

iapp



CIPP/CN Body of Knowledge and Exam Blueprint

Version 1.0.0

Effective date: 3 June 2024



IAPP CIPP/CN 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

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.**

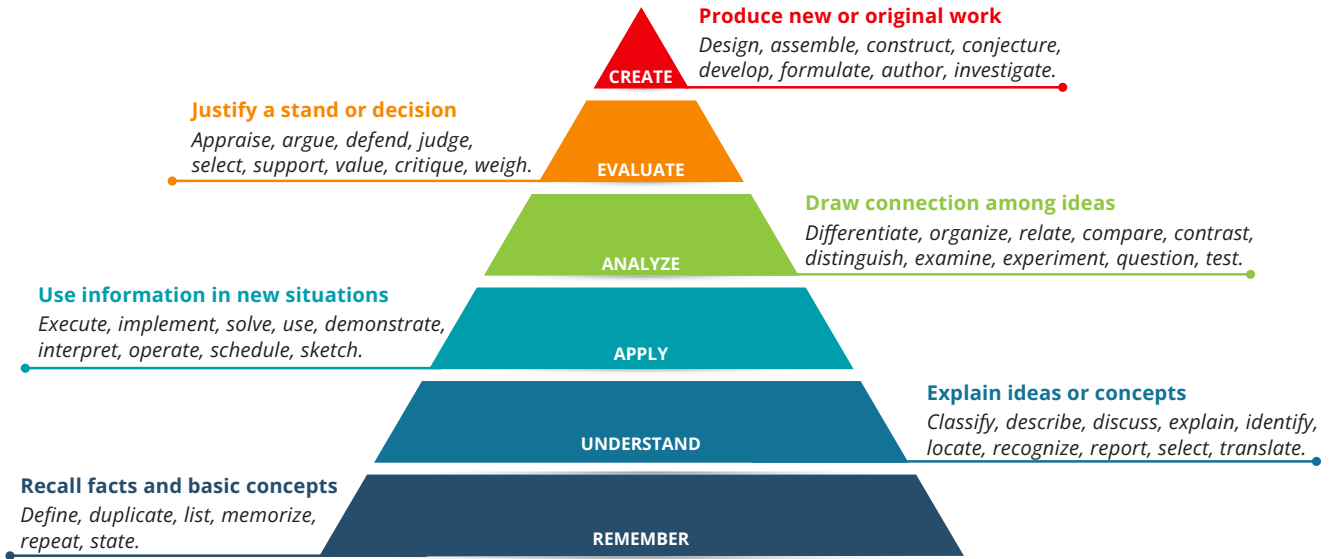
ANAB is an internationally recognized accrediting body that assesses and accredits certification programs that meet rigorous standards.

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 CIPP/CN 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.



IAPP CIPP/CN BODY OF KNOWLEDGE

MIN MAX Domain I: Introduction to Personal Information Protection in China

6 8

Domain I: “Introduction to Personal Information Protection in China” provides a foundational understanding of Chinese personal information protection laws and concepts including the roles of supervisory authorities – general, sectoral and judicial – in enforcing privacy laws.

COMPETENCIES

PERFORMANCE INDICATORS

4 5 I.A	Understand the main concepts of China’s statutory and regulatory frameworks.	Understand the parts of the Constitution of the People’s Republic of China that relate to personal information protection.
		Understand the provisions of the Civil Code that relate to personal information protection.
		Understand criminal law that relates to personal information protection.
		Understand the basics of Consumer Protection Law.
		Understand the basics of Minor Protection Law.
		Understand the main concepts of the Cybersecurity Law (CSL), including Critical Information Infrastructure (CII) Protection and the Multi-level Protection Scheme (MLPS).
		Understand the main concepts of the Data Security Law (DSL).
		Understand the purpose of the Personal Information Protection Law (PIPL).
		Understand administrative regulations related to personal information protection.
		Understand local rules and regulations related to personal information protection.
3 4 I.B	Understand the different roles and responsibilities of the supervisory authorities.	Understand the sectoral regulations related to personal information protection.
		Understand the national/industry standards and specifications related to personal information protection.
		Understand the roles of the General Authorities: <ul style="list-style-type: none"> • Cyberspace Administration of China (CAC). • Ministry of Public Security (MPS). • Ministry of Industry and Information Technology (MIIT). • State Administration for Market Regulation (SAMR).
3 4 I.B	Understand the different roles and responsibilities of the supervisory authorities.	Understand the roles of the Sectoral Regulatory Authorities: <ul style="list-style-type: none"> • People’s Bank of China (PBOC). • National Financial Regulatory Administrative (NFRA). • National Health Commission (NHC).
		Understand the roles of the judicial bodies, including The Supreme People’s Court and The Supreme People’s Procuratorate.



IAPP CIPP/CN BODY OF KNOWLEDGE

MIN MAX Domain II: The Personal Information Protection Law

36 39 **Domain II: “The Personal Information Protection Law”** focuses on elements such as the law’s scope of application. It defines personal information protection concepts as outlined in PIPL, clarifies the principles that inform personal information processing activities and provides guidance on compliance regarding personal information processing and personal information subjects’ rights. The domain outlines implementation of cross-border transfers and accountability procedures and requirements for internal and external stakeholders. It includes understanding PIPL enforcement penalties and reporting requirements as well as when personal information is used in automated decision-making.

COMPETENCIES

PERFORMANCE INDICATORS

4 5 II.A Understand the Personal Information Protection concepts as defined in PIPL.	Understand what is personal information.
	Understand the definition of a personal information subject.
	Understand what is sensitive personal information.
	Understand the requirements for data de-identification and anonymization.
	Understand the requirements for processing of personal information.
	Understand the consent and separate consent requirements.
	Understand the general obligation of personal information processors and the special obligations for large internet platform operators.
	Understand what an entrusted party is.
	Understand the requirements for personal information protection impact assessments (PIPIA).
	Understand the regulations governing cross-border data transfers.
3 4 II.B Understand the principles that inform personal information processing activities.	Understand the main responsibilities of the personal information protection officer (China DPO).
	Understand what it means for data processing to be lawful, legitimate and necessary.
	Understand what it means for data processing to be done in good faith.
	Understand what it means for data processing to be transparent.
	Understand purpose limitation in data processing.
	Understand what data minimization is and ensure minimum impact during processing activities.
	Understand the importance of data quality.
	Understand the importance of data security.
Understand the importance of accountability.	



IAPP CIPP/CN BODY OF KNOWLEDGE

MIN		MAX		Domain II: The Personal Information Protection Law		
			COMPETENCIES	PERFORMANCE INDICATORS		
2	3	II.C	Understand the scope of application of the Personal Information Protection Law.	Know the material scope, territorial scope and extra-territorial jurisdiction of PIPL.		
				Know the exceptions to the scope of PIPL.		
4	6	II.D	Comply with the legal requirements for personal information processing.	Ensure compliance with consent requirements.		
				Ensure compliance with the requirements necessary for the conclusion or performance of a contract or HR management.		
				Ensure compliance with the requirements necessary for the performance of statutory duties or legal and regulatory obligations.		
				Ensure compliance with the requirements necessary for the response to public health emergencies or necessary for the protection of life or asset in urgent situation.		
				Ensure personal information is reasonably processed for media reporting or media supervision in the public interest.		
				Ensure the reasonable processing of self-disclosed or legally disclosed information.		
6	7	II.E	Ensure organizational compliance with personal information subject's rights.	Ensure compliance with processing requirements in other circumstances as provided by laws or administrative regulations.		
				Ensure compliance with the specific requirements for Sensitive Personal Information processing.		
				Ensure procedures are in place to inform data subjects of their:		
				<ul style="list-style-type: none"> • Right to be informed. • Right to access. • Right to rectification. • Right to deletion. • Right to withdraw consent. • Right to restrict or refuse processing. • Right to refuse automated decision-making. • Right to request explanation. • Right to bring claims against processing entities. • Rights as next-of-kin of deceased individuals. • Right to personal information portability. 		
				Conduct a security assessment.		
				Obtain a personal information protection certification.		
5	6	II.F	Implement the requirements for cross border data transfers.	Conclude standard contractual clauses.		
				Comply with other conditions under laws, regulations or those stipulated by the CAC.		
				Ensure compliance with international treaties or agreements when applicable.		



IAPP CIPP/CN BODY OF KNOWLEDGE

MIN	MAX	Domain II: The Personal Information Protection Law	
		COMPETENCIES	PERFORMANCE INDICATORS
4	5	II.G Ensure accountability procedures and requirements for internal and external stakeholders are developed and implemented.	<ul style="list-style-type: none"> Develop and maintain a record of data processing. Ascertain different roles in personal information sharing and design proper contracts. <ul style="list-style-type: none"> a. Joint personal information processors. b. Personal information processor and entrusted party. Understand the requirements for the personal information protection officer. Contribute to the development of corporate privacy policies. Develop privacy notices and present to the personal information subject properly. Ensure compliance with personal information retention requirements. Conduct personal information protection impact assessments. Ensure that unauthorized access to, and breach, tampering or loss of personal information is prevented. Ensure that the personal information protection authority and impacted individuals are notified in the event of personal information breaches. Ensure that security requirements to prevent personal information breaches are implemented.
3	4	II.H Understand PIPL enforcement penalties and reporting requirements.	<ul style="list-style-type: none"> Understand what constitutes PIPL criminal offenses. Understand the administrative corporate and individual penalties for PIPL violations. Process complaints and reports related to PIPL violations. Conduct public interest actions.
4	5	II.I Understand the requirements when personal information is used in automated decision-making.	<ul style="list-style-type: none"> Ensure the requirements for transparency, fairness and impartiality are implemented.



IAPP CIPP/CN BODY OF KNOWLEDGE

MIN MAX Domain III: Sectoral Regulations and Compliance

28 32 **Domain III: “Sectoral Regulations and Compliance”** details compliance with sectoral-specific laws including those relevant to criminal records processing, Internet applications (apps) and electronic marketing, and child and minor protection. It also details compliance to sectoral regulatory requirements with regards to personal information processing by banks and financial institutions, Internet platforms, the automotive Industry, and employers. Responsible governance within emerging technologies, plus collection and processing restrictions of health and human genetic data are also addressed.

COMPETENCIES

PERFORMANCE INDICATORS

2	3	III.A	Ensure criminal records processing conforms to data processing requirements.	Understand the criminal penalties for personal information encroachment.
				Conduct criminal records inquiries.
3	4	III.B	Ensure compliance with the Internet applications (apps) and electronic marketing laws.	Ensure compliance with the personal information collection requirements of electronic marketing and apps laws.
				Ensure data minimization for apps and mini-programs is practiced.
				Implement prohibition against bundled consent and know the distinction between basic functions and non-basic functions.
				Ensure personal Information sharing with third parties (e.g., software development kits) is lawful.
3	4	III.C	Ensure compliance with child and minor protection laws.	Ensure compliance with SMS/e-mail marketing laws.
				Ensure privacy and personal information protection for minors.
4	5	III.D	Ensure compliance with processing requirements for banks and financial institutions	Ensure compliance with the regulation on the Protection of Children’s Personal Information Online.
				Understand consumer protection laws.
4	5	III.E	Understand the regulatory obligations that apply to Internet platforms.	Understand security obligations in the financial sector.
				Ensure compliance with industry regulators’ issued rules (People’s Bank of China (PBOC), National Financial Regulatory Administrative (NFRA), China Securities Regulatory Commission (CSRC)).
				Establish a personal information protection compliance system and ensure independent oversight.
4	5	III.E	Understand the regulatory obligations that apply to Internet platforms.	Understand platform governance obligations that apply to product / service providers’ processing of personal information.
				Ensure the release of social responsibility reports documenting personal information protection.



IAPP CIPP/CN BODY OF KNOWLEDGE

MIN	MAX	Domain III: Sectoral Regulations and Compliance	
		COMPETENCIES	PERFORMANCE INDICATORS
5	5	III.F Understand personal information processing requirements in the automotive industry.	<p>Understand security management requirements of automotive data.</p> <p>Ensure the lawful processing of vehicle-collected data.</p> <p>Understand the data processing requirements associated with connected and autonomous vehicles.</p>
2	3	III.G Ensure responsible governance of emerging technologies.	<p>Understand the Cyberspace Administration of China's measures for the management of generative artificial intelligence services.</p> <p>Understand consent requirements for the use of facial recognition technology.</p> <p>Understand algorithm use restrictions as detailed in the Algorithm Recommendation Regulation.</p>
3	4	III.H Ensure compliance with personal information processing requirements in an employment context.	<p>Ensure non-discrimination in employee recruitment.</p> <p>Ensure compliance with background check requirements.</p> <p>Understand limitations on workplace monitoring and surveillance (e.g., embedded software and CCTV).</p> <p>Understand the requirements for protecting personal information during internal investigations.</p>
2	3	III.I Ensure compliance with collection and processing restrictions of health and human genetic data.	<p>Ensure the protection and sharing limitations of sensitive personal health information.</p> <p>Secure doctor-patient confidentiality.</p> <p>Understand the restrictions on the collection, preservation and exploitation of Chinese human genetic resources implemented by the Human Genetic Resources Administration.</p>