iapp

CIPP/US Body of Knowledge and Exam Blueprint

Version 2.6.1

Effective date: 1 September 2025

IAPP CIPP/US 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

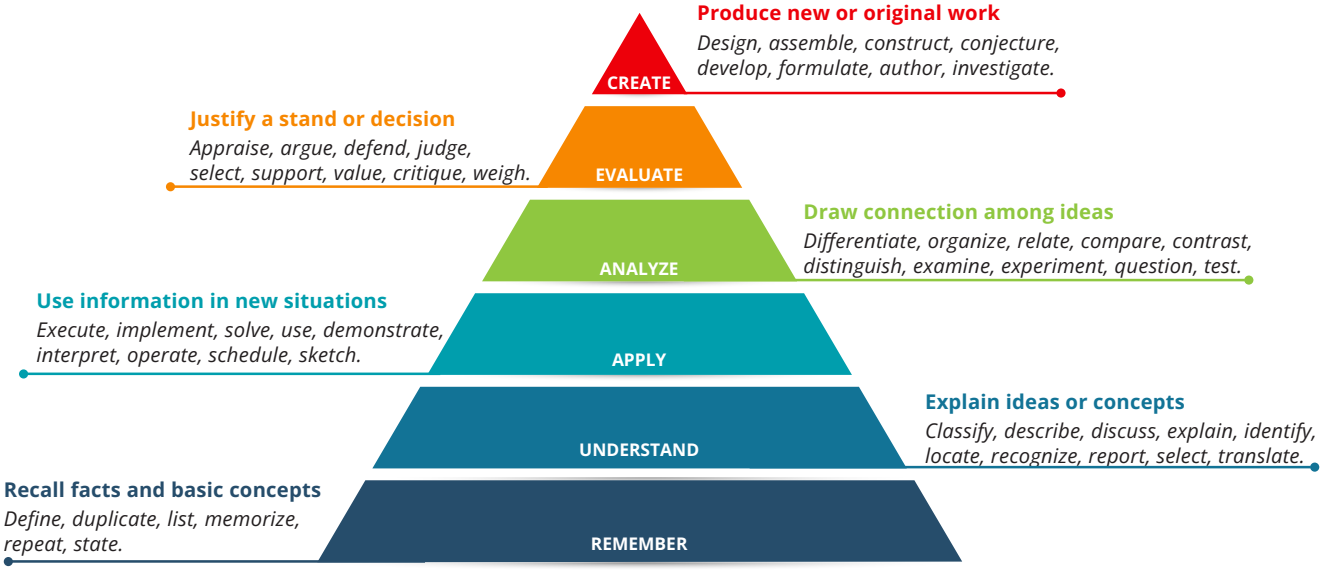
The IAPP's CIPM, CIPP/E, CIPP/US and CIPT credentials are accredited by the **ANSI National Accreditation Board (ANAB) under the International Organization for Standardization (ISO) standard 17024: 2012**.

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 CIPP/US 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 — The U.S. Privacy Environment
27	33	**Domain I – The U.S. Privacy Environment** identifies the legal concepts necessary for a foundational understanding of U.S. law and its relationship to privacy issues. The domain covers the privacy responsibilities of the major regulatory authorities and their roles in the enforcement framework. It also provides an overview of the principles of information management from a U.S. perspective, including issues of data subject rights, accountability and compliance in regard to domestic data management and international data transfers.

			COMPETENCIES	PERFORMANCE INDICATORS
3	5	I.A	Understand the U.S. legal framework	Identify the branches of government and know their roles and functions.
				Understand the various sources of law, including constitutions, legislation, regulations and rules, case law, common law and contract law.
				Know the key concepts involved in analyzing and applying laws, such as scope and application, jurisdiction, preemption, and private right of action.
				Know the roles and functions of, and the documents issued by, major regulatory authorities such as the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), the Department of Commerce (DoC), the Department of Health and Human Services (HHS), banking regulators such as the Federal Reserve Board and the Comptroller of the Currency, state attorneys general and state departments of insurance.
				Understand self-regulatory models

5	7	I.B	Understand the enforcement framework for U.S. privacy and security laws	Know general theories of legal liability (contract, tort, civil enforcement), and understand the differences between criminal and civil liability.
				Understand the concept of fiduciary duty.
				Understand negligence and unfair and deceptive acts and practices (UDAP) laws.
				Understand the purpose of federal and state enforcement actions and enforcement authorities (e.g., federal agencies, Department of Justice, state attorneys general, the California Privacy Protection Agency (CPPA)).
				Understand cross-border enforcement issues, including the role played by the Global Privacy Enforcement Network (GPEN).
				Understand the principles of self-regulatory enforcement efforts (PCI, Trust Marks).

18	22	I.C	Understand the principles of information management from a U.S. perspective	Know the practices and controls for managing personal information including data inventory, data classification, data flow mapping and data sharing and transfers.
				Know the basics of privacy program development, and understand the roles played by workforce training, vendor risk management, data processing agreements, requirements for cloud computing, third-party data sharing, and incident response programs (e.g., for cyber threats such as ransomware attacks and vendor incidents).
				Understand the importance of accountability and what ensures due diligence in determining data accountability.
				Know the requirements for managing user preferences, data and records retention and disposal, and the effective use of privacy notices.
				Identify privacy issues unique to the online environment (e.g., tracking and profiling).
				Understand the common requirements of international data transfers and how these have been shaped by the *Schrems* decisions.
				Adhere to the principles of accepted international data transfer mechanisms such as Standard Contractual Clauses and the EU-U.S. Data Privacy Framework.
				Adhere to key privacy considerations affecting U.S.-based multinational companies (e.g., GDPR requirements, APEC principles), and understand what is involved in resolving multinational compliance conflicts (e.g., EU data protection versus e-discovery).
				Understand the ways in which U.S. privacy laws intersect with non-U.S. privacy laws such as the GDPR and FADP.

MIN	MAX	Domain II — Federal Privacy Laws
15	19	**Domain II - Federal Privacy Laws** covers the role of the Federal Trade Commission in consumer privacy protection, including the acts and regulations it oversees, and the enforcement actions it has brought regarding privacy infringements. The domain also identifies privacy issues specific to federal sectors (healthcare and medical, finance, education, and telecommunications/marketing), including the major pieces of U.S. privacy legislation governing these sectors.

			COMPETENCIES	PERFORMANCE INDICATORS
3	5	II.A	Understand how the Federal Trade Commission addresses consumer protection in regard to privacy and security	Know the major acts and regulations overseen by the FTC, such as the Federal Trade Commission Act and the Children's Online Privacy Protection Act of 1998 (COPPA).
				Understand the purpose of the FTC's privacy and security enforcement actions.
				Identify priority areas in future federal enforcement (e.g., data brokers, IoT, AI, biometrics, unregulated data).
3	5	II.B	Understand how healthcare and medical privacy is regulated	Understand the basics of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), including the HIPAA privacy rule, the HIPAA security rule, and the use of online tracking technologies by HIPAA-covered entities and business associates.
				Understand how HIPAA was strengthened by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.
				Understand other laws and regulations governing the healthcare/medical sector, such as the 21st Century Cures Act and the Confidentiality of Substance Use Disorder Patient Records Rule (including 42 CFR Part 2).

3	5	II.C	Understand how financial sector privacy is regulated	Understand the requirements of the Fair Credit Reporting Act of 1970 (FCRA) and the Fair and Accurate Credit Transactions Act of 2003 (FACTA).
				Understand the basics of the Financial Services Modernization Act of 1999 ("Gramm-Leach-Bliley"), including the GLBA privacy rule, the GLBA safeguards rule and the various exemptions to these that exist under state laws.
				Know the Red Flags Rule and its role in the detection, prevention and mitigation of identity theft.
				Understand the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.
				Understand the roles and functions of the Consumer Financial Protection Bureau (CFPB).
				Understand the unique privacy issues involved in online banking, such as biometric data use, third-party tracking and data security.
				Understand the privacy issues involved in mergers, acquisitions and divestitures.
1	3	II.D	Understand how education sector privacy is regulated	Know the basics of the Family Educational Rights and Privacy Act of 1974 (FERPA).
				Understand the risks involved in the implementation and use of educational technologies, and the role privacy regulations play in mitigating them.
2	4	II.E	Understand how privacy is regulated in telecommunications and marketing activities	Understand the major rules and acts governing telecommunications and marketing, such as the Telemarketing Sales Rule (TSR) and the Telephone Consumer Protection Act of 1991 (TCPA), Combating the Assault of Non-solicited Pornography and Marketing Act of 2003 (CAN-SPAM), the Junk Fax Prevention Act of 2005 (JFPA), the Telecommunications Act of 1996, the Cable Communications Policy Act of 1984, and the Video Privacy Protection Act of 1988 (VPPA) (including the Amendments Act of 2012 (H.R. 6671)), and the Driver's Privacy Protection Act.
				Understand the role of the Do-Not-Call registry (DNC) and the Wireless Domain Registry in preventing unsolicited telemarketing calls and messages.
				Understand the privacy implications of digital advertising.
				Understand the privacy issues involved in web scraping activities.
				Understand the role of data ethics in telecommunications and marketing practices.

MIN	MAX	Domain III - Government and Court Access to Private-sector Information
3	5	**Domain III - Government and Court Access to Private-sector Information** focuses on privacy issues that emerge in response to subpoenas, court orders or law enforcement requests for private-sector data that includes personal information. It covers the key laws and acts regulating government access to communications, financial records and other sensitive data, and describes the privacy issues involved in civil litigation.

			COMPETENCIES	PERFORMANCE INDICATORS
1	2	III.A	Understand the relationship between law enforcement and privacy issues	Understand the laws and acts regulating access to financial data, including the Right to Financial Privacy Act of 1978 and the Bank Secrecy Act of 1970 (BSA).
				Understand the laws and acts regulating access to communications (e.g., through wiretaps, subpoenas and warrants), such as the Electronic Communications Privacy Act (ECPA) and the Communications Assistance to Law Enforcement Act (CALEA).
1	3	III.B	Understand the relationship between national security and privacy	Understand the basics of the Foreign Intelligence Surveillance Act of 1978, including Amendments Act: Section 702 (2008) and how it governs wiretaps, access to emails and stored records, and national security letters.
				Understand the role of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (or USA-PATRIOT Act) and the USA Freedom Act of 2015.
				Understand the role of the Cybersecurity Information Sharing Act of 2015.
1	2	III.C	Understand issues regarding civil litigation and privacy	Understand the privacy issues involved in the compelled disclosure of media information, and the role played by the Privacy Protection Act of 1980.
				Understand the role of electronic discovery in civil litigation.

MIN	MAX	Domain IV — Workplace Privacy
4	6	**Domain IV - Workplace Privacy** focuses on key concepts in workplace privacy in the U.S., the significant laws governing employee rights and the agencies tasked with enforcing them. The domain identifies workplace privacy issues in terms of pre-employment (e.g., automated employment decision tools and background screening), employment (e.g., employee monitoring) and post-employment (e.g., records retention).

			COMPETENCIES	PERFORMANCE INDICATORS
1	3	IV.A	Understand the issues involved in workplace privacy	Understand workplace privacy concepts and the laws governing them, including notice, appropriate expectations of privacy and anti-discrimination laws (e.g., the Civil Rights Act of 1964, Americans with Disabilities Act, and the Genetic Information Nondiscrimination Act (GINA)).
				Understand how workplace privacy in the U.S. is regulated, especially through agencies such as the Federal Trade Commission, the Department of Labor, the Equal Employment Opportunity Commission, the National Labor Relations Board (NLRB) and the Occupational Safety and Health Administration.

2	4	IV.B	Understand workplace privacy issues that arise before, during and after employment	Understand privacy issues related to the period prior to employment, such as automated employment decision tools (and their potential for bias), and employee background checks, including screening methods such as personality and psychological evaluations, polygraph testing, drug and alcohol testing, and social media monitoring, including unionized worker issues related to these practices.
				Understand privacy issues related to employee monitoring, especially as it relates to the use of technologies such as computer usage (including social media), biometrics, location-based services (LBS), wellness programs, mobile computing, email and postal mail, photography, telephony and video.
				Understand employer requirements under the Electronic Communications Privacy Act of 1986 (ECPA).
				Understand privacy issues related to internal investigations (e.g., employee misconduct), including data collection and handling, the use of third parties, documenting performance issues and balancing the rights of multiple individuals.
				Understand post-employment privacy issues, including those related to termination, transition management, records retention and reference requests.

MIN	MAX	Domain V — State Privacy Laws		
17	21	**Domain V - State Privacy Laws** focuses on the role of U.S. state privacy laws and their relationship to federal legislation. The domain primarily involves topics common to state data privacy and security laws (e.g. the observance of data subject rights, the implementation of data protection agreements), and also requires an understanding of the distinguishing characteristics of significant laws and acts in various states (e.g., California, Virginia, Colorado). Additionally, the domain also covers state laws governing specific areas of focus, such as health data rules, cookie regulations and AI bias laws.		
			COMPETENCIES	**PERFORMANCE INDICATORS**
1	**2**	**V.A**	Understand concepts of authority governing state privacy laws	Understand the relationship between federal and state authority in state privacy issues, including the roles played by state attorneys general and the California Privacy Protection Agency (CPPA).
13	**17**	**V.B**	Understand the key concepts and principles of state data privacy and security laws	Identify the key requirements of data privacy and security laws at the state level, including concepts of applicability (e.g., number of state residents, annual revenue), available exemptions and data subject rights (e.g., access, deletion/correction, portability, opt-out, consent and verifiable parental consent).
				Identify the key components and requirements of customer-based documents such as privacy notices.
				Understand common data protection requirements and best practices, including data protection assessments and risk assessments, data retention and destruction, issues involved in the selling and sharing of personal information, and data protection agreements.
				Understand common state data security requirements.
				Understand the purpose and common principles of state health data rules (e.g., geofencing bans and restrictions), and know the key components of significant recent health data legislation (e.g., Washington's My Health, My Data (MHMD) Act (2023), the Nevada Consumer Health Data Privacy Act (SB 370) (2023)), and the privacy class actions based on the Illinois Genetic Privacy Information Act (GIPA 2023).

13	17	V.B	Understand the key concepts and principles of state data privacy and security laws	Understand basic state enforcement concepts (e.g., cure periods, penalties for non-compliance).
				Understand state privacy and security laws specific to the online environment, including cookie and online tracking regulations.
				Identify facial recognition use restrictions, and assess the applicability of biometric privacy regulations (including those stipulated by acts and laws in Illinois, Washington, Texas and others).
				Understand the AI bias framework and related documents and laws, including the NAIC AIS Governance Guidelines, the NYC Automated Employment Decision Tool law and other major automated decision-making rules and regulations (e.g., California, Colorado), and Colorado's Protecting Consumers from Unfair Discrimination in Insurance Practices law.
				Know the basics of important comprehensive state privacy laws, including the California Consumer Privacy Act (CCPA) (2018) as amended by the California Privacy Rights Act (CPRA) (2020), the California Age-Appropriate Design Code Act (A.B. 2273) (2022), and the Delete Act (SB 362) (2023).
				Know the key provisions of other major state acts and laws that have a significant impact on the U.S. privacy landscape.
2	4	V.C	Understand the key principles of state data breach notification laws	Know the common elements of state data breach notification laws, including the definitions of relevant terms (personal information, security breach), the conditions for notification (who, when, how), and the rights afforded to data subjects (credit monitoring, private right of action).
				Identify key differences between states' breach notification regulations and practices.
				Know significant developments in state data breach notification laws, such as Pennsylvania SB 696, and the Utah S.B. 127 Cybersecurity Amendments.