Certified Information Privacy Technologist

CIPT
Body of Knowledge and Exam Blueprint

Version 4.0.0

Effective date: 1 September 2025

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 BoK 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 BoK is developed and maintained by the subject matter experts that constitute each designation exam development board and scheme committee. The BoK is reviewed and, if necessary, updated every year; 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 BoK 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).

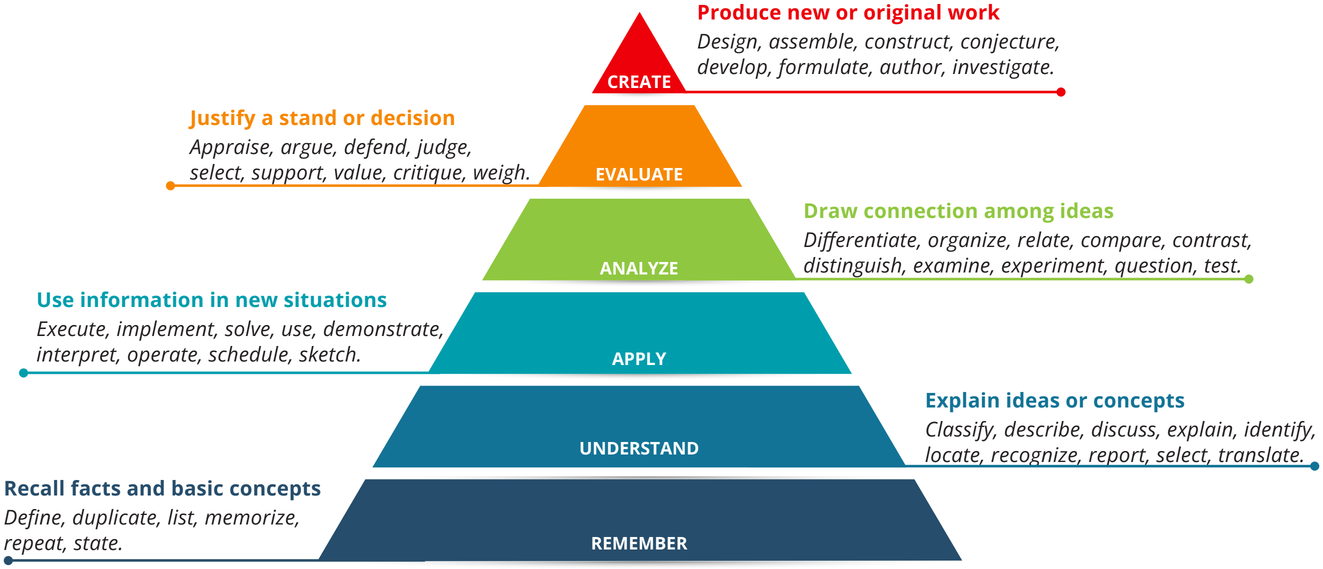
ANAB ACCREDITATION

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.



Produce new or original work
Design, assemble, construct, conjecture, develop, formulate, author, investigate.

Justify a stand or decision
Appraise, argue, defend, judge, select, support, value, critique, weigh.

Draw connection among ideas
Differentiate, organize, relate, compare, contrast, distinguish, examine, experiment, question, test.

Use information in new situations
Execute, implement, solve, use, demonstrate, interpret, operate, schedule, sketch.

Explain ideas or concepts
Classify, describe, discuss, explain, identify, locate, recognize, report, select, translate.

Recall facts and basic concepts
Define, duplicate, list, memorize, repeat, state.

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 and Freedoms 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 facts 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 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.

Domain I — The privacy technologist's role in the context of the organization

MIN	MAX		COMPETENCIES	PERFORMANCE INDICATORS
15	19		**Domain I: The privacy technologist's role in the context of the organization —** This domain addresses the general and technical responsibilities inherent to the role of the Privacy Technologist.	
5	7	I.A	Identify and implement legal and procedural roles and responsibilities.	Understand various roles and responsibilities related to the privacy function (e.g., Data Governance [DPO, Data Owner, Data Steward, Data Custodian], legal compliance, cybersecurity).
				Translate legal and regulatory requirements into practical technical and/or operational solutions.
				Implement internal and external data protection and privacy notices, policies, guidelines and procedures.
5	7	I.B	Identify and implement technical roles and responsibilities.	Oversee technical elements of privacy operations and audits including third-party assessments.
				Provide technical privacy support to identify and respond to privacy breaches and other types of incidents.
				Understand risk concepts (e.g., threat, vulnerability, attack, security exploit).
1	3	I.C	Demonstrate knowledge of privacy risk models and frameworks and their roles in legal requirements and guidance.	Apply common privacy risk models and frameworks (e.g., Nissenbaum's Contextual Integrity, Calo's Harms Dimensions, Factor Analysis in Information Risk (FAIR) model, NIST/NICE framework, FIPPS, OECD principles).
				Understand and apply common privacy threat models and frameworks (e.g., LINDDUN and MITRE PANOPTIC™).

2	4	I.D	Understand the connection between data ethics and data privacy.	Differentiate legal versus ethical processing of personal data (e.g., when comparing different jurisdictions).
				Understand the social and ethical issues when advising on privacy impacting designs and technologies (e.g., unlawful or unauthorized access to personal data, manipulating societal conversations and attitudes on controversial topics).
				Identify and minimize bias/discrimination when advising/designing tools with automated decision-making (e.g., incorporating personal preference into data decisions).

MIN	MAX		Domain II — Data collection, use, dissemination and destruction	
19	23		**Domain II: Data collection, use, dissemination and destruction —** This domain covers strategies and best practices to ensure responsible and secure processing of personal information, minimizing privacy risks during personal data collection, use, dissemination, retention and destruction.	
			COMPETENCIES	PERFORMANCE INDICATORS
8	10	II.A	Demonstrate how to minimize privacy risk during personal data collection.	Understand and apply requirements to provide data subjects with control over the processing of their personal data including consent requirements for personal data collection, use, disclosure, and retention (e.g., clear and accessible privacy notices, settings, dashboards, other consent management mechanisms).
				Implement measures to manage privacy risks associated with automatic collection of personal data.
				Leverage techniques to minimize risk when extracting personal data from publicly available sources.
				Practice appropriate data retention and destruction techniques.
6	8	II.B	Demonstrate how to minimize privacy risk during personal data use.	Practice appropriate data minimization techniques (e.g., abstract personal data for a specific use case).
				Implement data processing segregation.
				Use data analysis and other procedures to minimize privacy risk associated with the aggregation of personal data.
				Employ appropriate privacy-enhancing techniques (e.g., anonymization, pseudonymization, differential privacy) to reduce risk exposure.
				Use technical approaches that minimize the risks associated with secondary uses of personal data (e.g., profiling).

4	6	II.C	Demonstrate how to minimize privacy risk during personal data dissemination.	Use technical approaches that minimize risks associated with disclosure and accessibility.
				Leverage approaches and techniques that minimize the threat of: a. Data distortion. b. Data exposure. c. Breach of confidentiality (personal data breaches). d. Blackmail. e. Appropriation.
				Implement other defense in-depth techniques (e.g., identity and access management, authentication mechanisms) to protect personal data from risk exposure.

MIN	MAX		Domain III: Privacy risk management	
17	21		**Domain III: Privacy risk management —** This domain addresses the critical connection between data ethics and privacy, gaining insights into the ethical considerations that underpin responsible data handling. This domain covers strategies and best practices to ensure responsible and secure processing of personal information, minimizing privacy risks during personal data collection, use and dissemination, as well as addressing concerns on intrusion, decisional interference and software security.	
			COMPETENCIES	**PERFORMANCE INDICATORS**
2	4	III.A	Demonstrate how to minimize the threat of intrusion and decisional interference.	Implement technical approaches that minimize the risks of various types of interference (e.g., behavioral advertising, behavioral profiling, cyberbullying, social engineering).
				Avoid the use of dark patterns that limit privacy-preserving response options, and recognize which design patterns to emulate.
3	5	III.B	Identify privacy risks related to software security.	Implement measures to detect and fix software privacy vulnerabilities.
				Leverage intrusion detection and prevention tools and techniques.
				Implement measures to reduce privacy risks during change management (e.g., patches, upgrades).
				Recognize possible privacy violations by service providers.
4	6	III.C	Understand the privacy risks and impact of techniques that enable tracking and surveillance.	Understand the privacy risks and impact associated with e-commerce (e.g., behavioral advertising, cookies, chatbots, payments, behavioral profiling).
				Demonstrate knowledge of the privacy risks and impact of audio and video surveillance, including those involved in wearables and IoT technologies (e.g., smart home devices and IoT technology for smart cities).
				Understand privacy issues around biometrics (e.g., facial recognition, speech recognition, fingerprint identification, DNA).
				Demonstrate knowledge of the privacy risks and impacts of location tracking.
				Demonstrate knowledge of the privacy risks and impacts of internet monitoring and web tracking.

2	4	III.D	Understand the privacy risks and impact involved when using workplace technologies.	Identify and minimize privacy risks involved when using artificial intelligence, machine learning and deep learning.
				Identify and minimize privacy risk involved in the use of communications technologies (e.g., video calls and conferencing, messaging, mobile devices, social media, gaming platforms).
3	5	III.E	Demonstrate how to monitor and manage privacy risk	Conduct privacy audits and IT control reviews.
				Develop, compile, report, and monitor privacy Key Risk In dicators and Key Performance Indicators.
				Complete privacy and data protection impact assessments.

MIN	MAX		Domain IV – Privacy by design	
7	9		**Domain IV: Privacy by design —** This domain focuses on the strategic integration of principles to effectively manage privacy risks within user experiences, implement value sensitive design practices, and establish robust management and monitoring controls for comprehensive privacy governance.	
			COMPETENCIES	**PERFORMANCE INDICATORS**
4	6	IV.A	Implement privacy by design principles.	Understand and apply the seven privacy by design principles.
				Define and communicate privacy goals and objectives to guide privacy by design within an organization.
				Interpret high-level specifications and align them via low-level specifications with the privacy by design principles.
2	4	IV.B	Evaluate privacy risks in user experiences.	Understand and apply UX concepts, including how UX decisions impact user behavior.
				Perform usability testing where relevant to assess effectiveness of privacy-related functions.
				Understand and apply value sensitive design.

MIN	MAX		Domain V – Privacy engineering and privacy governance	
9	11		**Domain V: Privacy engineering and privacy governance —** This domain explains how to integrate privacy into an organization's technology policies and procedures, including the privacy engineering's role within the organization, privacy engineering objectives, privacy design patterns and privacy risk management throughout the phases of the development life cycle.	
			COMPETENCIES	PERFORMANCE INDICATORS
6	8	V.A	Understand and implement privacy engineering objectives.	Apply the NIST Privacy Engineering Objectives: predictability, manageability and dissociability.
				Understand enterprise architecture, use of data flow diagrams/data lineage tools, including cross-border transfer considerations.
				Manage privacy risks in the development life cycle.
2	4	V.B	Manage and monitor privacy-related functions and controls.	Catalog data assets, develop a data inventory and implement a record of processing activities.
				Conduct code reviews to identify potential privacy gaps that require attention.
				Conduct runtime behavior monitoring.