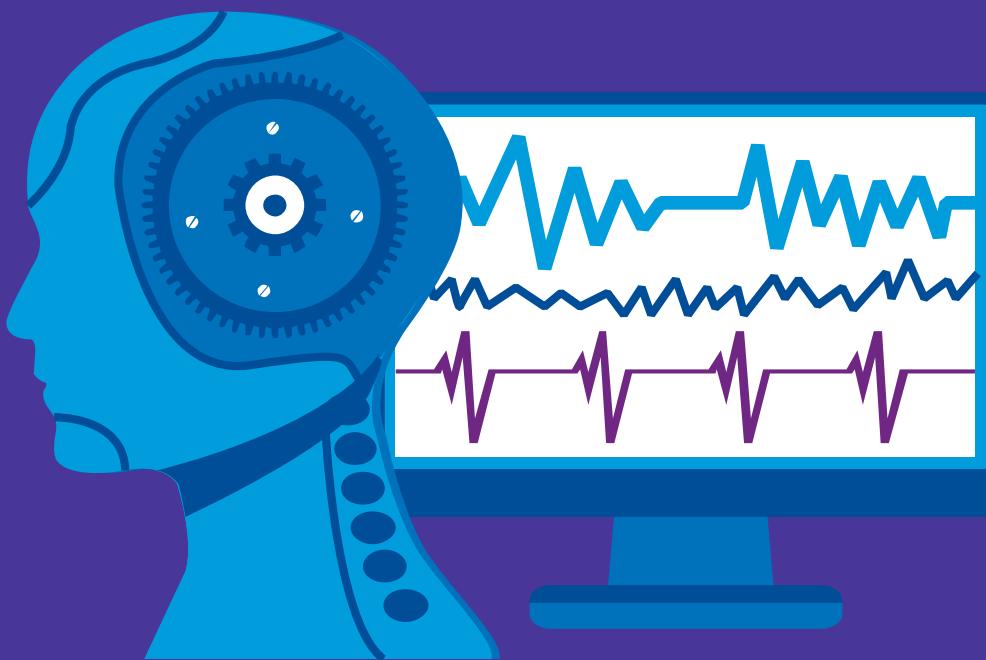


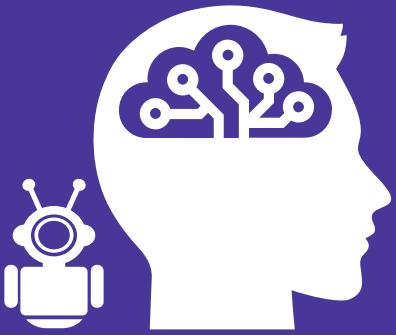


智能自动化的 风险管理

毕马威企业咨询（中国）有限公司

kpmg.com.cn





目 录

前言

2

智能自动化的管理困境

3

智能自动化的四大基础

4

智能自动化常见管控问题

6

毕马威服务介绍

8



智能自动化不仅为企业带来了新的机遇，同时也引入了新的风险。企业需从战略、交付、运营三个层面思考智能自动化的风险及管控。

智能自动化，又称为数字化劳动力，曾经是一个遥远的话题。目前，越来越多的组织与个人逐渐意识到智能化时代已经到来。几乎所有的商业组织都在积极投资前沿技术，包括大数据、预测分析、流程机器人、认知系统、自然语音处理、机器学习和人工智能等，以推动智能自动化的应用。

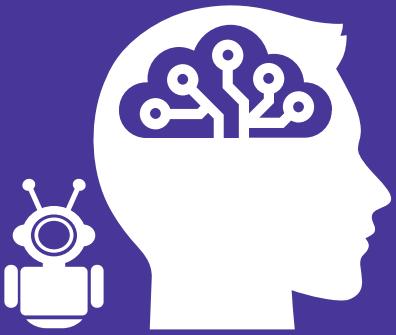
智能自动化的创新拥有变革潜力，可以提高业务处理速度、运营效率、成本效益、业务准确性和控制有效性，增强专业人员提供更具影响力见解的能力，从而帮助企业实现更快更明智的决策。

智能自动化不仅能处理简单重复的工作，还能执行智能及认知相关的工作。这种惊人的能力可以改变一个组织的业务模式，也为企业经营带来新的挑战；例如企业如何确保智能自动化程序是逻辑正确的？如何合理划分数字化劳动力的职

责范围等？同时，我们也不禁思考，企业是否了解与智能自动化相关的风险？在治理、风险管理、内部控制上，企业是否已具备应对智能自动化风险的能力？

根据《毕马威2019企业人工智能应用研究》，与开发人工智能的优先级相比，许多企业正在起步投资人工智能控制框架。大部分企业还未从战略层面思考智能自动化的效益和风险，也未在部署智能自动化的过程中进行有效的管控以确保智能化程序的可靠性。

本文分析了企业在规划及部署智能自动化过程中常见的管理困境及需要考虑的风险因素，并介绍毕马威的智能自动化的风险评估服务。



建立对人工智能的信任是领导层的首要目标。

45%的受访高管表示，建立对人工智能系统的信任极具挑战性。¹



围绕数据和人工智能发布的的新政策和法规表示自我监管时代的终结和一个全新监管模式的兴起。²



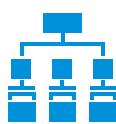
大多数领导者不清楚人工智能的治理方法应该是怎样的。

大约70%的受访高管表示他们不知道如何管理算法。³



企业正在努力厘清谁应该对人工智能程序和结果负责。

大多数企业仍在试图确定谁应该拥有部署人工智能的权限。一些公司成立了人工智能委员会或卓越中心进行集中化管理，另一些公司将职责分配给不同的领导者，如首席技术官或首席信息官。



一个包含技术支持方法的框架可以帮助企业解决智能自动化的固有风险和道德问题。

我们的目标是通过建立**完备性、可释性、公平性和适应性**四大信任支柱，帮助企业获得对他们智能自动化程序的控制。

¹ 《2018年二季度全球AI在线调查》，Forrester研究

² 《人工智能，互联网政策提案标志自我监管时代的远去》，华尔街日报专业版：人工智能，2019年4月9日

³ 《为什么审计必须覆盖人工智能》，毕马威，2018



智能自动化的损失不仅包括收入流失或监管罚款等的财务损失，还包括声誉、品牌和道德问题。企业需从四个方面搭建智能自动化的信任基础。



完备性

算法的完备性是智能自动化的核心。

管理层需要知道：

- 用于训练算法模型的数据的出处及关联关系
- 建立训练模型的控制
- 模型评估指标，并由始至终地维护指标
- 验证变更不会危害算法的初始目标
- 持续监控模型的性能指标



可释性

理解模型输出结论的原因，并且能够解释该原因是建立对智能自动化信任的必要条件。

管理层能解释模型的原理和步骤是基于：

- 对正确结果的清晰定义
- 对算法的整体治理体系
- 清晰和充足的规则集合
- 持续评估结果的合理性



公平性

如果人工智能和算法存在偏见，那么他们将不被信任。

建立公平性必须确保：

- 用于训练算法的参数与算法的目标必须是相关的及恰当的，且允许使用的
- 建立谨慎的监督和治理，以确保替代性指标不会被用于训练模型
- 运用技术手段理解数据中固有的偏差，并利用平衡、加权或反向消除等手段减低偏差
- 建立持续监控的工具和治理手段，以确保模型是持续地被训练的，训练数据和结果数据不会因为时间推移逐渐出现偏差



适应性

如果算法不能够自我修复，或不能抵消错误数据或异常数据带来的影响，那么算法容易受外部环境干扰而导致错误的结果。

适应性需要：

- 建立对训练数据及反馈数据的保护机制
- 建立持续监控模型终端和控制模型访问的基本措施



风险和治理

- 智能自动化程序的所有权不明确
- 普遍缺乏对风险的监督
- 普遍缺乏对程序的监督
- 对机器人程序缺乏统一和安全的开发和管理

机器人认证

- 缺乏对机器人ID所有权适当性，以及机器人ID与应用程序有效整合的控制
- 缺乏与机器人程序的安全性、隐私性和合规性要求相关的问责机制
- 机器人访问设置和密码管理的不合理

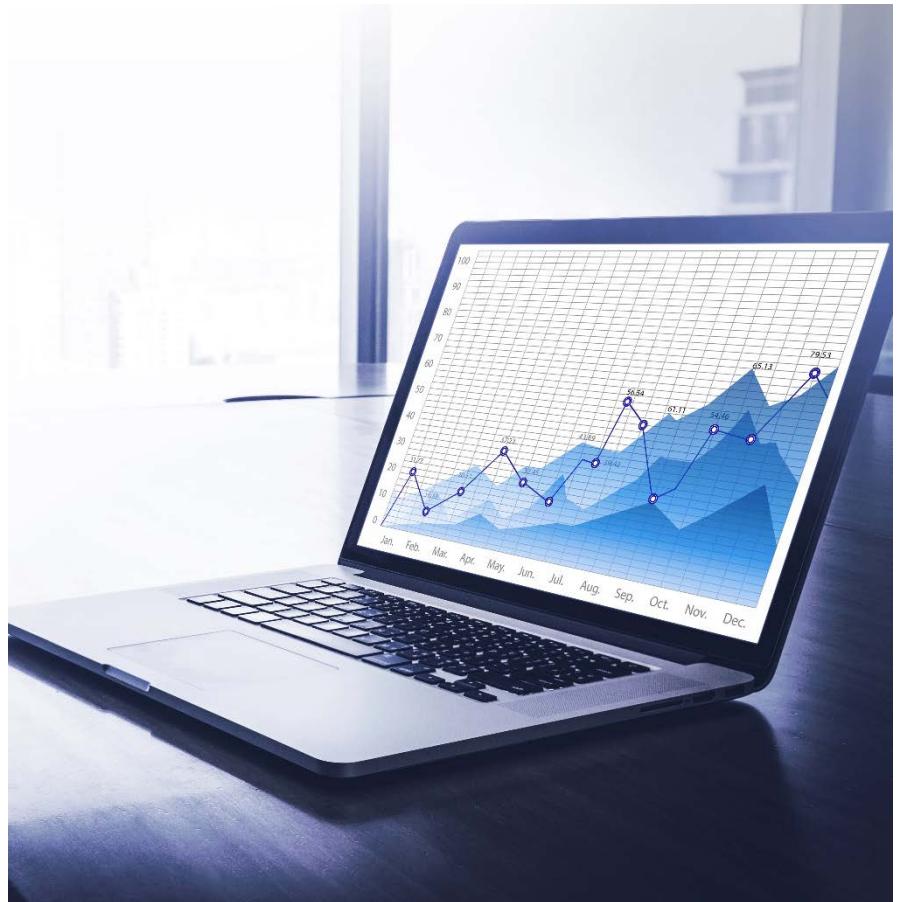


变更管理

- 缺乏评估源应用程序的修改将如何影响访问它们的机器人的正式流程
 - 申请和实施对机器人程序的更改缺乏正式和统一的流程
 - 机器人流程自动化（RPA）开发和生产缺乏隔离措施

开发和监控机器人程序

- 开发人员技能水平参差不齐，缺乏培训
 - 缺乏对错误进行处理和解决的自动预警工具
 - 普遍缺乏针对“机器人是否正在做着它应该做的事情”的控制





毕马威开发了一套智能自动化风险治理框架，协助企业评估智能自动化的风险，基于评估结果并结合企业实际提出管理提升建议，帮助利益相关方建立对智能自动化可靠性的信心。



毕马威智能自动化风险治理框架

- **战略风险评估：**从操作模式、实施路径、机器人、应用程序和基础设施等维度分析企业目前的智能自动化水平与公司战略发展及行业趋势的匹配度，并结合公司的风险偏好及风险概况，评估企业智能自动化的战略风险。

- **交付风险评估：**从安全开发、用户案例和用户体验设计、测试和质量保证等维度梳理智能自动化从设计到实施落地全生命周期涉及的流程与控制，评估交付风险。



- **运营风险评估：**从针对智能自动化的分析和优化流程，以及风险监控与报告机制设立的健全性和有效性，以及关键风险指标设置的适用性与合理性等维度评估运营风险。

我们致力于帮助客户建立对智能自动化程序、平台和机器人程序有效的管理，并将风险控制措施整合到智能自动化的解决方案中。我们的工作将帮助企业有效地遵从内部控制管理诉求及外部监管要求，并协助企业在智能自动化的数据安全和私隐、变更管理、处理完整性、可审计等方面向业界最佳实践靠拢。

如需获取更多信息，请与我们联系。

联系我们

胡丽芬

内部审计、风险管理及合规服务主管合伙人

毕马威中国

电话: +86 (21) 2212 2603

邮箱: lifern.woo@kpmg.com

梁安超

内部审计、风险管理及合规服务华南区主管合伙人

毕马威中国

电话: +86 (755) 2547 3338

邮箱: kelvin.oc.leung@kpmg.com

[kpmg.com/cn/socialmedia](https://www.kpmg.com/cn/socialmedia)



如需获取毕马威中国各办公室信息, 请扫描二维码或登陆我们的网站:

<https://home.kpmg.com/cn/en/home/about/offices.html>

本刊物所载资料仅供一般参考用, 并非针对任何个人或团体的个别情况而提供。虽然本所已致力提供准确和及时的数据, 但本所不能保证这些数据在阁下收取本刊物时或日后仍然准确。任何人士不应在没有详细考虑相关的情况及获取适当的专业意见下依据本刊物所载资料行事。

© 2019 毕马威企业咨询(中国)有限公司 — 中国外商独资企业, 是与瑞士实体 — 毕马威国际合作组织(“毕马威国际”) 相关联的独立成员所网络中的成员。版权所有, 不得转载。在中国印刷。

毕马威的名称和标识均属于毕马威国际的注册商标或商标。

二零一九年八月印刷