IAPP CIPM

IAPP Information Privacy Manager Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

CIPM

IAPP Certified Information Privacy Manager (CIPM)
90 Questions Exam – 77% Cut Score – Duration of 150 minutes

Table of Contents:

Discover More about the IAPP CIPM Certification

Are you interested in passing the IAPP CIPM exam? First discover, who benefits from the CIPM certification. The CIPM is suitable for a candidate if he wants to learn about Operations. Passing the CIPM exam earns you the IAPP Certified Information Privacy Manager (CIPM) title.

While preparing for the CIPM exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The CIPM PDF contains some of the most valuable preparation tips and the details and instant access to useful **CIPM study materials just at one click.**

IAPP CIPM Information Privacy Manager Certification Details:

Exam Name	IAPP Certified Information Privacy Manager (CIPM)
Exam Code	CIPM
Exam Price	First Time Candidate: $550 Retake: $375
Duration	150 mins
Number of Questions	90
Passing Score	77%
Books / Training	**CIPM Body of Knowledge** **CIPM Exam Blueprint** **GDPR Prep Online Bundle (CIPM)**
Schedule Exam	**CIPM**
Sample Questions	**IAPP CIPM Sample Questions**
Practice Exam	**IAPP CIPM Certification Practice Exam**

IAPP CIPM Syllabus:

Topic	Details
Developing a Privacy Program	
Create an organizational vision	- Evaluate the intended objective - Gain executive sponsor approval for this vision

Topic	Details
Establish a Data Governance model	- Centralized - Distributed - Hybrid
Define 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 • Business alignment - Finalize the business case for privacy - Identify stakeholders - Leverage key functions - Create a process for interfacing within organization - Align organizational culture and privacy/data protectio objectives • Obtain funding/budget for privacy and the privacy tea • Develop a data governance strategy for processing personal information (e.g. collect, use, access, share, transfer, destroy • Ensure program flexibility in order to incorporate legislative/regulatory/market/business requirements
Structure the privacy team	- Establish the organizational model, responsibilities and reporting structure appropriate to the size of the organization (eg Chief Privacy Officer, DPO, Privacy manager, Privacy analysts, Privacy champions, “First responders”) - Designate a point of contact for privacy issues - Establish/endorse the measurement of professional competency
Communicate	- Create awareness of the organization’s privacy program internally and externally (e.g. PR, Corporate Communication, HR) - Develop internal and external communication plans to ingrain organizational accountability

Topic	Details
	- Ensure employees have access to policies and procedures and updates relative to their role
Privacy Program Framework	
Develop the Privacy Program Framework	- Develop organizational privacy policies, procedures, standards, and/or guidelines - Define privacy program activities • Education and awareness • Monitoring and responding to the regulatory environment • Monitoring internal privacy policy compliance • Data inventories, data flows, and classifications designed to identify what personal data your organization processes • Risk assessment (Privacy Impact Assessments [PIAs]) (e,g., DPIAs etc.) • Incident response and process, including jurisdictional requirements • Remediation oversight • Program assurance, including audits • Plan inquiry/complaint handling procedures (customers, regulators, etc.)
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 • Understand territorial regulations and/or laws (eg GDPR, CCPA, LGPD) • Understand sectoral and industry regulations and/or laws (eg HIPAA, GLBA) • Understand penalties for noncompliance with laws and regulations Understand the scope and authority of oversight agencies (e.g., Data Protection Authorities, Privacy Commissioners, Federal Trade Commission, etc.)

Topic	Details
	• Understand privacy implications of doing business with or basing operations in countries with inadequate, or without, privacy laws • Maintain the ability to manage a global privacy function • Maintain the ability to track multiple jurisdictions for changes in - Understanding data sharing agreements • International data sharing agreements • Vendor agreement • Affiliate and subsidiary agreements
Develop Appropriate Metrics	- Identify intended audience for metrics - Define reporting resources - Define privacy metrics for oversight and governance per audience • Compliance metrics (examples, will vary by organization - Collection (notice) - Responses to data subject inquiries - Retention - Disclosure to third parties - Incidents (breaches, complaints, inquiries) - Employees trained - PIA/DPIA metrics - Privacy risk indicators - Percent of company functions represented by governance mechanisms • Trend Analysis • Privacy program return on investment (ROI) • Business resiliency metrics • Privacy program maturity level • Resource utilization - Identify systems/application collection points

Topic	Details
Privacy Operational Life Cycle: Assess	
Document current baseline of your privacy program	- Education and awareness - Monitoring and responding to the regulatory environment - Assess policy compliance against internal and external requirements - Data, systems and process assessment • Map data inventories, flows, lifecycle and system integrations - Risk assessment methods - Incident management, response and remediation - Determine desired state and perform gap analysis against an accepted standard or law (including GDPR) - Program assurance, including audits
Processors and third-party vendor assessment	- Evaluate processors and third-party vendors, insourcing and outsourcing privacy risks, including rules of international data transfer • Privacy and information security policies • Access controls • Where personal information is being held • Review and set limits on vendor internal use of personal information - Understand and leverage the different types of relationships • Internal audit • Information security • Physical security • Data protection authority - Risk assessment • Type of data being outsourced • Location of data • Technologies and processing methods deployed (eg Cloud Computing)

Topic	Details
	• Legal compliance • Records retention • Contractual requirements (incident response, etc.) • Determine minimum standards for safeguarding information • Cross-border transfers - Contractual requirements and review process - Ongoing monitoring and auditing
Physical assessments	- Identify operational risk • Data centers and offices • Physical access controls • Document retention and destruction • Media sanitization and disposal (e.g., hard drives, USB/thumb drives, etc.) • Device forensics • Device security (e.g., mobile devices, Internet of Things (IoT), geotracking, imaging/copier hard drive security controls)
Mergers, acquisitions and divestitures	- Due diligence procedures - Review contractual and data sharing obligations - Risk assessment - Risk and control alignment - Post integration planning and risk mitigation
Privacy Assessments and Documentation	- Privacy Threshold Analysis (PTAs) on systems, applications and processes - Define a process for conducting privacy assessments (e.g., PIA, DPIA, TIA, LIA) • Understand the life cycle of each assessment type • Incorporate privacy assessments into system, process, data life cycles
Privacy Operational Life Cycle: Protect	
Information security practices	- Access controls for physical and virtual systems

Topic	Details
	• Least privileged access (eg need to know) • Account management (e.g., provision process) • Privilege management - Technical security controls (including relevant policies and procedures) - Incident response plans
Privacy by Design (PbD)	- Integrate privacy throughout the system development life cycle (SDLC) - Establish privacy gates as part of the system development framework - Integrate privacy through business processes - Communicate with stakeholders the importance of PIAs and PbD
Integrate privacy requirements and representation into functional areas across the organization (eg Information Security, Human Resources, Marketing, Legal and Contracts, Mergers, Acquisitions & Divestitures)	
Technical and Organizational measures	- Quantify the costs of technical and organizational 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 - Determine and implement guidelines for secondary uses (ex: research, etc.) - Define policies related to the processing (including

Topic	Details
	collection, use, retention, disclosure and disposal) of organization's data holdings, taking into account both legal and ethical requirements - Implement appropriate administrative safeguards, such as policies, procedures, and contracts
Privacy Operational Life Cycle: Sustain	
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) • Internal audit • Self-regulation • Retention strategy • Exit strategy
Audit	- Align privacy operations to an internal and external compliance audit program • Knowledge of audit processes and maintenance of an "audit trail" • Assess against industry standards • Utilize and report on regulator compliance assessment tools - 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 policies • Operational privacy practices (e.g., standard operating instructions), such as - Data creation/usage/retention/disposal

Topic	Details
	- Access control - Reporting incidents - Key contacts
Privacy Operational Life Cycle: Respond	
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, including objection to processing - Complaints including file reviews
Privacy incident response	- Legal compliance • Preventing harm • Collection limitations • Accountability • Monitoring and enforcement • Mandatory reporting - Incident response planning • Understand key roles and responsibilities - Identify key business stakeholders Information security Legal Head of compliance Audit Human resources Marketing Business development Communications and public relations External parties • Establish incident oversight teams • Develop a privacy incident response plan • Identify elements of the privacy incident response plan

Topic	Details
	• Integrate privacy incident response into business continuity planning - Incident detection • Define what constitutes a privacy incident • Identify reporting process • Coordinate detection capabilities - Organization IT - Physical security - Human resources - Investigation teams - Vendors - Incident handling • Understand key roles and responsibilities • Conduct risk assessment • Perform containment activities • Identify and implement remediation measures • Develop a communications plan to notify executive management • Notify regulator, impacted individuals and/or the responsible data controller - Follow incident response process to ensure meeting jurisdictional, global and business requirements • Engage privacy team • Review the facts • Conduct analysis • Determine actions (contain, communicate, etc.) • Execute • Maintain an incident register and associated records of the incident management • Monitor • Review and apply lessons learned - Identify incident reduction techniques - Incident metrics—quantify the cost of a privacy incident

Broaden Your Knowledge with IAPP CIPM Sample Questions:

Question: 1

All of the following are deemed administrative safeguards except:

a) Security policy
b) Privileged access controls
c) Privacy policy
d) Security standards

Answer: b

Question: 2

In addition to regulatory requirements and business practices, what important factors must a global privacy strategy consider?

a) Cultural norms
b) Geographic features
c) Political history
d) Monetary exchange

Answer: a

Question: 3

How are individual program needs and specific organizational goals identified in privacy framework development?

a) By employing metrics to align privacy protection with objectives
b) Through conversations with the privacy team
c) By employing an industry-standard needs analysis
d) Through creation of the business case

Answer: a

Question: 4

By integrating privacy and security into business continuity planning, an organization ensures that:

e) Processes related to personal information are given priority for restoration.
f) Personal information protection and valid use continues to be the norm.
g) Processes related to personal information are more resilient.
h) Privacy and security are the most important characteristics of business processes.

Answer: b

Question: 5

What is generally the best approach when working with authorities?

a) Delay for as long as legally permissible.
b) Slowly and progressively provide requested information.
c) Cooperate and act with transparency.
d) Delay for as long as possible.

Answer: c

Question: 6

As part of understanding the organization's current state, a privacy strategist is examining the organization's privacy policy. What does the policy tell the strategist?

a) The level of management commitment to privacy
b) The maturity level of the organization
c) The compliance level of the organization
d) None of these

Answer: d

Question: 7

A system that intakes event data and produces alerts is known as a:

a) System event and information management system
b) System event and incident management system
c) Security information and event management system
d) Security event and incident management system

Answer: c

Question: 8

A privacy strategist recently joined a retail organization that operates with slim profit margins and has discovered that the organization lacks several important privacy capabilities. What is the best strategy here?

a) Insist that management support an aggressive program quickly to improve the program.
b) Develop a risk ledger that highlights all identified risks.
c) Recommend that the biggest risks be avoided.
d) Develop a risk-based strategy that implements changes slowly over an extended period of time.

Answer: d

Question: 9

Executive management is considering entering negotiations that, if successful, will result in the acquisition of another organization. What is the best time for the organization's privacy leader to become involved in the acquisition?

a) During final negotiations
b) As early as possible
c) After negotiations have concluded
d) When the transaction closes

Answer: b

Question: 10

If an organization maintains a separate ethics office, to whom would its officer typically report to in order to retain the greatest degree of independence?

a) The Board of Directors
b) The Chief Financial Officer
c) The Human Resources Director
d) The organization's General Counsel

Answer: a

Avail the Study Guide to Pass IAPP CIPM Information Privacy Manager Exam:

- Find out about the CIPM syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **IAPP CIPM syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the **Information Privacy Manager training.** Joining the IAPP provided training for this IAPP certification exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **IAPP CIPM sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. CIPM practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

Passing the IAPP CIPM exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the IAPP CIPM Certification

CertFun.Com is here with all the necessary details regarding the CIPM exam. We provide authentic practice tests for the CIPM exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on CertFun.Com for rigorous, unlimited two-month attempts on the **CIPM practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the IAPP Certified Information Privacy Manager (CIPM).

Start Online practice of IAPP CIPM Exam by visiting URL
https://www.certfun.com/iapp/cipm-iapp-certified-information-privacy-manager