
KPMG
代理式AI优势：
解锁人工智能价值
的下一阶段

在KPMG，未来是代理中心

人工智能达到了另一个拐点。就在组织开始扩展生成式人工智能时，一场更变革性的转变已经开始：人工智能代理的兴起。

代理不仅仅是下一波浪潮——它们是跨越式发展。这些系统将独立运作，追求目标，并在复杂的业务流程中运行。这种转变改变了一切：工作的执行方式、决策的制定方式以及价值的交付方式。

本文解析了自主AI的真正含义：如何定义它，它能够做什么，以及从何处开始。这些观点基于实际经验——源自我们与客户合作及公司内部的工作。

准备的时间就是现在。与云重塑企业基础设施花费了近二十年不同，这场转型正在几个月内展开。领先的组织没有等待——他们已经开始投资、扩展，并定位自身以快速捕捉AI代理带来的好处。

但这不仅仅是一场技术对话——它关乎领导力。代理人将要求比以往任何时候都更紧密的业务与技术领导层之间的协同。成功需要共同愿景、协调执行，以及一个清晰的计划，以大规模嵌入智能。

这包括为你的团队做准备。那些将领导变革的组织将是那些帮助其员工适应的组织——培训团队与代理合作，明确不断演变的角色，并领导这种变革所要求的这场文化转变。

随着代理承担更多自主权和影响力，信任变得更加关键。一个可扩展的策略并不仅仅是关于代理能做什么——它是关于确保它们可靠地、透明地运行，并在建立信任的护栏内运行。

在代理人的喧嚣中，很容易失去焦点。代理人将是人工智能战略的关键部分，但他们不是战略。领先的企业正在快速行动，但目标明确——坚持“不留遗憾”的举措：统一领导层，现代化技术和数据，提升员工技能，并在每一层嵌入信任。

这一转变不会轻易——但它将具有决定性意义。领导者今天做出的决策将重塑行业，并重新定义竞争优势。随着我们继续前行，我们将持续分享我们的所学——并且，当我们共同探索未来时，也欢迎你的想法和观点。

史蒂夫·切斯
人工智能与数字创新副主席

内容

你真的知道什么是AI代理吗？

最近使用“AI代理”一词的次数激增，字面意思是每个人都在谈论它们。 现在，似乎几乎一切都是某种代理。但这并不正确。在你开始认识到这种快速发展的新技术中内在的巨大潜力之前，你真的需要理解代理实际上是什么。

AI 代理是满足 • 通过采取有意义的独立行动来实现组织目标。他们通过融合来自大型语言模型的高级推理、规划、编排、知识、数据挖掘、精选工具和谨慎治理来实现这一点。

代理进行实时决策，适应新 • 情境，并从他们的互动和反馈中学习。

• AI代理可以摄取结构化和非结构化数据。

• 潜在的现实世界应用令人难以置信。它们从可以对照标准提取和比较数据的基础任务导向型代理，到端到端自动化代理，这些代理可能破坏整个组织价值链。

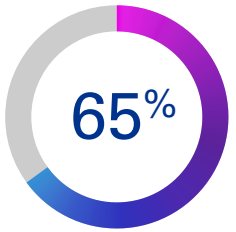
智能体的时代已经开始了

正如高管们开始在其组织中扩展生成式人工智能（GenAI）的游戏改变能力时，一种全新且更强大的AI技术已经出现。 虽然仍处于早期阶段，但自主AI已经展现出巨大的潜力，并且发展速度如此之快，以至于没有哪家企业高管或董事会可以忽视它变革其组织并获取竞争优势的潜力。

简单来说，GenAI构建“数字助手”，帮助员工节省时间，使其更高效、更有创意，即通过提供信息和指导来增强人类，帮助他们做出更好的决策和更快地行动。相比之下，代理式AI可以通过替人类采取行动来完全自动化人类的工作，以实现规定的业务成果。代理可以循环调用GenAI工具和其他数据和信息来源，有潜力带来显著更多的业务价值。

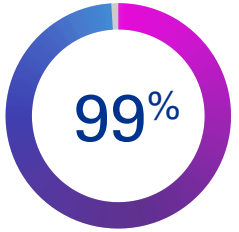
虽然仍在兴起和发展中，人工智能代理已经能够承担以往被认为过于复杂而难以自动化的任务，并且在某些以往用旧人工智能工具自动化的活动中，它们可能是一个更好的选择。因此，在我们最新的季度脉搏调查中，大多数公司（65%）已经正在试点人工智能代理，这个数字在三个月内几乎翻了一番（从上季度的37%上升）。[1] 到目前为止，然而，只有11%的人将代理投入生产，尽管99%的人计划这样做。[2]

KPMG 季度脉搏调查



公司试航智能体

从上 37% 上个季度



公司计划将代理放入生产

仅 11% 已完成所以已经

[1] KPMG AI 脉搏调查 Q1，2025年4月。
[2] KPMG人工智能脉搏调查Q1，2025年4月。

智能体自动化复杂任务的能力正快速增长，目前每三到七个月就能翻一番。在编程方面，他们的能力已经从处理人类只需要几秒钟就能完成的任务发展到自动化持续数小时的任务。如果这种指数级增长继续下去，智能体在六个月内的能力可能会翻四倍，在一年内的能力可能会增长十六倍。这将使他们能够从自动化人类任务转向自动化人类角色，从而创造一个全新的“数字同事”人才库。

智能体也日益能够相互沟通与合作，进一步增强了其商业效用。通过作为一个群体承担一系列复杂任务，“群组”[3] 具有不同技能的代理最终可能端到端自动化整个业务流程。一旦自动化，代理可以自主重构，并持续改进这些流程。这种多层方法可以解锁新的运营绩效水平，并为重新构想整个商业模式打开新的视野。同时，风险更高，必须仔细管理以确保价值安全可靠地释放。

虽然这些情景在今天可能听起来像科幻，我们预测大多数公司最终会转变为混合型组织，其中人类和AI代理能够无缝协作。数字

30万亿

毕马威估计，代理式人工智能将是每年解锁高达3万亿美元企业生产力的关键

工人初始规模可能较小,但可以快速增长,并根据需求几乎实时地上下灵活调整。这将使人类工人能够专注于最富有成效、最复杂和最刺激的任务,同时学习与智能体无缝协作,共同追求前所未有的绩效水平。

猜对的奖金规模可能令人震惊。IDC的预测表明，在未来10年，仅生成式AI就将为全球GDP增加近10万亿美元。[4] 代理型AI的价值潜力预计将呈指数级增长：KPMG估计，根据我们对AI对1700多万家公司影响的自有研究，代理型AI将成为每年解锁高达3万亿美元企业生产力改进的关键。[5] 我们也预计，代理式人工智能可以帮助至少解锁百分之五的仅平均福布斯1000强公司在劳动生产率上的年EBITDA。后者发现得到了许多行业分析师的呼应。例如，根据IDC最近的一项研究，采用代理式人工智能的组织可以实现员工生产力和满意度的提升18%。[6]

本文着重探讨从商业领袖的角度如何引领人工智能发展的下一阶段，从那些成功实施的组织所面临的潜在价值出发。我们还介绍了各类新兴智能体以及KPMG TACO框架™ 为了优化代理式AI的使用。最后，我们探讨了前方的挑战，包括需要克服的四个关键障碍，最后以您今天可以采取的实际行动作为结尾，以提高您在代理式AI领域的成功几率。

[3] 一个“蜂群”是一个自我同步、高效、有效的智能体团队。(阿巴斯·侯赛因和莫斯塔吉姆·萨纳兹，2025年，《蜂群系统的未来之路》) *皇家学会哲学汇刊A辑* 38320240135 http://doi.org/10.1098/rsta.2024.0135).
[4] Ritu Jyoti和David Schubmehl，《人工智能的商业机会》，IDC，2023年11月。
[5] 量化生成式AI机遇 ，普华永道, 2025.
[6] Ritu Jyoti 和 David Schubmehl,《人工智能的商业机会》, IDC, 2023年11月。

受险值

人工智能在先进能力和成本降低方面正飞速发展，以至于对未来价值的任何预测仍需被视为推测性的。例如，仅在过去的18个月中，具有同等性能的顶尖人工智能模型的使用成本就从每百万个token的20.00美元降至0.07美元，提高了240倍。[7] 生成式和代理式AI的发展速度将很可能在未来可预见的时期内继续，性能有望以比摩尔定律中硅芯片的速度更快的速率提升。

在自主人工智能市场的支出方面，领先分析机构的估计颇为乐观且增长迅速。此外，根据IDC的一项研究，除了许多分析师预测的500亿美元的市场价值外，自主人工智能投资的回报也充满希望。他们的研究表明，每公司在人工智能上投入1美元，平均可以获得3.50美元的回报，而全球5%的机构平均可以获得8美元的回报。[8]

利用我们的专利待审的GenAI价值评估模型，普华永道已首次尝试按行业、公司、职能和角色量化自主AI的潜在机会。虽然现在做出可靠的预测还为时过早，但采取了保守的方法，仅考虑了劳动生产率的影响。假设自主AI将是我们模型中自动化高复杂度任务的关键，这相当于每年给平均公司带来3万亿美元的企业生产力提升，以及5.4个百分点的EBITDA提升。[9]

KPMG 生成式人工智能价值评估

2024年，普华永道发起了一项大规模研究，旨在建立世界上最大的数据库，以帮助企业量化全球范围内GenAI对劳动生产力的潜在影响。

利用我们正在申请专利的GenAI价值评估模型，我们为超过1700万家公司构建了组织的数字孪生，使用了超过30亿个数据点。

由于可获得财务信息，我们聚焦于总样本中的7,000家上市公司，这些公司共同雇佣了超过7200万员工，从事2,000种不同的岗位，平均收入为75亿美元。

我们根据内部AI模型，例如推理程度和交互需求，将AI所接触的任务复杂度分为低、中或高。

在这些中，我们认为具有自主性的AI最擅长在高复杂性任务中释放价值。

[7] 2025年人工智能指数：用10张图表解读人工智能现状，斯坦福大学以人为本的人工智能（HAI），2025年4月7日。
[8] Ritu Jyoti和David Schubmehl，《人工智能的商业机会》，IDC，2023年11月。
[9] 量化生成式AI机遇，普华永道, 2025.

四种人工智能代理解锁价值的方法

智能体可以在至少四个重要方面解锁更大的企业价值：

代理扩大了自动化的机会。

随着智能体在推理和协作能力上呈指数级增长，它们可以自动化先前只能由人类执行的任务、角色和流程。这扩大了可以释放给人类人才的工作份额，同时也提高了工作的长期有效性。具体来说，在自动化之后，可以指示智能体持续努力优化其交互以实现特定目标。

代理不睡觉。

一旦代理自动化了一组任务，它们就可以被指示每天24小时不间断地运行，只要能源、数据和人工监督可用即可。只需将相同的工作从8小时延长到24小时，该组织就能将日生产率提高三倍。当多个代理同时工作时，它们也能比人类团队更快地完成任务。如果代理团队能在1/3的时间内完成相同的工作，那么该组织可以在24小时内交付九倍的工作量。这还可以使该组织更具敏捷性，通过更快地响应非工作时间的趋势。例如，在制造业中，代理可以通过优化日程安排和工作流程来管理生产线，并执行预测性维护以减少停机时间。当供应中断发生时，采购代理会寻找替代方案，而生产代理会自动重新配置日程安排。

代理人为变革而生。

一旦一个流程被一群智能体自动化，随着时间的推移，也更容易、更快地将其工作流应用于不断变化的形势。这些智能体被训练和激励以实现特定结果，但不需要详细的操作说明，也不需要花费时间从交付中脱离出来进行培训。此外，它们不受变化的威胁，也不不愿意合作，因此它们需要较少的变更管理。智能体式的工作流可以更快地进行迭代和适应实验，以在它们的指令的范围内达到最佳结果。这在例如金融服务中可能是一个关键优势，例如月底结账智能体识别异常并准备日记账条目，以减少结账周期。同时，查证智能体自动将发票与合同、采购订单和收据进行交叉核对，而无需人工审核即可标记差异。如果报告政策、组织结构或客户和供应商列表发生变化，智能体系统会自动调整端到端流程。

代理将知识转化为行动。

尽管通用人工智能可以显著提高生产力，但代理式人工智能由于其能够将知识转化为协调行动的能力，其潜在价值可能要大得多。随着组织部署多个代理，他们需要向它们提供正确的知识来驱动最有效的结果。这就需要系统地捕捉和结构化通常只存在于员工头脑中的隐性专业知识，使其可供代理使用。例如，在零售店绩效审计中，审计代理会持续监控店铺运营数据、顾客反馈和店铺销售额，标记不同地区的合规问题和绩效异常。同时，代理会自动为区域经理生成纠正行动建议。

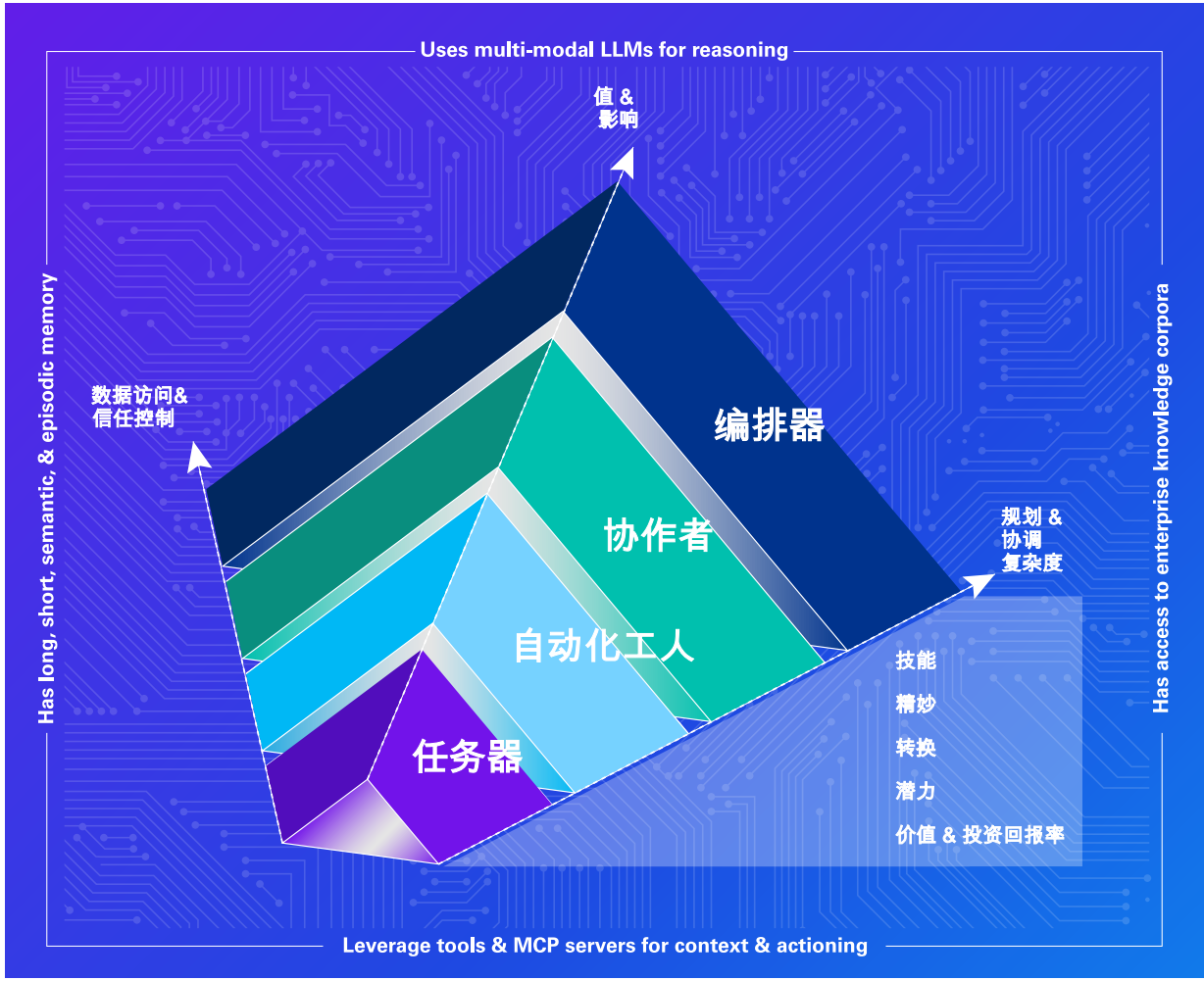
代理人的谱系正在演变满足关键需求

确定在何处使用特定代理类型可能很复杂。KPMG 开发了一个名为 KPMG TACO 框架的结构化分类系统 ™ –任务者、自动化者、协作者和编排者–它可以帮助组织理解这个不断变化的格局，并确定如何最好地利用智能代理AI。

跨类别，核心计算组件保持一致性，例如包含LLM的基础模型和推理模型、知识表示系统、上下文处理、记忆架构以及包含模型上下文协议（MCP）的工具集成框架。然而，在目标复杂度不断增加方面存在关键区别。

智能体可以完成相应的规划和编排能力。

这个渐进式框架为组织提供了一种系统的方法，以匹配其业务需求与适当的代理复杂程度。随着代理类型和复杂性的快速发展，组织也应该为代理如何相互协作和沟通做好准备，这是行业领导者已经围绕其进行对齐的事件。最后，拥有一个集中的“人工智能工厂”，其中新的代理能力可以被构思和开发，将是关键的，特别是对于那些想要构建自己的定制代理而不是购买现货产品的组织。



任务器

任务执行者执行定义明确、单一的目标，这些目标具有重复性任务和较低复杂性，例如审核发票或筛选合规风险。它们依赖于可在多个应用程序和业务流程中使用的坚实基础数据。“人在回路中”提供详细说明，概述了代理必须执行的步骤和操作。任务执行者需要关于需要完成什么的指导，而不是如何完成它的指导。

示例 Tasker 应用

- omer服务： 客 根据关键词对入站的支援工单进行分类，并分配给相应的团队。

供应商尽职调查： • 根据全球制裁名单核对屏幕供应商名称，并标记潜在问题。

- **语音验证：** 在 提取并验证数据以合规规则。
- **外交事务：** 腿 将过去的法律裁决转换为标准化格式。
- **行政：** 审核员工费用报告，以确保符合政策规定和提供支持性文件。

自动化工人

自动化工具会分解更复杂的目标，并管理跨越多系统工作流的任务，这些工作流可以包含应用程序、系统和功能领域。这类代理会借鉴“隐式知识”，这是一种基于员工过去在组织中经验而存在于他们头脑中的知识。自动化工具会执行端到端流程，协调相关任务，管理任务之间的依赖关系，并根据需要动态地使用工具、API或MCP服务器。

示例 Automator 应用程序

- **供应链：** 通过集成订单和运输管理系统以及供应商API来简化工作流程。
- e: **医疗** 通过整合医院计费系统、付款系统和监管数据库来自动化理赔审批。
- **金融：** 通过管理多个系统中的应计项目、对账和分录来加速月末结账。
- **应收账款：端到端域** 生成发票，支付调和，以及提醒。
- omer 引导： 客 自适应缺失信息或合规检查。

案例研究：在线贸易公司使用多智能体“自动化器”简化采购到付款流程

一家在线交易公司转向德勤和代理式人工智能平台公司Ema，以创建一个自动化的采购到付款系统。Ema的产品是一个多代理系统，可以连接到企业工具，以结构化和非结构化数据来执行复杂的多步骤任务。在这种情况下，德勤和Ema为他们共同的客户创建了一个简化的应计解决方案，其中Ema提取了Coupa数据，包括发票采购订单和收货单，识别出异常，然后可以升级给人类进行核对。结果是该公司现在能够在几小时内完成应计过程，而不是历史上需要三位全职员工花费10天的工作量。

协作者作为自适应人工智能队友，与人类互动协作以达成多维目标，同时动态响应用户反馈和环境演变。这些智能体整合多种人工智能能力（机器学习、自然语言处理、语音、计算机视觉），能够与结构化和非结构化数据源协同工作，提供基于专业知识的支持和增强。与简单的智能体不同，协作者保持上下文感知和长期记忆，能够在持续的复杂互动中发挥作用，从而成为真正的数字同事而非被动工具。

示例合作者应用程序

• **产品开发：** Pr 综合用户反馈，建议功能优先级并生成包含时间表和资源估算的发布计划。

Marketing: • 与营销团队一起头脑风暴活动创意，根据风格偏好优化广告文案，并自动安排社交媒体帖子。

财务规划和分析： • 与分析师合作开发情景模型，评估假设，并根据历史数据模式提供见解，同时适应每位团队成员偏好的特定分析方法。

编排器

协调器是一种高级代理系统，旨在大规模协调多个代理、工具和相互依赖的工作流。这些代理充当智能控制塔，从广泛的专业代理和服务生态系统中动态选择，以实现复杂、跨职能的目标。此类代理依赖于显式知识，这种知识更具客观性、可量化性，并且通常是技术性的。实时运行，协调器能够实现动态资源优化、多代理编排、任务委派、代理间通信（利用代理到代理[A2A]协议等协议）、以及跨系统的依赖关系协调。为其应用做好准备需要解决技术堆栈问题，并制定稳健的受信赖人工智能协议。作为当前最复杂的AI代理，协调器有潜力真正解锁新的商业模式、促进跨行业生态系统发展，并大规模推动经济转型。

示例编排器应用程序

金融： • 通过协调代理进行货币转换、账户匹配和异常报告，管理公司间对账流程。

合规性： • 通过分配代理来审查地方法规、确保合规性、进行审查，以协调多司法管辖区的合规性监控。 并升级手动违规行为

• **多主体采购优化:** 跨全球子公司协调采购、谈判和合规代理——企业内部和外部。 the

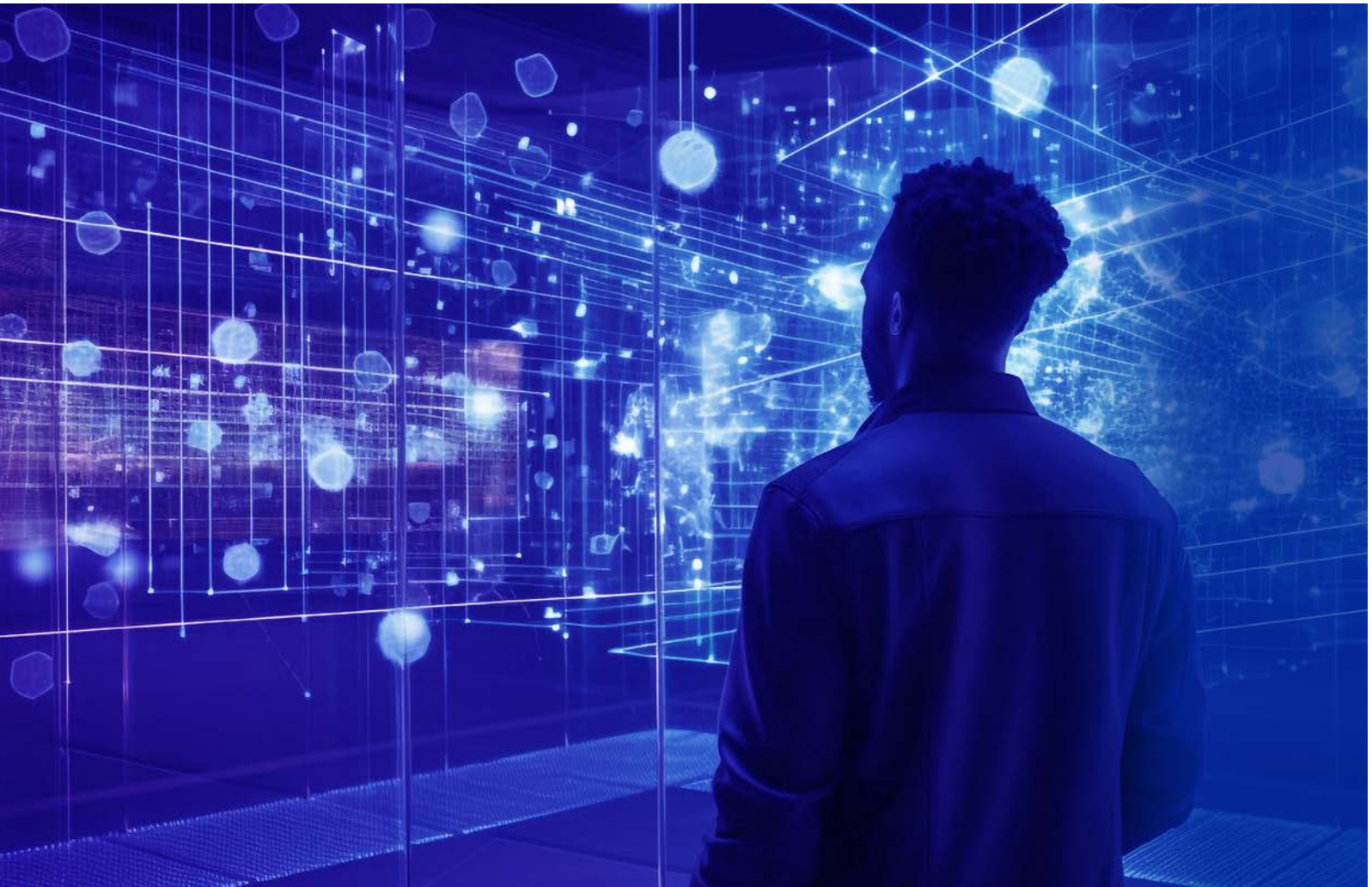
每个TACO代理——无论是任务执行者、自动化器、协作者还是编排者——本质上都是一个多代理系统。每个代理都由多个协调的代理和子代理组成，它们协同工作以实现既定目标，而不是作为一个单一的、整体化的单元运行。所有TACO代理都涉及一定程度的编排或协调，尽管这种协调的复杂性可能会有所不同。

KPMG TACO框架™

概述

	任务器	自动化工人	协作者	编排器
总体复杂度	**低**	**低至中等**	**中到高**	**高**
主要用途	执行单一目标，使用一或许多任务。	自动跨多个系统和流程领域。	人类/AI合作，其中AI作为解决问题的队友求解。	多智能体协调追求复杂的生态系统目标。
规划能力	简体：基于提示词的规划执行，包括链接和门控逻辑。	基本：几个子目标确定性逻辑与决策点，以及自适应提示。	中级：自适应和结合人类的情境规划协作。	复杂：多智能体与应急协调规划和资源优化。
价值主张	释放劳动力以创造更高价值任务。效率、创新和新的工作方式。	跨多个目标协调系统。重新构想工作流程流程。周期时间缩短。提升了客户体验。	提升员工创造力和创新。创造无限人类乘数效应。改进员工体验。	开拓新的收入来源和模型。释放经济转换。
所需知识 工具，包括MCP需要	明确目标指令 标准化API连接器用于 • St 具体动作 • MCP：最小复杂度与直接调用工具	• 复杂，跨应用和过程性目标指令 跨系统的深度知识 企业API连接器w/ • 身份验证处理 顺序工具操作	• 精选数据的可用性 领域知识语料库 专业 目标表达式带约束 • 并且偏好 xity w/ • • mcp: 适度复杂高级连接器 w/ • Se 错误处理 • MCP：复杂/高 xity for handling tool comple 相互依存和国家 管理	e知识与综合 • 目标表达式都在外部 在企业内部 对复杂政策的了解； • 精密连接器 生态系统 w/ 动态发现 MCP：高级编排 • w/ 并行工具执行和 复杂状态协调

为您的智能代理之旅奠定基础



智能体AI似乎正在加速发展，并承诺将比生成式AI更具颠覆性。与此同时，它仍然处于早期阶段。从可能性到可操作现实的企业路径充满不确定性，并且仍然缺乏跨越许多障碍的桥梁，一些是已知的，另一些尚未被发现。但正如爱因斯坦所说，“困难之中蕴藏着机遇。”率先成功的公司可能会获得优势，而其他公司在努力跟上步伐时可能会陷入困境。从炒作到超高性能之间的时间往往被低估，但也可能比我们想象的要短。赢家和输家可能将在12到36个月内决定。为了提高胜算，每家公司现在都可以开始这段旅程，展望未来想象未来，并通过解决四个关键基础问题来准备开始它们的智能体AI之旅。

策略

为您的智能代理之旅奠定基础

据著名物理学家尼尔斯·玻尔所言，“预测非常困难，尤其是关于未来的预测。”但我们愿意打赌，自主型人工智能将迫使并使组织更具战略敏捷性。将有必要比以往任何时候都更频繁、更深入、更迅速地审查和挑战企业战略——这些战略往往多年前形成且仅每年审查一次。在许多行业，随着劳动力数字化和知识自由化，进入壁垒正在降低。 [10] 同时，新的数字护城河 [11] 正在出现，例如，可以访问大型、高质量的数据库和负担得起的电力。为了在一个由人工智能重塑的市场中竞争，许多人需要重新思考竞争。 他们从头开始整个业务——包括他们服务的客户、他们提供的价值以及他们

评估您的企业战略。

与其举行年度外勤战略会议，我们建议采用更频繁的评估周期来应对自主AI环境中的不确定程度和变化速度。使用情景构建来指导你的选择，并在方法中至少包含三个组成部分：量化当前状态业务中的价值机会、评估他人可能颠覆你的风险、以及考虑颠覆他人的机会。公司可以从分析自身组织的机会入手，但也必须考虑所有客户、供应商和竞争对手可能也在采用自主AI的影响。

塑造您的代理策略。

结合企业整体战略，并与GenAI采用进程并行，企业需要确定开始构建能动型工作队伍的紧迫程度。决定您是要成为早期采用者、快速跟随者还是积极监测者。然后，在组织内部精准定位最高价值的初始部署领域，例如职能、工作流程或任务类型。这些分析需要量化代理可以解锁的增量价值，评估增量风险，并从技术和人员角度理解代理的成熟度。

进化你的合作伙伴生态系统。

随着代理将人工智能引入企业的核心运营，对技术提供商的依赖将增加。您选择合作伙伴以及您对他们的重要性，可能会实质性影响您进入市场的速度。 [12] 与大型科技公司和初创企业中的领先人工智能（AI）公司建立合作伙伴关系至关重要，并且已经非常受欢迎。不要忽视那些可以在特定职能、用途中带来竞争优势的新兴和小型潜在合作伙伴。 行业，或领域

[10] 理解人工智能代理及其商业影响，华尔街日报，2025年4月18日。
[11] 护城河是保护市场份额和盈利能力免受竞争对手侵害的人工智能技术。（来源：《你的数字护城河有多大？》标准普尔全球市场情报公司，2019年8月16日。）
[12] 通过合作伙伴生态系统加速增长和创新，KPMG，2025。

劳动力

为您的智能代理之旅奠定基础

通过现在花时间来设想自主型人工智能对组织的影响，公司能更好地管理角色、技能和工作力结构必要的转变。这种远见将帮助组织应对变化的程度，并增加获得竞争优势的机会。

人类活动可以分为结构化工作，它遵循标准化的流程和明确的规则，以及隐性工作，它涉及运用判断力、创造力和经验。结构化工作为代理提供了近期潜力，并且可以借助现有的流程挖掘和文档化软件工具来辅助。隐性工作更难自动化，但代理式人工智能随着时间的推移可能会产生更大的影响，有数家初创公司正在出现以捕捉隐性工作。现在能编码的工作越多，代理式人工智能的影响就越快、越大。在最近的一项KPMG人工智能脉搏调查中，78%的受访者表示他们 sẽ 使用代理式人工智能来分析复杂的数据集，这需要隐性工作，而66%的计划为日常行政任务雇佣代理。 [13] 建立体系化的方法来捕获和编码领域专家的隐性知识以提升代理人的有效性将变成一项运营必需品，并可能导致竞争优势。

[13] KPMG 人工智能脉搏调查 Q1，2025年4月。

劳动力如何？推动采用和参与

采用生成式人工智能是一个逐步的过程，通常受到员工抵制、怀疑和“旋转座椅”方法的影响，因为员工需要从日常工作流程中转换过来使用生成式人工智能。代理式人工智能的引入正在改变这种动态。通过将人工智能代理嵌入不同角色的独特工作流程和任务中，组织可以实现更高的采用率、接受度和利用率。

即便具有代理式AI相对易用的特点，一些员工也可能不愿意与AI代理并肩工作。在最近的一项KPMG AI脉冲调查中，45%的受访者表示他们的员工对变革持抵制态度。* 因此，有必要建立一个强大的变革管理计划，该计划应考虑AI代理对团队动态、士气和协作与创新文化的影响。此外，重要的是要传达将AI代理整合到劳动力中并不是要取代人类工作；它的设计是为了增强现有劳动力的能力。

由于人工智能代理将被嵌入专业人士的日常工作中，并与采取行动自动结合，组织将能够实现更大的劳动力专业化和留存，更高的结果信任度以及增强的创新能力。根据哈佛商业评论的报告，代理承诺到2027年将推动劳动力效率提高30%，运营成本降低25%。

同时采用生成式人工智能（GenAI）和人工智能代理，并同步解构和重建工作角色组织，更有可能实现显著的生产力和能力提升。一项调查超过10万名来自11个与生成式人工智能（GenAI）相关职业的工人的研究表明，人工智能工具可以将三分之一员工的工作任务的工作时间减少50%。**根据最近的一项KPMG人工智能脉冲调查，组织领导认为最能从代理式人工智能中获益的职能包括信息技术（76%）、运营（74%）、风险与合规（56%）、财务（39%）和市场营销（35%）。*

*毕马威人工智能脉搏调查2025年第一季度，四月。**马克·珀迪，什么是代理型人工智能，以及它将如何改变工作？哈佛商业评论，2024年12月12日。

劳动力持续。

为您的智能代理之旅奠定基础

改变你的改变方式。

在工 作 流程中采用人工智能正被许多公司证明比预期的更具挑战性。虽然自主型人工智能对人类日常行为的依赖程度较低，但类似的挑战最终将应用于工作初始转移以及数字同事和人类同事之间的互动。传统的自上而下的变革管理方法，依赖于技能提升、培训、绩效指标和问责制，尚未被证明对人工智能有效。公司应探索以角色模范、同伴间学习和心理安全为关键成分的行为改变方法，这些方法应包含旨在设计文化的多重干预措施的鸡尾酒组合。 为他们独特

想象一个流体混合型组织。

随着代理加入数字劳动力队伍，他们将和人类一起成为组织结构的一部分。这将要求为代理和人类提供新的报告、目标设定和绩效管理方式。挑战加剧的是，在未来，数字工作者的数量可能在几秒内以数百或数千的量级发生变化。对于人类而言，他们的角色、汇报线和绩效指标也可能需要发生显著且更频繁的变化；一个恰当的类比是每年进行一次大的并购整合。依赖外包的公司可能会发现，如果使用代理完全自动化，有可能以极低成本将工作重新设在国内。即使是从一开始就几乎或完全没有人类，成立一个完全由代理驱动的业务部门或新创业公司也可能证明是可行的。

以下是一些人类与人工智能代理协作的例子：

在金融领域，团队不再需要在月末结账过程中有意识地与一个生成式人工智能系统互动。相反，代理可以自动识别异常交易，准备分录，并在需要人类判断时向控制者发出警报。

在消费者和零售领域，人工智能代理可以作为虚拟购物助理，提供高度个性化的客户互动。这使得人类员工能够专注于更具战略性的任务，例如开发新产品和服务。

在生命科学领域，AI智能体可以与人类研究员合作，从而更快地取得突破性治疗方法，特别是对于那些仅靠人类努力可能无法治疗的罕见疾病和难治性癌症。

一个由自主AI赋能的增强型劳动力队伍可以驱动显著的进步和创新，使组织处于行业前沿。 of their

治理/信任

为您的智能代理之旅奠定基础

AI代理天生需要更严格的控制，并且需要更坚定地遵循可信AI原则，因为它们在相对自治的情况下运行。即使发生错误，在人类干预之前，AI代理也可能以更大的规模放大错误，传播和重复不利行为。因此，如果没有更健全的治理计划，组织将无法从代理AI中实现全部价值，也无法像那些拥有治理计划的公司一样快速行动。

提升安全与隐私。

除了人工智能的标准安全考量，如透明性、可解释性、数据隐私和合规性之外，采用自主式人工智能的组织应进行定期的压力测试、偏见检测和安全失效机制，以防止意外后果。想象一下，智能体内部的规划器在每次执行时都提出不一致的计划，或者更糟糕的是，执行行动时使用了错误的工具。与通常仅限于局部事件的人类错误不同，自主式人工智能编程或决策逻辑中的单个错误可能导致广泛后果，可能在问题被检测到之前就同时影响众多结果。

避免潜在的伦理违规。

在整个AI实施过程中，尤其是在代理式AI方面，组织应将伦理考虑放在首位。务必在开发过程的每个步骤中都考虑伦理问题，而不是在最后才附加。尽早建立伦理指南和治理协议，以减轻潜在的偏见和公平问题。扩展现有的伦理政策，以包含AI代理的具体风险。坚持要求所有AI代理的构建和监控过程的透明性。确保输入到代理式AI系统中的数据没有偏见，以避免持续有害行为。 刻板印象或排他性

将人置于闭环中。

而生成式人工智能受益于拥有人类 *在* 人工智能生成建议与采取行动之间的循环，这种情况并不适用于更自主的代理。相反，公司需要确保代理设计包含人类 *on* -循环原则，其中人类进行监督和监控，但不直接干预和批准每个动作。相反，他们监督整个过程，并在必要时拥有权力介入以覆盖系统。

技术、数据和安全

为您的智能代理之旅奠定基础

尽管人工智能代理对数据的广泛使用尚未到来，公司仍需确保其专有数据对代理来说是可访问且质量足够的。随着他们使用代理范围的扩大，组织还必须确保代理能够有效互动，并拥有可在公司人力资源系统中作为同事进行管理的数字身份。

开始构建你的智能供应链。

为获取代理，组织目前有三种主要选择：构建定制的解决方案、购买预构建的代理，或与外部供应商合作。每种方法都有其自身的优势和考虑因素，选择应与组织的具体需求、资源和战略目标相一致，以及所需代理的复杂性。许多人会发现，创建一个包含多种这些选项的多方面代理供应链有利，这些选项可以随着时间的推移应用于组织的不同部分。

如何获取代理：构建、购买或合作？

作为高管，尤其是首席财务官，在考虑以最经济的方式获取人工智能代理时，他们需要权衡每个选项的利弊。以下是详细分析： 看看每一个

构建：定制和控制

在内部构建AI代理使组织能够根据其特定需求定制它们，并使其与现有系统和流程无缝集成。组织还将拥有代理产生的知识产权。另一方面，由于该过程的复杂性，组织将需要一个在AI、数据科学和软件开发方面具有深厚专业知识的内部和/或外部团队来指导这个过程。例如，一家大型金融服务公司决定构建自己的AI任务员以自动化发票处理。通过在内部开发代理，该公司能够定制代理以处理与其组织相关的特定金融法规和内部流程。

科技，数据，和安全性持续。

为您的智能代理之旅奠定基础

组织掌握着大量专有数据，但许多人目前无法有效访问。要在代理时代取得成功，组织需要拥有一个现代的、云端的数仓平台和强大的数据基础，其中包含高质量、准确、可访问、无偏见且富有上下文的数据。建立强大的数据治理协议，以确保数据被合乎道德和安全地收集、存储和使用，并符合监管要求和数据隐私标准。MCP在使代理能够动态访问并将其相关数据注入推理过程中起着至关重要的作用。最后，组织应实施企业级数据治理——确保数据完整性，实现安全访问，通过DLP控制保护敏感信息，减少偏见，保证数据质量，并遵守隐私和CCPA规定。 GDPR、HIPAA等规定

购买：快速执行和效率

购买现有的代理式人工智能能力是最快且最直接的选择，并且是67%的最近KPMG人工智能脉搏调查受访者的首选获取代理的方式。*一方面，这种选择是最快速的，因为它涉及从成熟供应商处获取预构建的人工智能代理，这些代理可以立即部署以解决特定的业务需求。它还可以比从头开始构建更具成本效益，并且具有提供访问经过充分测试和验证的人工智能解决方案的额外好处。另一方面，这种选择并非没有挑战：现成的人工智能代理定制选项有限，因此，随着时间的推移，它们可能对某些客户变得过时。此外，将这些工具与现有的技术堆栈集成也存在潜在挑战，以及代理可能不符合标准的可能性。 具备与组织自身相媲美的数据安全能力

合作伙伴：获取先进专业知识

与外部供应商合作结合了自建和采购的优势。这种方法涉及与人工智能专家合作开发和实施人工智能代理，利用他们的专业知识和基础设施，同时分担风险和成本。挑战包括与内部自建相比，对人工智能代理的开发和定制控制力较弱，以及潜在的更高成本。与任何技术合作一样，第三方风险需要放在首位，并纳入服务水平协议。需要建立保护措施，以保护您的公司，如果在最初商定的开发计划中合作伙伴转变方向，如果系统失败，如果向系统输入了错误数据等情况。后者尤其关键，因为没有设置保护措施就向人工智能代理输入高度敏感信息可能导致严重的数据泄露。

最后，在评估选择哪个途径时，需要考虑的关键问题包括：组织内部是否具备构建AI代理的专业知识和资源？预制解决方案是否足够，还是有对高度定制化AI代理的需求？代理是否需要快速部署？哪种类型的代理最符合长期战略目标？是否有现成的运营模式来维护和更新这些代理？

*毕马威人工智能脉搏调查Q1，2025年4月

技术、数据和安全的持续发展

为您的智能代理AI旅程奠定基础

启用一致的代理间互操作性。
代理之间的通信必须超越自定义集成或脆弱的交接。组织可以采用代理到代理（A2A）标准，例如谷歌正在出现的相关协议，它为安全、可解释和可审计的代理交互提供了一个标准化的框架。A2A支持代理之间的消息传递、意图协商和结构化协作——从而实现多代理任务编排、代理链式处理和动态角色分配等用例。采用代理互操作性标准可以确保企业代理保持模块化、可组合和面向未来，同时避免供应商锁定和重复劳动。

跨代理通信和外部数据访问的通用标准

目前，AI模型所"知道"的内容在称为"预训练"的初始过程中被输入系统，这通常只发生一次或在进行定期更新时。在这种情况下，数据集有一个截止日期，功能仅包括用户提示、正在进行的对话历史记录以及一些被引入对话的外部信息。

随着代理的快速发展，一项并行工作正在进行中，允许它们跨组织进行交流，同时不断连接并获取外部信息来源、工具和服务。尽管仍处于开发中，Anthropic的模型上下文协议（MCP）已确立了标准和平台，消除了对定制集成的需求，并使更强大、更具上下文感知能力的AI应用得以实现。

MCP的核心组件包括：

MCP客户端

一个允许MCP服务器通过标准化协议访问外部数据和功能的AI应用程序或工具

MCP服务器

使用MCP协议以利用数据源、记录系统、代理等特定功能的程序

MCP运输

一个通信层，用于处理MCP客户端和MCP服务器之间的消息交换

最终，该协议将允许组织实现更小、更精准和高效的AI系统，这些系统能够相对无缝地与其他智能体以及外部数据交互，而无需定制化微调。

来源：Beni Edwards，MCP：新的"USB-C for AI"正在将激烈竞争对手聚集在一起，Ars Technica，2025年4月1日

技术、数据和安全的持续发展

强化代理身份和安全。
每个代理必须有唯一的身份标识，具有作用域权限、凭证和持续性

监管。同样重要的是运行时隔离，确保代理在分段的运行环境中操作，以便可以检测和限制数据暴露、工具滥用或异常行为。每个代理的操作都必须可审计、可撤销和可归因。组织还必须主动缓解新兴的安全威胁，例如内存中毒、代理劫持和身份伪装。 [14] 解决方案包括实现执行日志记录、身份认证、运行时隔离以及实时监控，以确保代理行为保持安全、可解释和合规。

Source:
[14] 针对LLM应用和代理系统的十大推荐，开放Web应用程序安全项目（OWASP）生成式AI，LLM安全指南和倡议。

加速代理人采用的实用下一步

在本文撰写之际，美国许多公司已在其智能代理旅程中迈出了第一步，开始探索或试点智能代理。然而，多数（88%）公司尚未在其运营中积极部署任何智能代理。[15] 无论您在您的自主AI旅程中身处何方，起点在哪里可能并不那么重要，而您向前迈进的速率、效果和安全度则更为重要。

要成功，企业需要明确如何将代理融入其整体人工智能转型旅程，包括为在何时何地启动跨关键职能的扩展方法提供一个坚实的基础。大多数企业若能加速其数据转型工作及其受信任的人工智能治理面临着更高的能动性风险。人才领导层将忙于为数字同事的到来而准备组织，例如为数字和人类员工制定新的绩效指标。

大步成功法

[15] KPMG人工智能脉搏调查Q1，2025年4月。

要加速一个智能体AI程序，领导者应该考虑以下六个后续步骤：

1. 阐述愿景

从清晰的战略和愿景开始，实现智能代理AI的集成。愿景应阐述智能代理将如何改变业务、期望成果、要追求的关键业务目标，以及如何开始供应智能代理。确定智能代理可以解决痛点并增加最大价值的地方，例如常规交互。 任务，复杂的流程或客户

2. 开始代理飞行员

启动代理式人工智能旅程的高管应考虑该技术在组织中哪些地方能提供最大价值，因此，应如何开展试点项目。正在尝试人工智能增强运营的组织可以尝试以下三种方法之一或多种：

关注"热点"： 组织此前已成功开展过GenAI试点的前沿领域，特别是那些用户参与度高之处。这些领域很可能具有最高的价值创造潜力，同时也拥有最成熟的AI基础设施和专业人士。

深入一个函数： 在特定的、高度重复、低风险的职能领域（如金融）中广泛嵌入AI代理。使用此试点项目作为可扩展的模型，将代理式AI应用于组织内其他职能。

广泛利用： 识别一个对业务运营至关重要的跨职能价值流，并在整个端到端流程中实施人工智能代理。

3. 准备在关键职能和/或工作流程中扩展代理

考虑是否存在一些可以快速启动以实现早期胜利的AI代理平台，这些胜利可以建立高管认可和势头。使用类似KPMG TACO框架的工具 ™ 为了识别能最好满足您需求的AI代理类型，并确定哪些部门和流程最适用于AI代理应用。最终，制定一个扩展到企业级战略的计划，涉及多种代理类型协同工作。

组织必须将现有的AI治理计划扩展以涵盖代理式AI，并建立机制以应对法律和监管问题。考虑创建一个包含所有AI代理的动态目录，以跟踪它们的目的、依赖关系和性能指标，从而实现有效的扩展和治理。开发强大的运营流程来管理和维护AI代理，包括监控系统、性能指标和持续改进方法。

6. 实施针对人工智能代理的Trusted AI评估

随着组织将人工智能治理实践与日益增长的监管规范和领先标准相一致，对人工智能代理的严格评估和报告方法将至关重要。人工智能系统卡记录了技术在组织中的使用方式，作为人工智能系统评估结果的单一、权威来源，详细说明预期用途、数据考虑因素、人工智能组件和局限性。此外，在将具有代理功能的人工智能系统投入生产之前，组织应进行彻底的测试，其中越来越多地包括运行严格攻击测试和防御评估的“紫队”。这些流程中的输入最终将形成信任分数，该分数反映了人工智能系统对组织人工智能原则的遵守程度。

6. 建立 代理人才绩效指标

建立衡量指标以评估试点项目的影响，以及收集试点阶段利益相关者反馈和学习机制。持续衡量并优化人工智能代理的性能。制定明确的性能指标以评估其有效性，包括错误率、处理时间和客户满意度。使用数据和反馈持续改进性能，包括优化算法、更新训练数据以及实施新功能。需要注意的是，人工智能代理实现遥测以监控其服务等级协议合规性、系统健康、工具性能和异常情况。

随着新型AI代理正在快速引入，重要的是要记住这只是开端中的开端。通过为代理AI时代的到来在今天奠定基础，组织将能够为不仅他们的运营，而且他们的整个业务进行全面加速。

KPMG如何提供帮助

我们帮助[illegible]式AI[illegible]化方[illegible]的竞争优势，从战略到执行并肩协作，秉持以人为本、基于信任的方法。通过优化人类和代理当今的合作，我们可以释放[illegible]的全[illegible]潜力[illegible]并[illegible]创造持久价值。

我们提供一系列定制服务，以帮助推动您的自主人工智能旅程：

人工智能战略

构想并制定您的智能代理AI战略和商业方案，并制定可行的路线图。

制定您的代理AI策略和执行计划 • 根据您的独特起点和商业需求。构建一个具有量化回报的可信商业案例/ • 评估指标，以推动投资、获得高管支持及资金。 项目

人工智能启动

开启你的智能体AI之旅，并驾驭AI颠覆以利于己。

利用我们可重复和可复制的方法 • 快速生成自动化和增强运营的解决方案，释放 AI 的全部价值。从概念验证加速到价值实现。 • 从推出到规模化采用。Saf • 尝试使用AI代理进行实验，并在整个组织中扩展已测试用例的采用规模。

人工智能劳动力

将您的组织转型，以在人工智能环境中蓬勃发展。

解锁代理式AI的全面潜力，为你和你的... • 旅途中的工作人员。通过人工智能代理增加您的工作力量，实现更多 • 战略工作与加速效率。 • 重塑你的员工队伍并定义代理式 AI 治理，以帮助你实现投资的全部价值。 • 为您的员工提供个性化的采用和技能提升体验，以便将人工智能融入日常工作中。

人工智能技术

构建可持续的AI和能动式AI解决方案，以及底层数据基础设施。

人工智能工厂方法 使用我们的可复制、概念验证 • 利用包括我们的咨询服务、KPMG TACO框架在内的多种资源来试点和扩展代理机构 ™ ，先进工具，成熟和新兴技术，以及有针对性的培训。

简化代理式人工智能框架的集成 • 平台，和 加速器。确保人工智能工具的快速推出以及所需的数据 • 运行它们。 • 加强和改进你的技术基础设施，以支持跨你的组织的AI和AI代理的规模化整合。

人工智能信任

安全地引入AI代理，并在整个企业中扩展。

管理风险，证券化 • y，以及遵守以实现安全人工智能
展开 自主AI • 确保您的自主AI解决方案具有伦理、安全性和框架性。 遵循我们的可信人工智能 • 遵循我们的10项道德人工智能支柱，大胆、透明、自信地部署代理式人工智能。

作者

钱德拉塞卡兰·斯瓦米
全球人工智能与数据实验室负责人
E: swamchan@kpmg.com

斯瓦米领导并执行公司在税务、审计、咨询及其他职能领域的AI战略，服务全球20万名专业人才。他指导并监督涵盖AI架构、高级知识助手、AI代理、领域调优的小语言模型（SLMs）、合成数据、企业发现与搜索以及硬件优化解决方案等各方面的研发工作与计划。他还主持KPMG AI技术审查委员会，确保值得信赖且可扩展的AI应用。

根据爱丁
全球AI销售加速领导者，提供咨询服务；美国AI技术、媒体和电信行业的首选市场领导者

E: pedin@kpmg.com

佩尔同时担任全球和美国的AI领导职务：他负责在全球顾问网络中协调AI客户产品的定位、信息传播和市场进入策略，并负责推动美国科技、媒体和电信行业的AI相关增长。他的工作包括领导公司帮助客户应对GenAI市场的颠覆，开发新的AI服务组合、AI思想领导力以及关键加速器，如GenAI价值评估。

托德·洛尔
生态系统负责人和国家运营顾问

E: tlohr@kpmg.com

托德负责制定和执行KPMG生态系统战略，该战略包括协调企业合资企业、技术联盟、供应商、下游合作伙伴、初创企业、学术界和资本投资者。托德与KPMG团队合作，开发新的市场产品，为客户制定最创新的解决方案，并拓展我们的新市场和技术覆盖范围。 利用最新

此处所描述的部分或全部服务可能对KPMG审计客户及其子公司或关联实体不适用。

kpmg.com

本文包含的信息具有普遍性质，并不旨在解决任何特定个人或实体的具体情形。尽管我们尽力提供准确和及时的信息，但无法保证所提供的信息在收到之日是准确的或将在未来保持准确。任何人在未经对具体情形进行充分审查并获得适当的职业建议之前，都不应依据此类信息行事。