CIPT BODY OF KNOWLEDGE AND EXAM BLUEPRINT

VERSION 3.2.0 **EFFECTIVE DATE: 2 Sept. 2024**

IAPP CIPT 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 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

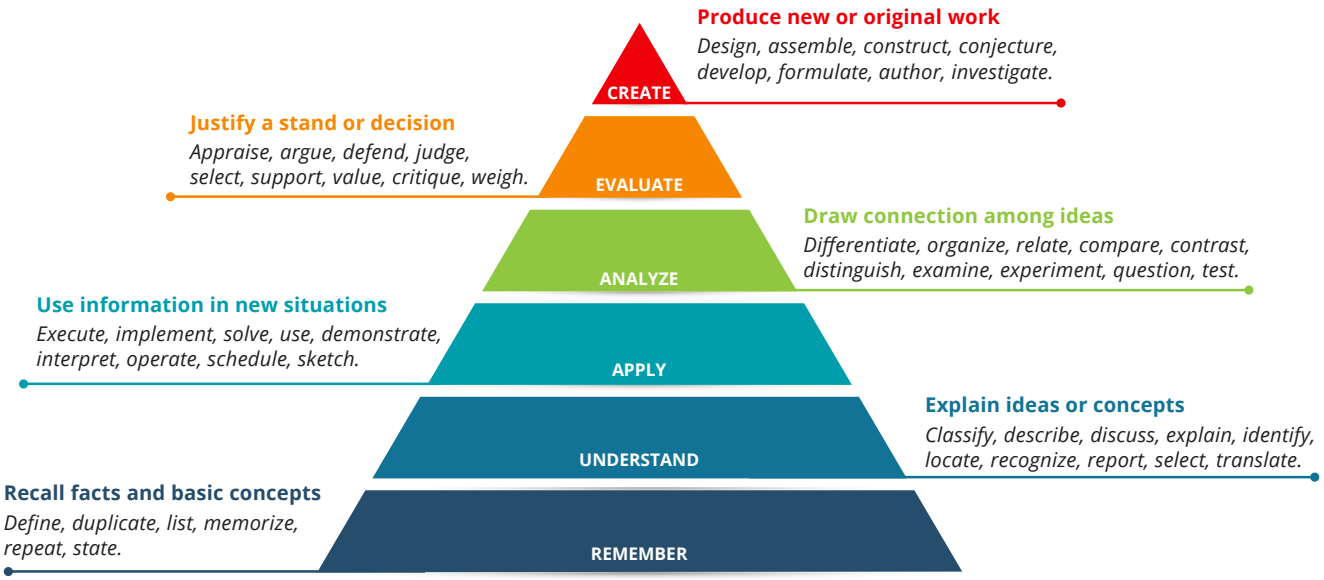
The IAPP's CIPM, CIPP/E, CIPP/US and CIPT credentials are accredited by the **ANSI National Accreditation Board (ANAB) under the International Organization for Standardization (ISO) standard 17024: 2012**.

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.

IAPP CIPT 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 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 — Foundational principles		
13	15	**Domain I — Foundational principles addresses the models, frameworks and technology concepts** that are essential to understanding and implementing privacy solutions.		
		COMPETENCIES		**PERFORMANCE INDICATORS**
1	3	I.A	Demonstrate knowledge of privacy risk models and frameworks and their roles in laws and guidance.	Apply FIPPs and OECD principles.
				Apply privacy frameworks (e.g., NIST/NICE, ISO/IEC 27701 and BS10012 Privacy Information Management System).
				Apply the concept of Nissenbaum's Contextual Integrity.
				Apply Calo's Harms Dimensions.
				Apply the Factor Analysis in Information Risk (FAIR) model.
3	5	I.B	Demonstrate knowledge of privacy by design principles.	Apply the principle of end-to-end security — full life cycle protection.
				Apply the principle of privacy embedded into design.
				Apply the principle of full functionality — positive-sum not zero-sum.
				Apply the principle of visibility and transparency.
				Apply the principle of proactive not reactive.
				Apply the principle of privacy by default.
				Apply the principle of respect for user privacy.

3	5	I.C	Demonstrate knowledge of privacy-related technology fundamentals.	Understand risk concepts (e.g., threat, vulnerability, attack, security exploit).
				Recognize the occurrence of a personal data breach and other types of privacy incidents.
				Identify privacy and security practices within an organization.
				Recognize how technology supports information governance in an organization.
				Implement internal and external data protection and privacy notices.
				Implement internal data protection and privacy policies, guidelines and procedures.
				Analyze third-party contracts and agreements.
				Catalog data assets, develop a data inventory and implement a Record of Processing Activities (RoPA).
				Understand enterprise architecture and use of data flow diagrams/data lineage tools, including cross-border transfer considerations.
				Complete data protection and privacy impact assessments (DPIA/PIAs).
				Identify privacy-related key risk indicators (KRIs) and key performance indicators (KPIs).
3	5	I.D	Demonstrate knowledge of the data life cycle.	Recognize privacy's role in data collection.
				Recognize privacy's role in data use.
				Recognize privacy's role in data disclosure.
				Recognize privacy's role in data transfer.
				Recognize privacy's role in data retention.
				Recognize privacy's role in data destruction.

MIN	MAX	Domain II — The privacy technologist's role in the context of the organization		
7	9	**Domain II — The privacy technologist's role in the context of the organization addresses** the general and technical responsibilities inherent to the role of the privacy technologist.		
		COMPETENCIES		**PERFORMANCE INDICATORS**
3	8	II.A	Identify and implement general 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).
				Implement privacy standards and frameworks.
				Analyze contractual and regulatory privacy and data protection requirements.
				Translate legal and regulatory requirements into practical technical and/or operational solutions.
				Consult on privacy notices and policies.
3	5	II.B	Identify and implement technical roles and responsibilities.	Analyze and implement technical measures for privacy and security practices.
				Advise on the privacy implications of new uses of existing technologies or new and emerging technologies.
				Advise on the effective selection and implementation during development or acquisition of products that impact privacy.
				Advise on privacy and data protection impact assessments (PIAs and DPIAs) in system development.
				Advise on privacy by design implementation via privacy engineering in systems engineering processes.
				Support individual's' privacy rights requests (e.g., access, deletion).

3	5	II.B	Identify and implement technical roles and responsibilities.	Support records of processing activities (RoPAs), data inventories and data flow mapping.
				Support oversight of technical elements of privacy operations and audits, including third-party assessments.
				Develop, compile, report, and monitor privacy key risk indicators (KRIs) and key performance indicators (KPIs).
				Provide technical privacy support to identify and respond to privacy breaches and other types of incidents.

MIN	MAX	Domain III — Privacy risks, threats and violations		
15	19	**Domain III — Privacy risks, threats and violations 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**
0	4	III.A	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).
2	6	III.B	Demonstrate how to minimize privacy risk during personal data collection.	Minimize privacy risk involved when collecting personal data from individuals.
				Employ privacy-enhancing techniques for high-risk personal data processing methods (e.g., tracking, surveillance).
				Demonstrate understanding of consent requirements when collecting personal data.
				Implement measures to manage privacy risks associated with automatic collection of personal data.
				Implement measures to correct personal data inaccuracies.
				Leverage techniques to minimize risk when extracting personal data from publicly available sources.
				Understand the jurisdictional implications of personal data collection (e.g., localization, government access).

2	6	III.C	Demonstrate how to minimize privacy risk during personal data use.	Use technical approaches that minimize the risks associated with: a. Securing the data. b. Identification/reidentification of previously de-identified data. c. Use of data aggregation. d. Secondary uses of personal data. e. Profiling.
2	6	III.D	Demonstrate how to minimize privacy risk during personal data dissemination.	Use technical approaches that minimize the 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.
0	3	III.E	Demonstrate how to minimize the threat of intrusion and decisional interference.	Implement technical approaches that minimize the risks associated with the use of behavioral advertising.
				Employ technical approaches that minimize the threat of cyberbullying.
				Use technical approaches that minimize the threat of social engineering.
				Avoid the use of dark patterns that limit privacy-preserving response options.
0	3	III.F	Identify privacy risks related to software security.	Understand measures to fix software vulnerabilities.
				Leverage intrusion detection and prevention tools and techniques.
				Implement measures to reduce privacy risks during change management (e.g., patches, upgrades).
				Utilize open-source versus closed-source software.
				Recognize possible privacy violations by service providers.

MIN	MAX	Domain IV — Privacy-enhancing strategies, techniques and technologies		
9	11	**Domain IV — Privacy-enhancing strategies, techniques and technologies addresses the methods used to fortify data assets during the data life cycle.** This domain involves the application of efficient privacy and security design approaches, as well as the integration of effective controls and cutting-edge technology.		
			COMPETENCIES	**PERFORMANCE INDICATORS**
2	4	IV.A	Identify and implement appropriate data-oriented strategies.	Implement data processing segregation to mitigate risk of linking and correlating personal data with other datasets.
				De-identify personal data by making it un-linkable or unobservable so that it cannot be discovered or traced back to its original user/identifier.
				Minimize personal data collection and use only what is necessary for the purposes for which the data was originally collected.
				Abstract personal data by reducing data precision while maintaining data accuracy and suitability for a specific use case.
2	4	IV.B	Identify and implement appropriate process-oriented strategies.	Inform individuals about how their personal data is processed.
				Provide data subjects with control over the processing of their personal data, including the ability to consent to data collection, use, disclosure, retention and destruction.
				Enforce processing of personal data that aligns with privacy risk reduction in policies and procedures.
				Demonstrate compliance with privacy laws, regulations, standards, frameworks, guidelines, policies and procedures.

3	5	IV.C	Identify and implement appropriate data protection strategies (e.g., privacy-enhancing techniques).	Use data analysis and other procedures and techniques to minimize the privacy risk associated with the aggregation of personal data.
				Employ privacy-enhancing techniques (e.g., anonymization or pseudonymization) to reduce risk exposure.
				Implement de-identification techniques (e.g., encryption) to protect personal data.
				Implement other defense in-depth techniques (e.g., identity and access management, authentication mechanisms) to protect personal data from risk exposure.
				Understand and effectively navigate the technological implications of requirements stemming from privacy regulations and the relevant techniques needed to address them: a. Processing/verification of data subject rights requests regarding their ability to view or manage their personal data. b. Notice and consent requirements. c. Data retention requirements. d. Privacy incident reporting requirements.

MIN	MAX	Domain V — Privacy by design		
8	10	**Domain V — Privacy by design addresses 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**
2	4	V.A	Implement the privacy by design methodology.	Define and communicate privacy goals and objectives to guide privacy by design within an organization.
				Document privacy requirements encompassing regulatory and organizational policies to ensure alignment with privacy by design principles.
				Incorporate privacy considerations into the design process by understanding relevant quality attributes, such as predictability, manageability and disassociability.
				Demonstrate how the principles of privacy risk are embedded into the design process.
				Interpret high-level specifications and align them via low-level specifications with the privacy by design principles.
1	3	V.B	Evaluate privacy risks in user experiences.	Assess potential impact of design choices on user behavior.
				Incorporate understanding of user experience (UX) concepts into the design of privacy-related functions.
				Implement clear and accessible privacy notices, settings and consent management mechanisms.
				Perform usability testing where relevant to assess effectiveness of privacy-related functions.
1	3	V.C	Implement Value Sensitive Design.	Understand how value sensitive design affects users.
				Apply value sensitive design aligned with privacy by design principles.

1	3	V.D	Manage and monitor privacy-related functions and controls.	Conduct privacy audits and IT control reviews.
				Conduct code reviews to identify potential privacy gaps that require attention.
				Conduct runtime behavior monitoring.
				Implement data management practices in production and nonproduction environments.

MIN	MAX	Domain VI — Privacy engineering		
10	12	**Domain VI — Privacy engineering addresses 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**
2	4	VI.A	Understand the role of privacy engineering in the organization.	Recognize aspects of effective implementation of privacy engineering.
				Identify technological controls to use for privacy engineering.
				Integrate privacy into the system development life cycle.
2	4	VI.B	Understand and implement privacy engineering objectives.	Apply predictability in privacy engineering activities.
				Apply manageability in privacy engineering activities.
				Apply disassociability in privacy engineering activities.
2	4	VI.C	Identify and evaluate privacy design patterns.	Recognize which privacy preserving design patterns to emulate.
				Recognize which dark patterns to avoid.
1	3	VI.D	Manage privacy risks in the development life cycle.	Impose multifaceted privacy controls throughout the development life cycle: a. Architect — Implement privacy controls at the architectural level. b. Secure — Implement measures to safeguard data in alignment with privacy requirements. c. Supervise — Establish monitoring mechanisms to ensure ongoing compliance with privacy regulations. d. Balance — Attain a balance between privacy protection and functional requirements.

MIN	MAX	Domain VII — Evolving or emerging technologies in privacy
5	7	**Domain VII — Evolving or emerging technologies in privacy addresses understanding and minimizing privacy risk** regarding use of types of current and advancing technologies with privacy implications, including robotics, the Internet of Things, e-commerce, biometrics, technology in the workplace, communications technologies, and advanced computing and other innovative technology approaches.

			COMPETENCIES	PERFORMANCE INDICATORS
0	2	VII.A	Understand the privacy implications of the use of robotics and Internet of Things (IoT).	Identify and minimize privacy risk involved when using wearable devices.
				Identify and minimize privacy risk involved when using smart home devices and IoT technology for smart cities (e.g., CCTV, tracking/surveillance).
				Identify and minimize privacy risk involved when using robots, including drones.
0	2	VII.B	Understand the privacy implications of the use of e-commerce.	Identify and minimize privacy risk involved when using adtech.
				Identify and minimize privacy risk involved when using cookies and other web tracking technologies.
				Identify and minimize privacy risk involved when using alerts and notifications.
				Identify and minimize privacy risk involved when using location tracking.
				Identify and minimize privacy risk involved when using chatbots.
				Identify and minimize privacy risk involved when using behavioral profiling.
				Identify and minimize privacy risk involved when using online/mobile payments.
0	2	VII.C	Understand the privacy implications of the use of biometrics.	Identify and minimize privacy risk involved when using facial recognition.
				Identify and minimize privacy risk involved when using speech recognition.
				Identify and minimize privacy risk involved when using fingerprint identification.
				Identify and minimize privacy risk involved when using DNA.

0	2	VII.D	Understand the privacy implications of the use of technology in the workplace.	Identify and minimize privacy risk involved when using shared data centers.
				Identify and minimize privacy risk involved when using data management and analytics.
				Identify and minimize privacy risk involved when using third-party vendor IT solutions.
				Identify and minimize privacy risk involved when using remote work.
				Identify and minimize privacy risk involved when using video calls and conferencing.
				Identify and minimize privacy risk involved when using Next Gen infrastructure deployment models (e.g., edge computing, cloud-based infrastructure).
				Identify and minimize privacy risk involved when using artificial intelligence (AI), machine learning (ML) and deep learning.
				Identify and minimize privacy risk involved when using quantum computing.
				Identify and minimize privacy risk involved when using blockchain, cryptocurrencies and non-fungible tokens (NFT).
				Identify and minimize privacy risk involved when using virtual/augmented reality.
0	2	VII.E	Understand the privacy implications of the use of communications technologies.	Identify and minimize privacy risk involved when using online platforms providing communications via text, voice, video and/or photo (e.g., social media, gaming platforms).
				Identify and minimize privacy risk involved when using mobile devices.
				Identify and minimize privacy risk involved when using messaging and video calling.