

AI时代的企业生存法则： 安全合规，赢在未来

2025年3月6日



The better the question. The better the answer.
The better the world works.

EY 安永

Shape the future
with confidence
聚信心 塑未来

AI时代的企业生存法则：安全合规，赢在未来

2025年3月6日

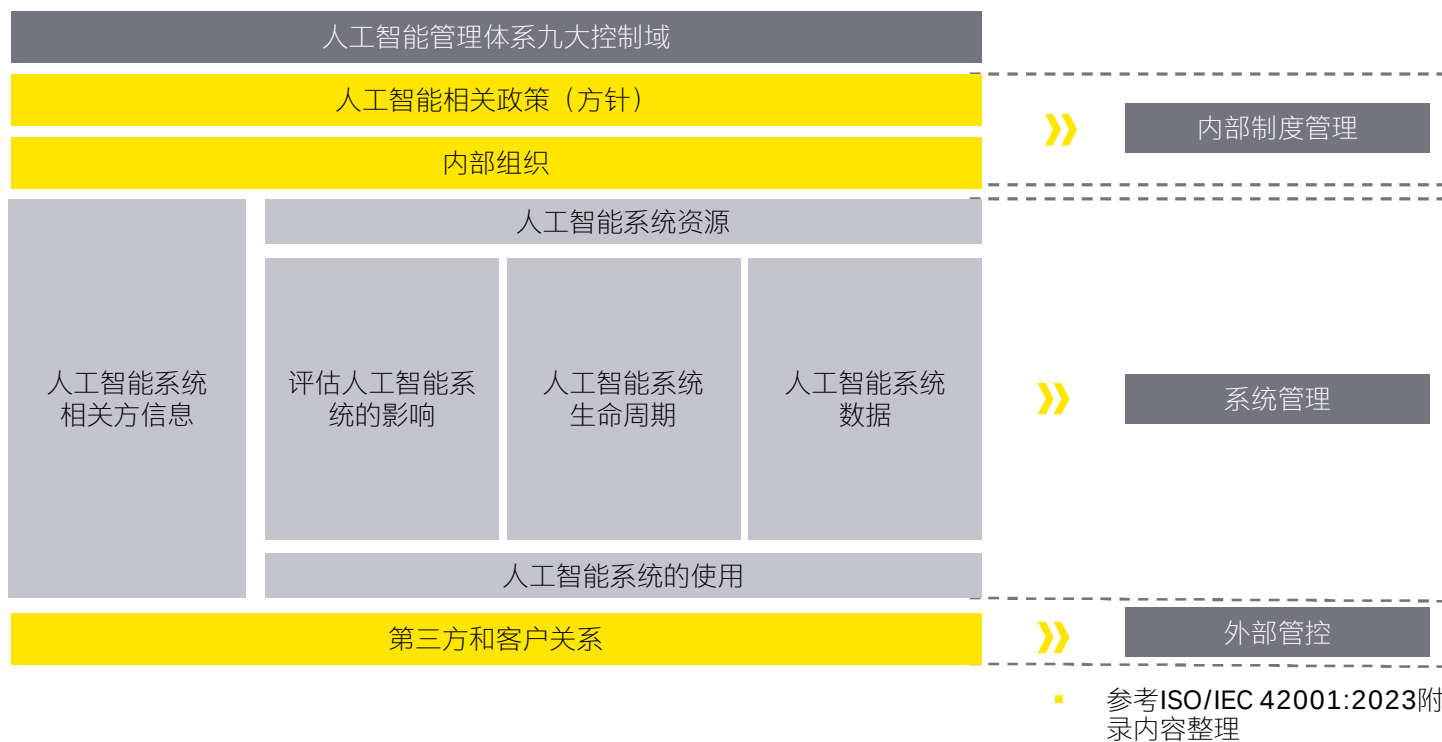


在数字化转型进程中，人工智能（AI）已成为推动各行业创新发展的核心驱动力。从金融领域的智能风控，到医疗行业的辅助诊断；从零售行业的个性化推荐，再到制造业的智能生产调度，AI技术正以前所未有的速度深度融入企业的核心业务。然而，繁荣背后暗藏危机，数据泄露、算法歧视、模型攻击等安全与合规问题不断涌现，严重威胁企业的稳健发展。

因此，构建全生命周期的AI安全治理体系，已成为企业在AI时代生存与发展的必由之路。

AI安全合规管理体系建设：筑牢安全根基

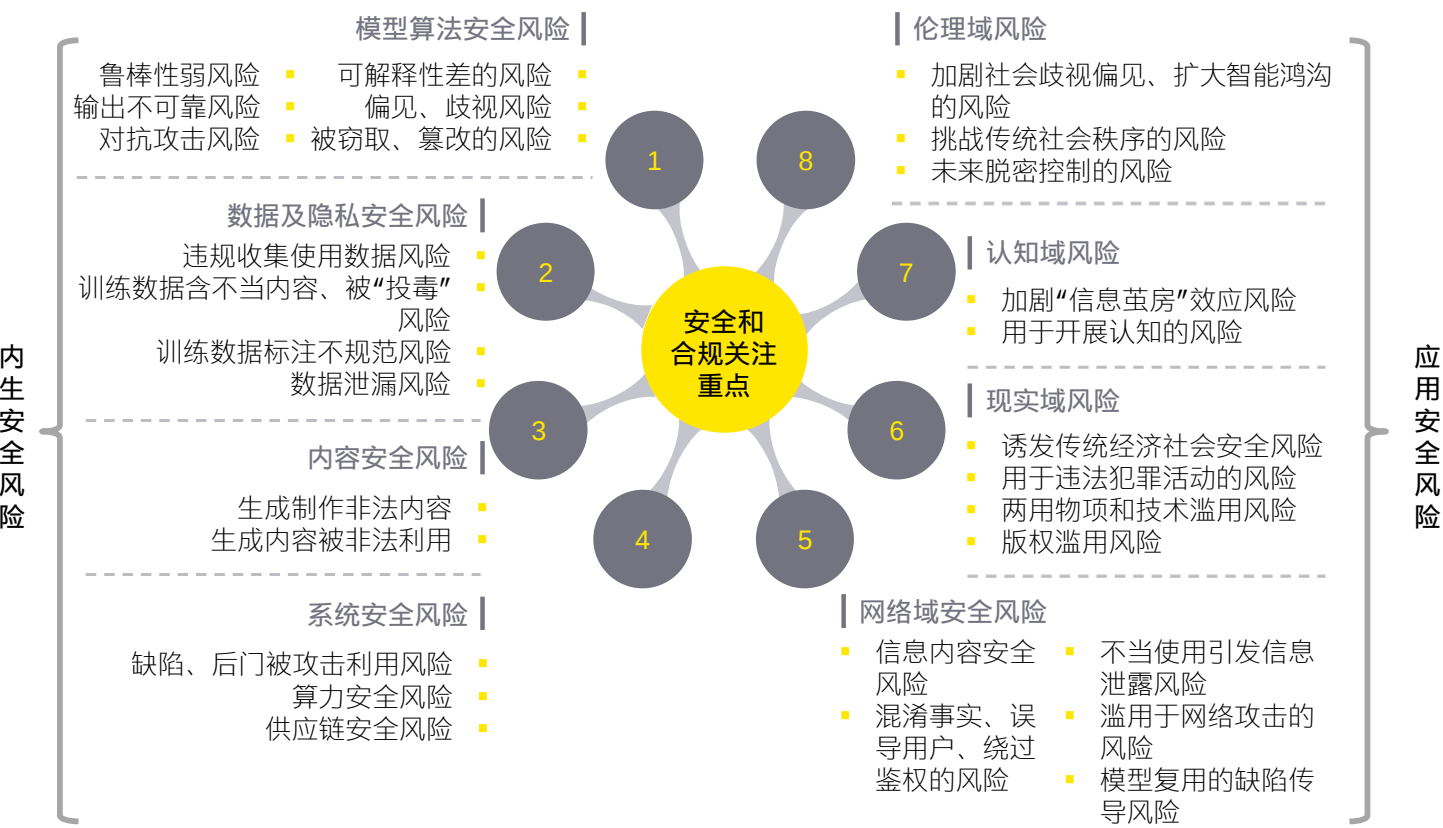
随着人工智能技术的快速发展，AI安全合规管理体系建设已成为企业稳健发展的关键。ISO/IEC 42001:2023作为全球首个AI管理体系国际标准，为企业提供了权威框架，确保AI系统从开发、实施到维护的每一个环节都安全可靠、符合规范。



企业应依据ISO/IEC 42001:2023等相关标准，明确AI战略与目标，全面识别AI相关风险。企业可通过构建涵盖数据、算法、模型等关键环节的管理机制，强化过程监控，确保AI系统的透明性和可解释性；同时，持续开展人员培训，提升全员安全合规意识，形成良好的AI治理文化。通过以上举措，企业能够打造出坚如磐石的AI安全合规管理体系，有效提升AI应用价值，在激烈的市场竞争中抢占先机，为可持续发展奠定坚实基础。

AI安全评估：识别潜在风险

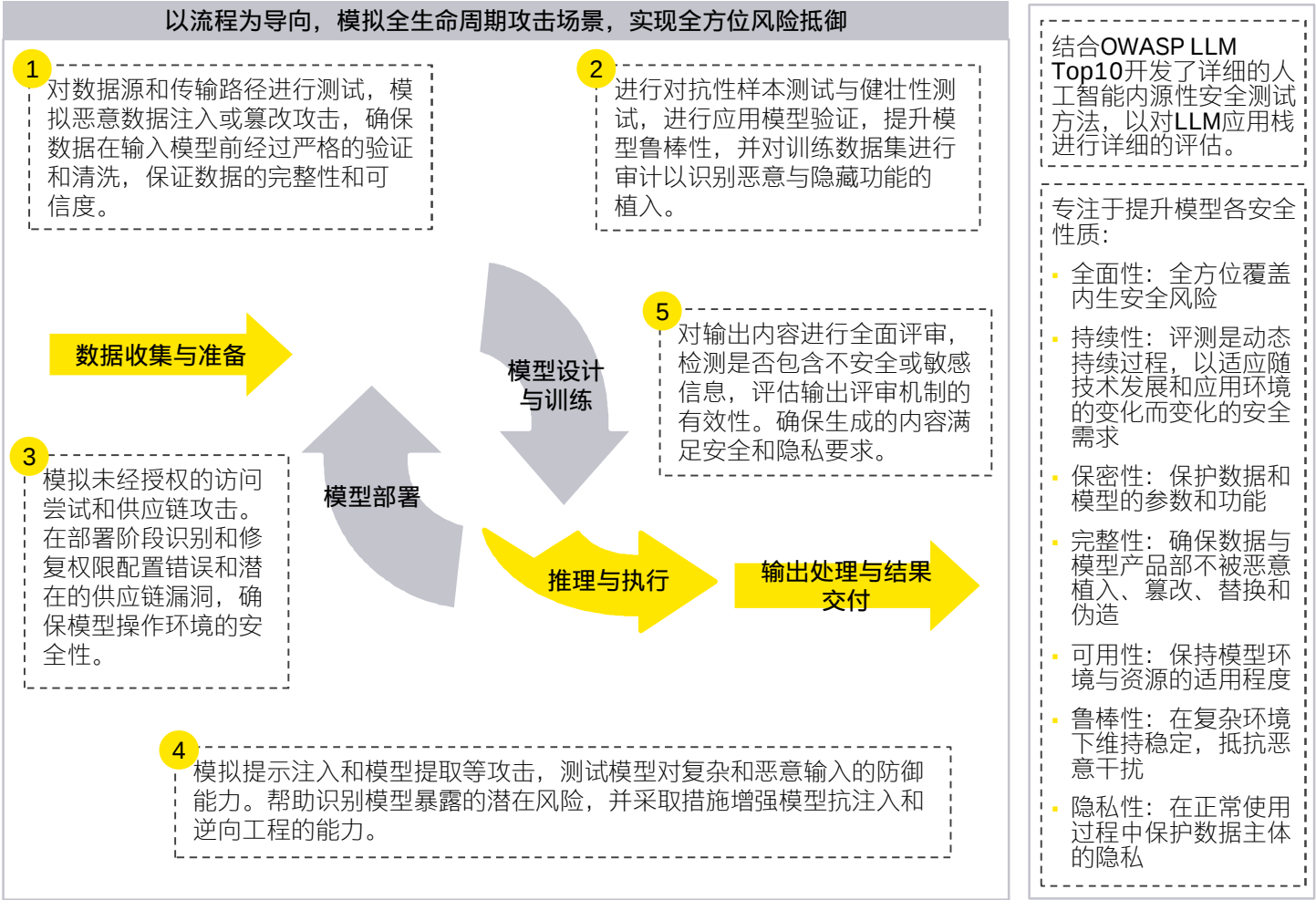
人工智能技术在带来巨大机遇的同时，也伴随着复杂多样的风险，主要可分为内生安全风险和应用安全风险两大类。内生安全风险源于AI系统自身的架构和运行机制，如模型算法安全风险、数据及隐私安全风险、内容安全风险和系统安全风险等；应用安全风险则涉及伦理域风险、认知域风险、现实域风险、网络域安全风险等外部威胁。



为有效应对这些风险，企业可参考相关法律法规要求，结合自身业务特点，建立全面且针对性强的安全合规基线。该基线应涵盖数据安全、算法透明性、模型鲁棒性等关键领域，为AI系统的开发和应用提供明确的规范。企业需定期依据此基线开展深入的安全合规评估，识别潜在风险，评估现有控制措施的有效性，并根据评估结果动态优化风险管理策略，及时查漏补缺，形成一个闭环的风险管理体系，将风险隐患扼杀在萌芽状态。

AI模型技术测评：强化防御能力

AI模型的安全性是企业AI安全的核心。企业要以流程为导向，模拟从数据输入到模型输出的全生命周期攻击场景，全面覆盖数据投毒、对抗样本攻击、模型窃取等多种威胁，确保在各个环节实现全方位的风险抵御。



同时，企业还可以结合OWASP LLM Top10等行业框架，开发一套适合自身的人工智能技术测试方法，从提示词注入、训练数据泄露、模型滥用等多个风险维度进行深入测评，识别潜在漏洞并制定针对性防护措施。通过这一系统化的测评流程，企业能够显著提升AI模型的安全性和鲁棒性，为AI技术的可靠应用筑牢根基，在安全的前提下实现创新发展。

AI算法和模型备案：确保合规运营

当前，中国对AI领域的监管日益严格，算法和模型备案已逐渐成为企业合规运营的硬性要求。算法备案要求企业对图像、视频、音频等合成技术进行详细登记，确保技术透明性和可追溯性，防止虚假信息传播和技术滥用。模型备案则聚焦于文本、图像生成等技术的监管，确保其符合伦理规范和法律法规，避免生成有害或误导性内容。

	★ 深度合成服务算法备案 (算法备案)	生成式人工智能服务备案 (模型备案)
覆盖范围	 所有商业化AIGC企业，技术支持者（提供API或SDK接口）、服务提供者（网页、APP、插件、小程序）	所有商业化AIGC企业，从事或提供生成式人工智能服务、技术的组织
审核部门	 国家网信办	省级网信办、国家网信办
审核方式	 线上提交资料，有概率被抽查，尤其重点、特殊行业（如医疗、生产制造、民生大数据产业等），一次性审核	线上填报、实际测试、线下审核
时间周期	 2-6个月，平均3个月左右。由于目前申请备案的企业数量不断增加，备案所需时间可能有所增加	3个月左右，具体需根据不同省级网信办情况而定
备案阶段	 上线的10个工作日内	上线前，已完成内测，有可对外提供的产品或Demo
★ 强制性备案 非强制性要求，相关部门正在准备实施细则 参考《互联网信息服务深度合成管理规定》和互联网信息服务算法备案系统 (https://beian.cac.gov.cn) 的相关信息整理		

企业应积极主动地参与备案流程，将其视为提升自身管理水平和竞争力的契机，并借此全面梳理算法逻辑、数据来源和应用场景，识别潜在风险并制定应对措施。通过算法和模型备案，企业不仅能够满足监管要求，避免因违规而遭受法律制裁和经济损失，还能提升自身技术透明度，赢得公众的信任。这不仅有助于营造安全可靠的AI生态环境，推动行业健康发展，也为企业自身合规发展提供了清晰的指引，确保AI技术在创新与安全之间找到平衡，实现可持续发展。

AI赋能安全合规管理：创新治理手段

在AI技术飞速发展的浪潮中，企业不仅要警惕其带来的风险，更要抓住这一契机，利用AI提升自身的安全合规能力。例如，在网络安全与数据保护方面，企业可利用AI进行实时的网络威胁监测，通过机器学习算法分析海量网络数据，精准识别异常流量和潜在攻击行为；AI技术也能够实现智能的数据加密与脱敏，自动识别敏感数据并进行处理，强化数据保护能力。此外，AI不仅能够帮助企业应对复杂多变的安全威胁，还能通过智能化手段优化合规管理流程，提升管理效率。

结语

AI技术的安全与合规管理是一场持续的挑战，安永可以帮助企业深入洞察AI安全与合规管理的复杂形势，同时，协助企业开展应用AI强化安全合规管理与运营机制，为企业制定切实可行的应对策略。企业需要树立长期作战的意识，摒弃传统的“事后补救”思维模式，构建“预防-检测-响应”一体化的治理体系。“积极应对挑战，迅速抓住机遇”，只有这样，企业才能在技术创新的道路上筑牢安全防线，在激烈的市场竞争中立于不败之地，真正享受到AI技术带来的红利。

如需了解更多信息，欢迎联系我们：



高轶峰

主管合伙人
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
kelvin.gao@cn.ey.com



包红霞

合伙人（华北）
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
alice.hx.bao@cn.ey.com



左超

总监
网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
chao.zuo@cn.ey.com



张爽

经理
网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
serena.s.zhang@cn.ey.com

安永 | 建设更美好的商业世界

安永致力于建设更美好的商业世界，为客户、员工、社会各界及地球创造新价值，同时建立资本市场的信任。

在数据、人工智能及先进科技的赋能下，安永团队帮助客户聚信心以塑未来，并为当下和未来最迫切的问题提供解决方案。

安永团队提供全方位的专业服务，涵盖审计、咨询、税务、战略与交易等领域。凭借我们对行业的深入洞察、全球联通的多学科网络以及多元的业务生态合作伙伴，安永团队能够在150多个国家和地区提供服务。

All in，聚信心，塑未来。

安永是指Ernst & Young Global Limited的全球组织，加盟该全球组织的各成员机构均为独立的法律实体，各成员机构可单独简称为“安永”。Ernst & Young Global Limited是注册于英国的一家保证（责任）有限公司，不对外提供任何服务，不拥有其成员机构的任何股权或控制权，亦不担任任何成员机构的总部。请登录ey.com/privacy，了解安永如何收集及使用个人信息，以及在个人信息法规保护下个人所拥有权利的描述。安永成员机构不从事当地法律禁止的法律业务。如欲进一步了解安永，请浏览ey.com。

© 2025 安永，中国。
版权所有。

APAC no. 03022269
ED None

本材料是为提供一般信息的用途编制，并非旨在成为可依赖的会计、税务、法律或其他专业意见。请向您的顾问获取具体意见。

ey.com/china

关注安永微信公众号
扫描二维码，获取最新资讯。

