Microsoft 365

提升 AI 就绪度的高管行动手册

面向 CIO 与 CISO 的共享运营模式，助力组织从 AI 愿景迈向全面就绪。





03
如何使用本行动手册

04
执行摘要：企业愿景正超越 AI 就绪能力

05
就绪度差距：评估阻碍 AI 采用的潜在因素

06
AI 就绪的安全基础框架

09
助力提升 AI 就绪度的三大转变

10
面向不同角色的后续行动指引

11
着手提升 AI 就绪度

如何使用本行动手册

本行动手册为 CIO 和 CISO 提供了一个共享框架，用于构建有助于其组织提升 AI 就绪度并赋能业务转型的基础。该框架可帮助你识别组织中可能存在的差距领域，然后确定如何弥补这些差距。其核心理念是：前沿转型始于一个安全的基础，将生产力、安全、数据和管理融为一体。使用本行动手册中的信息作为指引，完成以下三项工作：

1. **达成共识。**共同探讨并确定哪些就绪差距正阻碍 AI 价值的实现。
2. **评估研判。**使用 AI 就绪安全基础框架中的五个步骤，确定组织中影响最大和风险最高的领域，以此作为起点。
3. **采取行动。**共同制定计划，明确从何处着手，以及如何逐步实现规模化扩展。

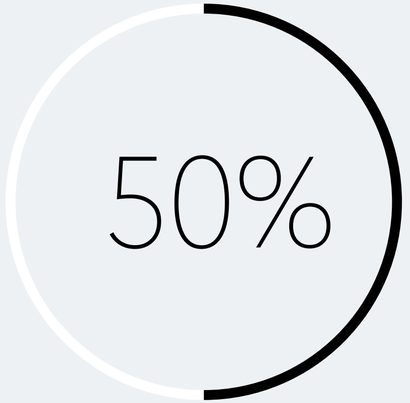


组织对 AI 的愿景可能正超越其实际就绪能力。

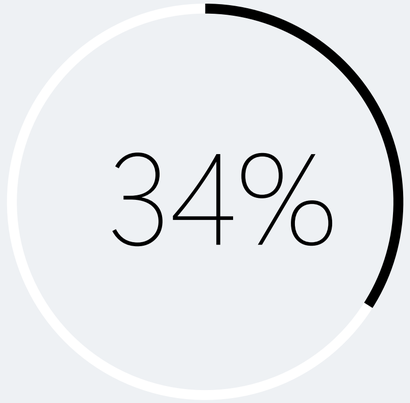
AI 已广泛普及。根据 Deloitte 于 2026 年发布的“State of AI in the Enterprise”报告，受访者表示，其所在组织在短短一年内将员工使用 AI 的权限扩大了 **50%**[1]，另有 **34%** 表示，其公司已开始利用 AI 对产品、流程和商业模式进行深度转型[1]。员工们满怀期待，已经在重新构想如何借助 AI 完成工作。他们积极尝试、构建新工作流，推进速度甚至可能超出组织预期。但与此同时，组织现有的系统、政策以及运营模式，往往仍在强化以往的工作方式。

Microsoft 的《2026 工作趋势指数》将这一现象称为“转型悖论”[2]，员工已经做好准备并开始重塑工作方式，但其所处的组织体系，包括指标、激励和规范，仍在强化过往的工作方式。加速 AI 采纳的同一股力量，也可能在阻碍其进展。这一差距不仅仅是技术采用层面的问题。它还可能因组织在特定领域是否做好了大规模应用 AI 的准备 而进一步加剧，包括工具、数据、身份、终结点和控制措施，本质上就是组织的基础。

当你的组织在互联且安全的基础上运作时，便能建立起规模化应用 AI 的底气。这一坚实的 AI 基础远不止于基础结构，更是一种运营模式。通过将人员、内容、通信、工作流、身份和设备连接到统一平台，组织还可以将安全、合规和管理集成到工作流中。这有助于建立信任与控制力，从而推动工作流转型并创造业务影响力。机遇不仅在于跟上 AI 的发展步伐，更在于重新构想工作方式。关键不在于你的组织采用和扩展 AI 体验的速度有多快，而在于如何安全地推动转型。



受访企业领导者表示，仅一年时间内，员工 AI 访问权限覆盖面便扩大了 50%。[1]



34% 的受访领导者表示，正利用 AI 对产品、流程及商业模式进行转型。[1]

就绪度差距：评估阻碍 AI 采用的潜在因素。

员工正采用 AI 以实现新的工作方式，团队不断挖掘新的用例，而早期试点项目也展示了潜在的生产力提升空间。在整个企业范围内，领导者们看到了更广泛、更大规模转型的潜力。挑战不在于缺乏对 AI 的热情，而在于运营基础未能始终与员工工作方式的转变保持同步。

在《2026 工作趋势指数》报告中，**超过 60%** 的受访 AI 用户[2]表示，AI 使他们能够将更多时间投入到高价值工作中；**超过 50%** 的用户表示，他们现在能够完成一年前无法实现的工作[2]。然而与此同时，这些 AI 用户[2]中仅有**四分之一**认为，领导层在 AI 应用策略上始终保持一致。

随着员工采用 AI 驱动的工作方式，传统流程、碎片化工具、不一致的控制措施以及未经管理的数据可能会拖慢进展。正是这股推动 AI 采用的势头，反而可能暴露出为过去时代构建的系统存在的问题。这就是就绪度差距， 往往属于基础层面的挑战。造成这一基础挑战的因素主要集中在两大方面：体验脱节与安全隐患。

- **2/3 的受访高管**表示，其所在组织过于复杂且效率低下。[3]
- **超过 90% 的受访 CIO 和 CTO** 表示，生成式 AI 已经或将会推动组织加大网络安全领域的投资。[4]

让我们通过几个典型场景来探讨员工体验和安全方面可能出现的就绪度差距。第一个场景聚焦员工体验。CIO 可能会开始注意到，员工越来越频繁地抱怨查找信息耗时过长，或难以访问完成工作所需的各类应用与工具。这些问题可能表明，由于应用、工作流、设备和数据之间的体验脱节，导致了就绪度差距，而且随着 AI 的规模化应用，这些问题可能会变得更加严重。

第二个场景聚焦安全方面。随着越来越多的人开始在日常工作流中尝试和使用 AI，CISO 可能会注意到，因过度共享信息或使用未经授权的 AI 工具的行为增加， 潜在安全事件也在不断增多。这些问题可能凸显出数据治理和访问管理方面的就绪度差距。

这些差距叠加在一起，可能会产生摩擦，从而使企业范围内大规模采用 AI 更难实现。最初看似独立的生产力、安全性和 IT 方面的挑战，可能会演变成一个共同的基础层面挑战。随着 AI 的普及，这些就绪度差距可能会变得更加明显，后果也更加严重。

虽然以上只是就绪度差距可能如何显现的假设性示例，但它们说明了机会成本不仅仅是 AI 采用方面的落后，更会在员工借助 AI 所能实现的目标与组织可支撑的 AI 规模化能力之间形成日益扩大的差距。员工可能已经准备好重塑工作方式；问题在于，组织的基础是否准备好赋能这种变革。

正因如此，规模化应用 AI 还意味着让业务、IT 和安全团队围绕一个共同的运营模式协同推进。那些能够充分挖掘 AI 潜力的组织，并非仅仅是部署更多的 AI，而是致力于夯实基础，实现生产力、安全性和管理方面的大规模协作。

就绪度自查

在进一步规模化应用 AI 之前，请先思考以下两个问题：

- 在你的组织中，哪些领域的 AI 采用速度**可能**已超前于 AI 使用和访问相关政策的制定与执行？
- AI 能否安全获取足够的组织上下文，以实质性地改进工作完成方式？

CIO 需思考：

- 我们是否拥有在整个业务范围内扩展 AI 的运营基础？

CISO 需思考：

- 我们是否拥有管控基础，支撑我们自信地规模化应用 AI？

AI 就绪的安全基础框架

要构建一个 AI 就绪的安全基础，需要具备哪些要素？有一个框架可以帮助你规划实施路径，通过五个相互配合的步骤开始构建这一基础架构。

在“连接工作”、“准备数据”、“安全访问”、“规模化管理”以及“防护与响应”这五大领域中， 你可以识别组织最关键的切入点，进而逐步进行构建、整合、转型和扩展。



1.

连接工作

构建一个连接人员、内容、对话和业务流程的工作图，让 AI 能够基于组织内的工作方式获取上下文信息。各项工具实现互联后，员工便可以从孤立的 AI 用例，迈向涵盖会议、文档、业务应用和协作工具的 AI 辅助工作流。

着手点
确定你最有价值的生产力工具、协作系统和数据，优先连接员工使用最频繁的资源。

预期收益
员工可以减少在搜索信息、在应用之间切换以及重建上下文方面所花费的时间[1]，同时 AI 将基于组织实际运作方式提供洞察、建议和行动方案。

就绪度自查

CIO 需思考：
- AI 能否访问员工提升工作效率所需的人员、内容、对话及工作流？

CISO 需思考：
- AI 能否在不造成新的可见性、治理或安全漏洞的情况下，获取组织上下文信息？

2.

准备数据

发现、分类、标记、保护和治理高价值数据，使 AI 能够有意识地运行，并确保其生成的内容遵循安全、合规和业务政策。当数据得到管理、可搜索且相互关联时，AI 才能基于组织知识做出响应，而非依赖不完整或过时的信息。

着手点
不要等待完整的标注策略。优先采用数据丢失防护 (DLP) 策略，重点防范财务、客户及知识产权数据等最敏感信息的泄露。同时，识别并自动标注既能创造最大业务价值，又伴随最大风险的最敏感数据。在此基础上，逐步构建覆盖整个组织的更广泛数据分类和治理计划。

预期收益
员工和智能体可以使用可信的敏感信息，而领导者则能够保持对数据的可见性、控制力，并确信数据在 AI 驱动的工作流中得到了妥善使用和保护。这些持久的策略会始终与敏感数据绑定，无论其在组织内如何流转、存储、共享或被访问。

就绪度自查

CIO 需思考：
- AI 工具和智能体能否发现、治理和使用我们最有价值的数据？

CISO 需思考：
- AI 能否区分敏感信息与其他信息，并采取适当的防护措施？

3.

安全访问

建立信任层，帮助验证用户、设备和访问请求，以便人员和 AI 可以安全地检索并操作组织信息，而不会增加风险。当身份、访问权限和许可保持一致时，员工和 AI 智能体便可以安全地访问完成工作所需的信息，从而推动组织在各团队、角色和业务流程中扩展 AI 的应用。

着手点
首先，对所有用户实施多重身份验证 (MFA) 和条件访问策略。这些控制措施有助于提供保护，同时为安全访问经批准的 AI 工具奠定基础。

预期收益
员工和智能体可以安全地访问信息和 AI 驱动的体验，而安全团队则能够控制跨身份、设备和智能体对敏感数据及系统的访问方式。

就绪度自查

CIO 需思考：
- 员工能否安全地访问所需的信息和 AI 工具，而且不会出现不必要的阻碍？

CISO 需思考：
- 在授予访问权限之前，我们能否验证每个用户、设备和 AI 智能体的可信度？

注意：这五个步骤是相互关联的能力体系，你可以根据组织的实际情况，决定合适的实施顺序。

4.

规模化管理

确保用户、设备、应用和云 PC 保持良好状态并受到有效治理，覆盖范围延伸至一线员工、合同工、智能体及个人设备。例如，拥有季节性员工的组织可以提供内置组织策略、应用程序和保护措施的安全云 PC，以便快速将这些团队纳入员工使用的同一受治理环境中，而无需为每个人运送、管理和回收物理设备。在终结点得到管理和保护的情况下，无论设备、地点或工作方式如何，AI 都可以在整个员工队伍中以一致且安全的方式部署。

着手点
优先通过设备合规性和应用程序保护政策，将未受管理的设备和个人设备纳入策略管控，再逐步扩展管理范围。将终结点纳入统一的管理框架，有助于即时实现安全性和运营效益，同时为更广泛的 AI 应用奠定基础。

预期收益
员工在公司、一线和个人设备上获得简化的体验，而 IT 部门则获得安全实现 AI 规模化应用所需的可见性、控制力与一致性。

就绪度自查

CIO 需思考：
- 我们能否在整个组织内一致地管理和治理用户、设备、应用以及 AI 赋能的终结点？

CISO 需思考：
- 我们的安全和合规控制措施能否在员工、合同工、一线工作人员和 AI 智能体之间实现一致的扩展？

5.

防护与响应

通过关联整个组织内的各类信号，检测、调查并应对身份、设备、数据和 AI 驱动工作流中的威胁，从而帮助组织在 AI 逐步普及的过程中保持复原能力。有了内置于基础层面的防护控制措施，组织便能自信地将 AI 扩展至更多用户、更丰富的数据及更广泛的业务场景。

着手点
首先，识别身份、终结点、数据、云资源和应用程序的整体风险暴露情况。不要等到事件发生才采取行动，而是要了解哪些方面风险最大，以及哪些举措能够显著降低这些风险。在此基础上，将 AI 引入防御策略，帮助安全团队关联信号、确定响应优先级，并更快地调查威胁。

预期收益
员工可以安全地使用 AI 来提升生产力，减少中断，而安全团队则能够提升可见性，更快地检测与响应威胁。

就绪度自查

CIO 需思考：
- 我们的安全运营能否跟上 AI 为业务带来的速度与规模？

CISO 需思考：
- 我们能否快速检测、调查和遏制威胁，以免影响数据、运营或 AI 驱动的工作流？

> 通过全面整合到 Microsoft 365，我们打造了一个能让 Copilot 充分发挥作用的环境。这或许正是我们能实现 Copilot 日均活跃使用率高达 90% 至 95% 的原因。

Elaine Smith
PepsiCo Copilot 项目负责人

阅读完整案例：PepsiCo 客户案例研究

注意：这五个步骤是相互关联的能力体系，你可以根据组织的实际情况，决定合适的实施顺序。

助力提升 AI 就绪度的三大转变。

安全基础框架中的每一步都旨在加强运营环境的特定环节：连接工作、准备数据、安全访问、规模化管理以及防护与响应。

这些步骤共同助力企业更广泛地推进 AI 转型，帮助你的组织做好准备。其成果不仅是一个坚实的基础，还有一系列切实可行的转变，可以帮助组织在把握业务背景、保持控制力并充满信心的前提下，推动实践的演进。

转变一：从孤立的工具和信息，迈向互联的工作智能。

当 AI 能够基于人员、内容、对话、会议、应用及工作流中的真实工作场景获取信息时，其价值将显著提升。若信息困于彼此孤立的工具中，AI 则只能提供片面答案，员工仍需耗费时间检索、切换上下文并重建背景。而互联的工作基础能为 AI 提供所需的组织上下文，使其生成相关洞察、总结进行中的工作、推荐后续步骤，并支持在工作流中直接采取行动。同样重要的是，工作体验本身应随员工而动，无论处于何种物理设备、云环境、地理位置或团队之中，都能保持上下文、访问权限与业务连续性。无论是全职员工、合同工，还是项目制贡献者，都能持续连接到相同的应用程序、信息、策略与 AI 体验，从而高效开展工作。这一转变有助于组织从脱节的体验过渡到 AI 就绪的工作环境，推动 AI 从提升个人生产力，进阶为驱动团队与业务流程的广泛变革。

转变二：从过度共享和访问风险，转向数据保护与控制。

随着 AI 的应用范围不断扩大，各组织需要确信敏感数据可发现、受治理，并且只有合适的人员、设备和智能体才能访问这些数据。如果缺乏这一基础， AI 可能会加剧现有的过度共享、访问权限及合规性方面的漏洞。这一转变旨在将保护措施融入运营模式：对高价值数据进行分类和标记，应用 DLP 和访问策略，验证身份和设备状态，并确保策略始终与数据的存储、共享、访问以及在 AI 驱动的工作流中使用保持一致。最终目标是创建一个更值得信赖的环境，员工和智能体可以利用相关的业务上下文，而领导者则可以保持可见性、治理和控制。

转变三：从碎片化的信号，迈向可扩展的统一防御。

AI 的规模化应用提高了工作的速度、体量与复杂性，这也增加了安全团队需要理解和处理的信号数量。更强大的基础有助于团队将身份、终结点、数据、应用和威胁信号建立关联，从而更全面地了解风险。它还有助于将 AI 引入防御策略，支持调查、响应和优先级排序，同时在用户、设备、云 PC、智能体和 AI 支持的工作流中保持一致的控制。这一转变可助力组织在保持复原能力的前提下规模化应用 AI，同时加强对 AI 部署、监控和保护的控制权。

面向不同角色的后续行动指引。

以这三大转变为主题，召开高管工作会议，将 AI 就绪工作转化为循序渐进的计划。目标并非一次性解决所有基础差距，而是就以下方面达成共识：CIO 和 CISO 的优先事项必须在哪些领域协同推进？CIO 应推进哪些现代化举措以实现规模化？随着 AI 的普及，CISO 应加强哪些方面以维持信任？

协同起步，就 AI就绪基础达成共识。

首先要达成共识，认清组织 AI 愿景已超前于底层运营模式的现实。CIO 和 CISO 应重点就对下一波 AI 采用浪潮至关重要的工作流、数据、身份、设备和控制措施达成一致。

1. 接下来我们应该扩展哪些 AI 支持的工作流？在扩展之前，必须夯实哪些基础？
2. 在哪些环节，我们需要更互联的上下文、更完善的治理机制，或更清晰的权责归属，才能让 AI 既实用又可信？
3. 优先解决以下哪项就绪度差距，将为企业带来更大的信心？

CIO 聚焦：实现数字资产现代化。

CIO 可以帮助将 AI 从孤立的用例转化为企业发展的动力，通过简化数字资产、连接员工依赖的工具和工作流以及实现终结点和工作区体验的现代化，使 AI 能够在整个企业中更顺畅地运行。

1. 随着 AI 融入日常工作，我们的生产力、协作和终结点策略需要如何演进？
2. 在 AI 能够广泛应用之前，哪些员工群体、设备或工作模式需要更一致的体验？
3. 整合和现代化可以在哪些方面降低复杂性，同时提高员工从 AI 中获得的价值？

CISO 聚焦：拓展信任与控制。

CISO 可以通过以下方式充满信心地规模化应用 AI：帮助确保敏感数据可被发现且受到保护，对用户、设备和智能体的访问实施统一治理，并整合安全信号，以便在 AI 可能加速风险传播、增加风险复杂性的背景下，有效检测和响应威胁。

1. 随着 AI 融入越来越多的工作流，哪些控制措施需要对数据、身份、设备和智能体进行跟踪？
2. 在扩大 AI 对敏感信息或高影响力流程的访问权限之前，我们需要在哪些方面提高可见性？
3. 我们的检测、响应和治理模型，应该如何随着 AI 和智能体承担更多工作而演变？

着手提升 AI 就绪度。

当工作实现互联、数据得到保护、访问受治理、终结点得到管理，且安全信号协同运作时，AI 转型才能实现规模化。随着工作变得更加分散和动态，组织可以受益于一致、受治理的工作环境；在此环境中，应用程序、数据、策略和用户体验在物理环境与云环境之间保持互联。

当工作体验能够跟随员工而不丢失背景信息时，AI 可以帮助提供更相关的洞察，支持跨工作流的行动，并在整个组织内更有效地扩展。这正是 Microsoft 365 致力于帮助组织构建的基础：将生产力、安全性、合规性、身份、终结点管理和 AI 集成到一个平台中，使 CIO、CISO 和业务领导者能够携手前进。

行动号召 →

1. **协同起步，**就对下一阶段 AI 应用至关重要的工作流、数据、身份、设备和控制措施达成一致。
2. **基于 Microsoft 365 进行构建。**利用 Microsoft 365 套件、智能 Microsoft 365 Copilot 副驾驶® 及 Windows 365 的集成基础，实现工作互联、数据保护、访问治理、规模化管理，并从容应对各类挑战。
3. **自信地规模化扩展。**逐步实施首批举措以积聚势头，从高价值的用例和高风险的数据入手，随着基础的不断强化逐步扩展。

来源：
1 Deloitte 于 2026 年发布的 “State of AI in Enterprise”，PDF 文件，一项针对来自 24 个国家/地区、在日常工作中至少部署了一项 AI 的组织的 3,200 余名业务和 IT 领导者的调研。
2 《2026 工作趋势指数》，Microsoft 365 遥测数据基于汇总并匿名化的 Microsoft 365 生产力信号，以及 2026 年 2 月 18 日至 2026 年 4 月 7 日期间，对 10 个市场中 20,000 名在工作中使用 AI 的全职或自雇知识型工作者进行的调研。调研涵盖的全球市场包括：澳大利亚、巴西、法国、德国、印度、意大利、日本、荷兰、英国和美国。
3 McKinsey 的 “The State of Organizations 2026”，一项针对全球 15 个国家/地区和 16 个行业的 10,000 多名高级管理人员的大规模调研。
4 “NTT Data Research Reveals C-Suite Misalignment Over GenAI Adoption”，2025 年 6 月 20 日。一项针对 34 个国家/地区 2,300 多名生成式 AI 高级决策者的调研，其中包括 1,500 名高管。

©2026 Microsoft Corporation. 保留所有权利。本文档“按原样”提供。文中信息和表达的观点（包括 URL 和其他 Internet 网站的引用）有可能更改，恕不另行通知。使用风险需自行承担。本文档未赋予你对任何 Microsoft 产品中任何知识产权的任何法律权利。您可以复制并使用本文件，供内部参考之用。