iapp

CIPM
知识体系和考试大纲

版本 **4.0.0**

生效日期：**2023** 年 **10** 月 **2** 日

IAPP CIPM 知识体系

了解 IAPP 的知识体系

知识体系 (BoK) 旨在记录将在认证考试中评估的知识和技能。这些部分反映了隐私专业人士应当具备的专业知识和能力。

知识体系还包括考试大纲数量，其中注明了考试中各部分试题数量的下限和上限。

知识体系由各指定考试开发委员会和考试架构委员会的主题专家开发维护。每年都会对知识体系进行审核（并根据需要进行更新）。有关变更将会反映在年度考试更新中，并在考试内容更新前至少 90 天通知考生。

胜任力和绩效指标

现行知识体系不再使用以前的大纲形式，而是将内容表述为一系列胜任力和绩效指标。

胜任力是由相关联的任务和能力组成的群组，构成一个广泛的知识部分。

绩效指标为一系列相互独立的任务和能力，进一步丰富胜任力。试题旨在评估隐私专业人士的绩效指标。

考试中会出现哪些类型的问题?

对认证候选人而言，绩效指标是证明胜任力所需的知识深度的指南。技能和任务陈述开头的动词（识别、评估、实施、定义）表示试题的复杂程度，相关理论请参见布鲁姆分类法（见下页）。

ANAB 认可

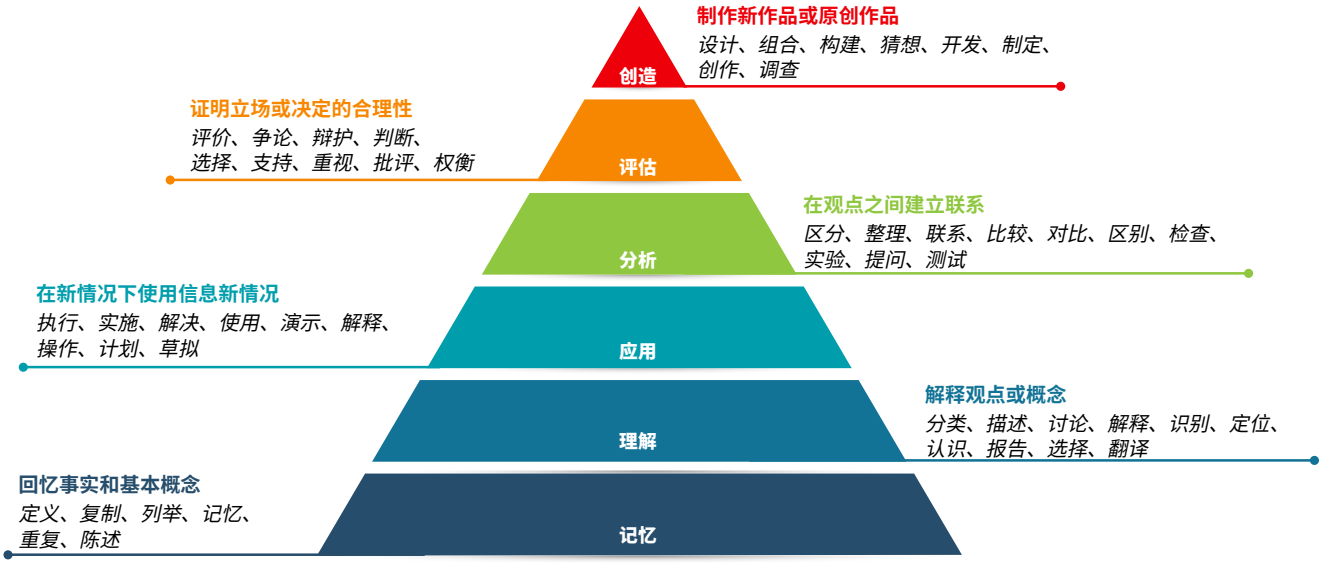
IAPP 的 CIPM、CIPP/E、CIPP/US 和 CIPT 证书均已获得**ANSI 国家认可协会 (ANAB) 认可，符合国际标准化组织 (ISO) 17024:2012标准**。

ANAB 为国际知名认可机构，负责评估认可认证计划，确保认证计划符合有关标准。

ANAB 认可是对 IAPP 认证计划质量和正规性的充分肯定：

- 证明 IAPP 证书符合全球公认的行业标准。
- 确保 IAPP 证书全球范围内的一致性、可比性和可靠性。
- 表明 IAPP 认证计划正规有效。
- 对雇主、同事、客户和供应商而言，表明经 IAPP 认证的专业人士具备所需知识、技能和能力。

IAPP CIPM 知识体系



不同职称的记忆/理解作废问题示例：

- 以下哪项是隐私增强技术的正确定义?
- 加拿大权利宪章适用于哪类活动?
- 哪个欧盟机构有权提出数据保护立法?
- 谁有权制定《公平信用报告法》(FCRA) 和《公平准确信用交易法》(FACTA) 规则?

这些问题的答案均为客观事实，无可争议。

不同职称的应用/分析作废问题示例：

- 在没有明确界定合同条款的情况下，以下哪项对欧盟数据控制者构成了**最大**的挑战?
- 以下哪个例子构成侵犯领域隐私?
- 有什么**最佳**方法可以确保所有利益相关者对组织面临的隐私问题有相同的基本认识?
- 如果信息技术工程师最初将客户信用卡信息默认设置为“不保存”，这一行为符合什么概念?

本题的答案将基于事实知识和理解，允许应用、分析和/或评估所提供的选项以选择最佳答案。

IAPP CIPM 知识体系

下限	上限	第 I 部分：隐私计划：制定框架		
14	18	**第 I 部分 - 隐私计划：制定框架**记录了为隐私计划奠定坚实基础所需的初步工作、隐私计划的目的和计划的负责人。重点讲述了制定符合组织隐私策略的隐私计划治理模式。由于每个组织需求不同，该模式可能因组织而异。		
		胜任力		**绩效指标**
4	6	I.A	确定计划范围并制定隐私策略。	选择适用的治理模式。
				确定组织范围内个人信息的来源、类型和使用。
				组建隐私团队。
				确定利益相关者和内部合作伙伴。
4	6	I.B	传达组织愿景和使命宣言。	建立加深内外部对组织隐私计划的认识。
				确保员工了解与其职责相关的政策、程序和更新。
				采用隐私计划词汇（例如事件与违规）。
5	7	I.C	指出计划的范围内适用的法律、法规和标准。	了解地区、部门和行业法规和/或法律。
				了解对违规行为的处罚。
				了解监管机构的监管范围和权限。
				了解在隐私法不健全的国家/地区开展业务面临的隐私问题。

IAPP CIPM 知识体系

下限	上限		第 II 部分：隐私计划：建立项目治理	
12	16		**第 II 部分 - 隐私计划：建立计划治理**确定如何通过隐私生命周期的各个阶段在整个组织内实施隐私要求。这部分重点介绍各利益相关者的角色、职责和培训要求，以及为确保持续合规而需要遵循的政策和程序。	
			胜任力	**绩效指标**
6	8	II.A	制定隐私计划生命周期的各阶段需要遵循的政策和流程。	根据组织规模设立适合的组织模式、职责和汇报结构。
				在考虑到法律和道德要求的情况下，制定与组织数据处理、数据共享相关的完善政策。
				根据数据收集的透明度和完整性限制确定收集点。
				制定违规管理计划。
				制定投诉处理程序。
1	3	II.B	明确角色和职责。	设立角色和职责，管理内外部数据共享和披露。
				按职能划分确定违规响应的角色和职责（包括利益相关者及其对监管机构的责任），协调检测团队（例如 IT、物理安全、人力资源、调查团队、供应商）并建立监督团队。
2	4	II.C	设定隐私指标，以便监督治理。	根据目标受众设定指标和/或确定指标的目标受众，建立清晰流程，明确指标的目的、价值和报告方式。
				了解审计的目的、类型、生命周期，以评估整个组织运营、系统和流程中控制措施的有效性。
				建立监督执行体系，跟踪多个司法管辖区隐私法律的变更，以确保持续一致。
1	3	II.D	开展培训和意识教育活动。	在隐私生命周期各阶段开展针对员工、管理人员和承包商的培训。
				持续开展隐私计划活动（例如意识教育、监控内部合规性、计划保证，包括审计、投诉处理程序）。

IAPP CIPM 知识体系

下限	上限		第 III 部分：隐私计划运营生命周期：评估数据	
12	16		**第 III 部分 - 隐私计划运营生命周期：评估数据**包括如何识别和最大限度降低隐私风险，以及评估组织的系统、流程和产品面临的隐私风险。及早消除潜在问题有助于建立更稳健的隐私计划。	
			胜任力	**绩效指标**
3	5	III.A	文档数据治理系统。	映射数据清单、数据流、数据生命周期和系统整合。
				根据内外部要求评估政策合规性。
				确定所需状态，并根据适用标准或法律进行差距分析。
1	3	III.B	评估处理者和第三方供应商。	识别内包和外包数据的风险，包括合同要求和国际数据传输的规则。
				在组织内最合适的职能层级开展评估（例如采购、内部审计、信息安全、物理安全、数据保护机构）。
0	2	III.C	评估物理和环境控制。	识别物理位置（例如数据中心和办公室）和物理控制（例如文件保留和销毁、介质清理和处置、设备取证和设备安全）的运营风险。
3	5	III.D	评估技术控制。	识别数字处理的运营风险（例如服务器、存储、基础设施和云）。
				审查并设定个人数据使用限制（例如基于角色的访问）。
				审查并设定记录保存期限。
				确定数据的位置，包括跨境数据流。
2	4	III.E	评估合并、收购、和资产剥离中共享数据的风险。	完成尽职调查。
				评估合同和数据共享义务，包括法律、法规和标准。
				协调风险和控制。

IAPP CIPM 知识体系

下限	上限	第 IV 部分：隐私计划运营生命周期：保护个人数据
9	13	**第 IV 部分 - 隐私计划运营生命周期：保护个人数据**概述如何通过在使用过程中实施有效的隐私和控制措施及技术保护数据资产的安全。无论规模大小、地理位置或何种行业，都必须在组织各个层级确保数据的物理和虚拟安全。

		胜任力		绩效指标
4	6	IV.A	应用信息安全实践和政策。	按照适用的分类方案（例如公开、机密、受限）对数据进行分类。
				了解不同控制措施的目的和限制。
				识别风险并实施适用的访问控制。
				采取适当的组织措施降低任何残余风险。
1	3	IV.B	整合隐私保护设计 (PbD) 的主要原则。	将隐私纳入整个系统开发生命周期 (SDLC)。
				将隐私纳入整个业务流程。
3	5	IV.C	遵循组织数据使用准则并确保执行技术控制。	确保遵循数据的二次使用准则。
				确保实施供应商和人力资源政策、程序和合同等行政保障措施。
				确保启动适用的员工访问控制和数据分类。
				与隐私技术专家合作，采取混淆技术控制，数据最小化、安全及其他隐私增强技术。

IAPP CIPM 知识体系

下限	上限		第 V 部分：隐私计划运营生命周期：维持计划绩效	
7	9		**第 V 部分 - 隐私计划运营生命周期：维持计划绩效**详细介绍如何使用相关指标和审计程序维持隐私计划。组织在管理隐私计划的周期中，必须确保所有流程和程序都能有效运作，并能在未来复制。	
			胜任力	**绩效指标**
1	3	V.A	使用指标衡量隐私计划的绩效。	为不同目标设定适当的指标，并依据指标分析收集的数据（例如趋势、投资回报、业务弹性、隐私成熟度模型）。
				收集指标，将培训和意识教育与隐私事件的减少联系起来，并根据收集的指标不断改进隐私计划。
1	3	V.B	审计隐私计划。	了解审计的类型、目的和生命周期，以评估整个组织运营、系统和流程中控制措施的有效性。
				根据计划目标选择适用的监控形式（例如审计、控制、分包商），并通过审计隐私政策、控制措施和标准，包括参照行业标准、监管和/或立法变更，完成合规监控。
3	5	V.C	管理隐私计划的持续评估。	对系统、应用程序、流程和活动进行风险评估。
				了解每种评估类型（例如 PIA、DPIA、TIA、LIA、PTA）的目的和生命周期。
				在合并、收购和资产剥离后实施风险缓释措施并与内外部利益相关者沟通。
				确保人工智能的使用符合道德、公正、满足数据最小化和目的限制要求，并遵循任何法规和/或隐私法。

IAPP CIPM 知识体系

下限	上限		第 VI 部分：隐私计划运营生命周期：响应请求和事件	
10	14		**第 VI 部分 - 隐私计划运营生命周期：对请求和事件作出回应**记录对隐私事件和数据主体权利作出回应的活动。组织需要根据适用的地区、部门和行业法律法规，为信息请求、隐私权和事件响应建立适当流程。	
			胜任力	**绩效指标**
5	7	VI.A	响应（数据主体信息请求和隐私权）	确保隐私告知和政策透明并明确阐明数据主体权利。
				遵守组织有关同意的隐私政策（例如，撤销同意、更正请求、反对处理、访问数据和投诉）。
				了解并遵守有关数据主体对个人信息控制权的现行国际、联邦和州立法（例如 GDPR、HIPAA、CAN-SPAM、FOIA、CCPA/CPRA）。
3	5	VI.B	遵循组织事件处理和响应程序。	对事件进行风险评估。
				采取控制措施。
				制定实施补救措施。
				根据司法管辖区、全球和业务要求与利益相关者沟通。
				让隐私团队参与审查事实、确定行动和执行计划。
				编制事件登记簿以及相关事件管理记录。
1	3	VI.C	评估并修改当前事件响应计划。	进行事件后审查，以提高计划的成效。
				实施更改以减少进一步违规的可能性。