iapp

CIPP/AU Body of Knowledge and Exam Blueprint

VERSION 1.0

EFFECTIVE DATE: 30 June 2026

IAPP CIPP/AU 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's exam development board and scheme committee. The BoK is reviewed every year and updated if necessary. 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 content in the body of knowledge 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 IS THE CIPP/AU CERTIFICATION?

The Certified Information Privacy Professional/Australia certification is designed for privacy professionals seeking to demonstrate a foundational understanding of Australian privacy law and practice. It recognises the legal, regulatory and operational considerations that shape privacy compliance in Australia.

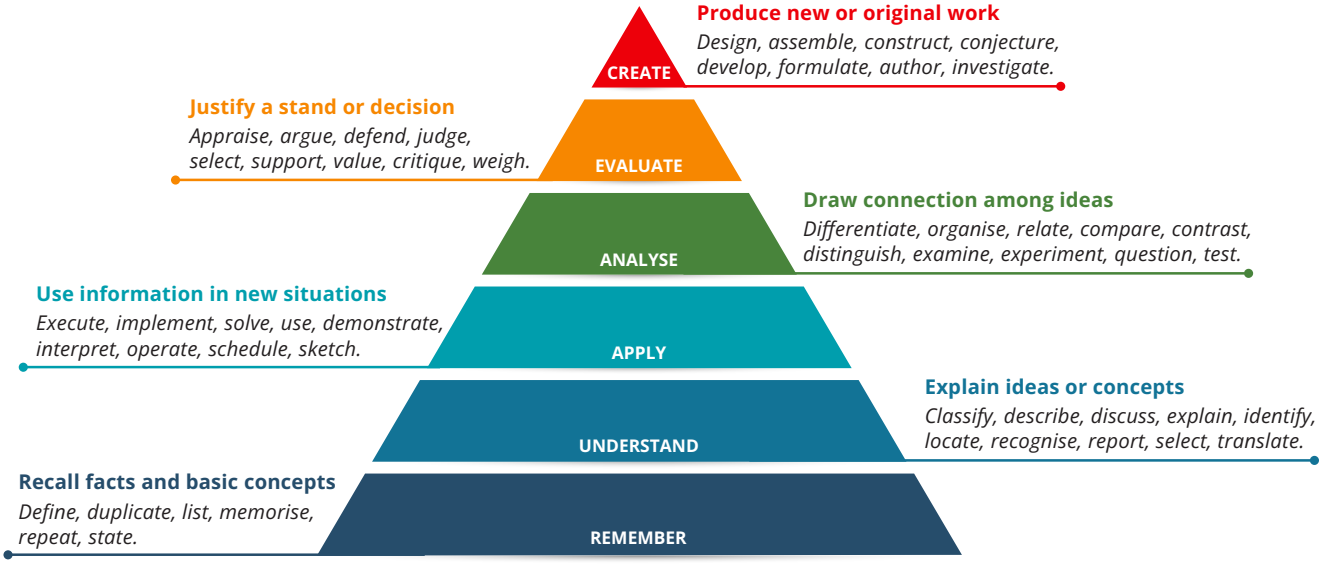
Grounded in the Privacy Act and the Australian Privacy Principles, Australia's privacy framework continues to evolve in response to developments in technology, data governance, cybersecurity, artificial intelligence and cross-border data flows. It is also being shaped by ongoing Privacy Act reforms and the Office of the Australian Information Commissioner (OAIC)'s heightened expectations and expanded enforcement powers, which are increasing the need for strong privacy governance and accountability.

The certification establishes a common professional standard for Australian privacy practice and supports professionals in applying these requirements in practical, risk-informed ways that promote responsible data handling, compliance and informed business decision-making.

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).

IAPP CIPP/AU 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 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 / Analyse 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 organisation?
- 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: The Regulatory Context of Australian Privacy		
14	18	**Domain I: The Regulatory Context of Australian Privacy** focuses on the federal legislative framework underpinning Australian privacy. It looks at the historical development and scope of state, territory and federal Australian privacy laws, and how these apply to contemporary issues like artificial intelligence. Additionally, the privacy obligations of government agencies under both the Privacy Act and the Australian Government Agencies Privacy Code are covered in this domain.		
			Competencies	**Performance Indicators**
6	10	I.A	Understand the federal legislative framework for Australian data protection	Know the basic structure of the Australian legal framework, and understand the role it plays in Australian privacy law.
				Understand the historical development of the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).
				Understand the Privacy Act's scope of application, its key components and the exemptions applicable to it (e.g., those afforded to the media, small businesses and political parties).
				Understand Australia's approach to AI regulation, and the ways in which it relies on existing laws to manage emerging AI risks; know relevant guidance published by the Office of the Australian Information Commissioner (OAIC), the National AI Centre (NAIC), and others.
3	5	I.B	Understand the privacy obligations of Australian federal government agencies	Understand the responsibility of government agencies to adhere to the Privacy Act.
				Understand the differences in exemptions from APP entities.
				Understand the Australian Government Agencies Privacy Code, including its provisions for privacy management plans, privacy officers, privacy impact assessments, and how these governance requirements support compliance with the Privacy Act, including the Notifiable Data Breaches scheme.
				Understand the importance of identifying and prioritising privacy risks for an agency, and the role privacy impact assessments (PIAs) play in doing so.
				Understand the requirements for, and the roles of, the Privacy Officer and Privacy Champion.
3	5	I.C	Understand Australia's state and territory privacy laws	Know the foundational laws that regulate the collection, storage and disclosure of personal information in the Australian Capital Territory, New South Wales, Northern Territory, Queensland, Tasmania, Victoria and Western Australia.
				Understand key principles of the various state and territory laws, including significant similarities and differences between them.
				Understand the roles and functions of jurisdictional regulators.
				Understand how the Privacy Act intersects with various state and territory laws, taking into account significant similarities and differences between them.

MIN	MAX	Domain II: The Australian Privacy Principles (APPs)		
21	25	**Domain II: The Australian Privacy Principles (APPs)** covers key aspects of the 13 Australian Privacy Principles, specifically the core requirements organisations must adhere to when handling, using and managing personal information. Also emphasise are the kinds of knowledge and skills needed to operationalise these principles in a comprehensive privacy program.		
			Competencies	**Performance Indicators**
3	**5**	**II.A**	Understand key considerations of personal information privacy	Understand the requirements governing the open and transparent management of personal information, and the obligations of APP entities to ensure that practices, procedures and systems are implemented in compliance with the APPs; adhere to the privacy by design (PbD) process, conducting privacy impact assessments (PIAs) when necessary; ensure that readily available privacy policies containing all required information are maintained. (APP 1)
				Understand the requirements governing individual rights to anonymity and pseudonymity when dealing with an APP entity in relation to a particular matter, and know the exemptions that apply to these rights. (APP 2)
4	**6**	**II.B**	Understand issues related to the collection of personal information	Understand the requirements governing the collection of solicited personal information, including the restrictions regarding sensitive and non-sensitive information; ensure that these types of information are collected through acceptable means, specifically in regard to issues involving consent. (APP 3)
				Understand the requirements governing the collection of unsolicited personal information, including the accepted means of using or disclosing it; adhere to requirements for the destruction or de-identification of unsolicited personal information where applicable. (APP 4)
				Understand notification requirements in regard to the collection of personal information; ensure that individuals are provided with required information such as contact details, the purpose(s) for collection, disclosure information, and that the collection rights guaranteed to the individual by the APP entity's privacy policy are honoured. (APP 5)

MIN	MAX	Domain II: The Australian Privacy Principles (APPs)		
			Competencies	Performance Indicators
4	6	II.C	Understand issues related to dealing with personal information	Understand the requirements governing the use and disclosure of personal information, including restrictions and exemptions (direct marketing, government identifiers) and the additional requirements placed upon agencies and organisations; adhere to the provision for de-identifying personal information prior to use or disclosure where applicable. (APP 6)
				Understand the requirements governing direct marketing, including the exceptions allowed for sensitive and non-sensitive personal information and for contracted service providers; ensure that individuals' rights to opt out of receiving direct marketing communications are honoured, and know how these rights are affected by other legislation such as the Do Not Call Register Act 2006 and the Spam Act 2003. (APP 7)
				Understand the requirements governing the cross-border disclosure of personal information; adhere to processes that ensure overseas recipients comply with all applicable APPs, and recognise situations in which exceptions to this rule applies. (APP 8)
				Understand the requirements governing the adoption, use or disclosure of government related identifiers, and know the exceptions allowed for agencies and organisations. (APP 9)
4	6	II.D	Understand issues regarding the integrity of personal information	Understand the requirements governing the quality of personal information; ensure that any personal information collected is accurate, up-to-date and complete and that any personal information used or disclosed is accurate, up-to-date, complete and relevant. (APP 10)
				Understand the requirements governing the security of personal information; ensure that technical and organisational measures are taken to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure; adhere to destruction or de-identification requirements when circumstances require it; understand the criteria of the Notifiable Data Breach (NDB) Scheme and adhere to its notification requirements. (APP 11)

MIN	MAX	Domain II: The Australian Privacy Principles (APPs)	Competencies	Performance Indicators
3	5	II.E	Understand issues regarding access to, and correction of, personal information	Understand the requirements related to individuals' right of access; honour specified obligations when dealing with an access request, such as appropriate response times and fees; know the conditions required for refusing an access request, and ensure that individuals are provided with a written notice detailing reasons for the refusal and the complaint mechanisms available; understand access exceptions afforded to agencies and organisations. (APP 12)
				Understand the requirements related to individuals' right of correction; recognise the conditions under which an individual's correction request must be honoured and what steps must be taken to ensure that the individual's information is accurate, up to date, complete, relevant and not misleading; understand the requirements for refusing a correction request, and ensure that individuals whose requests are refused are provided with a written notice detailing reasons for the refusal and the complaint mechanisms available to them. (APP 13)

MIN	MAX	Domain III: Australian Privacy Enforcement		
10	14	**Domain III: Australian Privacy Enforcement** focuses on the Office of the Australian Information Commissioner (OAIC), specifically in terms of its roles, functions and enforcement powers. The domain also examines the relationship between the OAIC and other regulatory bodies, and considers how the regulatory framework as a whole adapts to new privacy-related challenges.		
			Competencies	**Performance Indicators**
3	5	III.A	Understand the roles of regulators	Know the roles and functions of the Office of the Australian Information Commissioner (OAIC), including its enforcement powers.
				Understand the OAIC's regulatory escalation model, and the various enforcement mechanisms it encompasses.
				Know the OAIC's annual regulatory priorities, such as privacy policies and cyber security.
1	3	III.B	Understand regulatory intersections	Understand the overlap in regulatory jurisdictions between OAIC, ACCC, eSafety Commissioner, ACMA etc.
2	4	III.C	Understand concepts regarding infringements and penalties	Understand the OAIC's procedures for handling infringements, the penalties that may be issued as a result, and the role that case law plays in the enforcement process.
				Know when statutory torts may result from severe invasions of privacy.
2	4	III.D	Understand evolving regulatory issues	Understand how the regulatory framework adapts to new challenges, such as those involved in NDB schemes, AI, digital IDs, open data and cyber security; know OAIC and ACSC guidance on these topics.

MIN	MAX	Domain IV: Special Cases Involving Personal Information		
17	21	**Domain IV: Special Cases Involving Personal Information** covers privacy issues in areas such as health, finance, children's privacy, employment and surveillance, stressing the unique challenges posed by each, and the ways in which these areas are regulated by both the Privacy Act and other laws.		
			Competencies	**Performance Indicators**
3	5	IV.A	Understand Australian health privacy laws and practices	Understand how Australian law defines and categorises health information.
				Know the legislative frameworks that govern health information's collection, use and disclosure, including the My Health Records Act 2012, and equivalent state-based health privacy instruments.
				Understand the privacy implications of emerging health technologies, including wearables, AI-driven clinical tools such as AI scribes, software as a medical device, etc.
				Assess inferential risk and secondary use obligations of health information, including where it is collected or inferred about individuals in employment contexts through workplace monitoring and health programs.
3	5	IV.B	Understand Australian financial privacy protections	Understand how the Privacy Act regulates the protection of financial information.
				Know which types of financial institutions (e.g. banks, credit providers, insurers) are subject to the Privacy Act and other laws.
				Understand the role of the Consumer Data Right (CDR) framework and how it relates to financial information.
2	4	IV.C	Understand how children's privacy issues are governed by Australian privacy law	Understand the privacy obligations when organisations collect or process personal information belonging to children.
				Understand the interaction between the Online Safety Act 2021, the Children's Online Privacy Code, the Privacy Act and OAIC guidance on children's privacy.

MIN	MAX		Domain IV: Special Cases Involving Personal Information	
			Competencies	**Performance Indicators**
3	5	IV.D	Understand employment privacy protections in Australia	Understand how the Privacy Act governs how private-sector employers handle personal information, and know the exemptions available for organisations processing employee records.
				Understand how workplace surveillance is regulated, including by state-specific laws (e.g., NSW Workplace Surveillance Acts).
				Understand the requirements for automated decision-making (ADM), including what information must be disclosed in organisations' policies regarding its use.
				Understand the statutory tort of serious invasion of privacy as it relates to HR management and employee surveillance.
3	5	IV.E	Understand surveillance issues governed by Australian privacy law	Understand how the OAIC weighs rights of individual privacy against national security concerns and law enforcement needs.
				Know important foundational legislation for issues involving surveillance, such as the Telecommunications (Interception and Access) Act 1979, the Telecommunications Act 1997, the Intelligence Services Act 2001 (and amendments), and the Surveillance Devices Act 2004.
				Know the situations in which personal information is legally allowed or required to be collected, such as in the areas of biometric scanning, ID scanning, drone use and security camera use; understand the privacy implications of these areas, including the scope of information collected and data breach vulnerabilities.
				Understand the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021, its key aims and methods, and the privacy concerns related to it.