Microsoft 365 Copilot

影子 AI 风险冲刺套件

一份通用信息检查清单与行动规划表，旨在帮助安全和 IT 负责人与相关内部利益相关者，就潜在的非授权 AI 使用、过度共享的风险、数据保护考量及治理议题展开讨论。



概述

影子 AI 风险冲刺套件是一个通用信息框架，旨在支持就潜在的非授权 AI 使用、数据处理注意事项以及治理方法展开结构化讨论。该资源旨在帮助团队围绕 AI 相关决策的可见性、优先级及协调，与利益相关者展开讨论。

在使用该套件之前，应根据组织自身的环境对其进行调整，并参照当前的 Microsoft 文档、许可、可用性，以及适用的法律、隐私、合规、安全、IT、采购和业务要求进行审核。

目录

3
影子 AI 风险测验

4
五日冲刺路线图

5
行动规划表

6
了解详情

何时使用此冲刺套件

当 AI 应用程序、Copilot、智能体或扩展程序的采用速度可能快于内部审批流程时，可将此冲刺套件用作引导讨论的工具。其目的在于支持讨论和优先级排序，而非规定具体必须采取的行动。

建议的冲刺成果

- 制定一份可供讨论的 AI 工具和数据接触点的工作清单。
- 确定需要进一步审查的领域并明确优先级。
- 探讨潜在的数据保护和访问权限考量，供利益相关者审查。
- 讨论一种可能的治理方案，包括责任归属与推进节奏。

免责声明

此内容仅供参考，不构成法律、监管、合规或技术建议，亦不保证实现检测、防护、风险降低或合规等效果。各组织有责任独立评估自身义务、风险承受能力及技术配置，包括产品功能、可用性和许可等事项。

由此开始：影子 AI 风险小测验

作答结果仅作为讨论的方向性参考。若多项回答指向“高风险”，则可能表明需要对相关主题给予更多关注、供利益相关者审查或进行优先级排序。若多项回答指向“中等风险”，则可能表明在某些领域需要明确责任归属、完善政策或建立证据收集流程。若多为“低风险”，则可能表明可将本次冲刺用作就绪讨论和优化练习。

本测验并非正式的评估、评分方法、审计或合规性认定，任何后续步骤都应反映每个组织的法律、监管、合同、技术和运营背景。

讨论问题	低风险	中等风险	高风险
你是否能实时掌握当前正在使用的 AI 应用、扩展程序、Copilot、插件与智能体的情况?	□ 清单保持最新。	□ 部分可见。	□ 没有可靠的视图。
你能否了解 AI 工具可能访问的敏感数据?	□ 访问情况已建立对应关系。	□ 仅限核心工具。	□ 未知或不一致。
经批准的 AI 工具及使用路径是否明确?	□ 路径明确。	□ 指导标准不统一。	□ 团队独立选择工具。
控制措施是否已与 AI 相关数据路径建立对应关系?	□ 控制措施已建立对应关系。	□ 仅覆盖部分工作流。	□ 未对应于 AI 使用。
是否有关于 AI 治理决策的证据?	□ 已明确定义责任归属与推进节奏。	□ 证据是临时性的。	□ 没有一致的证明路径。

五日冲刺路线图

作答结果仅作为讨论的方向性参考。若多项回答指向“高风险”，则可能表明需要对相关主题给予更多关注、供利益相关者审查或进行优先级排序。若多项回答指向“中等风险”，则可能表明在某些领域需要明确责任归属、完善政策或建立证据收集流程。若多为“低风险”，则可能表明可将本次冲刺用作就绪讨论和优化练习。

本测验并非正式的评估、评分方法、审计或合规性认定，任何后续步骤都应反映每个组织的法律、监管、合同、技术和运营背景。

天数	关注重点	行动	交付成果	检查清单
1	讨论潜在的非授权 AI 使用。	审查相关信号，区分已知与未知工具，并收集业务背景信息。	草拟清单、工具列表，并指定后续负责人。	□ 已确定来源 □ 已记录未知工具 □ 已记录差距
2	讨论潜在的审查领域。	按敏感性、访问权限、共享、自动化和合规性考虑因素，对用例进行分组。	已确定优先级的讨论清单及利益相关者审查列表。	□ 已记录数据路径 □ 已识别高关注度工具 □ 已建议负责人
3	保护数据与访问。	讨论基线控制、数据保护情景以及访问或终结点考量因素。	控制考虑因素、政策事项及监测领域。	□ 已讨论控制措施 □ 已记录 DLP 或标签 □ 已记录监测差距
4	治理 AI 应用与智能体。	草拟责任归属、引入流程、例外路径及证据需求。	角色、审查路径和证据登记概念。	□ 已确定责任人 □ 已记录例外情况 □ 已启动登记
5	将冲刺转变为可重复的节奏。	确认优先级，起草指导方针，并提出 30 天的推进节奏。	规划优先事项、指导纲要、汇报主题和推进节奏。	□ 已记录优先事项 □ 已草拟指导 □ 已提议推进节奏

30 天行动规划表

推荐用于领导层汇报。示例主题包括：AI 使用模式、数据考量、行动优先级、利益相关者协调和近期规划。

优先级	负责人	行动	证据 / 成功信号	截止日期
1				
2				
3				
4				
5				
6				

从 Microsoft 了解更多信息

探索 Microsoft 安全关于保护和治理 AI 使用的资源，包括数据保护、身份与访问、终结点安全以及负责任 AI 采用方面的指导。

提前规避风险，依托 Microsoft 安全稳步前行
探索前沿转型，依托 Microsoft AI 实现智能与信任的融合
借助 Microsoft 365 保障 AI 和数据安全，提高工作效率

