CIPM
Body of Knowledge and Exam Blueprint

Version 4.2.0

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

We 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

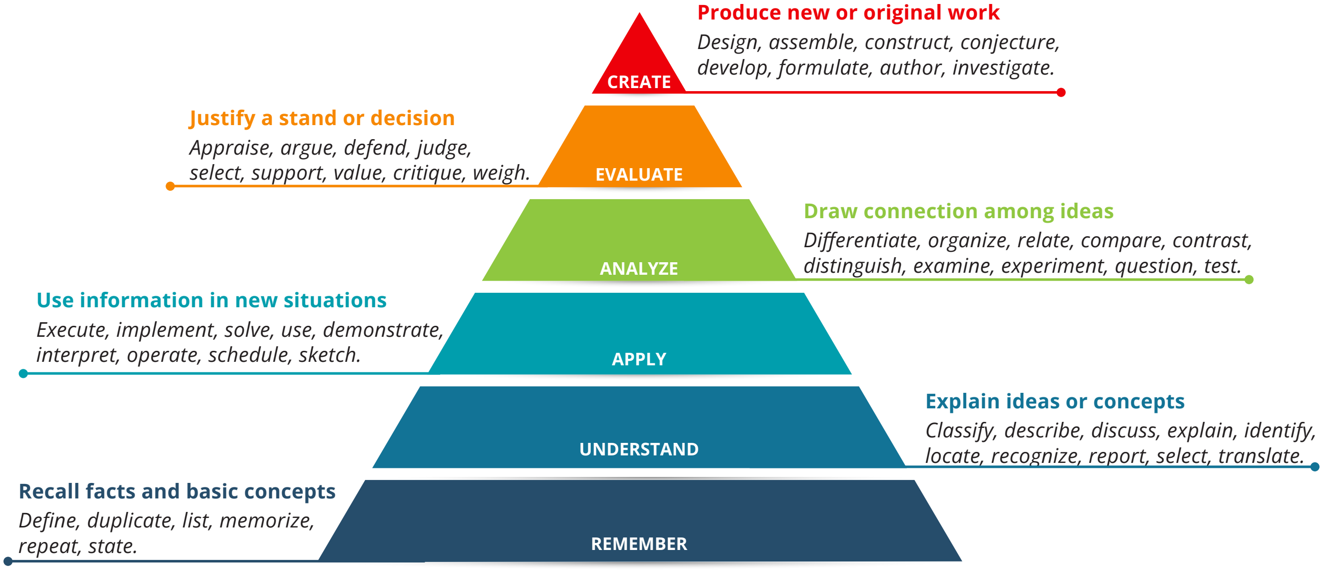
The IAPP's CIPM, CIPP/E, CIPP/US and CIPT credentials are accredited by the **ANSI National Accreditation Board (ANAB) under the International Organization for Standardization (ISO) standard 17024: 2012**.

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.

IAPP CIPM BODY OF KNOWLEDGE



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.

MIN	MAX		Domain I — Privacy Program: Developing a Framework	
14	18		**Domain I — Privacy Program: Developing a Framework** documents the preliminary tasks required to create a solid foundation for the privacy program, the purposes of the program and who is responsible for the program. It focuses on establishing the privacy program governance model within the context of the organization's privacy strategy. As each organization may have its own needs, the model could vary among organizations.	
			COMPETENCIES	**PERFORMANCE INDICATORS**
4	6	I.A	Define program scope and develop a privacy strategy.	Identify the source, types and uses of personal information (PI) within the organization.
				Understand the business model, operational environment and risk appetite.
				Choose applicable governance model.
				Define the structure of the privacy team.
				Identify stakeholders and internal partners.
4	6	I.B	Communicate organizational vision and mission statement.	Create awareness of the organization's privacy program internally and externally.
				Ensure employees have access to policies and procedures and updates relative to their role(s).
				Establish a common understanding of privacy terms across the organization.
5	7	I.C	Indicate in-scope laws, regulations and standards applicable to the program.	Understand territorial, sectoral and industry regulations, laws, codes of practice and/or self-certification mechanisms.
				Understand the potential impact of non-compliance at an organizational and/or individual level.
				Understand scope and authority of oversight agencies.
				Understand privacy implications and territorial scope when doing business or basing operations in other countries with differing privacy laws.
				Understand the privacy risks posed by the use of AI in the business environment.

MIN	MAX		Domain II — Privacy Program: Establishing Program Governance	
12	16		**Domain II — Privacy Program: Establishing Program Governance** identifies how the privacy requirements will be implemented across the organization through all stages of the privacy life cycle. The domain focuses on the roles, responsibilities and training requirements of the various stakeholders, as well as the policies and procedures that will be followed to ensure continuous compliance.	
			COMPETENCIES	PERFORMANCE INDICATORS
6	8	II.A	Create policies and processes to be followed across all stages of the privacy program life cycle.	Establish the organizational model, responsibilities and reporting structure appropriate to size of the organization.
				Define policies appropriate for the data processed by the organization, taking into account legal and ethical requirements.
				Identify collection points considering transparency requirements and data quality issues around collection of data.
				Create a plan for data breach management.
				Create plans for complaint procedures and data subject rights processes and procedures.
				Create data retention and disposal policies and procedures.
1	3	II.B	Clarify roles and responsibilities.	Define roles and responsibilities of the privacy team and stakeholders.
				Define the roles and responsibilities for managing the sharing and disclosure of data for internal and external use.
				Define roles and responsibilities for data breach response by function, including stakeholders and their accountability to various internal and external partners (e.g., detection teams, IT, HR, vendors, regulators, oversight teams).

2	4	II.C	Define privacy metrics for oversight and governance.	Create metrics per audience and/or identify intended audience for metrics with clear processes describing purpose, value and reporting of metrics.
				Understand purposes, types and life cycles of audits in evaluating effectiveness of controls throughout organization’s operations, systems and processes.
				Establish monitoring and enforcement systems to track multiple jurisdictions for changes in privacy law to ensure continuous alignment.
1	3	II.D	Establish training and awareness activities.	Develop targeted employee, management and contractor trainings, and awareness activities at all stages of the privacy life cycle to ensure compliance.

MIN	MAX		Domain III — Privacy Program Operational Life Cycle: Assessing Data	
12	16		**Domain III — Privacy Program Operational Life Cycle: Assessing Data** encompasses how to identify and minimize privacy risks and assess the privacy impacts associated with an organization's systems, processes and products. Addressing potential problems early will help to establish a more robust privacy program.	
			COMPETENCIES	**PERFORMANCE INDICATORS**
3	5	III.A	Document data governance systems.	Map data inventories, map data flows, map data life cycle and system integrations.
				Measure policy compliance against internal and external requirements.
				Perform a gap analysis against applicable laws and/ or accepted standards.
1	3	III.B	Evaluate processors and third-party vendors.	Identify and assess risks of outsourcing the processing of personal data (e.g., contractual requirements, rules of international data transfers).
				Carry out assessments at the most appropriate functional level within the organization (e.g., procurement, internal audit, information security, physical security, data protection authority).
0	2	III.C	Evaluate physical and environmental controls.	Identify operational risks of physical locations (e.g., data centers and offices) and physical controls (e.g., document retention and destruction, media sanitization and disposal, device security).
3	5	III.D	Evaluate technical controls.	Identify operational risks of digital processing (e.g., servers, storage, infrastructure, cloud).
				Review and set limits on use and retention of personal data.
				Determine the location of data, including cross-border data flows.
2	4	III.E	Evaluate risks associated with shared data in mergers, acquisitions and divestitures.	Complete due diligence procedures.
				Evaluate contractual and data sharing obligations, including laws, regulations and standards.
				Conduct risk and control alignment.

MIN	MAX		Domain IV — Privacy Program Operational Life Cycle: Protecting Personal Data	
9	13		**Domain IV — Privacy Program Operational Life Cycle: Protecting Personal Data** outlines how to protect data assets during use through the implementation of effective privacy and security controls and technology. Regardless of size, geographic location or industry, data must be physically and virtually secure at all levels of the organization.	
			COMPETENCIES	**PERFORMANCE INDICATORS**
4	6	IV.A	Apply information security practices and policies.	Classify data to the applicable classification scheme (e.g., public, confidential, restricted).
				Understand purposes and limitations of different controls.
				Identify risks and implement applicable access controls.
				Use appropriate technical, administrative and organizational measures to mitigate risk.
1	3	IV.B	Integrate the main principles of Privacy by Design (PbD).	Integrate privacy throughout the System Development Life Cycle (SDLC).
				Integrate privacy throughout business process.
				Understand the principles and purposes of privacy by design.
3	5	IV.C	Apply organizational guidelines for data use and ensure technical controls are enforced.	Verify that guidelines for secondary uses of data are followed.
				Verify that safeguards such as policies, procedures and vendor contracts are applied.
				Ensure applicable access controls and data classifications are appropriate and effective.
				Collaborate with privacy technologists to enable technical controls for obfuscation, data minimization, security and other privacy enhancing technologies.

MIN	MAX		Domain V — Privacy Program Operational Life Cycle: Sustaining Program Performance	
7	9		**Domain V — Privacy Program Operational Life Cycle: Sustaining Program Performance** details how the privacy program is sustained using pertinent metrics and auditing procedures. As an organization moves through the cycles of managing its privacy program, it is important to ensure all processes and procedures are functioning effectively and are replicable going forward.	
			COMPETENCIES	PERFORMANCE INDICATORS
1	3	V.A	Use metrics to measure the performance of the privacy program.	Determine appropriate metrics for different objectives (e.g., trending, ROI, business resiliency).
				Analyze collected data and link to program goals and compliance measures (PIAs performed, rights requests response rates, complaints volume, data breach metrics).
1	3	V.B	Audit the privacy program.	Select applicable forms of monitoring based upon program goals (e.g., audits, controls, subcontractors).
				Complete compliance monitoring through auditing of privacy policies, controls and standards, including against industry standards, regulatory and/or legislative changes.
3	5	V.C	Manage continuous assessment of the privacy program.	Conduct risk assessments on systems, applications, processes and activities.
				Understand the purpose and life cycle for each assessment type (e.g., PIA, DPIA, TIA, LIA, PTA).
				Implement risk mitigation and communications with internal and external stakeholders after mergers, acquisitions and divestitures.

MIN	MAX	Domain VI — Privacy Program Operational Life Cycle: Responding to Requests and Incidents
10	14	**Domain VI — Privacy Program Operational Life Cycle: Responding to Requests and Incidents** documents the activities involved in responding to privacy incidents and the rights of data subjects. Based upon the applicable territorial, sectoral and industry laws and regulations, organizations must ensure proper processes for information requests, privacy rights and incident responses.

			COMPETENCIES	PERFORMANCE INDICATORS
5	7	VI.A	Respond to data subject access requests and privacy rights.	Ensure privacy notices and policies are transparent and clearly articulate data subject rights.
				Comply with organization’s privacy policies around consent (e.g., withdrawals of consent, rectification requests, objections to processing, access to data, complaints).
				Understand and comply with established global legislations around data, subjects’ rights of control over their personal information.
3	5	VI.B	Follow organizational incident handling and response procedures.	Understand and execute incident handling and response procedures (e.g., assessment, containment, remediation).
				Communicate to stakeholders in compliance with jurisdictional, global and business requirements.
				Maintain an incident register and associated records of the incident.
1	3	VI.C	Evaluate and modify current incident response plan.	Carry out post-incident reviews to improve the effectiveness of the plan.
				Implement changes to reduce the likelihood and/or impact of future breaches.