iapp

CIPM 知识体系与考试大纲

版本 4.1.0

生效日期： 2024 年 9 月 2 日

IAPP CIPM 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。考察领域反映隐私专业人员应该了解的知识和能够完成的工作，以展示其在这一称号下的专业能力。

此外，知识体系还包括考试大纲数量，表示考试所评估的各领域中所含考题的最小和最大数量。

知识体系由主题领域专家开发和维护，这些专家是各个称号考试开发委员会和计划委员会的成员。知识体系将经过审查，必要时予以更新；所做更改会反映在每年的考试更新中，并于新内容在考试中出现之前至少 90 天内传达给考生。

能力和绩效指标

我们将知识体系内容以一系列能力和绩效指标来表示。

能力是指构成更广泛的知识领域的相关任务和能力的总称。

绩效指标是指构成更广泛的能力分组的各种任务和技能。考题评估隐私专业人员对绩效指标的掌握程度。

考试中会出现哪些类型的考题?

对于认证考生而言，绩效指标是展示其专业能力所需知识深度的参考。技能和任务陈述开头的动词（识别、评估、实施、定义）表明考题的复杂程度，并在布鲁姆分类法中具有相应的层次（见下一页）。

ANAB 认证

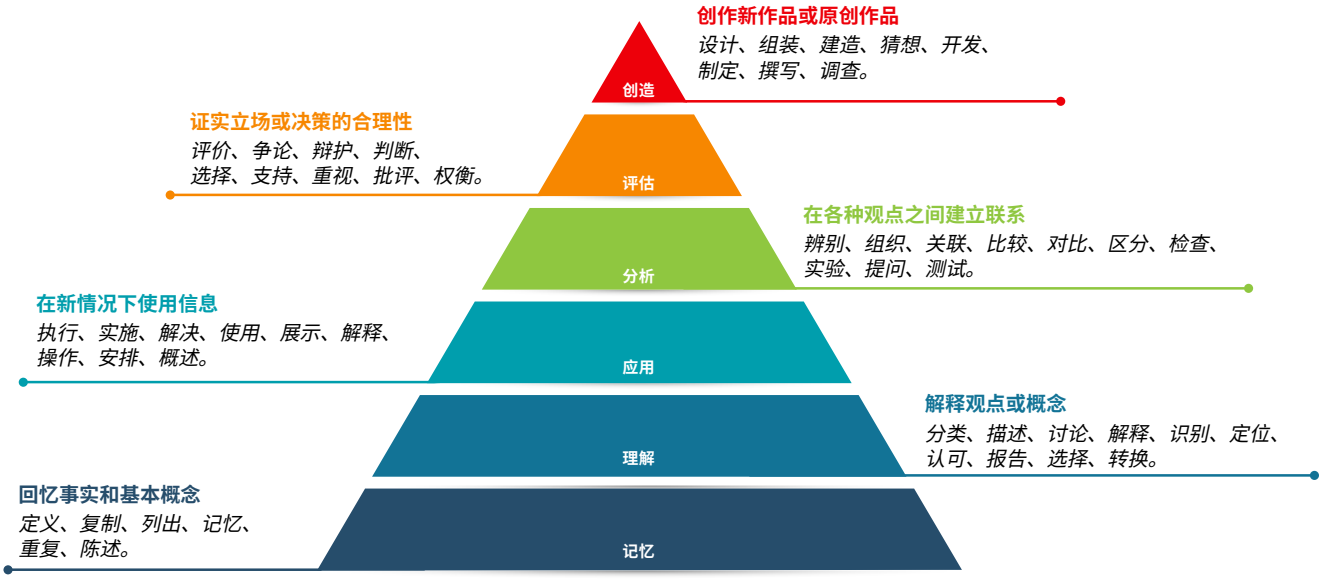
IAPP（国际隐私专业人员协会）的 CIPM（注册信息隐私管理师）、CIPP/E（欧盟注册信息隐私专家）、CIPP/US（美国注册信息隐私专家）和 CIPT（注册信息隐私技术专家）证书均得到 **ANSI 国家认证委员会 (ANAB) 的官方认可，符合国际标准化组织 (ISO) 标准 17024: 2012**。

ANAB 是一个国际公认的认证机构，负责对符合严格标准的认证计划进行评估和认可。

获得官方认可是对 IAPP 认证计划质量和完整性的极大肯定，这能够：

- 证明 IAPP 认证符合全球性的行业公认基准。
- 确保 IAPP 认证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各地完成工作所需的知识、技能和能力。

IAPP CIPM 知识体系



不同称号考试的历年记忆/理解类考题示例：

- 以下哪项是隐私增强技术的正确定义？
- 《加拿大权利与自由宪章》适用于哪类活动？
- 哪个欧盟机构有权提议数据保护立法？
- 哪个机构拥有《公平信用报告法 (FCRA)》和《公平准确信用交易法 (FACTA)》的立法权？

这些考题的答案都是无可辩驳的事实。

不同称号考试的历年应用/分析类考题示例：

- 以下哪项在没有明确定义的合同条款时会对欧盟数据控制者构成**最大的**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的基本理解的**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为“不保存”，该行为当时符合什么概念？

回答该考题时应基于事实性知识，并通过理解来应用、分析和/或评估所提供的选项，以此选择最佳答案。

下限	上限	领域 I — 隐私计划：制定框架
14	18	**领域 I — 隐私计划：制定框架**记录为隐私计划打下坚实基础所需的初步任务、计划的目标以及计划的负责人。侧重于在组织隐私策略的背景下建立隐私计划治理模型。由于每个组织可能都有自己的需求，该模型可能会因组织而异。

		能力		绩效指标
4	6	I.A	明确计划范围和制定隐私策略。	确定组织范围内个人信息的来源、类型和使用。
				了解组织的业务模式和风险偏好。
				选择适用的治理模型。
				定义隐私团队的组织架构。
				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。	建立内外部对组织隐私计划的意识。
				确保员工有权访问与其职责相关的政策、程序和更新内容。
				采用隐私计划词汇（例如“事件”和“泄露”）。
5	7	I.C	指出适用于该计划的相关法律、法规和标准。	了解地域性、部门性和行业性法规、法律、行为准则和/或自行认证机制。
				了解不合规所受到的处罚。
				了解监管机关的监管范围和权限。
				了解在具有不同隐私法的其他国家/地区开展业务或设立分公司时的隐私影响和地域范围。
				了解在商业环境中使用 AI 所带来的隐私风险。

下限	上限	领域 II — 隐私计划：建立计划治理		
12	16	**领域 II — 隐私计划：建立计划治理**确定隐私要求将如何跨整个组织在隐私生命周期的所有阶段中实施。该领域侧重于各利益相关者的角色、责任和培训要求，以及为确保持续合规而应遵循的政策和程序。		
		能力		**绩效指标**
6	8	II.A	制定在隐私计划生命周期所有阶段都要遵循的政策和流程。	建立适合组织规模的组织模型、责任和汇报结构。
				定义适合组织处理的数据的政策，将法律和伦理要求纳入考虑。
				确定数据收集点，考虑与数据收集相关的透明性要求和质量问题。
				制定数据泄露管理计划。
				制定投诉处理程序计划。
				制定数据保存和处置政策和程序。
1	3	II.B	明确职责和责任。	明确隐私团队和利益相关者的职责和责任。
				明确用于管理供内外部使用的数据共享和披露的职责和责任。
				明确不同职能的数据泄露响应职责和责任，包括利益相关者以及他们对各个内外部合作伙伴（例如检测团队、信息技术部、人力资源部、供应商、监管机关和监督团队）所承担的职责。
2	4	II.C	明确与监督和治理有关的隐私指标。	为每个受众建立指标和/或确定指标的预期受众，并明确制定描述指标目的、价值和报告方式的流程。
				了解评估整个组织的运营、系统和流程控制效果的审计的目的、类型和生命周期。
				建立监测和执行系统，以跟踪多个司法管辖区的隐私法变更，确保始终合规。

1	3	II.D	制定培训和意识教育活动。	在隐私生命周期的所有阶段开发 有针对性的员工、管理层和承包商培训。
				制定持续的隐私计划活动 （例如，教育和意识提升、内部合规监测、 计划保证（包括审计）、投诉处理程序）。

下限	上限		领域 III — 隐私计划运营生命周期：评估数据	
12	16		**领域 II — 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，以及评估与组织的系统、流程和产品相关的隐私影响。尽早解决潜在问题有助于制定更加健全的隐私计划。	
			能力	**绩效指标**
3	5	III.A	记录数据治理系统。	映射数据清单、数据流、数据生命周期和系统集成。
				根据内外部要求衡量政策合规性。
				确定所需的状态，并根据采用的标准或法律执行差距分析。
1	3	III.B	评估处理者和第三方供应商。	识别并评估委托处理个人数据（例如，按照合同要求和国际数据传输规则）的风险。
				在组织内最合适的职能级别（例如，采购、内部审计、信息安全、物理安全、数据保护监管机关）进行评估。
0	2	III.C	评估物理和环境控制。	确定物理场所（例如，数据中心和办公室）的运营风险以及物理控制（例如，文件保存和销毁、介质清理和处置、设备取证和设备安全）。
3	5	III.D	评估技术控制。	确定数字处理（例如，服务器、存储设备、基础设施和云）的运营风险。
				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限制。
				确定数据所在位置，包括跨境数据流动。
				与相关利益相关者合作，识别并评估技术控制。

2	4	III.E	评估与兼并、收购和资产剥离中的共享数据相关的风险。	完成尽职调查程序。
				评估合同和数据共享义务，包括法律、法规和标准规定的相关义务。
				使风险和控制保持一致。

下限	上限	领域 IV — 隐私计划运营生命周期：保护个人数据	
9	13	**领域 IV — 隐私计划运营生命周期：保护个人数据**概述如何通过实施有效的隐私和安全控制及技术为使用中的数据资产提供保护。无论组织的规模、地理位置或所在行业为何，都必须在组织的各个层级上实现数据的物理和虚拟安全。	

下限	上限	能力		绩效指标
4	6	IV.A	应用信息安全做法和政策。	根据适用的分类方案（例如，公开、保密、限制性）对数据进行分类。
				了解不同控制的目的和限制。
				识别风险并实施适用的访问控制。
				使用适当的技术、管理和组织措施来减轻任何剩余风险。
1	3	IV.B	融入隐私保护设计 (Privacy by Design, PbD) 的主要原则。	将隐私融入整个系统开发生命周期。
				将隐私融入整个业务流程。
3	5	IV.C	应用组织的数据使用指南并确保技术控制得到执行。	验证是否遵循了数据二次使用指南。
				验证是否应用了供应商和人力资源政策、程序和合同等保障措施。
				确保使用了适用的员工访问控制和数据分类。
				与隐私技术专家合作，启用模糊处理、数据最小化、安全性和其他隐私增强技术的技术控制。

下限	上限		领域 V — 隐私计划运营生命周期：维持计划效果	
7	9		**领域 V — 隐私计划运营生命周期：维持计划效果**详细说明如何使用相关指标和审计程序来维持隐私计划的效果。在组织推进隐私计划管理的各个环节时，确保所有流程和程序的有效运作和可复制性至关重要。	
			能力	**绩效指标**
1	3	V.A	使用指标衡量隐私计划的效果。	确定适用于不同目标的适当指标，并通过这些指标（例如，趋势分析、投资回报率、业务韧性）分析所收集的数据。
				收集指标，将培训和意识教育活动与隐私事件的减少相关联，并根据收集的指标持续改进隐私计划。
1	3	V.B	审计隐私计划。	了解评估整个组织的运营、系统和流程控制效果的审计的类型、目的和生命周期。
				根据计划目标（例如，审计、控制、分包商）选择适用的监测形式。
				通过审计隐私政策、控制和标准来完成合规性监测，包括对行业标准、规章和/或法律变更的审计。
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（例如，PIA、DPIA、TIA、LIA、PTA）的目的和生命周期。
				在兼并、收购和资产剥离后，实施风险缓解并与内外部利益相关者进行沟通。

下限	上限	领域 VI — 隐私计划运营生命周期：对请求和事件作出响应		
10	14	**领域 VI — 隐私计划运营生命周期：对请求和事件作出响应**记录对隐私事件和数据主体权利作出响应的相关活动。根据适用的地区、部门和行业法律法规，组织必须确保为信息请求、隐私权和事件制定适当的响应流程。		
		能力		**绩效指标**
5	7	VI.A	对数据主体访问请求和隐私权作出响应。	确保隐私告知和政策透明，并清楚阐明数据主体的权利。
				遵守组织关于同意的隐私政策（例如，同意的撤回、更正请求、反对处理、访问数据和投诉）。
				了解并遵守已制定的国际、联邦和州法律中关于数据主体对个人信息控制权的规定（例如，GDPR、HIPAA、CAN-SPAM、FOIA、CCPA/CPRA）。
3	5	VI.B	遵守组织事件处理和响应程序。	进行事件影响评估。
				开展遏制活动。
				识别并实施补救措施。
				按照管辖、全球和业务要求，与利益相关者进行沟通。
				与审查团队合作，审查事实、确定措施并执行计划。
				维护事件登记册以及事件的相关记录。
1	3	VI.C	评估并修改当前的事件响应计划。	执行事件后审查，改进计划效果。
				作出更改，降低未来泄漏的可能性和/或影响。