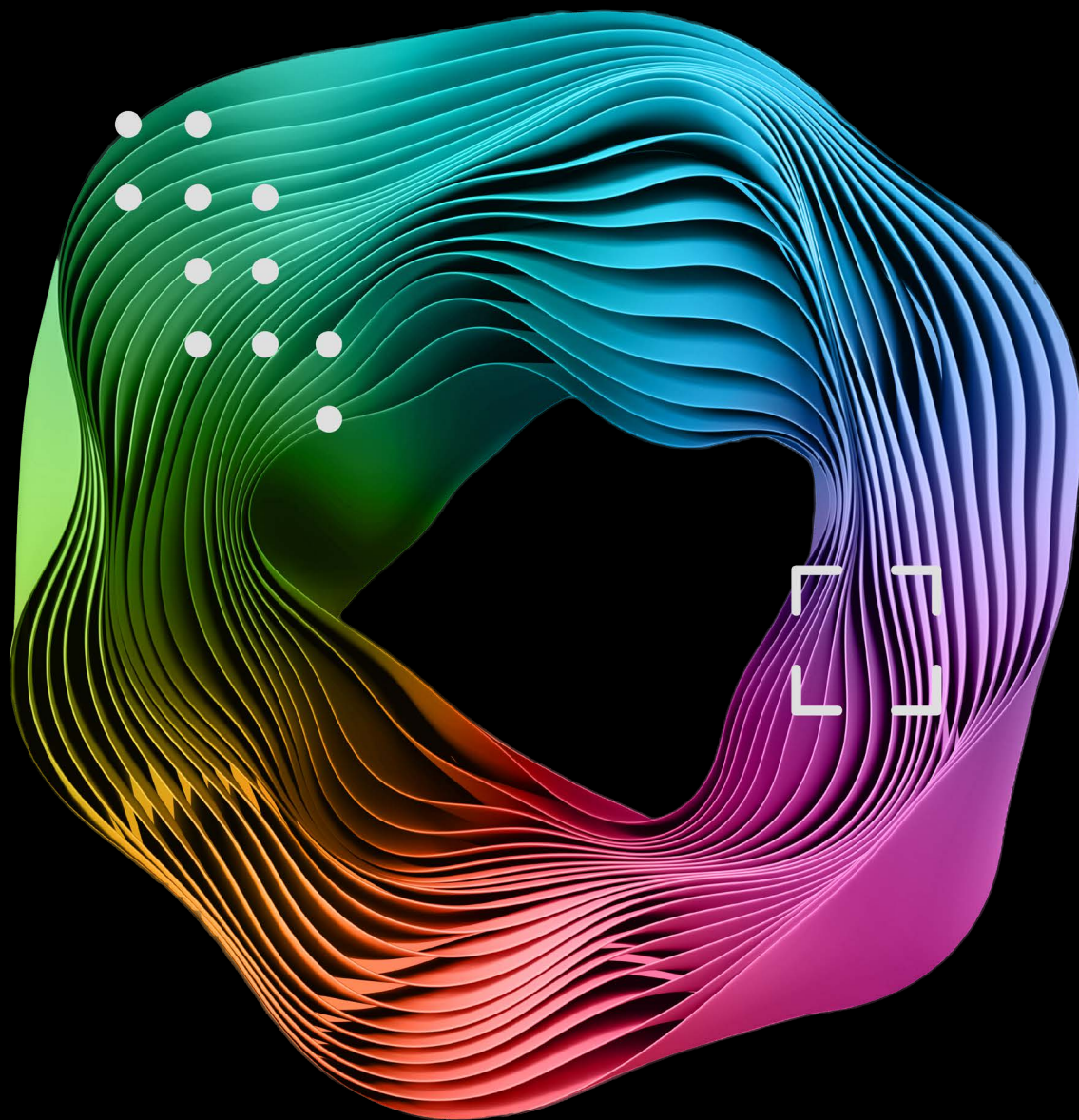


Deloitte.

德勤



Deloitte
Access Economics

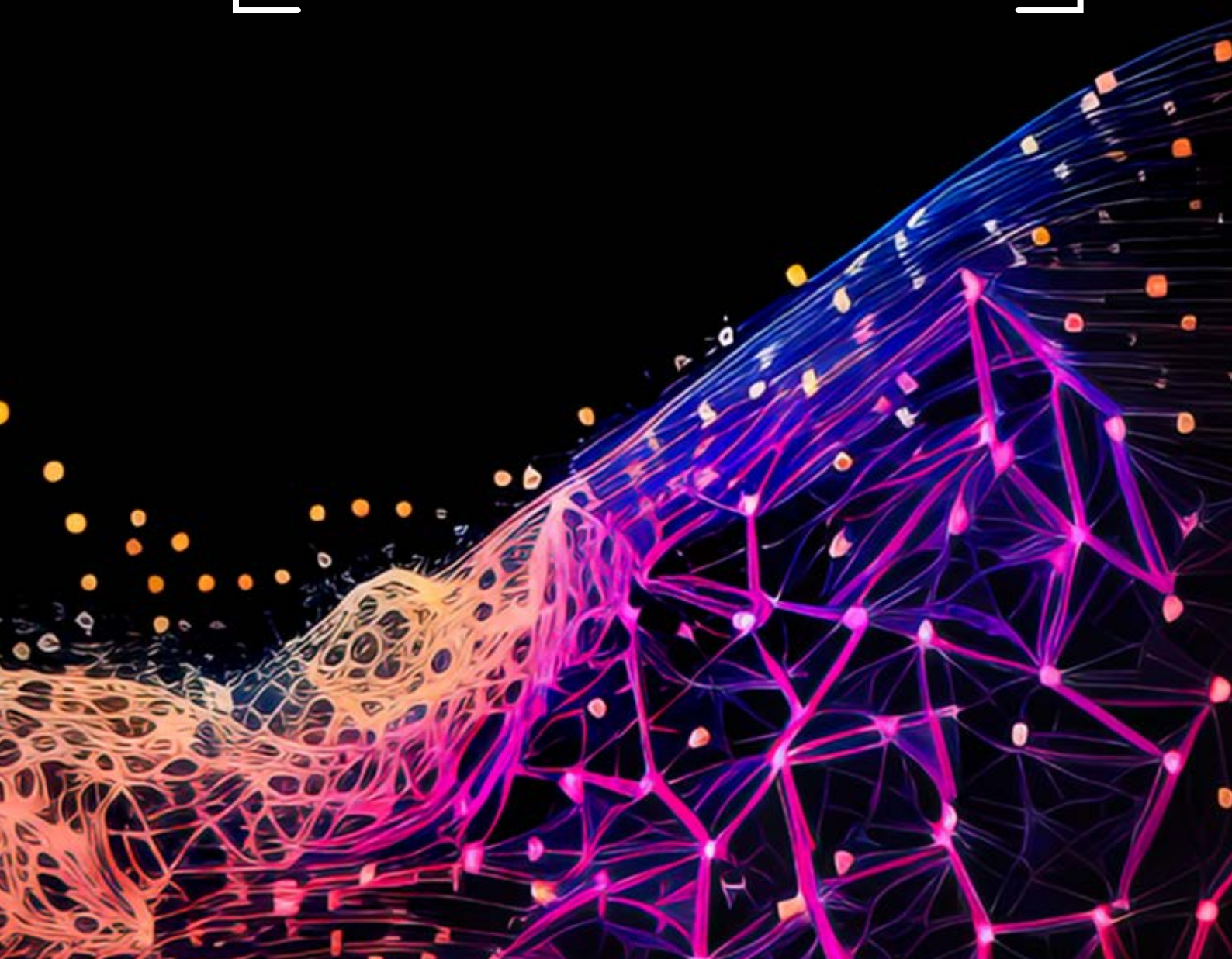
AI时代的抉择

以“信”筑基，行稳“智”远

德勤亚太 | 人工智能研究院

目录

报告概要	4
01 应对AI快速采用带来的风险	6
02 卓越AI治理之道	8
03 亚太地区AI治理现状	12
04 卓越AI治理的益处	21
05 搭建可信AI的基础	24
附录	28



报告概要

本报告由德勤经济研究所和德勤亚太人工智能研究院共同编制，旨在为亚太地区组织的首席高管和技术负责人提供洞察，助其改进治理结构和组织机制进而开发更可信的AI解决方案。

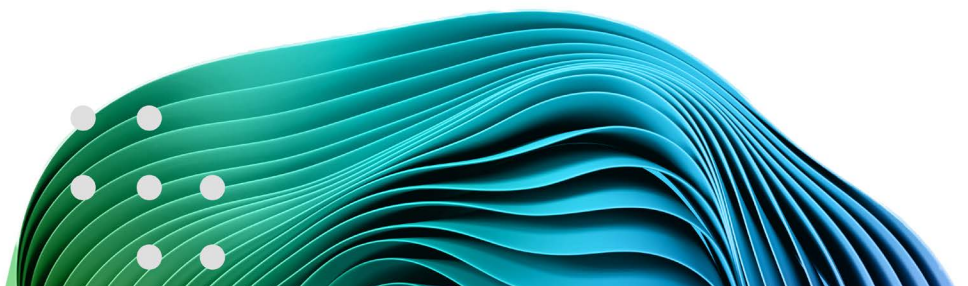
德勤高可信人工智能框架明确了AI解决方案建立可信性所必需的七大要素：透明、可解释；公平、中立；稳健、可靠；保护隐私；安全、稳妥；承担责任；问责。

组织实现可信AI的前提是什么？那就是卓越AI治理。

首席高管和董事会成员面临众多优先事项，启动并推进有效AI治理实践可能充满挑战。为助力组织解决这一难题，我们开发了AI治理成熟度指数，通过一系列评估标准来确定卓越AI治理实践。基于该指数，我们对亚太13个地区近900名高管进行调研，覆盖多个行业和部门以及不同组织规模。

我们的调研旨在了解组织AI治理成熟度水平，识别有效AI治理的关键推动因素，并评估采取治理举措给组织带来的益处。

- 1 透明、可解释
- 2 公平、中立
- 3 稳健、可靠
- 4 保护隐私
- 5 安全、稳妥
- 6 承担责任
- 7 问责



AI时代的抉择： 以“信”筑基，行稳“智”远

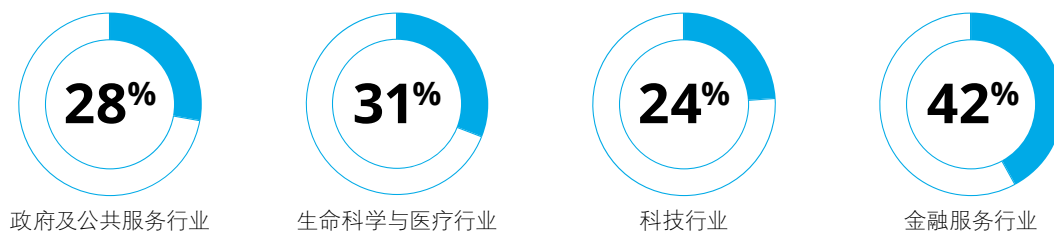
随着AI解决方案从试行进入推广阶段，组织面临着一些重大风险，例如安全漏洞、隐私问题和法律风险。尽管AI解决方案能带来巨大的效益，但如果这些风险无法得到妥善管理，就可能导致数据泄露、声誉和业务受损以及监管罚款。然而，令人担忧的是，超过半数的技术工作者并不认为其所在组织能够有效应对AI相关风险。

为了解有效AI治理如何助力应对这些风险并释放AI潜力，德勤对来自亚太13个地区的近900名高管开展调研，针对AI治理成熟度水平进行全面透彻的分析和研究。

各行业AI使用导致的事件数量均呈上升趋势

超过四分之一的组织过去一年发生的AI相关事件有所增加。

各行业过去一年AI相关事件数量增幅



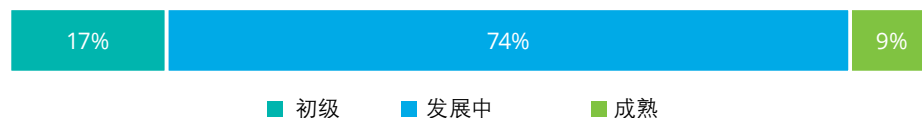
卓越治理也可促进AI应用扩大和财务收益提升



然而，90%以上的组织都需要提升AI治理

德勤AI治理成熟度指数采用12项指标来评估组织的AI治理成熟度水平。

亚太地区AI治理成熟度水平分布



建立可信AI的行动

- 1 重视AI治理以从AI获益
- 2 了解并利用更广泛的AI供应链
- 3 打造风险管理者，而非风险规避者
- 4 加强沟通，确保AI转型准备就绪

01 应对AI快速采用带来的风险

AI的采用正在改变亚太地区商业格局。生成式AI的快速崛起更是加速了这一过程，预计到2030年，亚太地区的AI投资将增长四倍，达到1170亿美元。¹生成式AI迅速成为亚太地区发展最快的企业技术。

在AI的快速采用上，员工往往比组织领导先行一步。德勤关于AI新生代的调研发现，超过五分之一的员工已在工作中使用生成式AI，其中年轻员工更是引领着AI热潮。²

AI应用达到如此速度和规模，组织领导在试行和推广AI技术的同时，也面临着与AI相关的风险。我们对近900名高管的调研显示，高管在AI使用中最普遍的担忧是安全漏洞（86%）、监控（83%）和隐私（83%）方面的风险（图1）。自从生成式AI问世以来，技术能力显著提升，工具界面更为人性化，用户人数大大增加，这些风险也就变得更加突出。

“德勤的一项研究显示，超过半数的技术工作者认为其所在组织并无适当的机制来识别或应对AI相关风险。”³

AI解决方案或其使用的海量数据可能存在安全漏洞，一旦遭到数据窃取或泄露，可能产生巨大的成本。2024年，全球数据泄露的平均成本接近500万美元，较去年增长了10%。⁴对于大型组织而言，这一成本可能会更高。

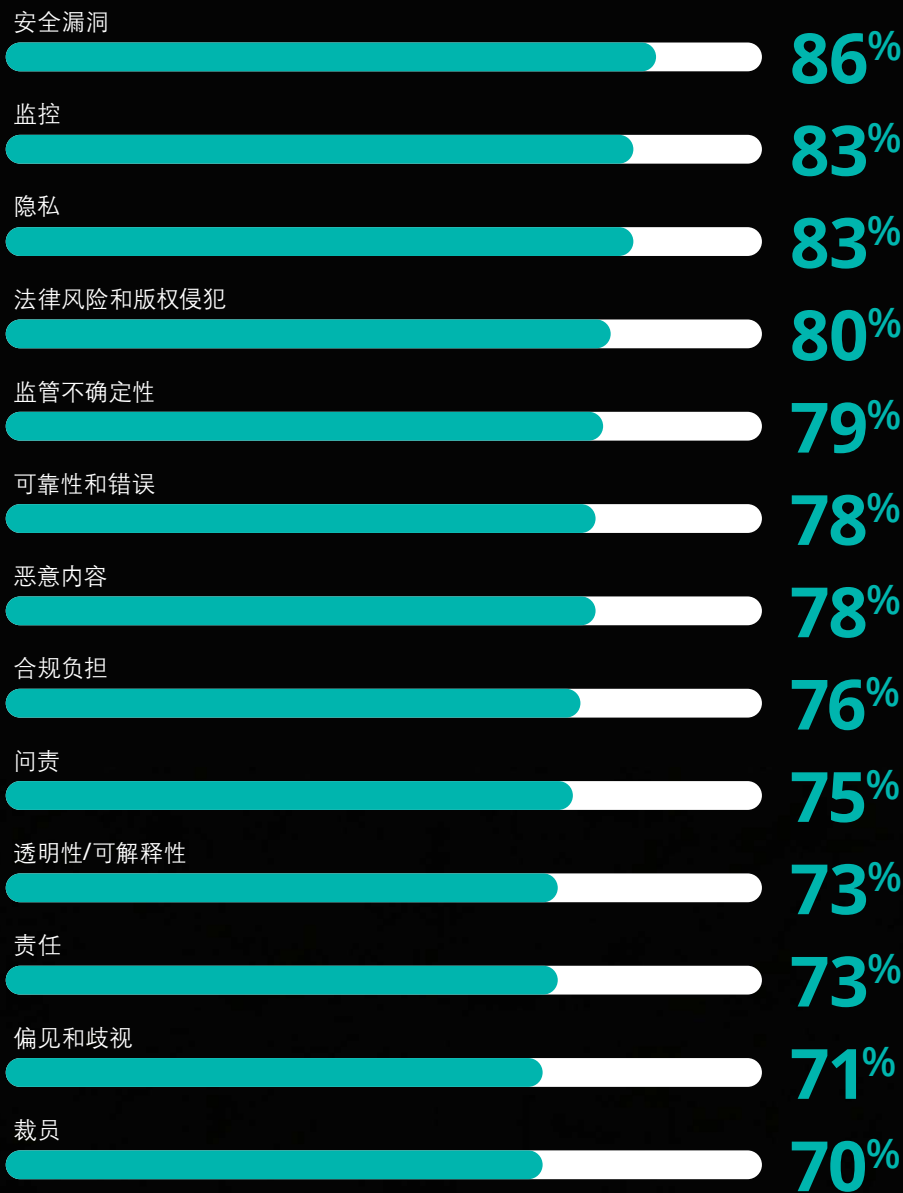
此外，还有一些难以量化的成本，如品牌形象受损和客户流失。消费者信心下降以及品牌声誉受损可能会带来持久的不利影响，组织必须有效管理AI风险并确保网络安全。同时，消费者更青睐在采用AI时遵从伦理规范的组织，例如对使用AI保持透明。研究显示，62%的消费者更信任其认为在AI使用上符合伦理的组织，而且有53%的消费者愿意为这样的产品和服务支付溢价。⁵

组织还必须确保其使用AI的方式符合不断发展的法律和监管要求，这是受访高管普遍表示担忧的风险之一。尽管亚太各地区一直在着力制定和实施法律法规，但**现行监管要求通常只是组织需达到的最低标准，而不是全方位的最佳实践。因此，组织高管必须制定、采纳并执行针对AI解决方案和系统的可信标准。**⁶

应对与AI相关的风险至关重要：如果应对不当，这些风险可能导致客户关系紧张、被处监管罚款或遭到公众抵制。此外，畏惧风险也可能阻碍组织应用AI。企业AI应用现状调研显示，在AI工具开发和使用所面临的四大挑战中，其中三大挑战是风险、监管和治理问题。由此可见，有效AI治理对于管理AI相关的伦理和运营风险以及充分利用AI技术尤为重要。

图1

组织在AI使用中最担忧的潜在风险



资料来源：德勤可信AI调研（2024年）。

开发符合这七项标准的可信AI解决方案并非易事。组织必须拥有健全的AI治理结构，以确保AI解决方案与这些标准保持一致。

卓越AI治理需要贯穿于技术生命周期各个阶段，并应融入到技术、流程和员工培训中。具体治理举措应根据AI解决方案的复杂程度、特定地域和行业的适用法规以及组织内部政策和标准进行调整。

由于适用标准不断变化，AI治理可能变得错综复杂。为助力组织采取切实行动实现可信AI，我们开发了AI治理成熟度指数。该指数在五大支柱领域（组织架构、政策与原则、程序与控制、人才与技能以及监控、报告和评估）设置12项关键指标，全面衡量组织的AI治理成熟度（表1）。根据这些指标，组织的AI治理成熟度可分为“初级”“发展中”“成熟”三个水平。有关该指数及相关问题的更多细节，请查阅附录二。

表1: 德勤AI治理成熟度指数

支柱领域	初级	发展中	成熟
 组织架构	未针对AI治理指定角色和责任	针对AI治理为相关人员和小组指定了部分角色和责任	已建立董事会问责制，并为管理层明确角色和责任以支持整个组织的AI治理
 政策与原则	未制定AI政策或原则来指导AI治理	已制定基本或草拟政策，确立了指导AI治理的一般原则	拥有健全的政策，确立了适合组织独特情况的明确原则
 程序与控制	未针对AI系统的开发、部署或使用建立风险相关程序或控制	正在针对AI系统的开发、部署或使用建立风险相关程序和/或控制	现有的风险相关程序和/或控制足以规范AI系统的开发、部署或使用
 人才与技能	未为员工负责任地使用AI提供资源或培训	正在开发为帮助员工负责任地使用AI的资源	已为员工负责任地使用AI提供资源，包括应用指引和相关培训
 监控、报告和评估	未实施对AI系统进行监控或报告的机制	正在开发对AI系统进行监控或报告的机制和工具	拥有对AI系统进行监控或报告的机制和工具

资料来源：德勤（2024年）。

下图呈现了德勤AI治理成熟度指数的各个支柱领域如何作为基本要素赋能组织实现可信AI。此外，该指数还明确了组织为实现德勤高可信人工智能框架的七大要素应采取的切实行动。

图3：德勤AI治理成熟度指数

实现
可信AI
需要夯实五大支柱领域



AI治理成熟度指数的五大支柱领域



组织架构



政策与原则



程序与控制



人才与技能



监控、报告和评估

资料来源：德勤（2024年）。

AI治理没有普遍适用的方案。具体的治理结构随行业、监管环境、AI目标和所采用AI解决方案的类型而异。例如，组织用于为员工提供人力资源政策相关信息的AI对话机器人，相比银行用于直接与客户交互的AI辅助信贷申请解决方案，所需的控制流程就有所不同。分析AI治理的共性将有助于组织找准其治理标准中有待改进的领域。

此外，需要注意的是，AI治理成熟度达到较高水平并不等同于实现可信AI输出结果。如果组织确立的治理程序并未得到有力执行、未被员工准确理解或者未能契合业务环境和战略，就可能无法实现可信AI输出结果。有效AI治理的标准因组织而异。为此，组织应当持续评估并完善AI治理框架，确保其适应组织独特的需求和不断变化的监管要求。

赋能未来： Energy Queensland 致力实现负责任的AI和可持续的创新

Energy Queensland是澳大利亚最大的国有电力公司，主要从事配电、零售和综合能源解决方案业务，拥有9,300多名员工，为超过230万客户提供服务。

Energy Queensland首席信息官Sharyn Scriven表示：“AI是一种颠覆性技术，随着技术发展日趋成熟，将帮助我们实现愿景和2032公司战略。”

Energy Queensland客户与新兴平台总经理Josh Gow认为，采用AI是公司的重点关注领域，将有助于推动运营卓越和提升客户体验，从而助力实现宏大战略。Energy Queensland采用AI已有数年，但此前只是小范围的专门应用场景，如今已拓展至更广范围的应用场景评估和部署。

为在引入新的AI解决方案之前确保适当的政策和机制部署到位，Energy Queensland围绕AI相关规范开展了多项重要工作，包括制定AI政策和用例实施路线图，以及采取必要措施建立可靠的防护机制。同时，为确保AI政策符合行业最佳实践并能够妥当执行，Energy Queensland不仅在内部进行了评估，也聘请外部机构进行了独立审核。Josh表示：





“由于AI环境快速变化并且行业标准和指南日趋成熟，我们的AI政策会进行持续审核和更新。由高管组成的AI指导委员会将定期讨论AI应用的进展以及所面临的风险和机遇。”

在全面实施之前对AI用例进行测试和试点是Energy Queensland AI战略的一个重要特点。Josh表示，通过内部用例进行试运行的战略旨在创造一个“以测试和学习为重点，逐步评估风险和机遇”的环境，具体包括试运行企业工具和构建AI平台服务，为企业用户处理繁重的文档、会务和电子邮件提供支持。

要高效且负责任地使用AI，有关人员需要具备适当的能力，同时要有强大的AI解决方案。为此，公司正在执行并审核“小范围测试”，让承担不同角色的员工参与上线、学习和培训计划，然后再进一步部署。

“在进一步采用AI的过程中，把握AI带来的价值和机遇并持续管理相关风险至关重要。AI将得到更广泛的应用，这只是时间早晚的问题。AI需要因人而异，也并非浮于表面。我们需要量身定制AI方案，以确保我们对AI的使用是有效的、负责任的和有价值的。”

确保实现可信AI的关键条件

-  AI政策
-  AI指导委员会
-  在内部进行AI项目的试点和试运行
-  培训计划

03

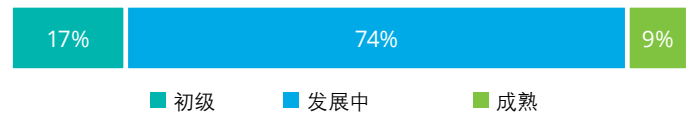
亚太地区AI治理现状

亚太地区仅有不到十分之一的组织拥有实现可信AI所需的治理结构。根据德勤AI治理成熟度指数，91%的组织AI治理结构尚处于“初级”或“发展中”水平，这表明其AI治理仍有非常大的改进空间(图1)。

从AI治理成熟度指数的五大支柱领域来看，亚太地区组织在“政策与原则”以及“程序与控制”领域的改进空间最大。目前，分别有31%和23%的组织在这两个支柱领域处于“初级”水平。相比之下，亚太地区组织在“组织架构”以及“监控、报告和评估”领域表现更佳，超过90%的组织都至少达到了“发展中”水平。

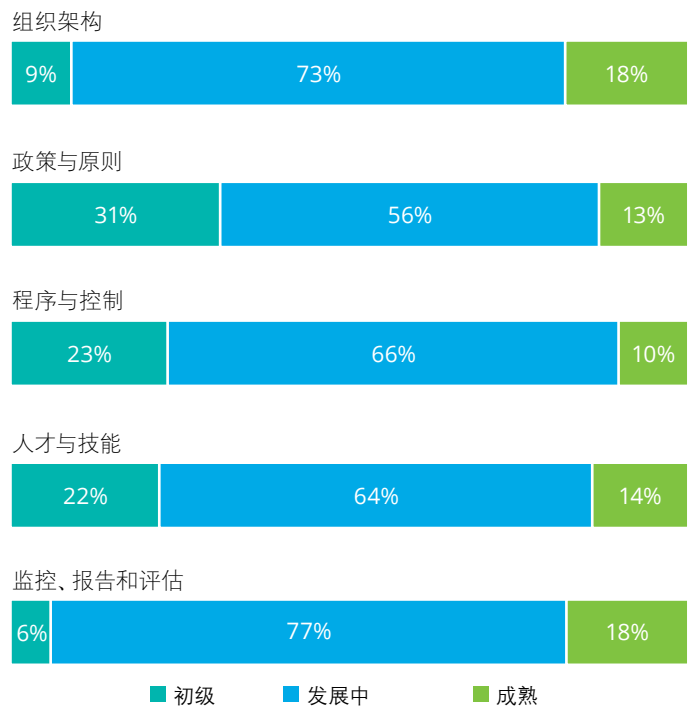
要全面达到“成熟”水平，组织需在AI治理成熟度指数五大支柱领域均表现优异。尽管单项支柱“成熟”达标组织已接近两成，但当中只有一半全面达到“成熟”水平。这表明组织需在完善AI治理上采取全局视角，为实现可信AI创造必要条件。

图1: 亚太地区可信AI指数水平分布



资料来源: 德勤可信AI调研 (2024年)。

图2: 各支柱领域可信AI指数水平分布



资料来源: 德勤可信AI调研 (2024年)。

纠正过度自信偏差

组织领导可能高估组织AI治理成熟度。德勤的企业生成式AI应用现状调研显示，23%的组织领导认为其风险管理程序和治理非常完备。然而，本次调研更加细致地分析AI治理的基础结构，结果显示仅有9%的组织在AI治理上达到了“成熟”水平。虽然两项调研的问题和样本有所不同，但调研结果偏差巨大，表明组织高管需要全面了解其AI治理成熟度。这一点至关重要，过度自信可能妨碍组织改进AI治理；如果组织领导认为其已建立足够的机制来管理AI风险，就不太可能努力探索如何实现进一步改进。

支柱一

组织架构



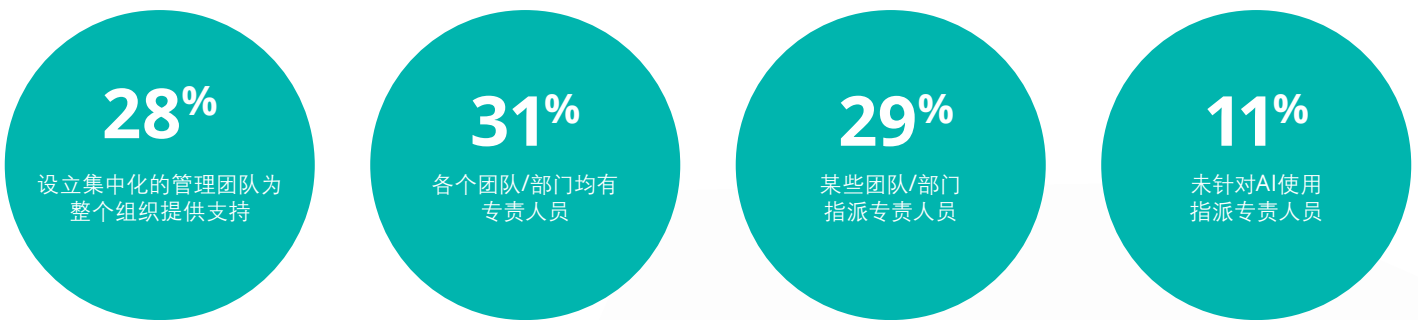
明确组织内负责管理AI标准的角色，有助于确保妥善应对与AI有关的任何新出现问题。大多数受访组织表示这一责任由高管团队承担，91%的组织明确指定一名董事会成员或首席高管负责相关事宜。另外，7%的组织委任AI负责人来管理相关风险和标准，但有不到2%的组织未在组织内指定相关负责人。

不同组织搭建AI伦理、法律和监管合规专责团队的方式可能会有所不同。只有略高于四分之一（28%）的组织设有集

中化的伦理和风险管理团队来监控AI使用趋势和识别相关风险，而大部分（61%）组织是在各个或某些部门/团队指派专责人员（图3）。其他组织则是在某些团队中指派专责人员，或者没有指派专责人员来管理AI使用。

相比团队架构，AI标准的责任制和问责制更为重要，但这在小型组织中较为罕见。员工人数超过1,000名的组织中，仅有3%未设立专门的AI风险管理岗位，而在员工人数不足100名的组织中，这一比例约为23%。

图3: AI伦理、法律和监管合规专责团队架构



资料来源：德勤可信AI调研（2024年）。

支柱二

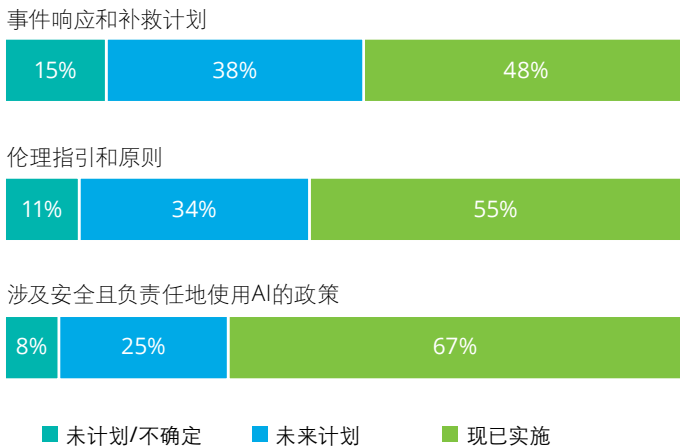
政策与原则



清晰明确、广泛宣贯的政策和原则是有效AI治理的基本前提。AI政策不同于AI战略，后者包括AI目标和衡量目标实现进展的关键指标等要素，所涉及的范围更广。尽管亚太地区大多数组织都制定了AI战略，但许多组织的AI政策并未涵盖卓越AI治理的关键要素。接近半数的组织AI政策中缺失AI治理目标实施时间表或未包含有关AI的伦理指引和原则。

将AI治理要素纳入AI政策是帮助员工认识战略价值的关键。在已制定组织层面AI战略的组织中，有30%的组织表示并非所有员工都能明白AI战略的价值。如果AI政策包括监控或审计流程，也就是说将风险偏好及事件响应和补救计划与更广泛层面的组织政策进行整合，员工会更可能认识到战略的价值。

图4: 可信AI政策的实施



资料来源：德勤可信AI调研（2024年）。

支柱三

程序与控制



程序与控制聚焦组织管理AI相关风险和标准的实践，包括用于识别和管理AI相关风险的评估程序，收录所使用AI解决方案的完整清单，以及旨在减轻AI解决方案所带来风险的控制框架。我们的调研显示，在该支柱领域达到“成熟”水平的组织数量最少，因此，完善程序与控制将是亚太地区提升可信AI治理的关键。

有效AI治理的一个关键要素在于建立报告机制，便于员工反映工作中与AI使用相关的问题或事件。然而，五分之一的组织都缺乏这样的报告机制。对比这些组织，拥有报告机制的组织所收到的问题数量高出五倍，所报告的事件数量多出一倍，这表明未建立报告机制的组织可能会忽视与AI相关的新风险。在亚太地区，AI相关问题和事件数量都在持续增加，建立应对机制会变得越来越紧迫（图5）。

图5: 2024年对比2023年AI相关事件数量变化



资料来源：德勤可信AI调研（2024年）。注：排除了回答“不确定”的样本（6%）。

支柱四

人才与技能

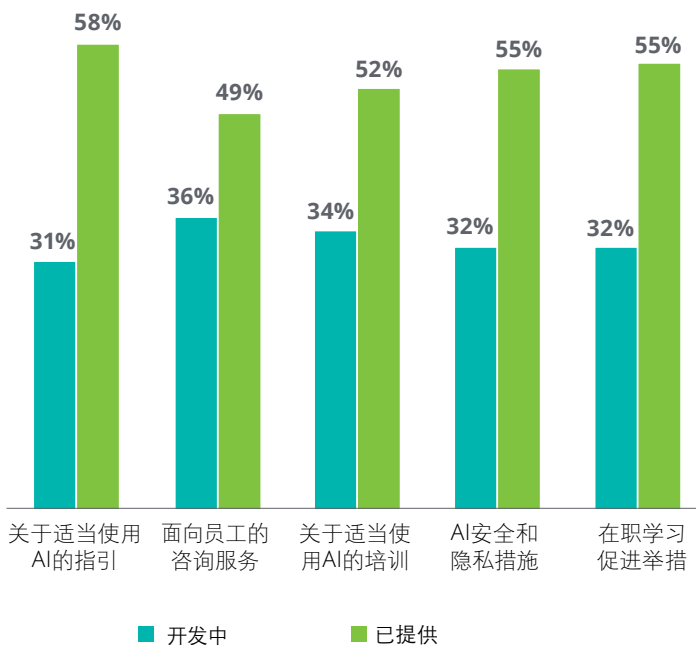


人才在实现可信AI中发挥着重要作用。然而，许多组织在这方面依然面临挑战，平均仅有56%的员工拥有负责任地使用AI所需的技能。

培训可以有力弥补技能差距。尽管仅有52%的受访组织提供AI培训，但与不提供相关培训的组织相比，能够安全使用AI的员工比例会高出27%。而在目前不提供相关培训的组织中，72%的组织正在积极制定培训计划。

大多数组织都为负责任地使用AI提供指引，55%的组织推出在职学习促进举措，49%的组织为员工提供咨询服务或成立咨询小组。私营部门组织积极提供AI应用指引和培训，而公共部门组织更多地专注于安全措施和在职学习促进举措。

图6: 帮助员工使用AI的资源



资料来源: 德勤可信AI调研 (2024年)。

支柱五

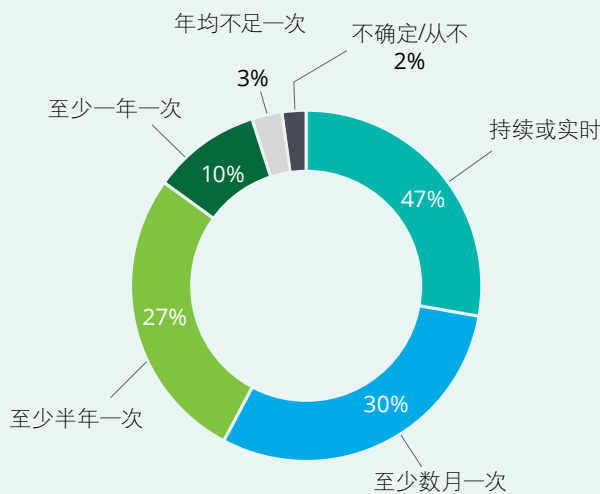
监控、报告和评估



AI治理系统必须能够应对不断变化的需求和不断出现的问题，这对确保组织迅速响应风险和事件至关重要。总体而言，受访组织在该支柱领域相对完善，18%的组织达到“成熟”水平。大部分(85%)组织根据内部标准对AI治理进行评估的频率是至少半年一次(包括至少半年一次、三个月一次和实时评估)。

同时，组织需要监控和评估AI治理是否符合监管环境的变化。近四分之三的组织至少每半年对法律和监管环境进行一次复核。

图7: 根据组织内部标准评估AI系统的频率



资料来源: 德勤可信AI调研 (2024年)。

创新无界 治理有方： 第一生命控股有限公司 迈向负责任的AI

第一生命控股有限公司 (Dai-ichi Life Holdings, Inc.) 是一家拥有122年历史的领先保险集团，专注于为亚太和全球市场提供寿险及投资产品服务。

第一生命控股始终致力于为客户提供高品质服务，并构筑坚实的信任基石。坚持以负责任且合乎伦理的方式实施AI解决方案，是实现公司愿景的关键之策。第一生命控股首席数据与AI官Figen Ulgen表示：

“我们须精心设计并妥善实施AI解决方案，以充分彰显公司‘客户至上’的价值主张。为此，需倾注大量时间和耐心，确保系统稳定运行并达到预期效果。我们深知，这不可一蹴而就，而是需要付出持之以恒的努力。”

第一生命控股目前正借助生成式AI，积极探索创新的无限可能，其中包括“数字助手” (digital agents)。数字助手能够执行多种任务，例如进行聊天互动。在客户交流会议中，数字助手可协助记录会议笔记、提取与客户问题相关的文档，并总结对话内容。第一生命控股正深入开展长期测试，确保以负责任的方式部署数字助手。实际上，数字助手已在多家销售办事处经历了近一年的实地测试，吸引数百名销售代表的广泛参与和使用。此外，第一生命控股秉持“人文关怀”的理念，对数字助手生成的每条信息都进行细致的人工审核，以确保所提供的内容准确无误。

第一生命控股将有效的AI治理视为全体成员的共同责任。在其举办的全球数据与AI协同领导力论坛上，公司及成员企业的高管共聚一堂，一致将AI治理列为重点讨论议题。与此同时，负责任的AI还被视为赋能所有利益相关者的重要手段。基于稳健的保障体系和灵敏的预警机制，企业可以安心地推出新型AI解决方案，内部用户也能自如地探索和运用AI。Ulgen博士指出，关键在于制定明确的流程，确保事件发生时能够及时应对：

“如果具备适宜的框架和流程，我们的员工就无需承受心理负担，也不会有冒险的感觉。他们可以放心地使用我们开发的解决方案，并且知晓何时对结果进行查询与核实。”

Ulgen博士还进一步强调了组织文化的重要性，尤其是同理心的价值，它不仅为高品质客户服务筑牢了根基，而且对于合乎伦理的AI部署也至关重要。在寿险领域，这意味着将“对客户高度负责的伦理观”深植于心。

确保实现可信AI的关键条件



立足长远



人文关怀



聚力协作

各行业可信AI的发展

不同行业的AI治理成熟度指数以及在各支柱领域的得分有所不同。我们的调研发现，科技、传媒和电信行业、金融和保险服务行业以及专业服务行业的组织在可信AI方面达到“成熟”水平的比例最高。同时，政府及公共服务行业、生命科学与医疗行业的组织达到“成熟”水平的比例较低。下文概述了四大行业的AI治理情况，附录四总结了亚太各主要区域的AI治理情况。



金融服务行业

作为知识与数据密集型行业，金融服务行业一直在数字化创新应用方面发挥引领作用，但也面临着更严格的监管和更多的敏感信息，因此，金融服务行业组织需要快速建立治理流程以妥善运用新兴技术。

德勤AI治理成熟度指数分析结果显示，金融服务行业的AI治理成熟度水平高于其他行业。由于金融服务需求不断增加，尤其是在精通技术的年轻消费者群体中，整个行业的未来发展离不开卓越AI治理。随着AI技术应用深化，遵守法律法规和保护客户数据将成为金融服务行业的关键议题。

AI治理成熟度指数

金融服务行业




所有业务





■ 初级 ■ 发展中 ■ 成熟

注：数据经过四舍五入处理，百分比之和可能不等于100%。


卓越AI治理可望为组织带来的三大益处


 对AI解决方案成效或成果的信任度提高 (57%)


 信任度提高带动AI解决方案使用增加 (47%)

 整个组织AI解决方案部署加速 (47%)


组织在AI使用中最担忧的三大风险


 可靠性和错误 (92%)


 法律风险和版权侵犯 (88%)

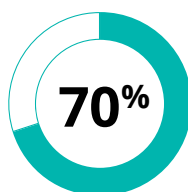
 安全漏洞 (87%)

组织在AI使用或实施中的三大障碍

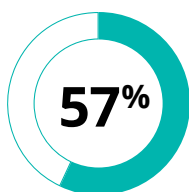
 对监管、法律、伦理、合规等风险的担忧 (45%)

 技术实施挑战 (38%)

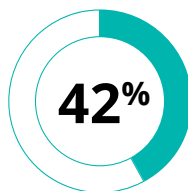
 缺乏创新意愿和/或试验干劲不足 (32%)



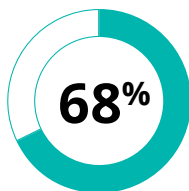
金融服务行业组织已建立便于员工反映问题的机制。



金融服务行业组织的员工具备所需技能，能够以符合伦理和法律的方式使用AI。



金融服务行业组织表示上一财年事件报告增加。



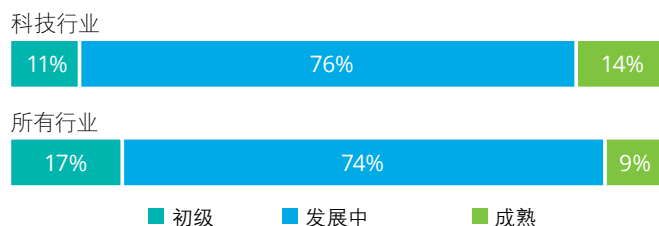
金融服务行业组织正在提高现有员工的技能，以缩小与以符合伦理和法律的方式使用AI相关的技能差距。

科技行业

科技行业处于AI颠覆浪潮的前沿，也是为其他行业开发AI解决方案的关键推动力量。由于长期使用AI解决方案，科技行业拥有更为成熟的治理流程，AI治理成熟度水平也高于其他行业。

德勤生成式AI报告显示，技术员工在工作流程中率先应用生成式AI，因此科技行业能够快速响应新兴趋势。然而，科技行业在管理技术解决方案数据使用相关的法律和保密风险上面临重大挑战。作为其他行业的技术支持者，科技行业实现审慎AI治理将成为维护客户信任的重中之重。

AI治理成熟度指数



注：数据经过四舍五入处理，百分比之和可能不等于100%。

卓越AI治理可望为组织带来的三大益处

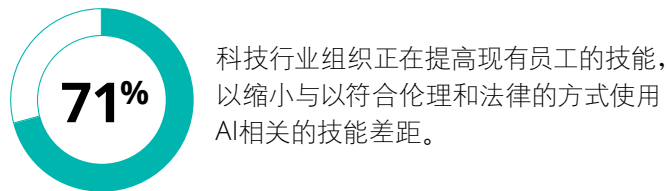
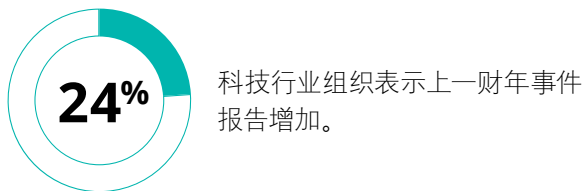
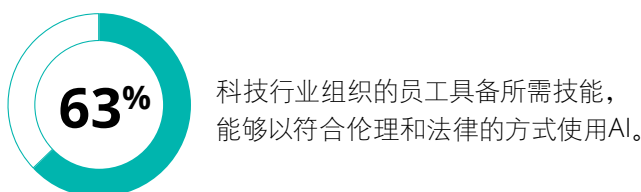
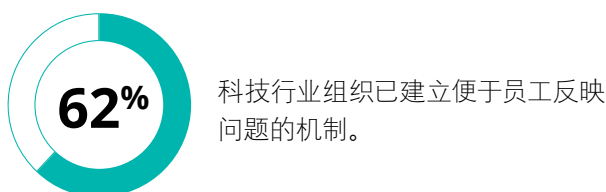
- 信任度提高带动AI解决方案使用增加 (58%)
- 对AI解决方案成效或成果的信任度提高 (54%)
- 整个组织AI解决方案部署加速 (53%)

组织在AI使用中最担忧的三大风险

- 法律风险和版权侵犯：法律责任 (84%)
- 隐私：敏感、保密或个人数据泄露风险 (83%)
- 安全漏洞：网络入侵/网络安全风险、AI系统未经授权的访问或滥用 (81%)

组织在AI使用或实施中的三大障碍

- 技术实施挑战 (39%)
- 对监管、法律、伦理、合规等风险的担忧 (34%)
- 对AI技术及其潜力的认识不足 (33%)

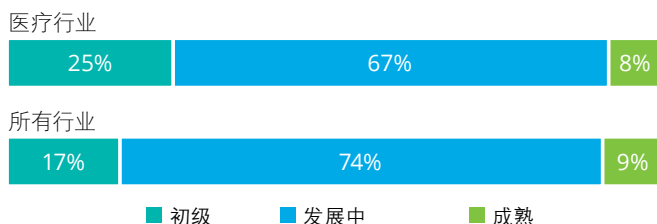


生命科学与医疗行业

医疗行业的AI解决方案通常离不开个人数据(如医疗状况和人口统计信息)，这类数据容易引发安全漏洞，而这是该行业面临的重大风险之一。为此，医疗行业必须制定严格的隐私及安全标准。患者需要确保个人数据能够得到保护才会同意将其数据用于AI解决方案，医疗行业组织通过卓越AI治理可获得的两大益处是提高在客户中的声誉和获得社会运营许可。

在医疗行业，AI治理成熟度处于“初级”水平的组织占比较高，这与医疗行业拥抱数字化转型速度缓慢以及员工存在抵触情绪的情况相吻合。这意味着，除非AI治理实现优化，否则医疗行业组织难以使用AI解决方案。

AI治理成熟度指数



注：数据经过四舍五入处理，百分比之和可能不等于100%。

卓越AI治理可望为组织带来的三大**益处**

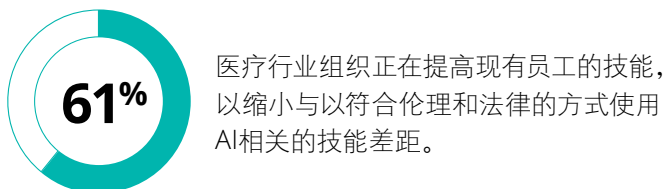
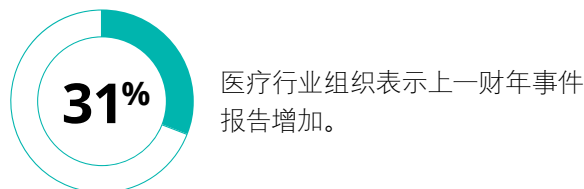
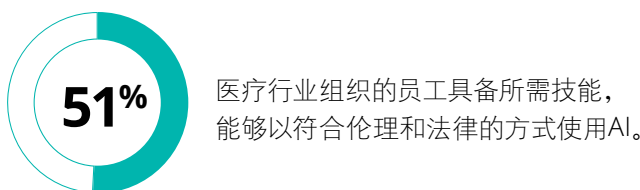
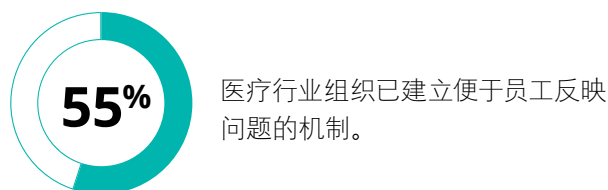
- 在客户中的声誉提高 (44%)
- AI解决方案获得广泛的社会许可 (42%)
- 监管合规程度提高 (42%)

组织在AI使用中最担忧的三大**风险**

- 安全漏洞：网络入侵/网络安全风险 (86%)
- 监控：监控泛滥导致隐私侵犯 (86%)
- 合规负担：与AI解决方案使用有关的报告及流程要求 (83%)

组织在AI使用或实施中的三大**障碍**

- 对AI技术及其潜力的认识不足 (39%)
- 高管承诺缺失 (33%)
- AI实施战略和愿景缺位 (33%)



公共部门

亚太地区公共部门的组织在AI监管合规及符合伦理规范上面临重大挑战。要妥善应对瞬息万变的环境，当务之急是快速建立灵活的应对机制，打消与AI技术使用有关的担忧。

在公共部门，AI有望提高为公民提供数字化服务的效率，但组织须保障数据安全，防范网络攻击风险。因此，该行业对安全漏洞和监控风险表示担忧的组织占比相对较高。

AI治理成熟度指数

公共部门



私营部门



■ 初级 ■ 发展中 ■ 成熟

注：数据经过四舍五入处理，百分比之和可能不等于100%。

卓越AI治理可望为组织带来的三大**益处**

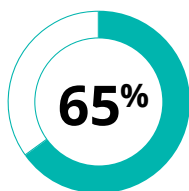
- 对AI解决方案成效或成果的信任度提高 (56%)
- 信任度提高带动AI解决方案使用增加 (54%)
- 整个组织AI解决方案部署加速 (48%)

组织在AI使用中最担忧的三大**风险**

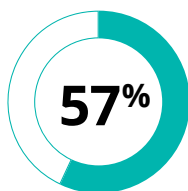
- 安全漏洞：网络入侵/网络安全风险 (87%)
- 监控：监控泛滥导致隐私侵犯 (83%)
- 恶意内容 (82%)

组织在AI使用或实施中的三大**障碍**

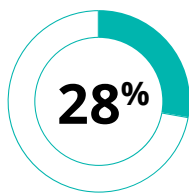
- 技术实施挑战 (38%)
- 对监管、法律、伦理、合规等风险的担忧 (37%)
- 对AI技术及其潜力的认识不足 (36%)



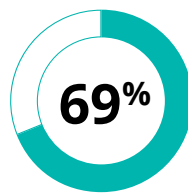
公共部门的组织已建立便于员工反映问题的机制。



公共部门组织的员工具备所需技能，能够以符合伦理和法律的方式使用AI。



公共部门的组织表示上一财年事件报告增加。

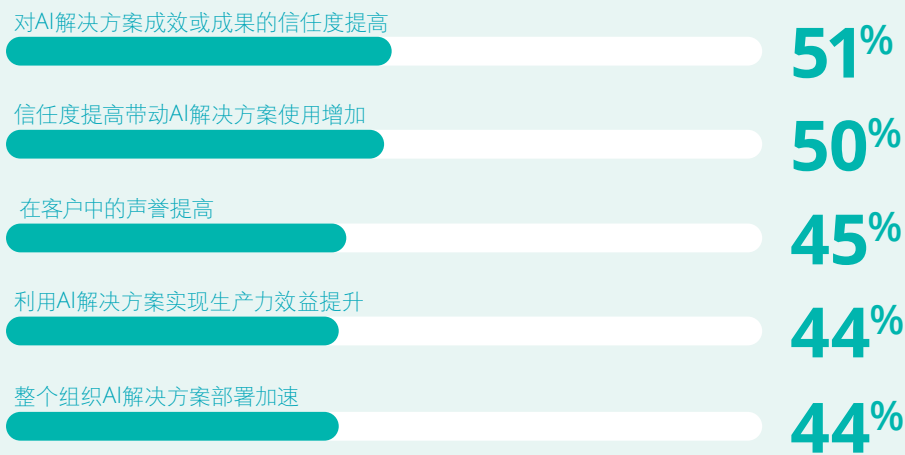


公共部门的组织正在提高现有员工的技能，以缩小与以符合伦理和法律的方式使用AI相关的技能差距。

04 卓越AI治理的益处

组织从提升AI治理成熟度中获益匪浅，高管意识到，除非他们可以信任AI的输出结果，否则将无法充分利用AI带来的机遇。

图8：
可信AI的五大益处



资料来源：德勤可信AI调研（2024年）。

有效AI治理的一大益处是**提高对AI解决方案成效或成果的信任度**，这一益处为一半以上（51%）的受访高管所选择（图8）。另一项研究发现，透明的AI系统可将用户对AI的信任度提高30%，从而增加用户采用和使用AI的可能性。⁹

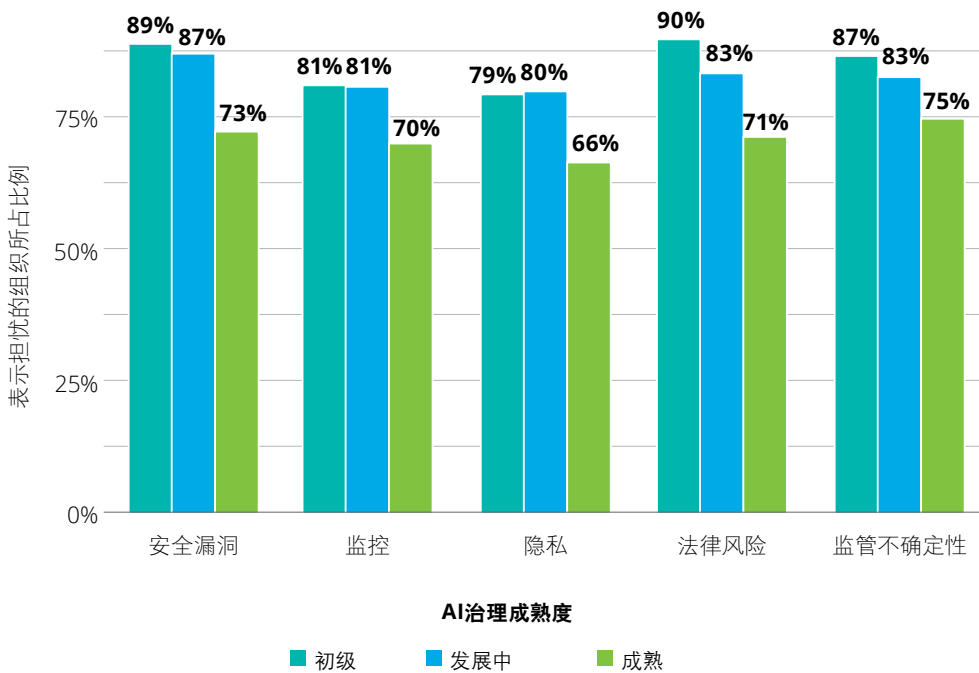
提高对AI输出结果的信任度需要进行有效AI治理，也就是需要采取切实行动来缓解组织在使用AI时所面临的风险。例如，实施事件响应和补救计划可为领导人建立信心，使其确信问题能够得到妥善处理。AI治理成熟度达到“成熟”水平的组织担忧安全、隐私或法律风险等主要风险的比例相对较低（图9），而处于“发展中”及“初级”水平的组织对于这些风险表示担忧的比例都相对较高，因此，在各支柱领域实施有效AI治理以解决对AI使用的担忧变得尤为重要。

半数受访高管表示，有效AI治理的另一大益处是**扩大AI解决方案在组织内的使用**。我们通过计量经济学建模对这一结果进行了验证：AI治理成熟度达到“成熟”水平的组织与处于“初级”水平的类似组织相比，部署AI解决方案的业务领域有所增加，范围已延伸到组织内部的另外三个领域。¹⁰例如，**达到“成熟”水平的组织在客户服务、销售和市场营销、生产和运营以及研发方面使用AI的可能性要高出两倍或更多。**

“本次研究进行的建模显示，有效AI治理既增加了组织中已部署AI解决方案的使用广度（整个组织范围），又增加了其使用深度（用户人数更多）。”

此外，制定AI治理举措还能扩大AI解决方案在其部署领域中的**使用范围**。与处于“初级”水平的组织相比，达到“成熟”水平的组织使用AI工具的员工比例平均多出16个百分点，这相当于**普通组织中AI用户数量增加28%**。对比在相同的业务次级领域（如销售及市场营销或研发领域）部署AI解决方案的组织，这一结果仍然成立——这表明可信AI总体上有助于员工更好地使用AI解决方案。有关本报告建模的更多详情，请参阅附录三。

图9: 对AI使用相关主要风险表示担忧的组织比例（按AI治理成熟度水平划分）



资料来源：德勤可信AI调研（2024年）。

客户越来越关注AI涉及的伦理因素和数据隐私问题。事实上，只有一半的客户认为，在线服务带来的益处超过了其在数据隐私方面造成的担忧。¹¹建立有效AI治理能够展现组织对客户关注点作出的承诺，提高组织声誉。这一益处得到了45%受访高管的认可。

传统AI工具和生成式AI工具均显示出显著提高生产力的优势。德勤对11,900名“AI新生代”（年轻员工和学生）进行的调研显示，日常使用生成式AI的用户每周可以节约5.3小时。¹²随着用户对技术的熟悉度提高以及技术能力不断发展，这一数字可能还会增加。

另一项研究指出，采用AI解决方案的企业称其运营效率和生产力提高了15%。¹³同时，**我们的研究发现，有效的治理框架能够提升AI解决方案的效益，有44%的高管提到组织获得了更高的生产力。**本报告进行的建模显示，在过去一年中可信AI指数达到的水平越高，组织实现的收入增长也越高。可信AI指数得分增加15分，收入增长会相应提高4.6个百分点，即使加入AI使用水平这个控制变量，结果也同样如此。假设可信AI指数提升到所述水平，对于在2024财年至2025财年期间实现1亿美元增长的大型组织（员工人数超过1,000人），将额外获得460万美元的收入增长；而对于中等规模的组织（去年收入增长率达19.5%）将能实现近25%的增长。有关本报告建模的更多详情，请参阅附录三。

“有效AI治理能够提升AI解决方案效益。即使将AI解决方案的使用量考虑在内，提高AI治理成熟度水平也可促成更高的收入增长。”

有一种误解认为AI治理可能会导致内部业务变得繁琐，从而延缓AI在组织中的应用。然而，有效AI治理能够通过建立明确的流程和控制来简化AI解决方案的部署流程。44%的高管认为，有效AI治理可以加快AI解决方案在整个组织的部署速度。另一项研究也发现，拥有健全AI治理框架的组织，其部署AI解决方案的速度要比缺乏此类框架的组织快20%。



05

搭建可信AI的基础

有效AI治理对于组织将AI解决方案融入运营及业务模式至关重要。如前文所述，提高治理有效性能够扩大技术应用、增加回报，同时也有助于管理负面风险。

组织领导当前能够采取哪些关键措施来改善AI治理呢？根据我们对调研结果的分析，以下四项行动具有突出的影响力。

建议一

重视AI治理以从AI获益

1

AI治理成熟度水平分布情况显示，大多数组织需要大幅提高AI治理水平。我们的研究表明，加强AI治理并非“锦上添花”，而是成为不可或缺的关键因素，赋能组织利用AI这项强大的企业技术。将AI治理列为优先重点，组织首先需要了解从何处着手。

AI治理成熟度指数涵盖五大支柱领域，即组织架构、政策与原则、程序与控制、人才与技能以及监控、报告和评估，组织

可据其评估相关制度并识别需要改善的领域。我们的研究发现，许多组织应主要关注“政策与原则”与“程序与控制”两大支柱领域。

为应对与AI相关的新风险或随着解决方案部署而出现的风险，组织还需对AI治理进行持续评估。特定地区和行业适用的法规不断变化，组织必须始终站在AI治理相关标准的最前沿。

AI治理成熟度指数的五大支柱领域



建议二

2

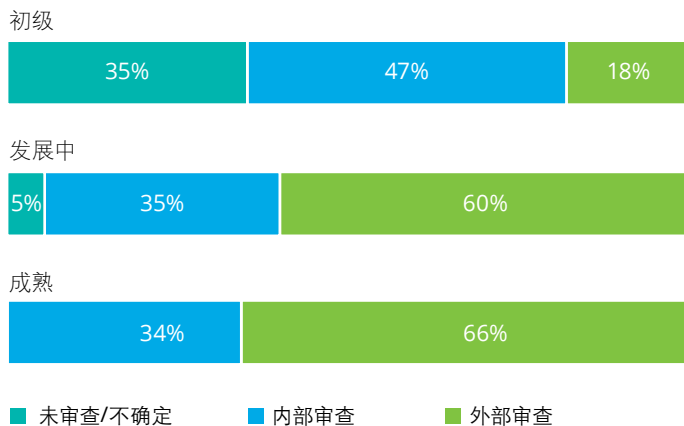
了解并利用更广泛的AI供应链

了解组织对AI的应用情况及与更广泛的“AI供应链”（即开发者、部署者、监管机构、平台服务商、终端用户及客户）的互动情况，能够帮助组织更全面地了解AI治理要求。例如，15%的受访高管表示，其组织正在综合使用外购的“现成”AI解决方案、内部开发的AI解决方案以及公开可用的AI应用程序。每一种来源的AI均要求采用定制化的治理方法。

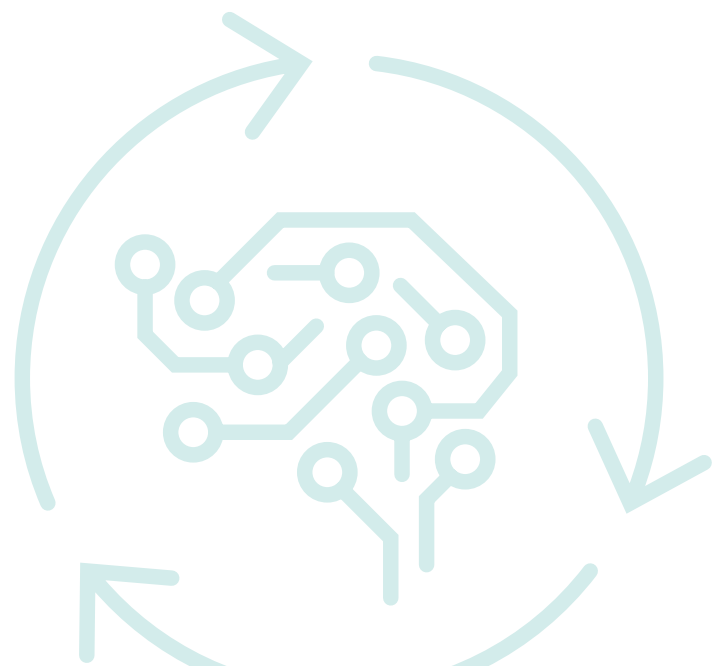
更广泛的“AI供应链”还能带来专业和/或不同的观点，从而帮助组织改善AI治理。越来越多的组织希望通过聘请外部审

计机构在其治理框架中搭建“第三层防御”。为了发挥这一作用，组织需要在AI解决方案的整个生命周期内安排外部审计。值得注意的是，已聘请外部机构进行审查的组织，所获得的可信AI指数更高（图10）。AI治理成熟度达到“成熟”水平的组织中，有三分之二的组织都聘请了外部机构来审查其AI解决方案的实施情况。该项研究进行的咨询还表明，与相关行业协会进行互动有助于了解AI治理的独特要求。

图10: AI实施情况审查类型与AI治理成熟度指数



资料来源：德勤可信AI调研（2024年）。



建议三

3

打造风险管理者，而非风险规避者

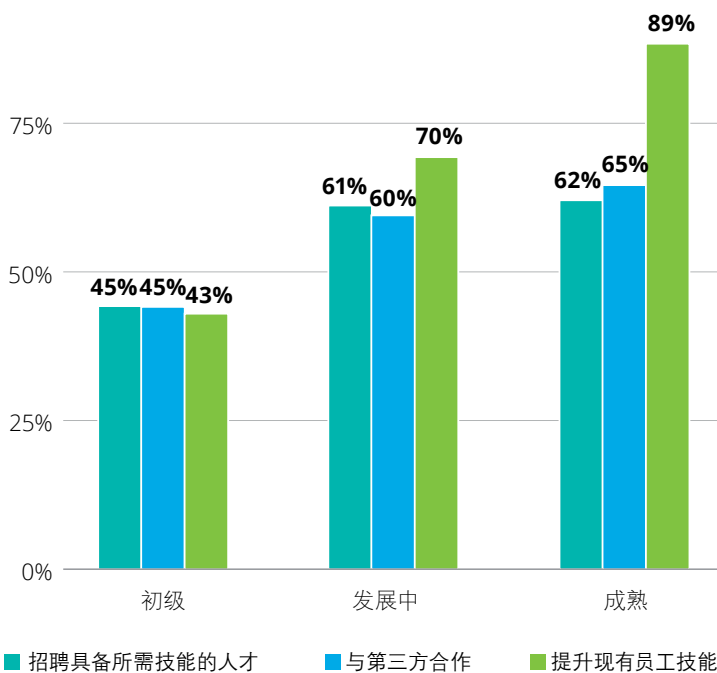
人的判断和行动（或反应）对实施成功的AI治理十分关键。无论是作为AI解决方案的设计者、部署者还是使用者，员工都能在AI解决方案的功能特性及潜在风险方面提供宝贵见解。重要的是，发展员工的技能有助于识别、评估和管理风险，从而能够预防或缓解出现的风险，而不是规避或忽视风险。有鉴于此，作为AI治理成熟度指数的一大关键支柱领域，“人才与技能”的重要性不言而喻，却仍然是受访组织平均得分最低的领域。

AI治理成熟度达到“成熟”水平的组织更可能积极发展员工技能，以确保员工以符合伦理、负责任的方式使用AI。达到“成熟”水平的组织中，近90%的组织正在提高现有员工

的技能，以缩小与以符合伦理和法律的方式使用AI相关的技能差距，而处于“初级”水平的组织中，仅43%的组织为缩小这一差距而提升员工技能。此外，达到“成熟”水平的组织还与拥有适当技能的第三方机构合作（65%），以及招聘拥有适当技能的员工（63%）。

这些行动对缩小AI技能差距产生了切实的影响，而随着技术能力及监管环境的不断发展，持续提高和更新技能将变得十分重要。达到“成熟”水平的组织中，具备所需的技能来以符合伦理和法律的方式使用AI的员工比例达到73%，而在处于“初级”水平的组织中，这一比例仅有40%。

图11: 缩小技能差距的方法与AI治理成熟度指数



资料来源：德勤可信AI调研（2024年）。

建议四

加强沟通，确保AI转型准备就绪

4

在AI的日常治理中，有效沟通非常重要，也是让员工参与其中的必要条件。这包括披露AI长期战略，明确AI为组织带来的益处和风险，提高员工使用AI模型的技能，以及对其工作在未来可能由AI执行的人员进行技能提升。组织必须确保所有利益相关者都了解AI带来的风险和益处，以及确保他们可以对AI的使用作出知情决策并提出疑虑。这便要求清晰、透明的沟通，以及开展对话的意愿。对此，组织可采取的实际行动包括针对高风险事件进行情景规划；编写故事，以便领导者和员工能够针对技术的作用和影响讲述出一个可信、充满人性化的故事；以及进行危机演习，以测试应对严重但可能发生事件的准备情况。

“建立卓越AI治理通常需要组织内部的思维转变。最开始，一些同事会提出疑问，认为AI治理是否仅仅只是IT方面的问题。然而，经过讨论AI如何渗透各个领域，包括IT、网络安全、风险评估和监管合规，我们认识到了一个要点：在实现卓越AI治理方面，每一个团队都承担着责任。”

某大型电信服务提供商，数据战略总监

附录



附录一 调研

2024年9月和10月，我们对亚太十三个地区899名高管进行调研，旨在评估AI治理结构成熟度，以及了解卓越AI治理益处。

我们选定首席风险官、首席合规官和首席数据官等高管作为受访者，覆盖多个部门（包括公共、私营和非营利部门）及行业（包括金融、教育、健康和技术行业）。

表A1列示亚太各地区受访者数量。图A1和A2列示受访者所属行业及所任职务。

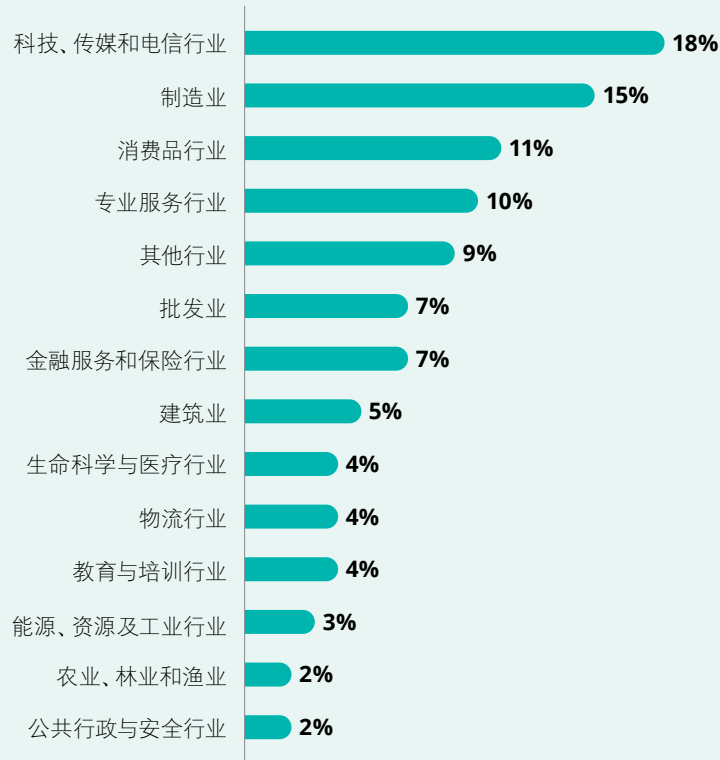
表A1：受访者地区分布

地区	受访者数量
澳大利亚	112
中国大陆	103
印度	102
日本	104
新西兰	53
东南亚	321
印度尼西亚	64
马来西亚	51
菲律宾	52
新加坡	51
泰国	51
越南	52
韩国	52
中国台湾	52
合计	899

资料来源：德勤可信AI调研（2024年）。

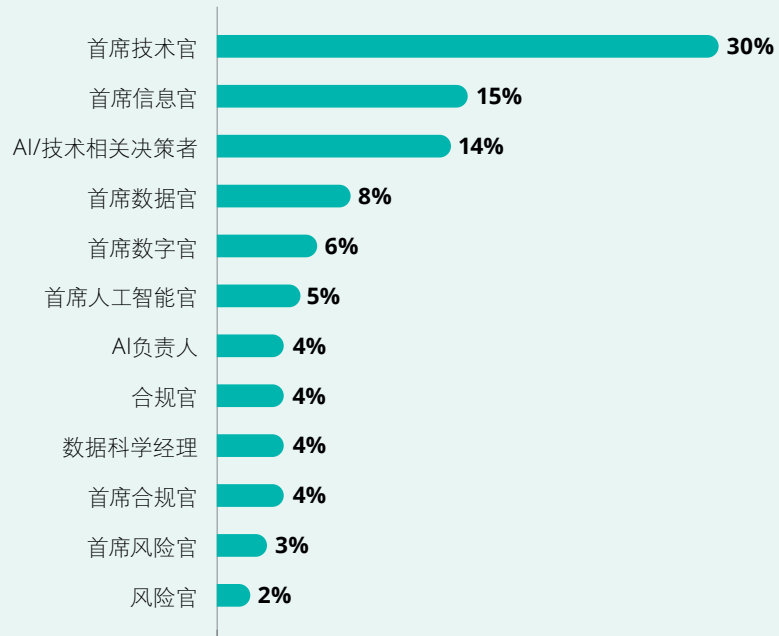


图A1: 受访者所属行业



资料来源: 德勤可信AI调研 (2024年)。

图A2: 受访者所任职务



资料来源: 德勤可信AI调研 (2024年)。

附录二

德勤AI治理成熟度指数

我们针对本次调研开发德勤AI治理成熟度指数，利用以下五大关键支柱领域的12个问题（部分问题包含多个子问题）的答案作为指数构建依据。我们通过收集问卷答复已将该方法运用于近900家组织。



组织架构

1) 在贵组织中，AI相关伦理、法律和技术标准宣贯和评估由谁/什么机构主要负责？

可能的回答：董事会、首席执行官、首席技术官、首席数字官、首席数据官、首席合规官、首席信息官、首席风险官、首席人工智能官、高管团队、合规专员、AI负责人、部门主管/总经理/高级经理）、AI开发团队、其他

2) 贵组织目前具备以下哪些AI使用相关组织架构要素？

- a. 设有由董事会监督的AI治理机构
- b. 设有负责监督AI治理的AI委员会（由法律、合规、信息技术、人力资源等相关部门代表组成）
- c. 针对AI全生命周期明确界定AI治理相关角色和责任，如业务成果负责人、AI系统负责人、数据负责人、领域架构师等。

3) 以下哪项可恰当反映贵组织负责管理AI的伦理、法律和监管合规专责团队的组建形式？

- a. 我们未设负责管理AI使用的伦理、风险或合规专责岗位
- b. 某些部门/团队有负责管理AI使用的伦理、风险和合规专责人员
- c. 各部门/团队均有负责管理AI使用的伦理、风险和合规专责人员
- d. 组织设有伦理、风险和合规专责团队负责监控组织范围AI使用趋势并甄别相关风险
- e. 以上均不是
- f. 不确定/不愿透露



政策与原则

1) 您如何描述贵组织的AI战略?

- a. 尚无AI战略, 且当前并未采取行动制定相关战略
- b. 目前尚无AI战略, 但正积极采取行动制定相关战略
- c. 某些部门/团队已制定自身AI战略
- d. 已制定组织层面AI战略, 但并非人人都明白其价值
- e. 已制定组织层面AI战略且将其作为优先重点, 但未跟进其进展
- f. 已制定组织层面AI战略, 具备明确界定的流程, 可据以优先实施分析举措并评估价值
- g. 不确定/不愿透露

2) 贵组织的AI战略或治理框架包含以下哪些要素?

- a. 指导组织内部以安全和负责任的方式使用AI的AI政策
- b. 伦理指引和原则
- c. 明确界定的AI风险偏好
- d. AI治理目标和程序实施时间表
- e. 实施治理举措的资金来源
- f. 监控和审计流程
- g. 事件响应和补救计划
- h. 成效指标和关键绩效指标
- i. 与组织其他相关政策(隐私、数据治理和网络安全政策)或战略目标整合

3) 贵组织使用或部署的AI系统具备以下哪些要素?

- a. 针对AI系统的监督和持续监控明确角色和责任
- b. 针对使用AI系统作出或推导的决策明确责任分配
- c. 已采取保护措施, 以确保AI系统的数据使用不会超出预定和声明的用途
- d. 用户了解AI系统如何作出影响他们的决策
- e. 已采取适当机制来甄别和减少AI系统偏见, 以确保公平和公正
- f. AI系统以负责任的方式设计和运行, 旨在造福人类、社会和环境
- g. AI系统的设计和运行性能使其具备一致和准确输出的能力、容错能力, 以及从意外中断中快速恢复的能力
- h. AI系统具备完善防护, 以避免被攻击者非法访问和利用
- i. 已采取数据匿名及假名化处理措施, 以保护个人和敏感信息



程序与控制

1) 是否具备相关机制，允许员工就AI使用和输出反映问题？

可能的回答：是、否、计划实施、不确定

2) 贵组织实施了以下哪些AI使用相关实践、程序或控制？

- a. 对AI解决方案的风险集进行界定的AI风险分类法
- b. 支持在开发、测试和实施过程中识别和管理相关风险的AI风险评估程序
- c. 旨在缓解AI解决方案使用相关风险的AI控制框架
- d. 贵组织所用AI解决方案（包括内部开发或外购）的最新清单
- e. 评估和监控AI系统活动风险和合规性的AI治理平台
- f. 用以支持独立第三方审计的AI全生命周期信息采集系统
- g. 外部各方（客户或其他利益相关方）处理AI使用相关风险或投诉的程序



人才、技能和文化

1) 贵组织为员工提供了以下哪些资源来支持他们以符合伦理、合法、合规和准确的方式使用AI？

- a. 提供AI工作应用指引
- b. 为员工提供咨询服务或成立咨询小组，供员工向具有风险和合规经验的团队成员咨询有关AI使用的问题
- c. 提供AI工作应用培训，宣贯AI所涉伦理、法律及监管合规风险
- d. 针对AI系统使用采取安全和隐私保护措施（如数据加密和访问控制）
- e. 在职学习促进举措（如鼓励员工自行独立试验或是通过加入实践社区或参与团队讨论开展独立试验）

2) 根据您的合理估计，有多少员工的技能和能力水准足以支持他们以符合伦理且合法的方式使用AI？



监控、报告和评估

- 1) 贵组织多久复核一次规范AI工作应用的现行法律或监管要求，以保护权利并防止不当使用？
 - a. 至少数月一次
 - b. 至少半年一次
 - c. 至少一年一次
 - d. 年均不足一次
 - e. 以上均不是
 - f. 不确定/不愿透露

- 2) 贵组织多久评估一次自有AI系统，以确保其符合组织AI标准？
 - a. 持续或实时
 - b. 至少数月一次
 - c. 至少半年一次
 - d. 至少一年一次
 - e. 年均不足一次
 - f. 以上均不是
 - g. 不确定/不愿透露

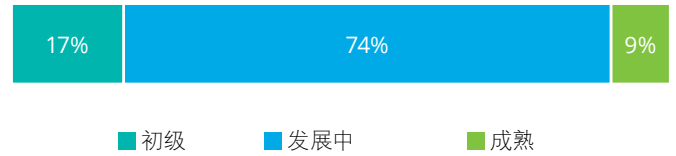
每个答案的得分为0至100分，每个问题的“最佳”答案得分为100分。例如，如果某组织的答案是“我们已制定组织层面AI战略，具备清晰的流程来确定优先次序和评估价值”，则该组织相关问题得分为100分，而如果答案是只有某些部门制定了AI战略，则相关问题得分为60分。各支柱领域得分是相应支柱领域所有问题的平均得分，总体指数反映所有支柱领域的平均得分。

得分50分以下的组织为“初级”，50至90分为“发展中”，90分以上为“成熟”。按得分统计的成熟度分布情况如下图所示：

AI治理成熟度指数各支柱领域得分的平均值、中位值以及处于“初级”或“成熟”水平的组织占比如下表所示：

AI治理成熟度指数	平均值	中位值	初级组织占比	成熟组织占比
总体指数	70.8	68.0	9%	17%
组织架构	73.9	72.0	9%	18%
政策与原则	58.4	66.3	31%	13%
实践、流程和控制	64.8	67.5	23%	10%
人才、技能和文化	67.2	70.0	22%	14%
监控、报告和评估	76.0	80.0	6%	18%

图B1: AI治理成熟度水平分布



资料来源：德勤可信AI调研（2024年）

附录三

计量经济学建模

为量化卓越AI治理实践与业务绩效指标之间的关系，我们使用普通最小二乘法求解回归值。为降低遗漏变量偏差风险，我们纳入组织关键特征作为控制变量，具体如下表所示：

控制变量	详细信息
总部所在国家/地区	组织自行报告的总部所在国家/地区 (包含13个选项)
行业	组织自行报告的ANZSIC (一位数) 代码 (包含19个选项)
员工人数	组织自行报告的全职员工人数 (包含4个选项)
部门	组织所属部门 (公共、私营或非营利部门)
营业收入	组织自行报告的2023-24财年营业收入 (连续计算并按照2024年10月汇率换算为美元)

两个因变量分别为受访组织已“全面实施”AI解决方案的业务领域数量 (包含10个选项)，以及在工作中使用AI解决方案的员工比例 (0%-100%)。

关键自变量是德勤AI治理成熟度指数，其计算方法详见上述附录。我们使用具体得分和所处水平来评估组织AI治理成熟度。

此外，考虑到组织的AI应用水平可能与误差项和自变量相关，我们还将在工作中使用AI的员工比例作为控制变量。纳入这些变量不会显著改变关键参数估计值。对于以在工作中使用AI的员工比例为自变量的模型，我们将全面实施AI解决方案的业务领域数量作为控制变量。

我们使用以下公式求解回归值：

- 1) 使用AI的员工比例 = $\beta_0 + \beta_1 * \text{指数得分} + \beta_2 * \text{使用AI工具的业务领域数量} + \text{控制变量}$
- 2) 使用AI工具的业务领域数量 = $\beta_0 + \beta_1 * \text{指数得分} + \beta_2 * \text{使用AI的员工比例} + \text{控制变量}$
- 3) 营业收入增长率 = $\beta_0 + \beta_1 * \text{指数得分} + \beta_2 * \text{使用AI的员工比例} + \text{控制变量}$

回归模型汇总如下。鉴于有关数据由组织自行报告，可能存在一些未观察到的因素与解释变量和误差项相关，或导致估计值出现偏差，建议谨慎解读模型。结果仅反映相关性。

模型一：因变量 - 使用AI工具的员工比例

变量	估计值	标准误差	P值
指数得分	0.30543	0.0646	<0.00001
使用AI工具的业务领域	2.02022	0.3996	<0.00001
决定系数	0.1978		
调整后的决定系数	0.1510		

模型二：因变量 - 使用AI工具的员工比例

变量	估计值	标准误差	P值
指数水平 - “发展中”	8.27383	2.865	<0.00001
指数水平 - “成熟”	15.7533	4.123	0.004
使用AI工具的业务领域	2.257	0.393	<0.00001
决定系数	0.1881		
调整后的决定系数	0.1394		

模型三：因变量 - 使用AI工具的业务领域

变量	估计值	标准误差	P值
指数得分	0.0555	0.0061	<0.00001
使用AI的员工比例	0.0197	0.0039	<0.00001
决定系数	0.3352		
调整后的决定系数	0.2965		

模型四：因变量 - 使用AI工具的业务领域

变量	估计值	标准误差	P值
指数水平 - “发展中”	1.3557	0.283	<0.00001
指数水平 - “成熟”	3.0569	0.396	<0.00001
使用AI的员工比例	0.0226	0.004	<0.00001
决定系数	0.3120		
调整后的决定系数	0.2707		

模型五：因变量 - 2023-24财年营业收入增长率

变量	估计值	标准误差	P值
指数得分	0.0031	0.0018	0.0884
使用AI的员工比例	0.0017	0.0011	0.1355
决定系数	0.0677		
调整后的决定系数	0.004769		

附录四

地区聚焦



澳大利亚




人口：2,710万 | 国内生产总值 (GDP)：1.7万亿美元






卓越AI治理可望为组织带来的三大**益处**

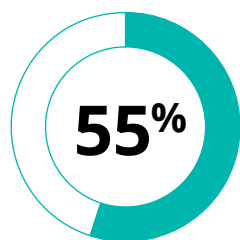
-  对AI解决方案成效或成果的信任度提高 (47%)
-  信任度提高带动AI解决方案使用增加 (46%)
-  监管合规水平提高 (42%)

组织在AI使用中最担忧的三大**风险**

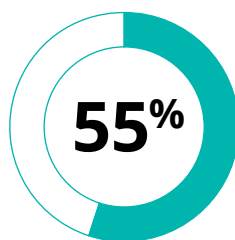
-  监控：监控泛滥导致隐私侵犯 (88%)
-  隐私：AI系统中敏感、保密或个人数据泄露风险 (88%)
-  安全漏洞：网络入侵/网络安全风险 (85%)

组织在AI使用或实施中的三大**障碍**

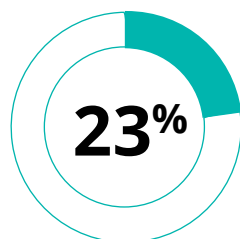
-  对监管、法律、伦理、合规等风险的担忧 (44%)
-  对AI技术及其潜力的认识不足 (34%)
-  人才和/或技术技能短缺 (29%)



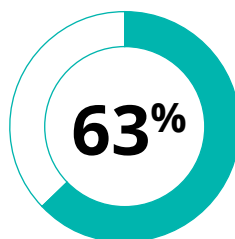
澳大利亚组织已建立便于员工反映问题的机制。



澳大利亚组织的员工具备所需技能，能够以符合伦理和法律的方式使用AI。



澳大利亚组织表示上一财年事件报告增加。



澳大利亚组织正在提高现有员工的技能，以缩小与以符合伦理和法律的方式使用AI相关的技能差距。

注：澳大利亚样本容量 = 112

中国大陆



人口: 14.19亿 | GDP: 18.2万亿美元






卓越AI治理可望为组织带来的三大**益处**

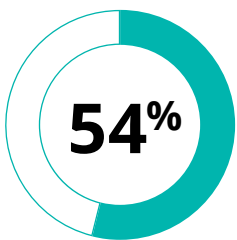
-  信任度提高带动AI解决方案使用增加 (52%)
-  利用AI解决方案实现生产力效益提升 (51%)
-  整个组织AI解决方案开发加速 (50%)

组织在AI使用中最担忧的三大**风险**

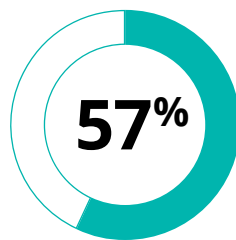
-  安全漏洞: 网络入侵/网络安全风险 (86%)
-  法律风险和版权侵犯 (80%)
-  合规负担: AI解决方案使用相关报告或流程要求的严格程度 (80%)

组织在AI使用或实施中的三大**障碍**

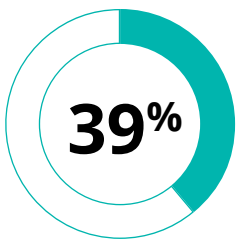
-  技术实施挑战 (38%)
-  缺乏创新意愿和/或试验干劲不足 (36%)
-  人才和/或技术技能短缺 (34%)



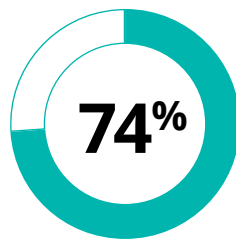
中国大陆组织已建立便于员工反映问题的机制。



中国大陆组织的员工具备所需技能,能够以符合伦理和法律的方式使用AI。



中国大陆组织表示上一财年事件报告增加。



中国大陆组织与第三方合作,以缩小与以符合伦理和法律的方式使用AI相关的技能差距。

注: 中国大陆样本容量 = 103

印度






人口: 14.51亿 | GDP: 3.95万亿美元

卓越AI治理可望为组织带来的三大**益处**

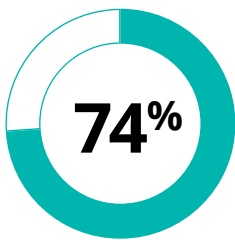
-  对AI解决方案成效或成果的信任度提高 (63%)
-  在客户中的声誉提高 (60%)
-  信任度提高带动AI解决方案使用增加 (57%)

组织在AI使用中最担忧的三大**风险**

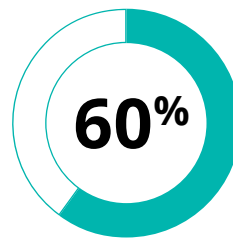
-  安全漏洞: 网络入侵/网络安全风险 (92%)
-  隐私: 敏感、保密或个人数据泄露风险 (91%)
-  监管不确定性: 不断变化的要求可能导致合规义务盲区 (89%)

组织在AI使用或实施中的三大**障碍**

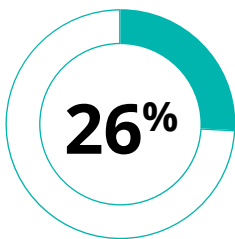
-  技术实施挑战 (50%)
-  对AI技术及其潜力的认识不足 (35%)
-  对监管、法律、伦理等风险的担忧 (32%)



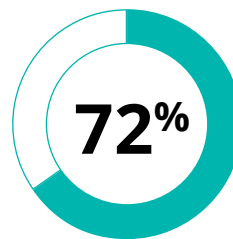
印度组织已建立便于员工反映问题的机制。



印度组织的员工具备所需技能，能够以符合伦理和法律的方式使用AI。



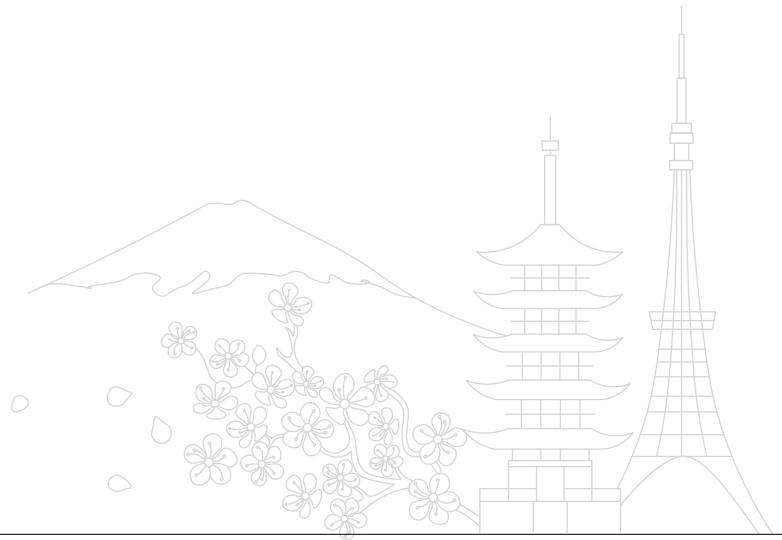
印度组织表示上一财年事件报告增加。



印度组织通过招聘拥有适当技能的员工，以缩小与以符合伦理和法律的方式使用AI相关的技能差距。

注: 印度样本容量 = 102

日本






人口：1.238亿 | GDP：4.1万亿美元


卓越AI治理可望为组织带来的三大**益处**

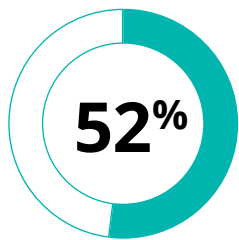
-  对AI解决方案成效或成果的信任度提高 (51%)
-  在客户中的声誉提高 (49%)
-  信任度提高带动AI解决方案使用增加 (45%)

组织在AI使用中最担忧的三大**风险**

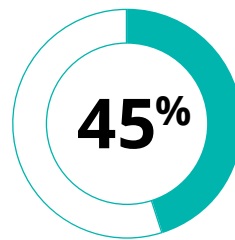
-  安全漏洞：网络入侵/网络安全风险 (88%)
-  监控：监控泛滥导致隐私侵犯 (85%)
-  隐私：敏感、保密或个人数据泄露风险 (83%)

组织在AI使用或实施中的三大**障碍**

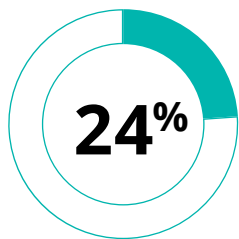
-  人才和/或技术技能短缺 (38%)
-  对监管、法律、伦理、合规等风险的担忧 (36%)
-  技术实施挑战 (33%)



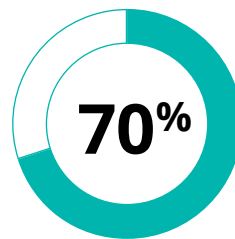
日本组织已建立便于员工反映问题的机制。



日本组织的员工具备所需技能，能够以符合伦理和法律的方式使用AI。



日本组织表示上一财年事件报告增加。

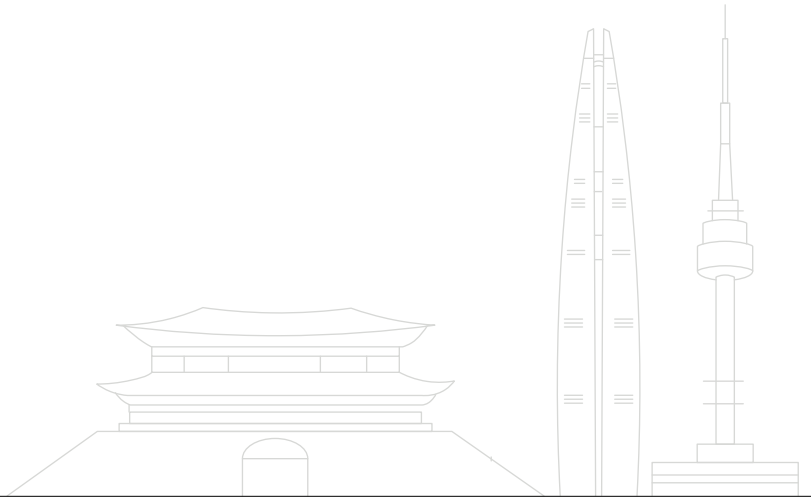


日本组织正在提高现有员工的技能，以缩小与以符合伦理和法律的方式使用AI相关的技能差距。

注：日本样本容量 = 104

韩国

人口: 5,180万 | GDP: 1.7万亿美元



卓越AI治理可望为组织带来的三大**益处**

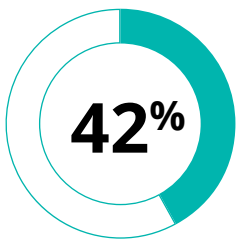
- 信任度提高带动AI解决方案使用增加 (46%)
- 监管合规水平提高 (42%)
- 整个组织AI解决方案开发加速 (40%)

组织在AI使用中最担忧的三大**风险**

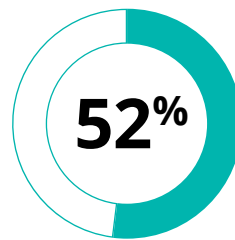
- 安全漏洞: 网络入侵/网络安全风险 (85%)
- 监控: 监控泛滥导致隐私侵犯 (85%)
- 合规负担: AI解决方案使用相关报告或流程要求的严格程度 (83%)

组织在AI使用或实施中的三大**障碍**

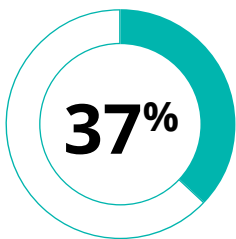
- 技术实施挑战 (35%)
- AI实施战略和愿景缺位 (33%)
- 对监管、法律、伦理、合规等风险的担忧 (31%)



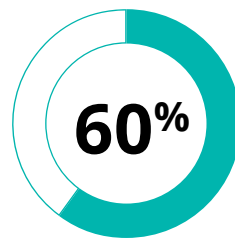
韩国组织已建立便于员工反映问题的机制。



韩国组织的员工具备所需技能，能够以符合伦理和法律的方式使用AI。



韩国组织表示上一财年事件报告增加。

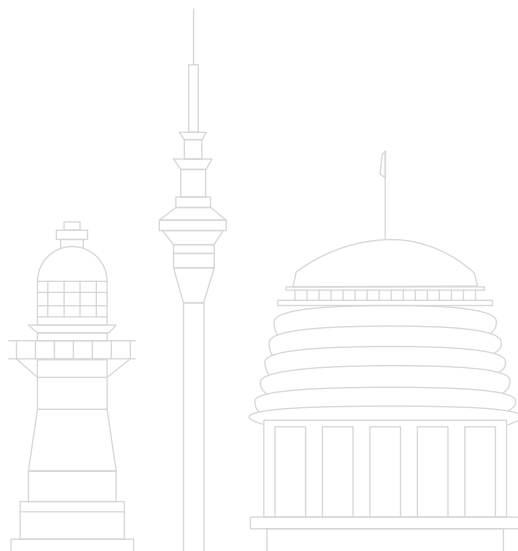


韩国组织通过招聘拥有适当技能的员工，以缩小与以符合伦理和法律的方式使用AI相关的技能差距。

注: 韩国样本容量 = 52

新西兰




人口: 520万 | GDP: 2,530亿美元





卓越AI治理可望为组织带来的三大**益处**

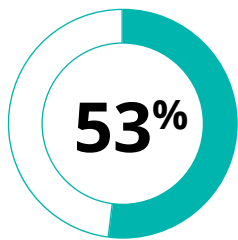
-  信任度提高带动AI解决方案使用增加 (51%)
-  利用AI解决方案实现生产力效益提升 (42%)
-  在客户中的声誉提高 (38%)

组织在AI使用中最担忧的三大**风险**

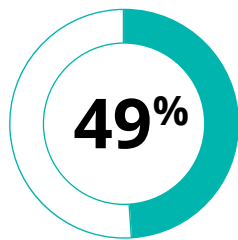
-  可靠性和错误 (87%)
-  安全漏洞: 网络入侵/网络安全风险 (85%)
-  隐私: AI系统中敏感、保密或个人数据泄露风险 (85%)

组织在AI使用或实施中的三大**障碍**

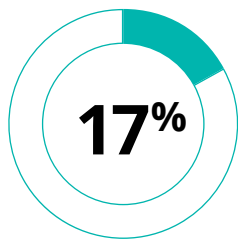
-  对监管、法律、伦理、合规等风险的担忧 (40%)
-  对AI技术及其潜力的认识不足 (38%)
-  资金不足 (36%)



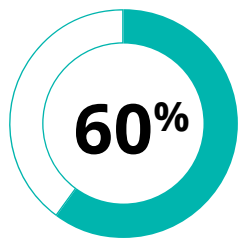
新西兰组织已建立便于员工反映问题的机制。



新西兰组织的员工具备所需技能，能够以符合伦理和法律的方式使用AI。



新西兰组织表示上一财年事件报告增加。

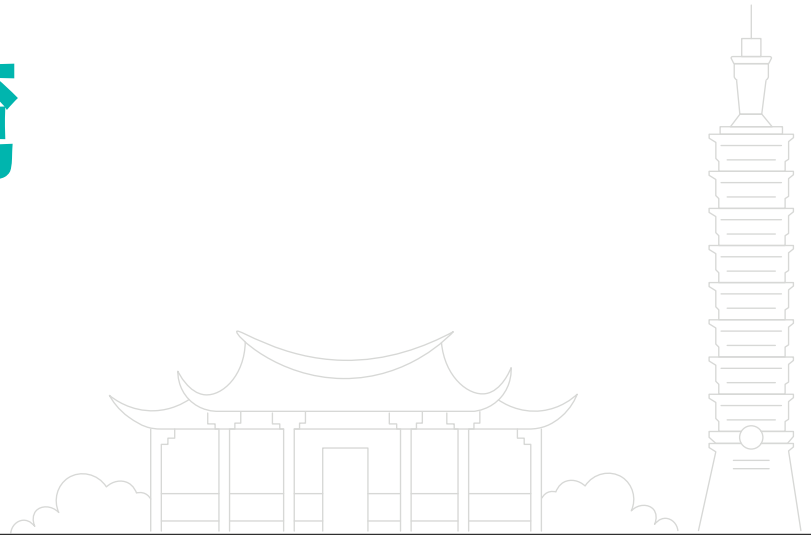


新西兰组织与第三方合作，以缩小与以符合伦理和法律的方式使用AI相关的技能差距。

注: 新西兰样本容量 = 53

中国台湾

人口: 2,340万 | GDP: 7,565.9亿美元



卓越AI治理可望为组织带来的三大**益处**

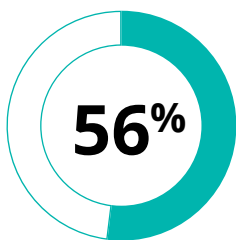
- 利用AI解决方案实现生产力效益提升 (64%)
- 整个组织AI解决方案部署加速 (48%)
- 在客户中的声誉提高 (44%)

组织在AI使用中最担忧的三大**风险**

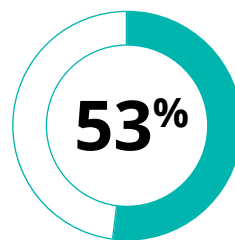
- 安全漏洞: 网络入侵/网络安全风险 (85%)
- 监控: 监控和数据采集泛滥导致隐私侵犯 (85%)
- 监管不确定性: 不断变化的要求可能导致合规义务盲区 (81%)

组织在AI使用或实施中的三大**障碍**

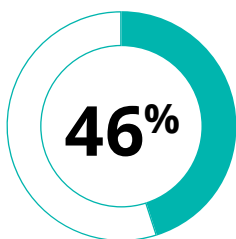
- 技术实施挑战 (40%)
- AI用例和投资与战略脱节 (40%)
- 缺乏创新意愿和/或试验干劲不足 (37%)



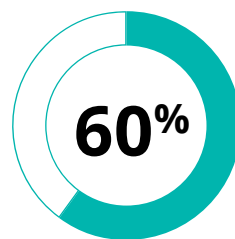
中国台湾组织已建立便于员工反映问题的机制。



中国台湾组织的员工具备所需技能,能够以符合伦理和法律的方式使用AI。



中国台湾组织表示上一财年事件报告增加。

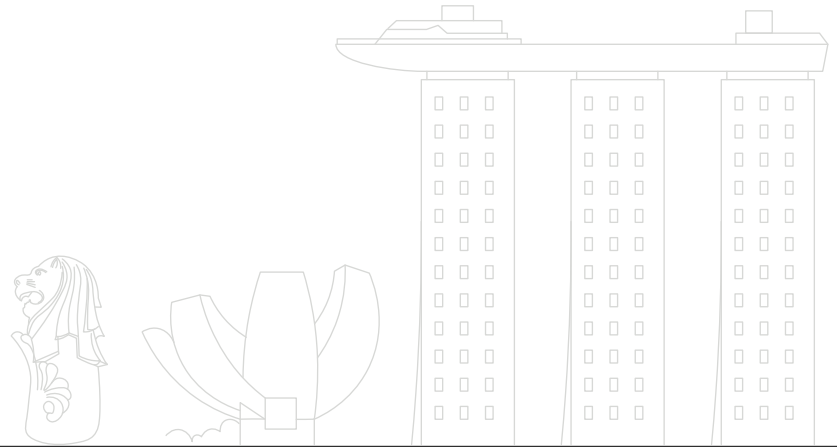


中国台湾组织通过招聘拥有适当技能的员工,以缩小与以符合伦理和法律的方式使用AI相关的技能差距。




注: 中国台湾样本容量 = 52

新加坡




人口: 580万 | GDP: 5,010亿美元





卓越AI治理可望为组织带来的三大**益处**

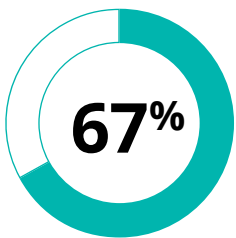
-  在客户中的声誉提高 (43%)
-  对AI解决方案成效或成果的信任度提高 (43%)
-  监管合规水平提高 (39%)

组织在AI使用中最担忧的三大**风险**

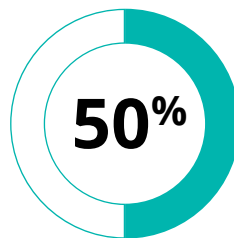
-  安全漏洞: 网络入侵/网络安全风险 (96%)
-  隐私: AI系统中敏感、保密或个人数据泄露风险 (94%)
-  可靠性和错误 (94%)

组织在AI使用或实施中的三大**障碍**

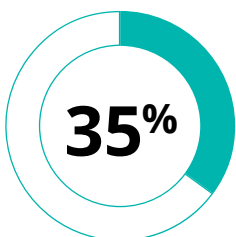
-  对AI技术及其潜力的认识不足 (41%)
-  对监管、法律、伦理、合规等风险的担忧 (37%)
-  技术实施挑战 (31%)



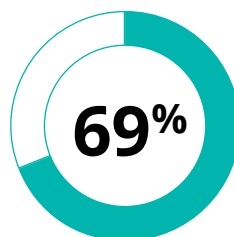
新加坡组织已建立便于员工反映问题的机制。



新加坡组织的员工具备所需技能，能够以符合伦理和法律的方式使用AI。



新加坡组织表示上一财年事件报告增加。



新加坡组织通过招聘拥有适当技能的员工，以缩小与以符合伦理和法律的方式使用AI相关的技能差距。

注: 新加坡样本容量 = 51

印度尼西亚






人口: 2.787亿 | GDP: 1.37万亿美元


卓越AI治理可望为组织带来的三大**益处**

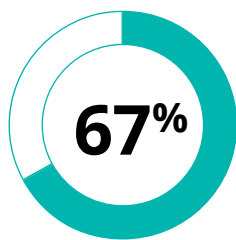
-  对AI解决方案成效或成果的信任度提高 (67%)
-  整个组织AI解决方案开发加速 (63%)
-  信任度提高带动AI解决方案使用增加 (61%)

组织在AI使用中最担忧的三大**风险**

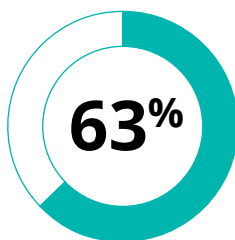
-  安全漏洞: 网络入侵/网络安全风险 (88%)
-  监控: 监控泛滥导致隐私侵犯 (84%)
-  法律风险和版权侵犯: AI解决方案数据使用相关法律责任 (83%)

组织在AI使用或实施中的三大**障碍**

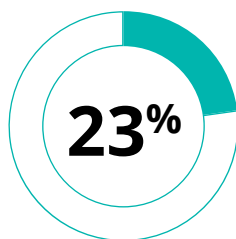
-  对AI技术及其潜力的认识不足 (41%)
-  对监管、法律、伦理、合规等风险的担忧 (38%)
-  技术实施挑战 (如维护、与现有系统集成所涉挑战) (36%)



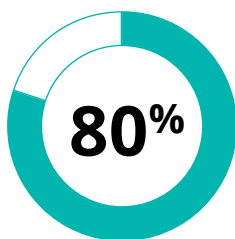
印度尼西亚组织已建立便于员工反映问题的机制。



印度尼西亚组织的员工具备所需技能,能够以符合伦理和法律的方式使用AI。



印度尼西亚组织表示上一财年事件报告增加。

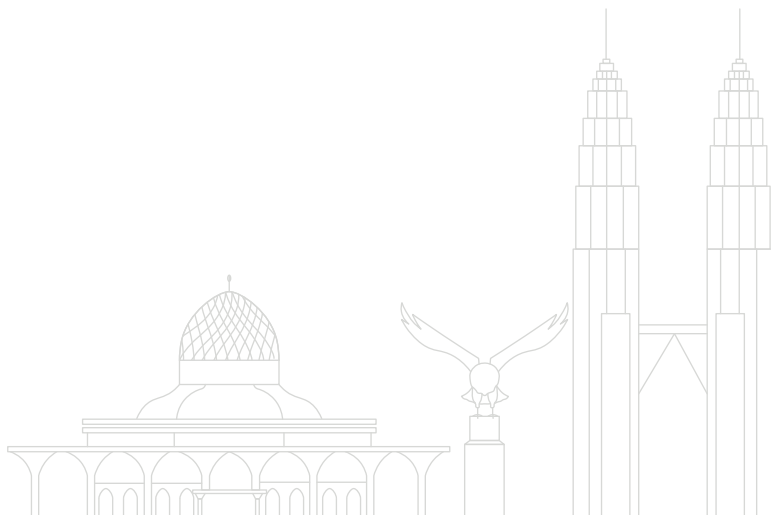


印度尼西亚组织正在提高现有员工的技能,以缩小与以符合伦理和法律的方式使用AI相关的技能差距。




注: 印度尼西亚样本容量 = 64

马来西亚




人口: 3,340万 | GDP: 4,000亿美元






卓越AI治理可望为组织带来的三大**益处**

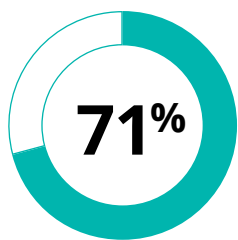
-  对AI解决方案成效或成果的信任度提高 (65%)
-  信任度提高带动AI解决方案使用增加 (63%)
-  整个组织AI解决方案开发加速 (53%) 增加 (61%)

组织在AI使用中最担忧的三大**风险**

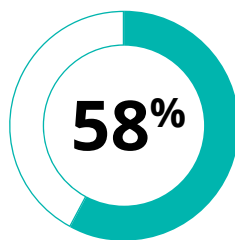
-  安全漏洞: 网络入侵/网络安全风险 (90%)
-  监控: 监控泛滥导致隐私侵犯 (84%)
-  隐私: AI系统中敏感、保密或个人数据泄露风险 (82%)

组织在AI使用或实施中的三大**障碍**

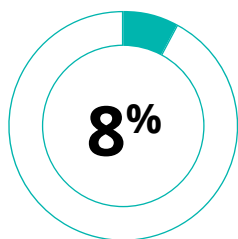
-  技术实施挑战 (如维护、与现有系统集成所涉挑战) (51%)
-  对AI技术及其潜力的认识不足 (37%)
-  人才和/或技术技能短缺 (33%)



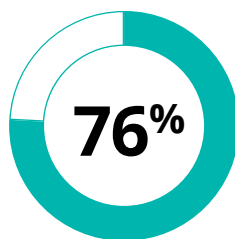
马来西亚组织已建立便于员工反映问题的机制。



马来西亚组织的员工具备所需技能,能够以符合伦理和法律的方式使用AI。



马来西亚组织表示上一财年事件报告增加。



马来西亚组织正在提高现有员工的技能,以缩小与以符合伦理和法律的方式使用AI相关的技能差距。




注: 马来西亚样本容量 = 51

越南




人口: 1.003亿 | GDP: 4,300亿美元






卓越AI治理可望为组织带来的三大**益处**

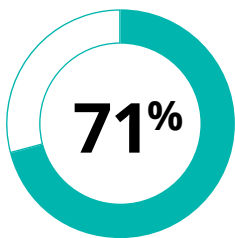
-  在客户中的声誉提高 (67%)
-  利用AI解决方案实现生产力效益提升 (65%)
-  对AI解决方案成效或成果的信任度提高 (62%)

组织在AI使用中最担忧的三大**风险**

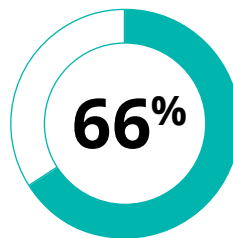
-  隐私: AI系统中敏感、保密或个人数据泄露风险 (81%)
-  责任: AI系统开发者和使用者缺乏责任意识, 存在不当或不道德使用风险 (81%)
-  可靠性和错误: 输出有误、不可预测性和潜在故障或意外行为 (如幻觉问题) (79%)

组织在AI使用或实施中的三大**障碍**

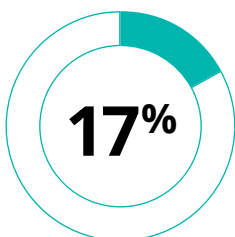
-  人才和/或技术技能短缺 (56%)
-  对监管、法律、伦理、合规等风险的担忧 (40%)
-  AI实施战略和愿景缺位 (37%)



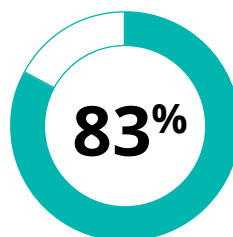
越南组织已建立便于员工反映问题的机制。



越南组织的员工具备所需技能, 能够以符合伦理和法律的方式使用AI。



越南组织表示上一财年事件报告增加。



越南组织正在提高现有员工的技能, 以缩小与以符合伦理和法律的方式使用AI相关的技能差距。

注: 越南样本容量 = 52

泰国




人口: 6,610万 | GDP: 5,150亿美元




卓越AI治理可望为组织带来的三大**益处**

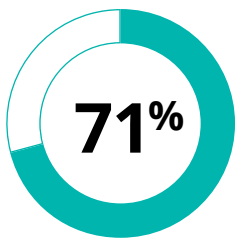
-  对AI解决方案成效或成果的信任度提高 (55%)
-  信任度提高带动AI解决方案使用增加 (51%)
-  整个组织AI解决方案部署加速 (43%)

组织在AI使用中最担忧的三大**风险**

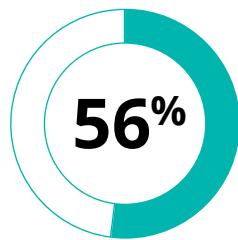
-  安全漏洞: 网络入侵/网络安全风险 (76%)
-  监控: 监控泛滥导致隐私侵犯 (75%)
-  法律风险和版权侵犯: AI解决方案数据使用相关法律责任 (71%)

组织在AI使用或实施中的三大**障碍**

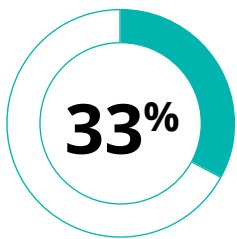
-  对AI技术及其潜力的认识不足 (41%)
-  技术实施挑战 (37%)
-  对监管、法律、伦理、合规等风险的担忧 (35%)



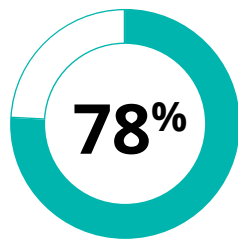
泰国组织已建立便于员工反映问题的机制。



泰国组织的员工具备所需技能，能够以符合伦理和法律的方式使用AI。



泰国组织表示上一财年事件报告增加。



泰国组织正在提高现有员工的技能，以缩小与以符合伦理和法律的方式使用AI相关的技能差距。


注: 泰国样本容量 = 51

菲律宾






人口: 1.158亿 | GDP: 4,370亿美元

卓越AI治理可望为组织带来的三大**益处**

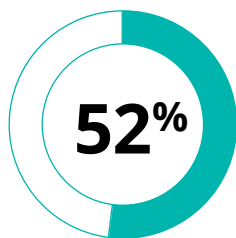
-  对AI解决方案成效或成果的信任度提高 (67%)
-  信任度提高带动AI解决方案使用增加 (52%)
-  在客户中的声誉提高 (48%)

组织在AI使用中最担忧的三大**风险**

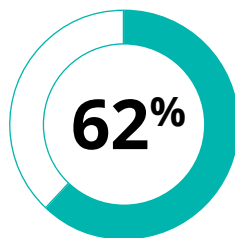
-  监控: 监控泛滥导致隐私侵犯 (90%)
-  安全漏洞: 网络入侵/网络安全风险 (85%)
-  隐私: AI系统中敏感、保密或个人数据泄露风险 (83%)

组织在AI使用或实施中的三大**障碍**

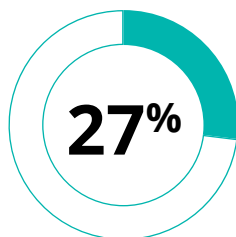
-  人才和/或技术技能短缺 (38%)
-  技术实施挑战 (37%)
-  AI实施战略和愿景缺位 (33%)



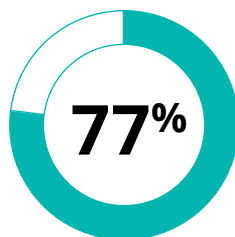
菲律宾组织已建立便于员工反映问题的机制。



菲律宾组织的员工具备所需技能，能够以符合伦理和法律的方式使用AI。

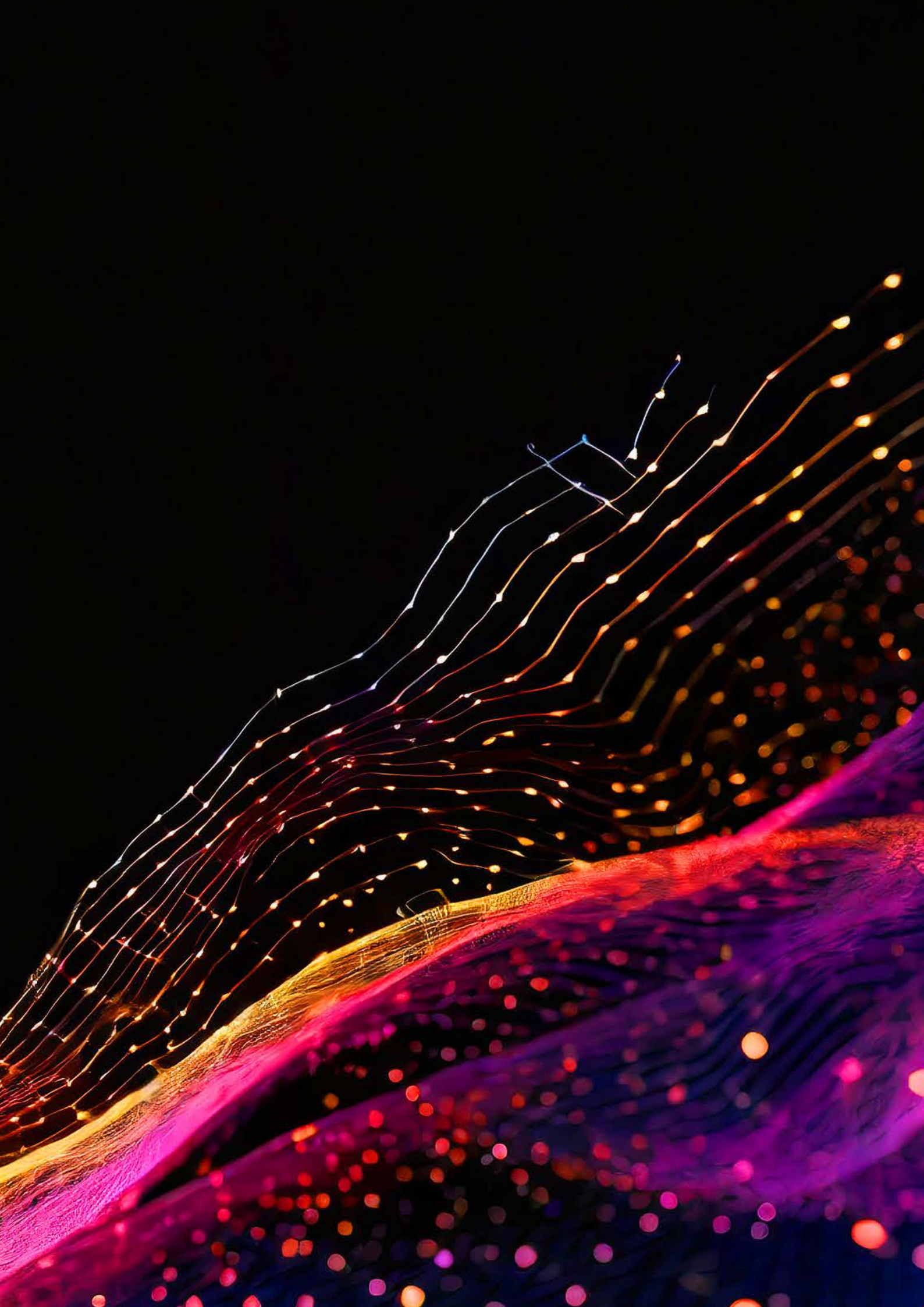


菲律宾组织表示上一财年事件报告增加。



菲律宾组织正在提高现有员工的技能，以缩小与以符合伦理和法律的方式使用AI相关的技能差距。

注: 菲律宾样本容量 = 52



尾注

- 1 Deloitte (2024) “Generative AI in Asia Pacific”, <https://www.deloitte.com/nz/en/services/consulting/perspectives/generative-ai-in-asia-pacific-may-2024.html>
- 2 Ibid
- 3 Deloitte Access Economics (2024) “ACS Australia’s Digital Pulse 2024: Decoding the Digital Decade”, <https://www.deloitte.com/au/en/services/economics/perspectives/acs-australias-digital-pulse-decoding-the-digital-decade.html>
- 4 IBM (2024), “Cost of a data breach Report”, <https://www.ibm.com/reports/data-breach>
- 5 Capgemini Research Institute (2020), “AI and the ethical conundrum” Report, <https://www.capgemini.com/news/press-releases/ai-and-the-ethical-conundrum-report/>
- 6 Deloitte Centre for Regulatory Strategy (2024), “Generative AI: Application and Regulation in Asia Pacific”, <https://www.deloitte.com/au/en/Industries/financial-services/analysis/generative-ai-application-regulation-asia-pacific.html>
- 7 Deloitte (2024) State of AI in Enterprise, <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-state-of-gen-ai-q3.pdf>
- 8 Deloitte (2024) State of AI in Enterprise, <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-state-of-gen-ai-q3.pdf>
- 9 Haresamdram et.al, IEEE Access (2023), “Three levels of AI transparency”, <https://ieeexplore.ieee.org/document/10042109>
- 10 建模中覆盖的十大业务领域：生产和/或运营、销售和市场营销、财务、人力资源、客户服务、研发、信息技术、行政管理、法律和合规以及物流领域。
- 11 Deloitte (2023), Data privacy and security worries are on the rise, while trust is down. Consumer data privacy and security | Deloitte Insights
- 12 Deloitte Access Economics (2023), “Generation AI: ready or not, here we come!”, <https://www.deloitte.com/content/dam/assets-zone1/au/en/docs/services/economics/deloitte-au-generation-ai-2023-160524.pdf>
- 13 Schrage, M. et. AI, MIT Sloan Management Review (2023), “AI is helping companies redefine, not just improve, performance”; <https://sloanreview.mit.edu/article/ai-is-helping-companies-redefine-not-just-improve-performance/>
- 14 三层防御是指风险管理机制，其中第一层防御是企业用户或直接管理者，第二层防御是风险管理与合规团队，第三层防御是独立鉴证。

联系人 与 供稿人

如需了解更多信息或进一步探讨本文内容，敬请联系：

主要联系人



Chris Lewin

人工智能主管合伙人
亚太地区

chrislewin@deloitte.com



Elea Wurth博士

可信AI服务主管合伙人
亚太地区及澳大利亚

ewurth@deloitte.com.au



John O'Mahony

德勤经济研究所合伙人
澳大利亚

joomahony@deloitte.com.au



Stuart Scotis

前沿技术转型合伙人
德勤全球

sscotis@deloitte.com.au



朱灏

可信AI服务合伙人
中国大陆

silzhu@deloittecn.com.cn



范为

德勤人工智能研究院主管合伙人
中国大陆

rfan@deloittecn.com.cn



Toyohiro Sometani

可信AI服务合伙人
日本

toyohiro.sometani@tohmatu.co.jp



Jessica Kim

可信AI服务合伙人
韩国

jessicakim@deloitte.com



Amy Dove

可信AI服务合伙人
新西兰

amydove@deloitte.co.nz



Jayant Saran

可信AI服务合伙人
南亚

jsaran@deloitte.com



Dishell Gokaldas

可信AI服务合伙人
东南亚

dgokaldas@deloitte.com



Chris Chen

可信AI服务合伙人
中国台湾

chrisachen@deloitte.com.tw

供稿人



Nick Hull

总监

nhull@deloitte.com.au



Jennifer Wright

亚太卓越中心总监

jenniwright@deloitte.com



Sanjukta Mukherjee

亚太研究负责人

sanjumukherjee@deloitte.com



Tory Rowley James

高级经理

trowleyjames@deloitte.com.au



Maud Dumont

高级分析师

madumont@deloitte.com.au



Dominic Behrens

分析师

dobehrens@deloitte.com.au



Tara Naidu

分析师

tarnaidu@deloitte.com



Angela Watzdorf

分析师

awatzdorf@deloitte.com.au



关于德勤

德勤中国是一家立足本土、连接全球的综合性专业服务机构，由德勤中国的合伙人共同拥有，始终服务于中国改革开放和经济建设的前沿。我们的办公室遍布中国31个城市，现有超过2万名专业人才，向客户提供审计、税务、咨询等全球领先的一站式专业服务。

我们诚信为本，坚守质量，勇于创新，以卓越的专业能力、丰富的行业洞察和智慧的技术解决方案，助力各行各业的客户与合作伙伴把握机遇，应对挑战，实现世界一流的高质量发展目标。

德勤品牌始于1845年，其中文名称“德勤”于1978年起用，寓意“敬德修业，业精于勤”。德勤全球专业网络的成员机构遍布150多个国家或地区，以“因我不同，成就不凡”为宗旨，为资本市场增强公众信任，为客户转型升级赋能，为人才激活迎接未来的能力，为更繁荣的经济、更公平的社会和可持续的世界开拓前行。

Deloitte（“德勤”）泛指一家或多家德勤有限公司，以及其全球成员所网络和它们的关联机构（统称为“德勤组织”）。德勤有限公司（又称“德勤全球”）及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体，相互之间不因第三方而承担任何责任或约束对方。德勤有限公司及其每一家成员所和它们的关联机构仅对自身行为承担责任，而对相互的行为不承担任何法律责任。德勤有限公司并不向客户提供服务。请参阅www.deloitte.com/cn/about了解更多信息。

德勤亚太有限公司（一家担保责任有限公司，是境外设立有限责任公司的其中一种形式，成员以其所担保的金额为限对公司承担责任）是德勤有限公司的成员所。德勤亚太有限公司的每一家成员及其关联机构均为具有独立法律地位的法律实体，在亚太地区超过100个城市提供专业服务，包括奥克兰、曼谷、北京、班加罗尔、河内、香港、雅加达、吉隆坡、马尼拉、墨尔本、孟买、新德里、大阪、首尔、上海、新加坡、悉尼、台北和东京。

本通讯中所含内容乃一般性信息，任何德勤有限公司、其全球成员所网络或它们的关联机构并不因此构成提供任何专业建议或服务。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前，您应咨询合资格的专业顾问。

我们并未对本通讯所含信息的准确性或完整性作出任何（明示或暗示）陈述、保证或承诺。任何德勤有限公司、其成员所、关联机构、员工或代理方均不对任何方因使用本通讯而直接或间接导致的任何损失或损害承担责任。