

《智能体规范应用与创新发展实施意见》

商业影响调研报告

管理层简报 · 专业服务行业影响研判

报告日期：2026 年 5 月 10 日

北京锐意智能科技有限公司

密级：公开报告

一、管理层摘要

本报告的核心判断是：该文件不是单纯的产业鼓励政策，而是中国针对“具备执行能力的智能系统”建立治理底座的起点。其影响将首先体现在高价值流程的准入、授权、日志、评测和责任边界上。

1.1 五个核心判断

- 1. 治理对象升级：监管重点从“AI 生成什么内容”，进一步扩展到“智能体被授权做什么动作、调用什么工具、留下什么证据”。
- 2. 合规控制前置：智能体进入真实业务流程前，必须先补齐身份、权限、授权、日志、回滚、供应链和第三方评测能力。
- 3. 专业服务两段式变化：短期先提升检索、整理、起草、项目管理效率；中长期进入受控流程执行和“人机协同签发”。
- 4. 金融与强监管行业先行：金融风控、交易监测、反洗钱、账户安全、合规审计等场景被直接点名，预计将率先形成可复制案例。
- 5. 新增服务市场形成：AI 治理咨询、控制设计、系统审计、合规评测、成熟度评估、运行日志取证和证据包生成将成为专业服务机构的新业务。

一句话建议 现在不宜只追求“更强智能体”，而应先建立“台账—分级—授权—留痕—回滚—评测”的控制底座，再逐步放开流程自动化。

1.2 对专业服务行业的直接含义

维度	判断	对专业服务机构的含义
市场机会	第三方评测、系统审计、合规咨询、控制设计需求上升	传统审计、法务、咨询可扩展 AI 治理与智能体控制服务
交付模式	从报告交付转向“工具 + 流程 + 持续运营”	服务机构需要沉淀行业模板、证据包、检查清单和持续监控机制
风险边界	高风险动作必须保留人类授权和最终决策	不能把 AI 输出直接等同于专业意见或法定签字责任
产品机会	可审计、可追溯、可管控的专业服务项目管理系统价值提升	“语言即操作”必须与权限、审批、日志和责任链绑定

二、政策原文研读：文件真正强调什么

国家网信办、国家发展改革委、工业和信息化部于 2026 年 5 月 8 日联合发布《智能体规范应用与创新发展实施意见》。文件将智能体定义为具备自主感知、记忆、决策、交互与执行能力的智能系统，并将其定位为人工智能产品及服务的重要形态。

从结构看，文件不是单点监管规则，而是覆盖技术底座、标准协议、安全治理、典型场景、产业生态和保障机制的系统性实施意见。公开文本包含 6 章、38 项措施，并提出 19 个典型应用场景。

政策模块	核心要求	商业含义
发展基础	完善技术底座，建设标准协议，推动 AI P、注册平台、数字身份、能力声明等基础设施	智能体将从单个应用进入“可注册、可互联、可认证、可分发”的平台化阶段
产品准则	明确三类决策边界，强调用户知情权、授权范围和最终决策权	涉及付款、审批、提交、删除、修改等动作时，不能只靠模型能力，必须有授权机制
安全底线	强化内生安全、供应链安全、应用衍生风险治理	企业采购智能体时，供应商、插件、API、外部知识库都将进入审查范围
治理体系	分类分级、第三方评测、信息报告、行业自律、信用评价、问题产品召回	高风险场景的准入门槛提高，低风险场景仍保留创新空间
应用牵引	推动金融、司法、政务、招投标、办公、工业、医疗、教育等典型场景	B2B/B2G 场景会先于纯 C 端场景形成规模化落地

资料来源：国家网信办公开原文、答记者问与专家解读；锐意知能整理。

2.1 已明确事项与待明确事项

已明确	待后续细化
智能体的定义与政策定位	敏感领域和重点行业的正式目录
安全可控、规范有序、创新驱动、应用牵引的基本原则	分类分级的具体等级、指标和判定口径
三类决策权限边界及用户最终决策权	何种情形触发备案、检测、召回和信用惩戒
第三方功能、性能、质量、合规评测方向	第三方评测报告格式、认证互认规则和发证主体
金融风控、司法服务、政务协同等重点场景	智能体注册平台、AIP 协议和软件商店治理的实施细则

重要判断 企业不应等待全部细则落地后再行动。监管细则虽未完全明确，但“可控、可审计、可追溯、可停机、可解释”的底座方向已经明确。

三、合规框架：企业要管理的不是“回答”，而是“行动”

智能体与普通聊天机器人的关键差异在于“行动能力”。当系统从回答问题转向调用工具、修改数据、提交材料、触发审批、发起支付或影响客户决策时，企业面对的核心风险就从内容风险变成行为风险、权限风险和责任风险。

3.1 四层控制模型

控制层	关键问题	建议控制点
-----	------	-------

权限控制	谁可以让智能体做什么？动作是否越权？	角色权限、授权范围、二次确认、可撤销授权、最终人工签发
行为控制	智能体是否按规则行动？是否可被停止？	行为围栏、沙盒、阈值限制、敏感动作阻断、人工接管、回滚机制
系统与供应链控制	外部模型、插件、API、知识库是否可信？	供应商尽调、组件清单、版本锁定、接口审计、密钥管理、漏洞预警
治理与证据控制	未来能否证明系统合规运行？	日志留存、链路追踪、测试报告、成熟度评估、合规证据包、第三方评测

3.2 企业应重点关注的“动作阈值”

智能体的合规强度不是由“模型是否先进”决定，而是由它能否影响真实业务后果决定。以下动作一旦开放，必须进入更高等级的审批和留痕管理：

- ▮ 资金动作：自动付款、自动下单、自动开票、自动记账、自动调整账务数据。
- ▮ 法律动作：自动出具法律意见、自动提交诉讼或监管材料、自动发送具有法律后果的通知。
- ▮ 审计动作：自动生成关键审计结论、自动判断控制有效性、自动替代复核签字。
- ▮ 客户动作：自动对外承诺、自动报价、自动变更合同或项目范围。
- ▮ 系统动作：自动删除、修改、导出敏感数据，或调用外部插件/API 传输数据。

四、媒体与行业评论：市场如何解读

公开舆论大体分为三类：官方与主流媒体强调“安全与发展并重、典型场景牵引”；市场化媒体关注组织重构、入口变化和 ROI；安全与金融行业评论则更关注权限、可审计、供应链和准入成本。

来源类型	代表性观点	商业含义
官方/新华社/人民日报	强调智能体从聊天工具进化为解决实际问题的助手，并提出 19 个典型场景	政策信号偏积极，鼓励在可控前提下进入真实业务流程
36氪等创业媒体	以快讯方式确认政策方向和四方面举措	对创业公司是“赛道合法化”信号，但也意味着合规门槛前置
21世纪经济报道	关注“智能体成为互联网下一阶段用户”、企业组织护城河重构	入口、流程和组织能力可能被智能体重重新分配
金融行业评论	银行 AI 投入进入算账阶段，重点从 Demo 转向 ROI、治理和业务嵌入	金融机构将优先要求可审计、可解释、可回滚的企业级智能体平台
安全/垂直行业评论	强调从能力竞争转向可信竞争、从内容风险转向行为风险	合规评测、系统审计和供应链安全将成为采购门槛
待观察媒体	公开检索中未见财新、晚点 LatePost 问题深度商业评论	暂不把其作为实质观点来源，后续可继续跟踪

注：本报告优先采用可公开验证的官方、主流媒体与垂直行业来源；对无法核验的自媒体观点未作为关键依据。

五、对专业服务行业与职能部门的影响

对财务、法律、审计、金融、咨询等行业和职能部门而言，该文件的影响不是“岗位立即被替代”，而是高频知识工作和流程管理将逐步智能化，同时责任、授权和证据要求显著提高。

领域/部门	短期最先落地	中长期变化	关键约束与机会
财务与共享服务	报销初审、对账、合同/发票字段抽取、结账材料整理、管理报表初稿	从辅助处理走向受控记账、付款建议、预算执行跟踪和异常预警	涉及资金、账务和主数据变更时必须保留授权、复核、日志和回滚
法律与合规	法规检索、合同初稿、条款比对、证据整理、法务问答分流	形成“AI 草拟 + 人类签发”的分层交付模式	法律判断和外部承诺仍需专业人员最终负责；保密与可追溯要求上升
审计与内控	AI 系统台账、权限矩阵、日志检查、控制测试、供应商审查	形成 AI 控制审计、系统合规鉴证、运行日志取证等新服务线	政策利好系统审计与合规审计，不等于改变法定财报审计边界
银行与金融机构	风控、交易监控、反洗钱、账户安全、客服分流、授信材料预审	企业级 AI 平台、模型集中治理、智能体场景准入成为标配	金融是文件直接点名行业，预计最先形成高标准评测和准入要求
咨询与实施服务	场景筛选、试点设计、供应商评估、制度流程搭建	从一次性咨询项目转向持续运营托管、评测和证据包服务	机会大，但同时需要具备业务流程、AI 技术和合规控制能力
企业合规/风控/IT	建立智能体台账、分级分类、采购审查和试点审批	形成 AI 治理办公室或智能体控制塔	从被动合规转向前置治理，成为智能体上线的关键把关方

5.1 对审计、法务、咨询机构的新机会

文件中提到的第三方评测、成熟度报告、信用评价、合规审计和问题产品召回，为专业服务机构提供了新的服务切入点。关键不是“替客户写提示词”，而是帮助客户把智能体纳入正式治理体系。

服务机会	客户痛点	可交付成果
AI 治理咨询	不知道哪些智能体在用、哪些场景高风险	智能体台账、场景分级、治理制度、职责矩阵
控制设计与内控整改	授权、日志、回滚和人工复核机制缺失	权限矩阵、审批流程、留痕方案、异常处置机制
第三方评测/预评估	未来采购、投标和备案可能需要评测材料	功能/性能/质量/合规检查表、预评估报告、整改清单
系统审计与日志取证	无法证明智能体是否合规执行	日志抽样、证据链复核、系统控制测试、审计底稿
持续运营托管	上线后缺少常态化监控和更新机制	月度风险报告、模型/插件变更审查、事件复盘

5.2 对专业服务项目管理类产品的启示

产品启示 “语言即操作”会更有价值，但必须从一开始就内置权限、审批、日志、项目责任链和客户数据边界。专业服务行业需要的不是泛化聊天助手，而是可被经理控制、可被复核、可被审计的流程执行系统。

- ▮ 定位上：避免只讲“智能体很强”，应强调“流程可控、证据完整、责任清晰”。
- ▮ 功能上：任务分派、进度跟踪、材料清单、客户沟通和复核意见是低风险高频入口。
- ▮ 控制上：任何自动创建、修改、分派、提醒、归档动作都应形成可追溯日志。
- ▮ 商业上：中小型事务所可能更愿意购买“可直接落地的行业模板 + 轻量治理底座”，而不是重型定制系统。

六、行动参考：30/90/180 天路线图

企业和服务机构可参考按“先治理、再试点、后规模化”的顺序推进。短期目标不是做出最复杂智能体，而是让现有智能体使用状态可见、可控、可复盘。

时间	行动参考	牵头对象	目标
未来 30 天	建立智能体台账，盘点内部已使用、试用、采购中的模型、插件、API 和工具	IT / 合规 / 业务部门	从“看不见”变成“可治理”
未来 30 天	按场景分级：低风险辅助、受控自动化、高风险待审	合规 / 法务 / 风控	优先识别并冻结高风险动作
未来 30 天	明确授权矩阵：授权人、范围、期限、二次确认、撤销机制	业务负责人 / 内控	满足权限边界和最终决策权要求
未来 60-90 天	为重点智能体补齐日志、回滚、人工接管和停机机制	IT / 内审 / 信息安全	形成可审计、可追溯、可处置能力
未来 60-90 天	将供应商尽调扩展到模型、插件、MCP/API、外部知识库和数据流向	采购 / 法务 / 信息安全	响应供应链安全要求
未来 90-180 天	选择 1-3 个低风险高价值场景做正式试点	业务部门 / 产品团队	形成可复制案例与 ROI 证据
未来 90-180 天	准备第三方评测材料和内部成熟度评估模板	产品 / 合规 / 外部顾问	为采购、投标、认证、备案预留空间
180 天以后	建立跨部门 AI 治理办公室或智能体治理委员会	管理层 / 合规 / IT	从项目制转为常态化治理机制

七、风险矩阵

以下风险排序基于政策文本、现有 AI 执法环境和专业服务行业流程特征。概率和影响为本报告分析口径，不代表官方评级。

风险	概率/影响	典型触发	首要控制措施
----	-------	------	--------

越权执行	高 / 高	自动付款、自动审批、自动发送外部承诺、自动删改关键数据	权限分层、二次确认、强制人工签发、可撤销授权
数据与隐私泄露	高 / 高	外部插件调用、共享上下文、日志暴露、记忆污染	最小权限、脱敏、隔离、密钥管理、供应商审查
供应链失控	中高 / 高	第三方 API 变更、插件异常、开源组件漏洞	组件清单、版本锁定、风险扫描、异常熔断
行为失控与运行事故	中高 / 高	错误规划、循环执行、错误工具调用	行为围栏、沙盒、阈值控制、停机开关、回滚机制
虚假信息与声誉风险	中 / 高	错误法律、财务、审计判断被对外使用，或营销/客服误导客户	专业复核、来源校验、人工签发、抽样检查、投诉处置
评测/备案准备不足	中 / 高	进入金融、司法、政务等高风险场景但缺少证据包	预评估、测试材料、成熟度评估、第三方评测准备

八、结论

这份文件的核心价值在于：它把智能体从“能不能做”的技术问题，转化为“能否被授权、被控制、被审计、被问责”的组织治理问题。对专业服务行业而言，这既是效率工具的扩散，也是新型合规与控制服务市场的形成。

最值得提前布局的不是单个智能体功能，而是行业知识、流程模板、权限体系、留痕审计和第三方评测能力。谁先把这些底座产品化，谁就更可能在财务、审计、法律、金融和咨询等高信任场景中获得长期优势。

附录：主要参考资料

[1] 国家网信办等三部门：《智能体规范应用与创新发展实施意见》官方原文

https://www.cac.gov.cn/2026-05/08/c_1779979789523320.htm

[2] 新华社：三部门部署智能体规范应用与创新发展

<https://www.news.cn/politics/20260508/13043a992f834853a7ce009ba7ecaabc/c.html>

[3] 新华社/新华网：《智能体规范应用与创新发展实施意见》印发

<https://www.news.cn/tech/20260509/0b2262715c7a41babde83870ccd08128/c.html>

[4] 人民日报：智能体开启应用新图景

https://paper.people.com.cn/rmrb/pc/content/202605/09/content_30155713.html

[5] 国家网信办专家解读：统筹高质量发展与高水平安全

https://www.cac.gov.cn/2026-05/08/c_1779979790736565.htm

[6] 国家网信办专家解读：以规范应用护航智能体发展行稳致远

https://www.cac.gov.cn/2026-05/08/c_1779979790817217.htm

[7] 国家网信办专家解读：把握智能体发展机遇，加快构建智能体治理体系

https://www.cac.gov.cn/2026-05/08/c_1779983775418216.htm

[8] 36氪：三部门印发《智能体规范应用与创新发展实施意见》

<https://36kr.com/newsflashes/3800477731838985>

[9] 21世纪经济报道：面对 AI 智能体，企业组织如何重构“护城河”

<https://www.21jingji.com/article/20260508/herald/f5ac0294fc229d7dbaa913ff426270db.html>

[10] 中国电子银行网：1900 亿砸向 AI 后，银行开始算账了

<https://www.cebnet.com.cn/20260508/103002499.html>

[11] 安全内参：智能体正式进入监管周期

<https://www.secrss.com/articles/901111>

[12] 国务院/相关部门：《关于深入实施“人工智能+”行动的意见》公开文本

https://www.cac.gov.cn/2025-08/27/c_1758018277755538.htm

[13] 国家金融监督管理总局：银行业保险业数字金融高质量发展实施方案

<https://www.nfra.gov.cn/cn/view/pages/ItemDetail.html?docId=1239739&itemId=917>

[14] 中国电子银行网：中国银联发布智能体支付开放协议框架

<https://www.cebnet.com.cn/20260408/103002065.html>

[15] 国家网信办：生成合成内容标识违法问题查处案例

https://www.cac.gov.cn/2026-04/28/c_1779119736411711.htm

说明：本报告基于截至 2026 年 5 月 10 日的公开资料整理