iapp

CIPP/C
Body of Knowledge and Exam Blueprint

Version 3.1.0

Effective date: 1 September 2025

IAPP CIPP/C BODY OF KNOWLEDGE

UNDERSTANDING THE IAPP'S BODY OF KNOWLEDGE

The main purpose of the body of knowledge (BoK) is to document the knowledge and skills that will be assessed on the certification exam. The domains reflect what the privacy professional should know and be able to do to show competency in this designation.

The body of knowledge also includes the exam blueprint numbers, which show the minimum and maximum number of questions from each Domain that will be found on the exam.

The body of knowledge is developed and maintained by the subject matter experts that constitute each designation's exam development board and scheme committee. The BoK is reviewed every year and updated if necessary. Changes are reflected in the annual exam updates and communicated to candidates at least 90 days before the new content appears in the exam.

COMPETENCIES AND PERFORMANCE INDICATORS

Instead of the former outline format we used for our bodies of knowledge, we now represent the content as a series of Competencies and Performance Indicators.

Competencies are clusters of connected tasks and abilities that constitute a broad knowledge domain.

Performance Indicators are the discrete tasks and abilities that constitute the broader competence group. Exam questions assess a privacy professional's proficiency on the performance indicators.

WHAT TYPES OF QUESTIONS WILL BE ON THE EXAM?

For the certification candidate, the performance indicators are guides to the depth of knowledge required to demonstrate competency. The verbs that begin the skill and task statements (identify, evaluate, implement, define) signal the level of complexity of the exam questions and find their corollaries on the Bloom's Taxonomy (see next page).

ANAB ACCREDITATION

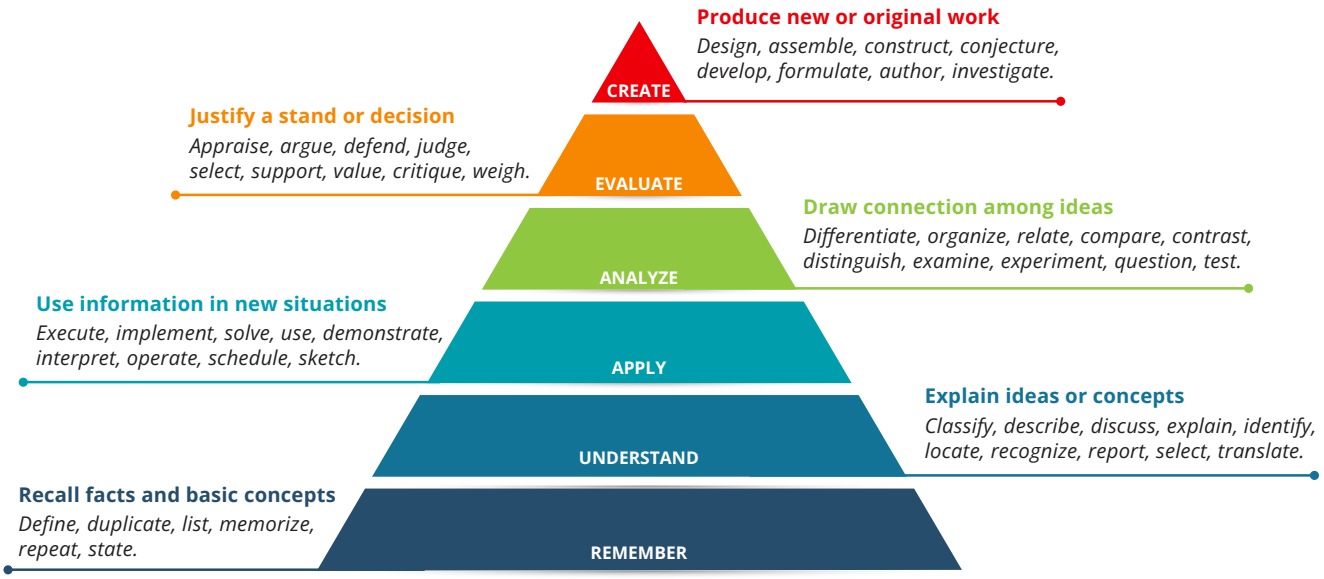
The IAPP's CIPM, CIPP/E, CIPP/US and CIPT credentials are accredited by the **ANSI National Accreditation Board (ANAB) under the International Organization for Standardization (ISO) standard 17024: 2012**.

ANAB is an internationally recognized accrediting body that assesses and accredits certification programs that meet rigorous standards.

Achieving accreditation is a tremendous acknowledgement of the quality and integrity of the IAPP's certification programs, which:

- Demonstrates that IAPP credentials meet a global, industry-recognized benchmark.
- Ensures IAPP credentials are consistent, comparable and reliable worldwide.
- Protects the integrity and ensures the validity of the IAPP certification program.
- Promotes to employers, colleagues, clients, and vendors that IAPP-certified professionals have the necessary knowledge, skills and abilities to perform their work anywhere in the world.

IAPP CIPP/C BODY OF KNOWLEDGE



Examples of Remember / Understand retired questions from various designations:

- Which of the following is the correct definition of Privacy-Enhancing Technologies?
- To which type of activity does the Canadian Charter of Rights apply?
- Which European Union institution is vested with the competence to propose data protection legislation?
- Who has rulemaking authority for the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA)?

The answers to these questions are a fact and cannot be disputed.

Examples of Apply / Analyze retired questions from various designations:

- Which of the following poses the **greatest** challenge for a European Union data controller in the absence of clearly defined contractual provisions?
- Which of the following examples would constitute a violation of territorial privacy?
- What is the **best** way to ensure that all stakeholders have the same baseline understanding of the privacy issues facing an organization?
- If the Information Technology engineers originally set the default for customer credit card information to "Do Not Save," this action would have been in line with what concept?

The answer to this question will be based upon factual knowledge and an understanding that allows for application, analysis and/or evaluation of the options provided to choose the best answer.

MIN	MAX	Domain I: Introduction to Privacy in Canada		
25	31	**Introduction to Privacy in Canada** provides candidates with a foundational understanding of Canadian laws and government structures; it focuses on privacy principles applicable to private, public and health sectors under both federal and provincial regulations. It covers the development of Canadian privacy principles and emphasizes the roles of Privacy Commissioners, courts and administrative bodies in enforcing privacy laws.		
		Competencies		**Performance Indicators**
2	4	I.A	Understand the Canadian governmental structure	Understand the basics of the Canadian government and legal system (e.g., the political structure, the division of powers, the role of courts and administrative tribunals).
				Understand Canadian laws and their interpretations (e.g., the difference between civil and common law, the sources of law, the scope and application of law).
				Know the purposes and roles of Privacy Commissioners, courts and remedies (e.g., the scope of Federal, Provincial and Territorial Commissioners, the scope of Federal and Provincial courts).
18	22	I.B	Apply privacy basics	Understand that definitions of personal information vary among Canadian jurisdictions and legislation (e.g., employee and work related information, public records, publicly available information).
				Understand what constitutes private or sensitive information.
				Understand how to safeguard personal information (e.g., standards / frameworks, categories of controls applicable to third parties, privacy enhancing technologies).
				Understand privacy incidents, privacy breaches and reporting obligations (e.g., high-level processes for dealing with each, notification to privacy commissioner according to legislation as applicable to each sector).
				Understand the common governance principles for responsible AI (e.g., the OECD AI Principles, NIST's 'AI RMF,' Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems).
				Understand the significance of court and commissioner rulings and how they impact the relevant privacy laws and interpretation of those laws.
				Identify the roles and responsibilities of the relevant stakeholders in supporting the organization's compliance efforts, including the privacy officer when applicable.

3	5	I.C	Understand the development of privacy principles	Understand the general concepts and development of fair information practices and when to use applicable practices (e.g., notice, types of consent, access controls and accountability).
				Know the Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy.
				Know the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information.
				Know the Generally Accepted Privacy Principles (GAPP).
1	2	I.D	Understand international privacy and implement where applicable	Understand the implications of international data transfers under relevant privacy laws, including mechanisms and protections for cross-border data flows.
				Understand when or how international privacy laws and their adequacy standards may or may not impact Canadian organizations in specific sectors such as healthcare, education or finance.

MIN	MAX	Domain II: Canadian Privacy Laws and Practices – Private Sector
18	22	**Domain II: Canadian Privacy Laws and Practices – Private Sector** addresses the privacy principles in PIPEDA and 'substantially similar' provincial laws. It covers commercial activities, accountability, consent and rules for personal information handling. The domain also includes Canada's Anti-Spam Legislation (CASL) focusing on consent, identification and unsubscribe mechanisms.

			Competencies	Performance Indicators
15	19	II.A	Know the Privacy Principles that are the foundation of the Personal Information Protection and Electronic Documents Act (PIPEDA) and provincial private sector laws	Understand what is and is not a commercial activity.
				Understand organizational accountability for personal information including when engaging third parties.
				Identify the purpose(s) for collecting personal information.
				Identify and apply requirements for obtaining valid consent (e.g., form of consent, notice of processing, consent as a condition of service, opt-out mechanisms).
				Adhere to requirements respecting collection, use, disclosure, retention and deletion of personal information, including identifying situations that may benefit from a consent exception.
				Keep information accurate and up to date as necessary for original purpose of collection.
				Safeguard personal information in virtual and physical storage throughout the information life cycle.
				Ensure openness in your policies concerning the processing of personal information, including at the point of collection.
				Understand how to respond to individuals seeking access to personal information, including what information can be provided or withheld, the timelines for response and identity verification requirements.
				Ensure proper policies and procedures are in place to deal with compliance complaints and investigations.
1	2	II.B	Know when provincial legislation is applicable instead of PIPEDA	Know the provinces that have privacy laws deemed substantially similar to PIPEDA.
				Know the differences between PIPEDA and provincial private sector laws (e.g., individual rights, breach notification, transfers, PIA, profiling technologies, automated decision making).

1	2	II.C	Understand Canada's Anti-Spam Legislation (CASL)	Understand the scope of and follow rules for consent, identification and unsubscribe mechanisms (e.g., installation of computer programs, automatic downloads).
				Understand the penalties for non-compliance with CASL.

MIN	MAX	Domain III: Canadian Privacy Laws and Practices – Public Sector		
11	15		**Canadian Privacy Laws and Practices – Public Sector** covers privacy principles in the Privacy Act and its provincial/territorial equivalent acts. It includes guidelines on consent, access, correction and data management. The domain also covers Privacy Impact Assessments (PIAs).	
			Competencies	**Performance Indicators**
7	9	III.A	Know the Privacy Principles that are the foundation of the Privacy Act	Understand the expectations of consent governing personal information, including when the collection, use and disclosure is permitted without consent.
				Understand the individual's right of access and correction to their personal information, including when requests to access or to correct personal information may be denied.
				Follow storage, retention and destruction of personal information requirements.
1	3	III.B	Conduct Privacy Impact Assessments	Understand how and when to complete a PIA.
				Understand what should be included in a PIA report.
1	3	III.C	Understand the applicability of the Freedom of Information and Protection of Privacy Acts of the different provinces and territories	Know the different responsibilities of public bodies regarding privacy when provincially regulated.
				Know which public bodies fall under the Privacy Act and which are provincially regulated.

MIN	MAX	Domain IV: Canadian Privacy Laws and Practices – Health Sector
9	13	**Canadian Privacy Laws and Practices – Health Sector** covers provincial health privacy acts, defining Personal Health Information (PHI) and its handling. It emphasizes consent, access, correction and safeguarding of PHI, including third-party involvement, and outlines protocols for breaches.

			Competencies	Performance Indicators
9	13	IV.A	Understand when to apply the various health privacy acts of the provinces and territories	Know which provincial health laws have been deemed "substantially similar."
				Know what defines personal health information (PHI).
				Determine the purpose(s) for when the collection, use and disclosure of PHI is necessary.
				Understand when the right to access and the right to correct information are allowed or not.
				Demonstrate oversight and accountability, including proper use, retention, safeguarding and disposal of PHI, including when used by third parties.
				Demonstrate meaningful consent to the collection, use and disclosure of PHI, including when implicit/implied consent is considered appropriate and what constitutes the circle of care for an individual.
				Establish safeguarding and breach protocols, including reasonable administrative, technical and physical safeguards.
				Understand and implement practices that facilitate transparency and openness.