iapp

CIPP/CN 知识体系和考试大纲

版本 1.0.0

生效日期：2024 年 6 月 3 日

IAPP CIPP/CN 知识体系

了解 IAPP 的知识体系

知识体系的主要目的是记录将在认证考试中评估的知识和技能。各领域反映了隐私专业人员为了表现出胜任此称号的能力所应该了解和能够做到的内容。

知识体系还包括考试大纲编号，这些编号表示考试中出现的各领域问题的最小和最大数量。

知识体系由组成各个资格考试开发委员会和计划委员会的主题专家开发和维护。每年都会对知识体系进行一次审查，并在必要时更新；变更会反映在年度考试更新中，并在新内容出现在考试中之前至少 90 天告知考生。

能力和绩效指标

我们用一系列能力和绩效指标来表示知识体系。

能力是构成广泛知识领域的相互关联的任务和技能的集合。

绩效指标是构成更广泛能力分组的具体任务和技能。考试题目旨在评估隐私专业人员在绩效指标方面的熟练程度。

考试中将出现哪些类型的题目？

对于认证考生而言，绩效指标是指导其展示能力所需知识深度的指南。技能和任务陈述开头的动词（如识别、评估、实施、定义）表明了考试题目的复杂程度，并与布卢姆分类法（见下一页）中的相应层次相对应。

ANAB 认证

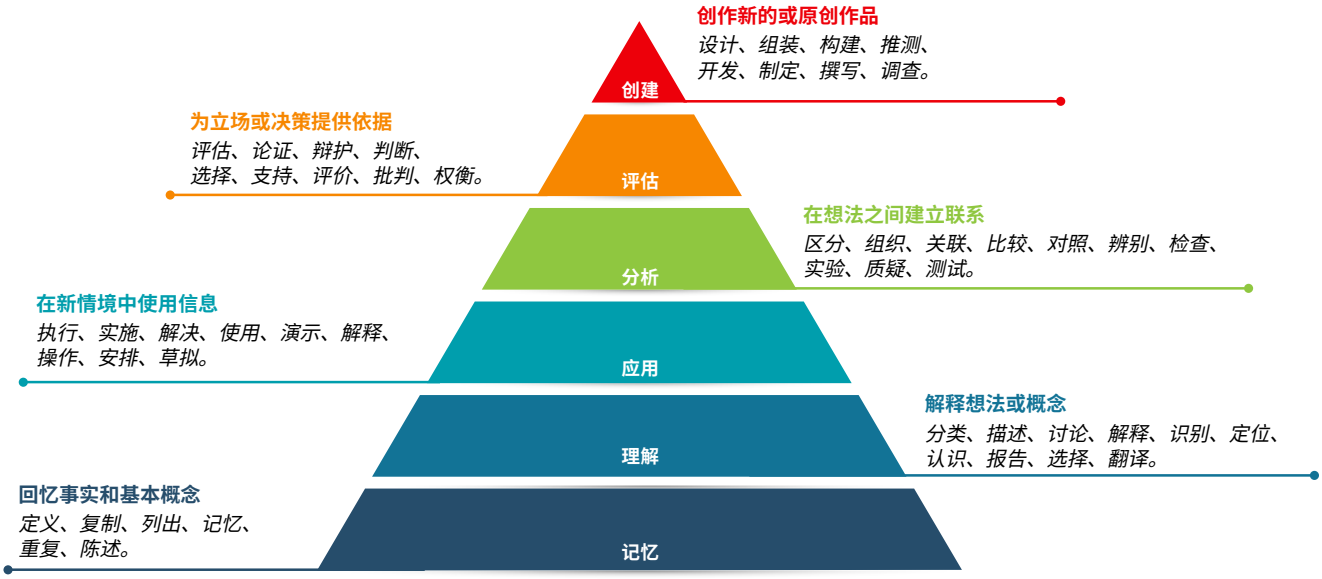
IAPP（国际隐私专业人员协会）的 CIPM（注册信息隐私经理）、CIPP/E（欧洲注册信息隐私专家）、CIPP/US（美国注册信息隐私专家）和 CIPT（注册信息隐私技术专家）证书均得到 **ANSI 国家认证委员会 (ANAB) 的官方认可，符合国际标准化组织 (ISO) 的 17024: 2012** 标准。

ANAB 是一个在国际上公认享有盛誉的认证机构，负责对符合严格标准的认证项目进行评估和认可。

获得官方认可是对 IAPP 认证计划质量和完整性的极大肯定，因为这能够：

- 表明 IAPP 证书符合全球性的行业公认的基准。
- 确保 IAPP 证书在全球范围内具有一致性、可比性和可靠性。
- 保护 IAPP 认证计划的完整性并确保其有效性。
- 向雇主、同事、客户和供应商表明，经 IAPP 认证的专业人员具备在世界任何地方完成工作所需的知识、技能和能力。

IAPP CIPP/CN 知识体系



来自不同认证称号的“记忆/理解”类已作废问题示例：

- 以下哪一项是对隐私增强技术的正确定义？
- 《加拿大权利与自由宪章》适用于哪一类活动？
- 哪个欧盟机构有权提出数据保护立法？
- 《公平信用报告法（FCRA)》和《公平准确信用交易法 (FACTA)》的立法权归谁所有？

这些问题的答案都是事实，无可争议。

来自不同认证称号的“应用/分析”类已作废问题示例：

- 在缺乏明确合同规定的情况下，以下哪一项对欧盟数据控制者构成了**最大**挑战？
- 以下哪个示例会构成对地域隐私的侵犯？
- 确保所有利益相关者对组织面临的隐私问题有相同基本理解的**最佳**方式是什么？
- 如果信息技术工程师最初将客户信用卡信息默认设置设为“不保存”，这一行为将符合什么概念？

这个问题的答案将基于事实知识和理解，这种知识和理解允许对提供的选项进行应用、分析和/或评估，以选择最佳答案。

下限	上限		领域 I：中国个人信息保护简介	
6	8		**领域 I：“中国个人信息保护简介”**提供了对中国个人信息保护法律与概念的基础理解，包括监督机关（包括综合监督机构、行业监督机构和司法监督机构）在执行隐私法律方面的作用。	
			能力	**绩效指标**
4	5	I.A	了解中国法律法规框架的主要概念。	了解《中华人民共和国宪法》中与个人信息保护相关的部分。
				了解《民法典》中与个人信息保护相关的规定。
				了解与个人信息保护相关的刑法。
				了解《消费者权益保护法》的基础知识。
				了解《未成年人保护法》的基础知识。
				了解《网络安全法 (CSL)》的主要概念，包括关键信息基础设施 (CII) 保护和多级保护方案 (MLPS)。
				了解《数据安全法 (DSL)》的主要概念。
				了解《个人信息保护法 (PIPL)》的目的。
				了解与个人信息保护相关的行政法规。
				了解与个人信息保护相关的地方性法律法规。
				了解与个人信息保护相关的行业法规。
				了解与个人信息保护相关的国家/行业标准与规范。
3	4	I.B	了解监管机关的不同角色与职责。	了解统筹监管机关的角色： • 中国国家互联网信息办公室 (CAC)。 • 公安部 (MPS)。 • 工业和信息化部 (MIIT)。 • 国家市场监督管理总局 (SAMR)。
				了解行业主管机关的角色： • 中国人民银行 (PBOC)。 • 国家金融监督管理总局 (NFRA)。 • 国家卫生健康委员会 (NHC)。
				了解司法机关的角色，包括最高人民法院和最高人民检察院。

下限	上限		领域 II： 个人信息保护法	
36	39		**领域 II：“个人信息保护法”**侧重于法律的适用范围等要素。它定义了 PIPL 中概述的个人信息保护概念，明确了个人信息处理活动应遵循的原则，并就个人信息处理合规及个人信息主体权利提供指导。该领域概述了跨境传输的实施、问责程序以及对内外部利益相关者的要求。其内容包括了解 PIPL 的执行处罚和报告要求，以及个人信息在自动化决策中的使用情形。	
			能力	**绩效指标**
4	5	II.A	了解 PIPL 中定义的个人信息保护概念。	了解个人信息的含义。
				了解个人信息主体的定义。
				了解敏感个人信息的含义。
				了解数据去标识化和匿名化的要求。
				了解个人信息处理的要求。
				了解同意和单独同意的要求。
				了解个人信息处理者的一般义务及大型互联网平台运营者的特殊义务。
				了解受托方的含义。
				了解个人信息保护影响评估 (PIPIA) 的要求。
				了解跨境数据传输的相关规定。
				了解个人信息保护官（中国 DPO）的主要职责。
3	4	II.B	了解个人信息处理活动的指导原则。	了解数据处理合法、正当、必要的含义。
				了解数据处理需诚信进行的含义。
				了解数据处理需透明的含义。
				了解数据处理中的目的限制原则。
				了解数据最小化的含义，并确保在处理活动中将影响降至最低。
				了解数据质量的重要性。
				了解数据安全的重要性。
				了解问责制的重要性。

下限	上限		领域 II： 个人信息保护法	
			能力	绩效指标
2	3	II.C	了解《个人信息保护法》的应用范围。	了解 PIPL 的内容范围、地域范围以及域外管辖权。
				了解 PIPL 适用范围中的例外情况。
4	6	II.D	遵守个人信息处理的法律要求。	确保遵守同意要求。
				确保遵守为订立或履行合同或进行HR管理所必需的要求。
				确保遵守为履行法定职责或法律法规规定的义务所必需的要求。
				确保遵守为应对公共卫生突发事件或在紧急情况下保护生命或财产所必需的要求。
				确保个人信息为了公共利益进行媒体报道或媒体监督而得到合理处理。
				确保自我披露或依法披露的信息得到合理处理。
				确保遵守法律或行政法规规定的其他情形的处理要求。
				确保遵守处理敏感个人信息的具体要求。
6	7	II.E	确保组织遵守个人信息主体的权利。	确保已制定程序，告知数据主体以下权利： • 知情权。 • 访问权。 • 更正权。 • 删除权。 • 撤回同意权。 • 限制或拒绝处理权。 • 拒绝自动化决策权。 • 要求解释权。 • 对处理者的起诉权。 • 死者近亲属的权利。 • 个人信息可携带权。
5	6	II.F	实施跨境数据传输的要求。	进行安全评估。
				获得个人信息保护认证。
				签订标准合同条款。
				遵守法律法规或 CAC 规定的其他条件。
				确保遵守适用的国际条约或协议。

下限	上限		领域 II： 个人信息保护法	
			能力	绩效指标
4	5	II.G	确保为内外部利益相关者制定并实施问责程序和要求。	建立并维护数据处理记录。
				明确个人信息共享中的不同角色，并设计适当的合同。 a. 个人信息共同处理者。 b. 个人信息处理者与受托方。
				了解个人信息保护官的要求。
				协助制定企业隐私政策。
				制定隐私通知，并恰当地向个人信息主体展示。
				确保遵守个人信息保存要求。
				进行个人信息保护影响评估。
				确保防止个人信息未经授权的访问、泄露、篡改或丢失。
				确保在个人信息泄露时，通知个人信息保护主管机关和受影响个体。
				确保实施防止个人信息泄露的安全要求。
3	4	II.H	了解 PIPL 的执法处罚和报告要求。	了解 PIPL 刑事犯罪的构成要素。
				了解 PIPL 违规的行政、法人和个人处罚。
				处理与 PIPL 违规相关的投诉和报告。
				开展公益诉讼。
4	5	II.I	了解个人信息用于自动化决策时的要求。	确保满足透明性、公平性和公正性要求。

下限	上限	领域 III：行业法规与合规性	
28	32	**领域 III：“行业法规与合规性”**详细阐述了遵守特定行业的法律要求，包括与犯罪记录处理、互联网应用 (App) 和电子商务营销以及儿童和未成年人保护相关的法律。还详细说明了银行与金融机构、互联网平台、汽车行业和雇主在处理个人信息方面需遵守的行业监管要求。同时，还讨论了新兴技术中的负责任治理问题，以及健康数据和人类遗传数据的收集和处理限制。	
		能力	**绩效指标**
2	3 III.A	确保犯罪记录处理符合数据处理要求。	了解个人信息侵占的刑事处罚。
			进行犯罪记录查询。
3	4 III.B	确保遵守互联网应用 (App) 和电子商务营销法律。	确保遵守电子商务和 App 法律中的个人信息收集要求。
			确保 App 和小程序践行数据最小化原则。
			禁止捆绑同意，并了解基本功能与非基本功能的区别。
			确保与第三方（如软件开发工具包）共享个人信息是合法的。
			确保遵守短信/电子邮件营销法律。
3	4 III.C	确保遵守儿童和未成年人保护法。	确保未成年人的隐私和个人信息得到保护。
			确保遵守《儿童个人信息网络保护规定》。
4	5 III.D	确保遵守银行和金融机构的处理要求。	了解消费者保护法。
			了解金融行业的安全义务。
			确保遵守行业监管机关（如中国人民银行 (PBOC)、国家金融监管总局 (NFRA)、中国证监会 (CSRC)）发布的规则。
4	5 III.E	了解适用于互联网平台的监管义务。	建立个人信息保护合规体系，并确保独立监督。
			了解适用于产品/服务提供者处理个人信息的平台治理义务。
			确保发布记录个人信息保护的社会责任报告。

下限	上限	领域 III：行业法规与合规性		
			能力	绩效指标
5	5	III.F	了解汽车行业的个人信息处理要求。	了解汽车数据的安全管理要求。
				确保车辆收集的数据得到合法处理。
				了解与网联和自动驾驶汽车相关的数据处理要求。
2	3	III.G	确保新兴技术得到负责任的治理。	了解中国国家互联网信息办公室对生成式人工智能服务的管理措施。
				了解使用面部识别技术的同意要求。
				了解《互联网信息服务算法推荐管理规定》中详细规定的算法使用限制。
3	4	III.H	确保遵守就业环境中的个人信息处理要求。	确保员工招聘中无歧视。
				确保遵守背景调查要求。
				了解工作场所监控和监视（如嵌入式软件和闭路电视）的限制。
				了解内部调查中保护个人信息的要求。
2	3	III.I	确保遵守健康与人类遗传数据收集和处理的限制。	确保敏感个人健康信息的保护和共享限制。
				确保医患保密。
				了解人类遗传资源管理办公室实施的中国人类遗传资源收集、保存和利用的限制。