STUDY GUIDE

iapp

Certified Information Privacy Manager

Effective September 2024

WELCOME

Congratulations on taking the first step toward achieving an IAPP privacy certification. This study guide contains the basic information you need to get started, including:

- Key areas of knowledge for the CIPM exam.
- Recommended steps to help you prepare for your exam.
- An outline of the body of knowledge for the CIPM certification.
- General exam information.
- An explanation of the IAPP certification structure.

CIPM key areas of knowledge

The CIPM certification was developed in response to overwhelming demand to collate common practices for managing privacy operations. It covers governance and the skills to establish, maintain and manage a privacy program across all stages of its operational life cycle.

Key subject matter areas include:

I. Privacy program governance

- Creating a company vision.
- Establishing a privacy program.
- Structuring the privacy team.
- Developing and implementing a privacy program framework.
- Communicating to stakeholders.
- Performance measurement.

II. Privacy operational life cycle

- Assessing or evaluating a privacy regime.
- Protecting information assets through the implementation of industry-leading privacy and security controls and technology.
- Sustaining the privacy operation through communication, training and management actions.
- Responding to privacy incidents.

Preparation

Privacy certification is an important effort that requires advance preparation. Deciding how you will prepare for your exams is a personal choice that should include an assessment of your professional background, scope of privacy knowledge and your preferred method of learning.

In general, the IAPP recommends you plan for a minimum of 30 hours of study time in advance of your exam date. However, you might need more or fewer hours depending on your personal choices and professional experience.

You can read more about preparation suggestions and resources on our website.

The IAPP recommends you prepare in the following manner:

1. Review the body of knowledge

The body of knowledge for the CIPM is a comprehensive outline of the subject matter areas covered by the CIPM exam. The integrated exam blueprint indicates the minimum and maximum number of items included on the CIPM exam from the major areas of the body of knowledge. Questions may be asked from any of the topics listed under each area and can be used to guide your preparation. Studying the body of knowledge can help you further target your primary study needs and determine which areas merit additional focus in your preparation.

2. Study the CIPM textbook

"Privacy Program Management: Tools for Managing Privacy Within Your Organization" is the authoritative reference for the CIPM exam. The IAPP strongly recommends you take the time to carefully read and study it. Print and digital versions of the textbook are available through the IAPP store.

3. Get certification training

The IAPP offers in-person, live online and self-paced online certification training to help you prepare for your exams. You can find a list of scheduled trainings or purchase self-paced online training in the IAPP store.

4. Take the CIPM practice exam

IAPP practice exams provide insight into how you might perform on your certification exam. Practice exams consist of 90 questions in the same format as official certification exams. The questions are developed by IAPP-selected experts to match the depth and rigor of the actual exam.

5. Review other IAPP preparation resources

Additional resources are available on the IAPP website, including a searchable glossary of terms.

CIPM body of knowledge outline

I. Privacy program: developing a framework

A. Define program scope and develop a privacy strategy.
B. Communicate organizational vision and mission statement.
C. Indicate in-scope laws, regulations and standards applicable to the program.

II. Privacy program: establishing program governance

A. Create policies and processes to be followed across all stages of the privacy program life cycle.
B. Clarify roles and responsibilities.
C. Define privacy metrics for oversight and governance.
D. Establish training and awareness activities.

III. Privacy program operational life cycle: assessing data

A. Document data governance systems.
B. Evaluate processors and third-party vendors.
C. Evaluate physical and environmental controls.
D. Evaluate technical controls.
E. Evaluate risks associated with shared data in mergers, acquisitions and divestitures.

IV. Privacy program operational life cycle: protecting personal data

A. Apply information security practices and policies.
B. Integrate the main principles of Privacy by Design (PbD).
C. Apply organizational guidelines for data use and ensure technical controls are enforced.

V. Privacy program operational life cycle: sustaining program performance

A. Use metrics to measure the performance of the privacy program.
B. Audit the privacy program.
C. Manage continuous assessment of the privacy program.

VI. Privacy program operational life cycle: responding to requests and incidents

A. Respond to data subject access requests and privacy rights.
B. Follow organizational incident handling and response procedures.
C. Evaluate and modify current incident response plan.

CIPM exam format

The CIPM is an 2.5 hour exam comprised of 90 items. Most of the items are multiple choice, including both single, stand-alone questions and others associated with case studies. There are no essay questions. Each correct answer is worth one point.

Example questions

1. Which descriptor best describes the general attitude an organization should exhibit regarding its practices and policies for data protection?
   A. Security.
   B. Openness.
   C. Secrecy.
   D. Education.

2. Where should procedures for resolving complaints about privacy protection be found?
   A. In written policies regarding privacy.
   B. In the Emergency Response Plan.
   C. In memoranda from the CEO.
   D. In the minutes of corporate or organizational board meetings.

Sample scenario

Country Fresh Sundries started in the kitchen of its founder Margaret Holmes as she made soap following a traditional family recipe. It is a much different business today, having grown first through product placement in health and beauty retail outlets, then through a thriving catalog business. The company was slow to launch an online store, but once it did so, the online business grew rapidly. Online sales now account for 65% of a business which is increasingly international in scope. In fact, Country Fresh is now a leading seller of luxury soaps in Europe and South America, as well as continuing its strong record of growth in the United States. Despite its rapid ascent, Country Fresh prides itself on maintaining its homey atmosphere, as symbolized by its company headquarters with a farmhouse in front of a factory in a rural region of Maine in the U.S. The company is notably "employee friendly," allowing, for instance, employees to use their personal computers for conducting business and encouraging people to work at home to spend more time with their families.

Continued on next page

As the incoming director of privacy, you are the company's first dedicated privacy professional. During the interview process, you found that while the people you talked to, including Shelly Holmes, CEO, daughter of the founder, and Jim Greene, vice president for operations, meant well, they did not possess a sophisticated knowledge of privacy practices and regulations, and were unsure of exactly where the company stood in relation to compliance and security. Jim candidly admitted, "We know there is a lot we need to be thinking about and doing regarding privacy, but none of us know much about it. We have put some safeguards in place, but we are not even sure they are effective. We need someone to build a privacy program from the ground up."

The final interview ended after the close of business. The cleaning crew had started its nightly work. As you walked through the office, you noticed that computers had been left on at employee workstations, and the only shredder you saw was marked with a sign that said "Out of Order. Do Not Use."

You have accepted the job offer and are about to report to work on Monday. You are now on a plane headed toward your new office, considering your course of action in this position and jotting down some notes.

1. How can you discover where personal data resides at the company?
   A. Focus solely on emerging technologies as they present the greatest risks.
   B. Check all public interfaces for breaches of personal data.
   C. Conduct a data inventory and map data flows.
   D. Interview each department head.

2. In analyzing the company's existing privacy program, you find procedures that are informal and incomplete. What stage does this represent in the AICPA/CICA Privacy Maturity Model?
   A. Early.
   B. Ad hoc.
   C. Nonrepeatable.
   D. Preprogram.

See page 9 for answers.

General exam information

The IAPP offers testing via computer-based delivery at more than 6,000 testing locations worldwide, or you can take your certification exam from home with online proctoring. Remote proctoring is currently available for in-language exams but requires enough knowledge of English to communicate with exam proctors.

You can find detailed information about how to register for exams, as well as exam-day instructions, in the IAPP Certification Information Candidate Handbook on our website.

Questions?

The IAPP understands that privacy certification is an important professional development effort requiring commitment and preparation. We thank you for choosing to pursue certification, and we welcome your questions and comments.

Please don't hesitate to contact us at certification@iapp.org.

Example questions: Answers

1. Which descriptor best describes the general attitude an organization should exhibit regarding its practices and policies for data protection?
   A. Security.
   B. Openness.
   C. Secrecy.
   D. Education.

2. Where should procedures for resolving complaints about privacy protection be found?
   A. In written policies regarding privacy.
   B. In the Emergency Response Plan.
   C. In memoranda from the CEO.
   D. In the minutes of corporate or organizational board meetings.

Sample scenario

Country Fresh Sundries started in the kitchen of its founder Margaret Holmes as she made soap following a traditional family recipe. It is a much different business today, having grown first through product placement in health and beauty retail outlets, then through a thriving catalog business. The company was slow to launch an online store, but once it did so, the online business grew rapidly. Online sales now account for 65% of a business which is increasingly international in scope. In fact, Country Fresh is now a leading seller of luxury soaps in Europe and South America, as well as continuing its strong record of growth in the United States. Despite its rapid ascent, Country Fresh prides itself on maintaining its homey atmosphere, as symbolized by its company headquarters with a farmhouse in front of a factory in a rural region of Maine in the U.S. The company is notably "employee friendly," allowing, for instance, employees to use their personal computers for conducting business and encouraging people to work at home to spend more time with their families.

Continued on next page

As the incoming director of privacy, you are the company's first dedicated privacy professional. During the interview process, you found that while the people you talked to, including Shelly Holmes, CEO, daughter of the founder, and Jim Greene, vice president for operations, meant well, they did not possess a sophisticated knowledge of privacy practices and regulations, and were unsure of exactly where the company stood in relation to compliance and security. Jim candidly admitted, "We know there is a lot we need to be thinking about and doing regarding privacy, but none of us know much about it. We have put some safeguards in place, but we are not even sure they are effective. We need someone to build a privacy program from the ground up."

The final interview ended after the close of business. The cleaning crew had started its nightly work. As you walked through the office, you noticed that computers had been left on at employee workstations, and the only shredder you saw was marked with a sign that said "Out of Order. Do Not Use."

You have accepted the job offer and are about to report to work on Monday. You are now on a plane headed toward your new office, considering your course of action in this position and jotting down some notes.

1. How can you discover where personal data resides at the company?
   A. Focus solely on emerging technologies as they present the greatest risks.
   B. Check all public interfaces for breaches of personal data.
   C. Conduct a data inventory and map data flows.
   D. Interview each department head.

2. In analyzing the company's existing privacy program, you find procedures that are informal and incomplete. What stage does this represent in the AICPA/CICA Privacy Maturity Model?
   A. Early.
   B. Ad hoc.
   C. Nonrepeatable.
   D. Preprogram.

The IAPP certification program structure

The IAPP currently offers four certifications: the Artificial Intelligence Governance Professional, the Certified Information Privacy Professional, the Certified Information Privacy Manager and the Certified Information Privacy Technologist.

AIGP certification demonstrates comprehension of AI systems and the ability to deploy AI in a manner that abates risk and ensures safety and trust. It confirms an understanding of AI ecosystems, identification and mitigation of bias, and the capability to effectively communicate best practices for responsible AI management.

CIPP certification demonstrates a mastery of data privacy laws and regulations and how to apply them (e.g.,jurisdictional laws, regulations and enforcement models), plus legal requirements for handling and transferring data. Within the CIPP, there are four concentrations:

Asian privacy (CIPP/A).
Canadian privacy (CIPP/C).
European data protection (CIPP/E).
U.S. private-sector privacy (CIPP/US).

CIPM certification demonstrates understanding of implementing privacy regulatory requirements in day-to-day operations. It confirms the ability to create a company vision, structure a data protection team, develop and implement system frameworks, communicate to stakeholders and measure performance.

CIPT certification demonstrates a deep understanding of privacy's role in technology, including building privacy-friendly products, services and systems; deploying emerging technologies while respecting consumer privacy; establishing privacy practices for data security and control.

There are no concentrations within the CIPM or CIPT — they cross all jurisdictions and industries.

Requirements for IAPP certification

1. You must pay a two-year certification maintenance fee of USD250. If you are not an IAPP member, we recommend purchasing the certification maintenance fee at the time of your exam purchase so it will activate automatically upon passing the exam.

   OR

   You can become a member of the IAPP with access to numerous benefits, like discounts, networking opportunities, members-only resources and more, for just USD295 annually, which includes your maintenance fee.

2. You must meet the annual continuing privacy education requirements of 20 credits in order to keep your certification active.

More information about IAPP membership, including levels, benefits and rates, is available on the IAPP website.