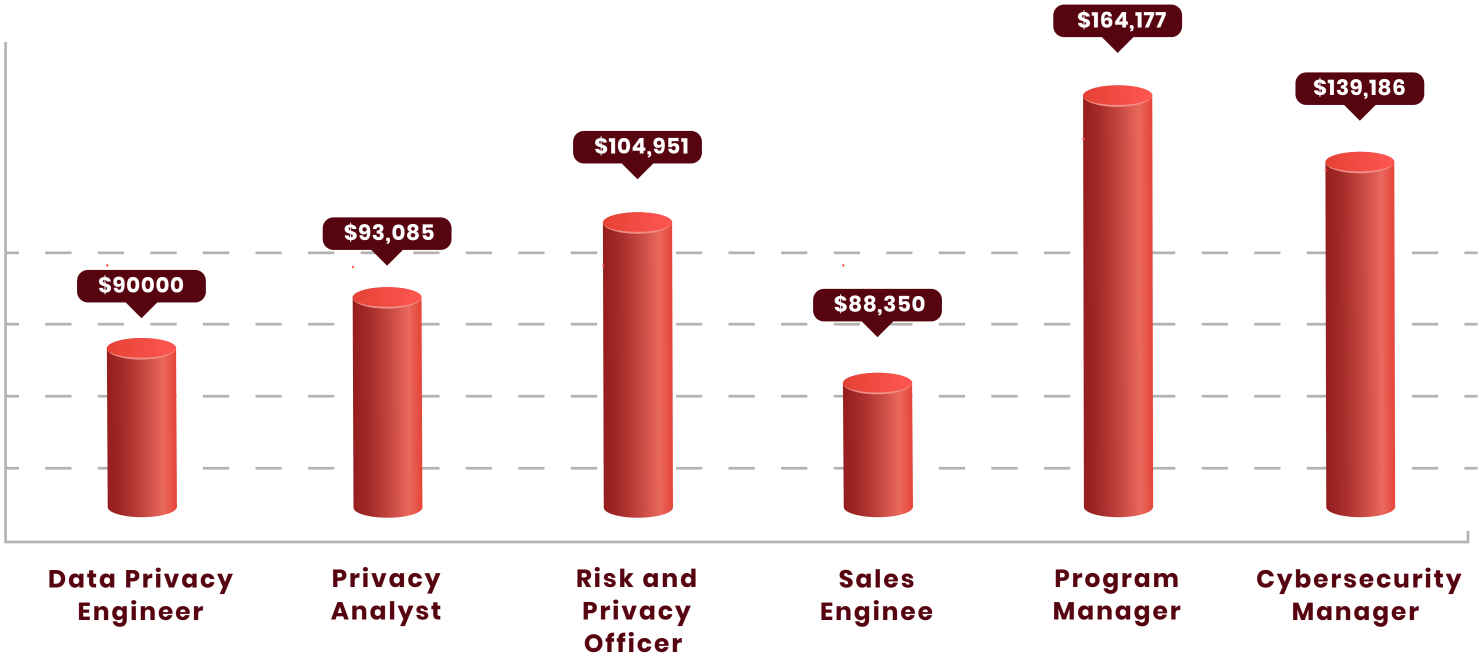
2. Privacy incident response

- Legal compliance
- Incident response planning
- Incident detection
- Incident handling
- Follow incident response process to ensure meeting jurisdictional, global and business requirements
- Identify incident reduction techniques
- Incident metrics—quantify the cost of a privacy incident

INFOSECTRAIN

IAPP
OFFICIAL
TRAINING
PARTNER

Career
Benefits



HIRING COMPANIES

align

osano

Deloitte.

Google

EY
Building a better working world

"Source: Glassdoor"

Certified Information Privacy Manager

CIPM

iapp

ENROLL NOW

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com