CIPM
BODY OF KNOWLEDGE AND EXAM BLUEPRINT

VERSION 4.0.0

EFFECTIVE DATE: 10/02/2023

IAPP CIPM 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 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 communicate 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

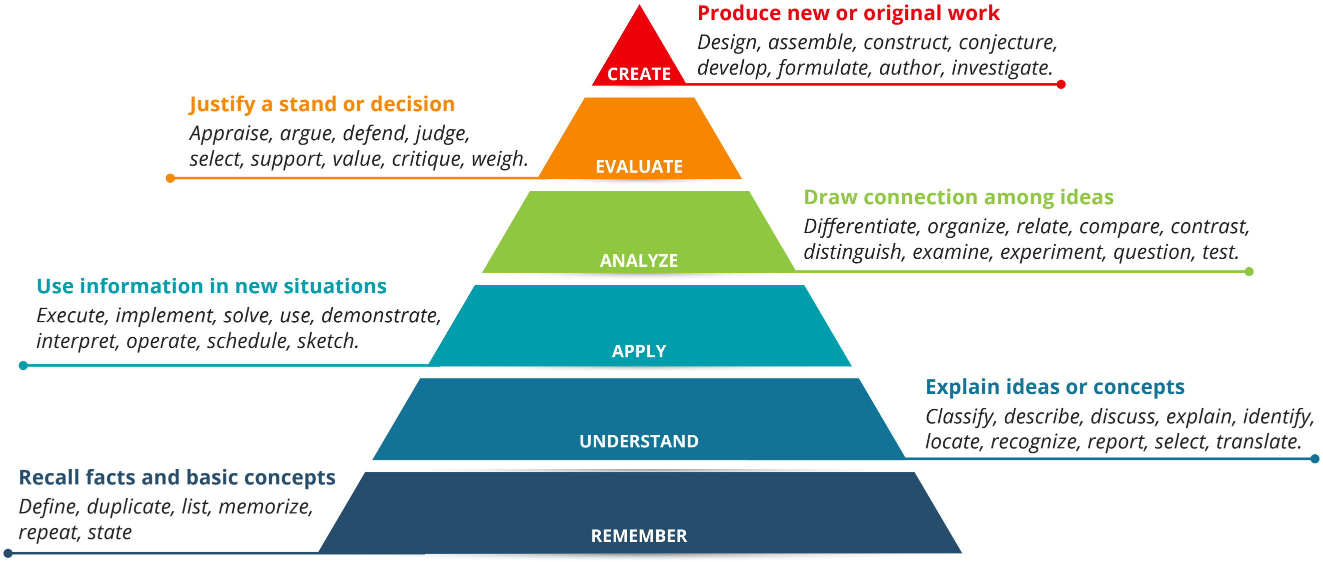
The IAPP's CIPM, CIPP/E, CIPP/US and CIPT credentials are accredited by the **ANSI National Accreditation Board (ANAB) under the International Organization for Standardization (ISO) standard 17024: 2012**.

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 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 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: 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 & develop a privacy strategy.	Choose applicable governance model.
				Identify the source, types and uses of personal information (PI) within the organization.
				Structure the privacy team.
				Identify stakeholders and internal partnerships.
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).
				Adopt privacy program vocabulary (e.g., incident vs breach).
5	7	I.C	Indicate in-scope laws, regulations and standards applicable to the program.	Understand territorial, sectoral and industry regulations and/or laws.
				Understand penalties for non-compliance.
				Understand scope and authority of oversight agencies.
				Understand privacy implications of doing business or basing operations in countries with inadequate privacy laws.

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, and 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 organization.
				Define well-designed policies related to the processing of the organization's data holdings, data sharing, taking into account both legal and ethical requirements.
				Identify collection points considering transparency and integrity limitations of collection of data.
				Create a plan for breach management.
				Create a plan for complaint handling procedures.
1	3	II.B	Clarify roles and responsibilities.	Define the roles and responsibilities for managing the sharing and disclosure of data for internal and external use.
				Define roles and responsibilities for breach response by function, including stakeholders and their accountability to regulators, coordinating detection teams (e.g., IT, physical security, HR, investigation teams, vendors) and establishing 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 at all stages of the privacy life cycle.
				Create continuous privacy program activities (e.g., education and awareness, monitoring internal compliance, program assurance, including audits, complaint handling procedures).

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.
				Determine desired state and perform gap analysis against an accepted standard or law.
1	3	III.B	Evaluate processors and third-party vendors.	Identify risks of insourcing and outsourcing data, including contractual requirements and 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 forensics and device security).
3	5	III.D	Evaluate technical controls.	Identify operational risks of digital processing (e.g., servers, storage, infrastructure and cloud).
				Review and set limits on use of personal data (e.g. role-based access).
				Review and set limits on records retention.
				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 organizational measures to mitigate any residual risk.
1	3	IV.B	Integrate the main principles of Privacy by Design (PbD).	Integrate privacy through the System Development Life Cycle (SDLC).
				Integrate privacy through business process.
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 administrative safeguards such as vendor and HR policies, procedures and contracts are applied.
				Ensure applicable employee access controls and data classifications are activated.
				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 their privacy program, it is important to ensure that 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 and analyze data collected through metrics (e.g., trending, ROI, business resiliency, PMM).
				Collect metrics to link training and awareness activities to reductions in privacy events and continuously improve the privacy program based on the metrics collected.
1	3	V.B	Audit the privacy program.	Understand the types, purposes, and life cycles of audits in evaluating effectiveness of controls throughout organization's operations, systems and processes.
				Select applicable forms of monitoring based upon program goals (e.g., audits, controls, sub-contractors) and 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.
				Ensure AI usage is ethical, unbiased, meets data minimization and purpose limitation expectations and is in compliance with any regulations and/or privacy laws.

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 and complaints).
				Understand and comply with established international, federal, and state legislations around data subject’s rights of control over their personal information (e.g., GDPR, HIPAA, CAN-SPAM, FOIA, CCPA/CPRA).
3	5	VI.B	Follow organizational incident handling and response procedures.	Conduct a risk assessment about the incident.
				Perform containment activities.
				Identify and implement remediation measures.
				Communicate to stakeholders in compliance with jurisdictional, global and business requirements.
				Engage privacy team to review facts, determine actions and execute plans.
				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 chance of further breaches.