

iapp



CIPM 知识体系 与考试大纲

版本 4.2.0

生效日期：2025 年 9 月 1 日



IAPP CIPM 知识体系

了解 IAPP 的知识体系

本知识体系旨在整理认证考试中涉及的知识和技能，包括隐私专业人员应当掌握的知识，以及如何成为一名胜任的隐私专业人员。

此外，还包括考试大纲编号，显示了考试中各部分涉及的题目数量下限和上限。

本知识体系由各认证考试发展委员会和计划委员会的主题专家编写并维护。每年审核并根据需要进行更新，反映每年考试的变化，并会在考试中加入新内容前至少 90 天通知考生。

胜任力和能力指标

本知识体系囊括了一系列胜任力和能力指标。

胜任力为一组相互关联的任务和能力，共同构成相应部分的知识体系。

能力指标为每种胜任力包含的一系列独立任务和能力。

考试题目用于评估隐私专业人员的能力指标。

考试中将包含哪些类型的题目？

能力指标为考生提供了每种胜任力所需知识的详细指南。能力指标中技能和任务描述开头的动词（“确定”、“评估”、“实施”、“定义”）表明了考试题目的难度，并使用 Bloom 分类法进行了详细解释（见下一页）。

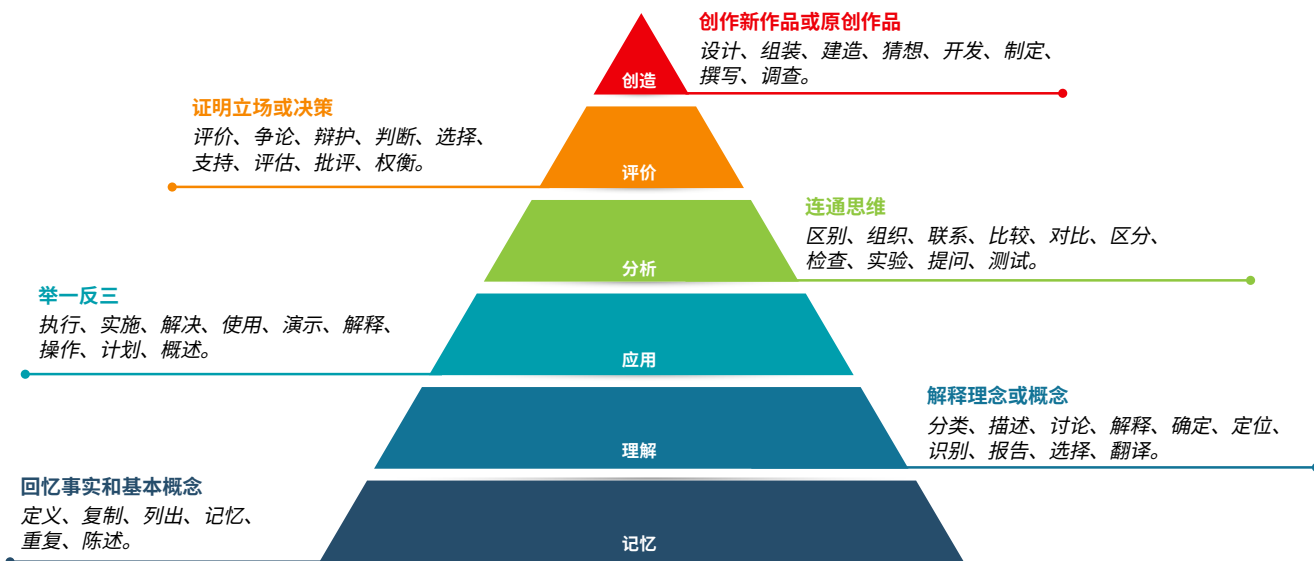
ANAB 认证

IAPP 的 CIPM、CIPP/E、CIPP/US 和 CIPT 证书均得到美国国家认证委员会 (ANAB) 的认证，符合国际标准化组织 (ISO) 的 17024: 2012 标准。

ANAB 是一个国际公认的认证机构，负责对认证计划进行评估认定，确保符合严格标准。

获得 ANAB 认可是对 IAPP 认证计划质量和专业性的充分肯定：

- 证明了 IAPP 证书符合全球行业的公认标准。
- 确保了 IAPP 证书在全球范围内得到一致认可。
- 确保了 IAPP 认证的专业、有效。
- 经 IAPP 认证的专业人员可证明自己具备必要的专业知识、技能和能力，获得雇主、同事、客户和供应商的认可。



记忆/理解类真题示例：

- 以下关于增强私隐技术的定义正确的是？
- 《加拿大权利和自由宪章》适用于哪一类活动？
- 哪个欧盟机构被赋予了提出数据保护立法的权力？
- 谁拥有为《公平信用报告法 (FCRA)》和《公平准确信用交易法 (FACTA)》制定规则的权力？

这些题目的答案都是客观事实，无可辩驳。

应用/分析类真题示例：

- 如果缺少明确界定的合同条款，下列哪项对欧盟数据控制者构成最大挑战？
- 下列哪个例子构成侵犯领土隐私？
- 要确保所有利益相关者都能对组织面临的隐私问题有基本的了解，最佳方法是什么？
- 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”，那么该操作符合什么概念？

此类题目的答案基于事实知识和理解，允许应用、分析和/或评估提供的选项，从而选出最佳答案。



下限 上限

第一部分 — 隐私计划： 建立框架

14 18 **第一部分 — 隐私计划：建立框架**包含基础任务（为隐私计划奠定坚实基础）、计划的目的和计划负责人。重点关注根据组织的隐私策略建立隐私计划治理模型。由于每个组织的需求各不相同，模型可能因组织而异。

胜任力

能力指标

4 6 I.A	定义计划范围并制定隐私策略。	确定个人信息 (PI) 的来源、类型和用途。
		理解业务模式、运营环境和风险偏好。
		选择适用的治理模型。
		定义隐私团队的结构。
		确定利益相关者和内部合作伙伴。
4 6 I.B	传达组织愿景和任务宣言。	加强内外部对组织隐私计划的认识。
		确保员工有权访问与其职责相关的政策、规程和更新。
		在整个组织内普及隐私术语。
5 7 I.C	明确适用于隐私计划的法律、法规和标准。	了解地区、行业和行业法规、法律、行为准则和/或自我认证机制。
		了解不合规对组织和/或个人的潜在影响。
		了解监管机关的管辖范围和权限。
		了解在拥有不同隐私法律的国家开展业务对隐私的影响和影响的区域范围。
		了解在商业环境中使用 AI 带来的隐私风险。



下限 上限 **第二部分 — 隐私计划： 计划治理**

12 16 **第二部分 — 隐私计划：计划治理**是关于隐私生命周期的各个阶段如何在整个组织内贯彻隐私要求。重点关注各种利益相关者的角色、职责和培训要求，以及为确保始终合规需要遵守的政策和规程。

胜任力		能力指标
6 8 II.A	制定隐私计划生命周期的各个阶段需要遵循的策略和流程。	根据组织规模建立适合的组织模型、责任和汇报结构。
		根据法律和道德要求，为组织处理数据制定适合的策略。
		根据数据收集的透明度要求和数据质量问题，确定收集点。
		制定数据泄露管理计划。
		制定计划，建立投诉程序和数据主体权利处理流程。
		制定数据保留和处理策略和规程。
1 3 II.B	明确角色和职责。	定义隐私团队和利益相关者的角色和职责。
		针对内部和外部的数据使用，定义管理数据共享和披露的角色和职责。
		按职能定义响应数据泄露的角色和职责，包括利益相关者及其对各种内外部合作伙伴的责任（例如，检测团队、IT、HR、供应商、监管机关、监督团队）。



IAPP CIPM 知识体系

2 4 II.C	定义隐私指标，用于监督 and 治理。	根据受众制定指标和/或确定指标的目标受众，并制定清晰流程，描述指标的目的、价值和报告程序。
		了解审计的目的、类型和生命周期，评估整个组织运营、系统和流程控制措施的效果。
		建立监测和执行系统，追踪多个司法管辖区隐私法的变化，始终确保合规。
1 3 II.D	开展培训和意识教育活动。	在隐私计划生命周期的各个阶段为员工、管理层和外包员工针对性地开展培训和意识教育活动，确保合规。



下限 上限

第三部分 — 隐私计划运营生命周期： 评估数据

12 16

第三部分 — 隐私计划运营生命周期：评估数据包括如何识别和最小化隐私风险，以及评估组织的系统、流程和产品相关的隐私影响。及早解决潜在问题有助于建立更健全的隐私计划。

胜任力

能力指标

3	5	III.A	记录数据和治理系统。	映射数据清单、映射数据流、映射数据生命周期和系统集成。
				根据内外部要求评估政策合规性。
				根据适用法律和/或公认标准进行差距分析。
1	3	III.B	评估处理者和第三方供应商。	识别和评估外包处理个人数据的风险（例如，合同要求、国际数据传输规则）。
				在组织内最适合的职能部门（例如，采购、内部审计、信息安全、物理安全、数据保护监管部门）开展评估。
0	2	III.C	评估物理和环境控制措施。	识别物理场所（例如，数据中心和办公室）和物理控制措施（例如，文件保存和销毁、媒体消毒和处置、设备安全）的运营风险。
3	5	III.D	评估技术性控制措施。	识别数字处理的运营风险（例如服务器、存储、基础设施、云）。
				审查个人数据的使用和保存并设定限制。
				确定数据的位置，包括跨境数据流。
2	4	III.E	评估合并、收购和剥离中共享数据相关的风险。	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。
				协调风险与控制措施。



下限 上限

第四部分 — 隐私计划运营生命周期： 保护个人数据

9 13 **第四部分 — 隐私计划运营生命周期：保护个人数据**概述了如何通过实施有效的隐私和安全控制措施及技术，在使用过程中保护数据资产。无论规模大小、地理位置或行业，必须确保组织各级数据的物理安全和虚拟安全。

胜任力

能力指标

4 6 IV.A	应用信息安全实践和策略。	根据适用的分类方案将数据分类（例如公开、保密、限制）。
		了解不同控制措施的目的和限制。
		识别风险并实施适当的访问控制措施。
		使用适当的技术、管理和组织措施降低风险。
1 3 IV.B	整合隐私保护设计的主要原则 (PbD)。	将隐私融入整个系统开发生命周期 (SDLC)。
		将隐私融入整个业务流程。
		理解隐私保护设计的原则和目的。
3 5 IV.C	应用组织的数据使用指导准则，落实技术控制措施。	验证是否遵循数据二次使用的指导准则。
		验证是否采用政策、规程和供应商合同等保障措施。
		实施适当的访问控制措施，确保数据分类恰当有效。
		与隐私技术人员合作，对模糊处理、数据最小化、安全和其他隐私增强技术实施技术控制措施。



下限 上限

第五部分 — 隐私计划运营生命周期： 维持计划效果

7 9

第五部分 — 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维持隐私计划。在整个隐私计划周期中，确保所有流程和程序有效运行并可复制至关重要。

胜任力

能力指标

1 3 V.A	使用指标衡量隐私计划的效果。	针对不同的目标（例如趋势、ROI、业务弹性）确定适当的指标。
		分析收集到的数据，并与目标和合规措施关联（PIA、权利请求响应速度、投诉量、数据泄露指标）。
1 3 V.B	审计隐私计划。	根据计划目标选择适合的监测形式（例如审计、控制、分包商）。
		通过审计隐私政策、控制措施和标准（包括行业标准、法规和/或法规变更），监测合规性。
3 5 V.C	持续评估隐私计划。	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（如 PIA、DPIA、TIA、LIA、PTA）的目的和生命周期。
		在合并、收购和剥离后，进行风险缓释并与内部和外部利益相关者沟通。



下限 上限

第六部分 — 隐私计划运营生命周期： 响应请求和事件

10 14

第六部分 — 隐私计划运营生命周期：响应请求和事件是关于如何响应隐私事件和数据主体权利。组织必须根据适用的地区和行业法律法规，建立适当的信息请求、隐私权和事件响应流程。

胜任力

能力指标

5 7 VI.A	响应数据主体的访问请求和隐私权。	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（例如撤销同意、纠正请求、反对处理、访问数据、投诉）。
		了解并遵守有关数据和数据主体个人信息控制权的全球法规。
3 5 VI.B	遵循组织的事件处理和响应程序。	理解并执行事件处理和响应程序（例如评估、遏制、补救）。
		根据司法管辖区、全球和业务要求与利益相关者沟通。
		维护事件登记册和事件的相关记录。
1 3 VI.C	评估和修改当前事件响应计划。	事件后审查，提升计划有效性。
		进行整改，减少未来违规的可能性和/或影响。