

目录

1. 执行摘要
2. 研究范围、方法与知识截止
3. 五大核心判断
4. 全球市场与需求图景
5. 技术演进
6. 跨行业落地：价值池与成熟路径
7. 投融资与产业格局
8. 组织、人才与能力建设
9. 治理、风险与监管窗口
10. 未来12-24个月情景分析
11. 企业行动议程（90天 / 12个月）
12. 附录
13. 参考文献
14. 关于浩瀚博策（出品方）

1. 执行摘要

2023年下半年，生成式 AI 议程从「全员试用」切换为「收口与平台化」。中国《生成式人工智能服务管理暂行办法》自 **2023年8月15日** 施行；开源可商用权重扩散降低私有化试验门槛；企业级助手与更长上下文能力进入采购清单；欧盟就 AI 法案于 **2023年12月** 达成政治协议。董事会的问题变为：哪些试点该关，哪些该并入统一平台，合规证据能否备齐。

本报告基于截至 **2023年12月31日** 的公开资料，观察到五组事实：

第一，成熟度从试点波峰向受控生产迁移。 广泛 PoC 仍多，但 1-2 场景受控生产与初步平台化份额抬升；转化率成为预算门槛。

第二，技术栈重心上移到企业 AI 平台层。 模型网关、RAG、评测回归、成本配额与技能目录成为共用组件；旗舰 API 与开源可商用权重构成供给层。

第三，场景热度收敛到可治理入口。 知识助手、客服辅助、代码辅助、营销与办公嵌入居前；多步骤代理保持低份额实验。

第四，成本治理成为 CFO 新课题。 仍有相当比例组织缺乏场景级核算；熔断、缓存与路由开始进入实践。没有标签的调用会在 2024 年成为财务争议焦点。

第五，中欧监管同步硬化。 中国暂行办法已可执行；欧盟政治协议明确风险分级与通用目的 AI 透明度取向，对欧业务须启动差距预评。

对经营层而言，未来 12-24 个月赢家不是立项最多者，而是把平台底座做成组织资产、并完成多个场景转化的企业。

如果说上半年关键词是「试用」，下半年则是「收编」。生成式工具边际试用成本极低，但边际治理成本随用户与场景数快速上升。未能建立平台层的组织，将同时面对账单失控、幻觉事故与合规检查。对亚洲尤其是中国企业，暂行办法意味着「可合规创新」成为发版约束。

【要点框 | 给 CEO / 董事长】

- 把 AI 从项目清单升格为经营系统：明确可量化场景与停损清单。
- 优先投资平台（网关/RAG/评测/成本），再扩模型种类。
- 负责任 AI 与业务上线并行。
- 用转化率、单位经济、复用次数做投资决策。
- 对照当期监管义务维护证据包。

读者	72 小时动作
CEO	批准组合雷达与关停清单
CFO	设定成本熔断与阶段门禁
CIO/CTO	平台缺口与生产监控自评
业务一把手	提名 P&L 场景与 Owner
法务/合规	义务差距初评
CHRO	素养课与翻译官配置

【本期研判焦点】

平台底座、暂行办法合规、发布门禁与证据包。

2. 研究范围、方法与知识截止

2.1 研究问题

- 截至知识截止日，全球 AI 市场、技术与资本处于何种位置？
- 哪些行业与职能已显现可规模化价值？
- 组织、人才与治理如何决定转化率？
- 未来 12-24 个月情景与企业议程如何配置？

2.2 方法

- **桌面研究：** 公开市场调研、行业公开统计、监管公开文本与主流技术节点二次综述（均不晚于本期知识截止）。
- **监管文本精读：** 中国生成式/深度合成/算法推荐相关规定，欧盟 AI 法案进程与公开说明，OECD 可信 AI 原则，以及数据安全与个人信息保护法律语境。
- **技术节点交叉验证：** 以官方博客、开源发布说明与权威二次综述确认发布时间。
- **咨询式综合：** 将外部事实转化为管理层可决策的判断、情景与行动项；非原始问卷调查。数值凡属管理推演或示意，均在图注与正文标明属性。

2.3 知识截止与表述约定

约定	说明
知识截止	2023年12月31日
发布设定	2023年12月（2023下半年报告）
禁止引用	此后旗舰全模态世代、推理模型产品化浪潮等
时态	「当前」「过去两年」「未来12-24个月」
数字口径	预测/情景/示意均标明属性

2.4 关键定义

采用指至少在一个职能部署；**规模化**指多场景可复用并嵌入标准流程并持续产生可审计业务结果；**企业 AI 平台**指网关、检索、评测、成本与权限的共用层；**受控生产**指有评测、监控、审核与回滚的正式上线；**单位经济性**指单次任务成本与业务收益对照；**证据包**指可提交监管或客户尽调的控制与版本材料目录。

3. 五大核心判断

【判断 1 | 转化率取代立项数】

预算审查应转向「是否进入受控生产」：无 Owner、无评测、无单位经济的试点应关停或降级。立项数上升而转化率不动，是组织能力停滞的信号，不是创新繁荣的证据。

【判断 2 | 平台层是新护城河】

模型世代会迭代，但网关、语料权限切片、评测集、成本标签与工作流编排可沉淀为组织资产。2024 年竞争焦点是平台复用次数，而不是又接一套新 API。

【判断 3 | 开源可商用改变私有化经济学】

可商用开源权重降低试验门槛，也把运维、漏洞补丁与许可证合规责任上移到企业。私有化不是「下载即完成」，而是运维体系承诺。

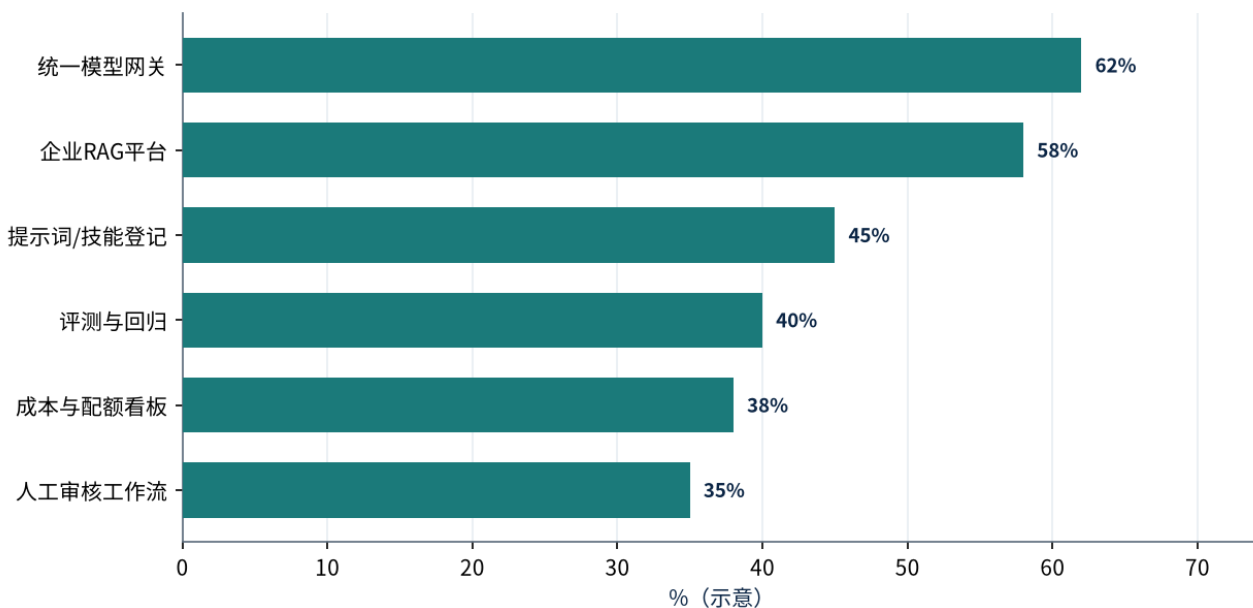
【判断 4 | 成本必须场景化】

没有熔断、路由与场景标签的生成式支出，将很快成为财务争议焦点。推理单价下降并不自动降低总账单——调用量与上下文长度常同步上升。

【判断 5 | 合规已从预整改变为可检查】

标识、安全评估与面向公众服务路径成为可审计项；欧盟政治协议预告跨境义务加码。发版与证据包必须同表。

图 3-1 企业平台能力建设优先级（2023年末）



来源：公开市场调研综合 / 本报告综合测算（≤2023-12）

洞察：平台化成为主叙事——比拼共用组件。

【图注 3-1】 企业平台能力建设优先级（2023年末）。来源：公开市场调研综合 / 本报告综合测算（≤2023年12月31日）。洞察：网关/RAG/评测/成本是共用层，模型只是可替换供给。

4. 全球市场与需求图景

4.1 成熟度与需求

公开市场调研与产业观察显示：买方更强调工作区管控、数据不出域与可验收指标。传统判别式 AI 生产系统与生成式 workflow 并存，而非被替代。影子 IT 正在被正式服务目录收编——成功组织提供合规替代路径，而不是一刀切禁用。

4.2 支出与成本纪律

宽口径 AI 支出仍以基础设施与服务为重要组成部分；生成式新增推理 API、向量检索、评测与人工审核等科目。建议单列运营成本并设月度熔断。推理单价下降并不自动降低总支出——调用量与上下文长度

同步上升。降本来自路由到小模型、缓存命中、禁止无业务标签调用，以及把高频问答沉淀为知识条目。

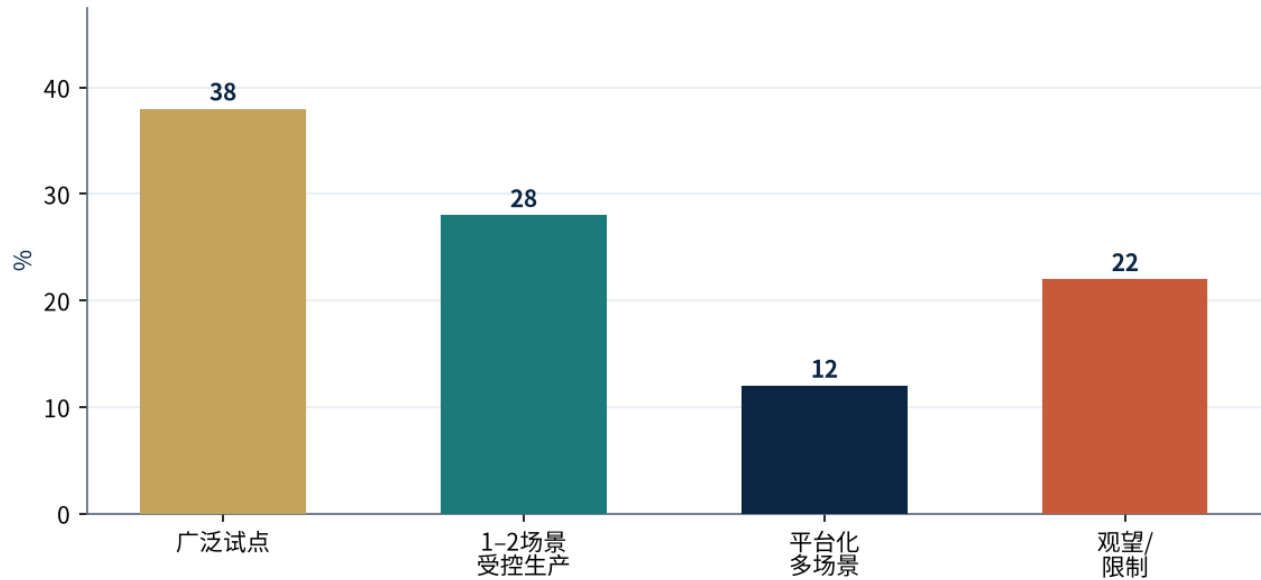
4.3 区域与买方行为

美中继续主导供给与应用密度；欧洲以立法政治协议强化规制输出。合同中私有化、不用于再训练、评测透明度与退出条款更常见。内部 CoE 从创新实验室转向平台产品团队。

4.4 人效测量陷阱

要求对照实验：基线任务时长、返工率、审核负荷、事故率。自愿使用者自我报告不足以写入经营计划。

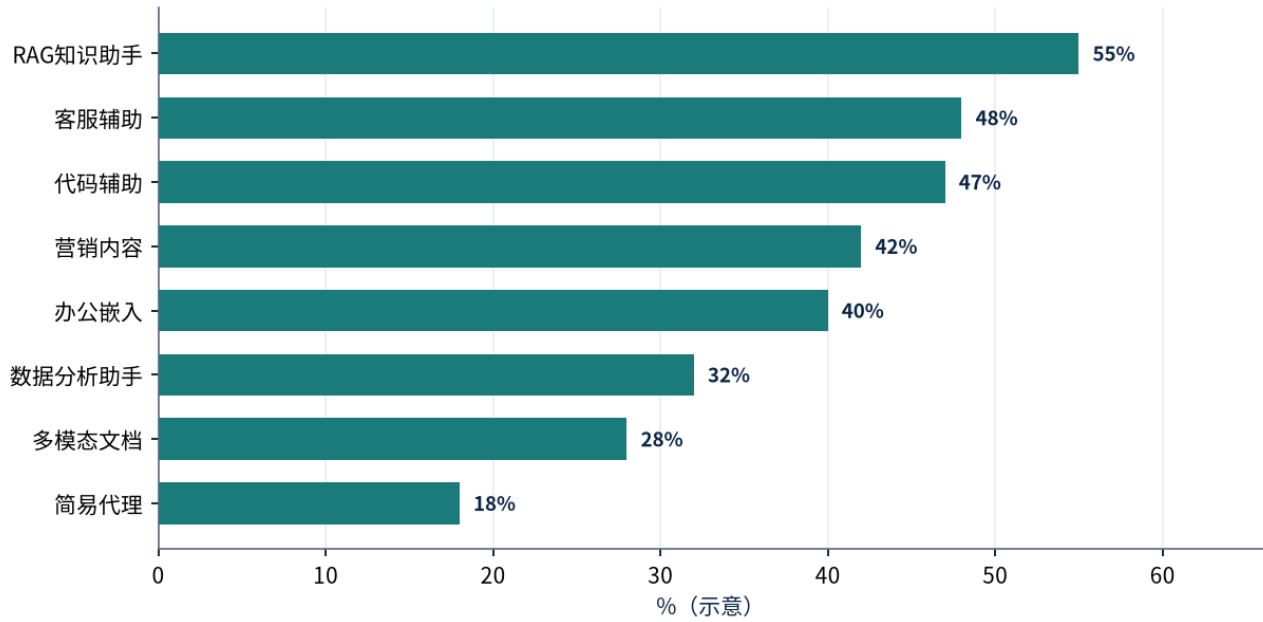
图 4-1 生成式成熟度分布（2023年末）



来源：公开市场调研综合 / 本报告综合测算（≤2023-12）

洞察：受控生产抬升，观望层仍厚。

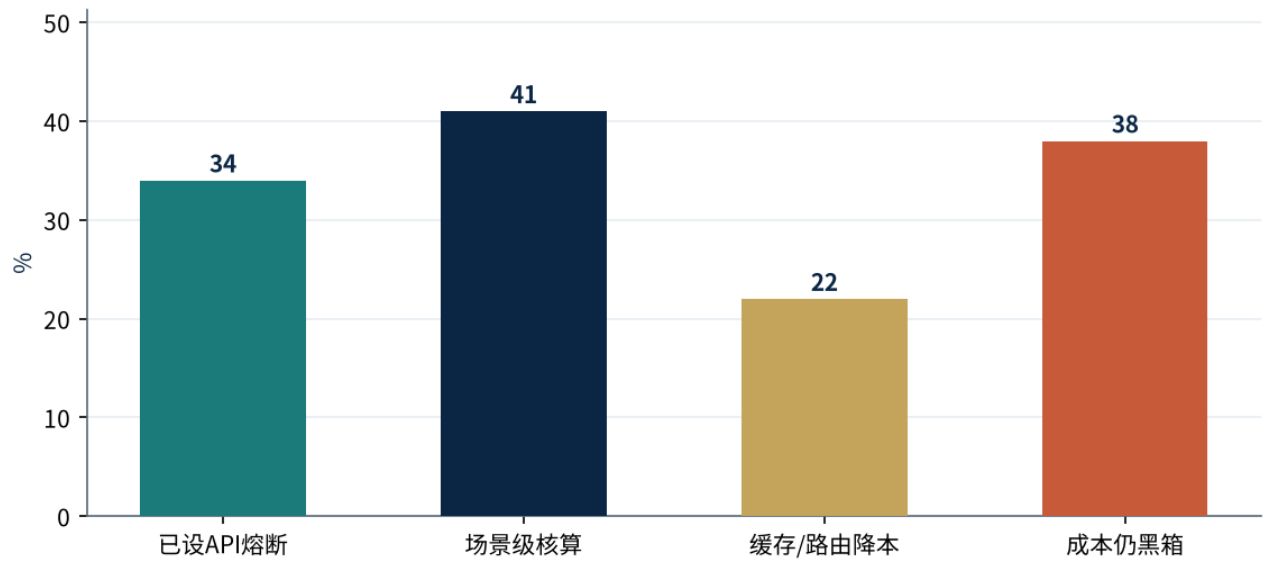
图 4-2 受控生产场景热度 (2023H2)



来源：公开市场调研综合 / 本报告综合测算 (≤2023-12)

洞察：RAG与客服/代码居前；代理仍实验。

图 4-3 成本治理成熟度 (2023年末)



来源：公开市场调研综合 / 本报告综合测算 (≤2023-12)

洞察：成本黑箱仍普遍。

公开市场调研与产业观察交叉显示：买方更强调工作区管控、数据不出域与可验收指标。传统判别式 AI 生产系统与生成式工作流并存，而非被简单替代。影子 IT 正在被正式服务目录收编——成功组织提供合规替代路径，而不是一刀切禁用后失去业务信任。

对 CFO 而言，2023 下半年最有用的管理动作不是「再砍一刀创新预算」，而是要求每笔生成式调用带场景标签，并设定月度熔断。对 CIO 而言，是把网关、评测与检索做成共享服务，阻止每个事业部重复采购。对业务一把手而言，是接受「关停」与「转化」同为成功结局——僵尸试点比没有试点更昂贵。

4.5 买方组织机制与采购纪律

领先买方将生成式/大模型采购并入既有技术采购与风险委员会，而不是单独「创新绿色通道」。共享服务（平台团队）负责网关、评测与成本；业务单元负责场景 KPI 与验收。失败项目的共性仍是：缺少 Owner、缺少停损、缺少与平台复用计划。

建议在采购文件中固定四类附件：**评测集共创计划、数据不用于再训练承诺、事故通知时限、退出与数据导出协助**。纯演示型供应商在尽调中应折价。

工作区与数据不出域成为标配诉求；内部 CoE 从创新实验室转向平台产品团队。

4.6 需求侧职能迁移与「影子采用」

公开市场调研长期显示：运营优化、服务、营销与产品增强是常见受益职能；生成式浪潮叠加后，知识工作与软件工程入口显著抬升。管理层须区分三类采用：

类型	特征	治理要点
正式生产	有 Owner、评测、监控	纳入价值审计
部门试点	有限流量、有停损	双周转化评审
影子采用	员工自用外部工具	可见化→收编或阻断

影子采用不是「文化先进」的证据，而是风险面扩大的信号。正确响应是提供合规替代路径（企业网关+许可工具），而不是假装看不见或一刀切禁用后失去业务信任。

【行动建议框 | 需求治理】

- 72 小时内完成影子工具盘点抽样（浏览器扩展、个人 API Key、外部账号）。
- 对高敏数据岗位强制企业通道；对低敏提效场景给白名单与培训。

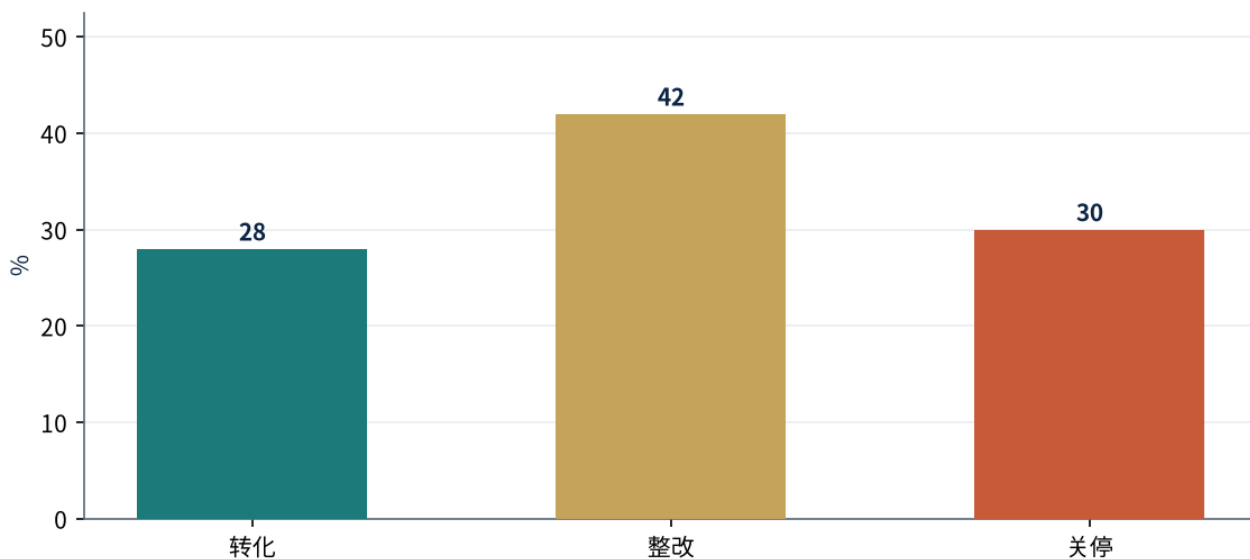
6.0 平台收口的组织政治

平台化失败很少因为技术不会做，而因为组织不愿意关停。事业部把试点当领地，平台团队缺少产品权，财务只看到账单看不到转化。破解方式是公开客观门槛：评测、Owner、单位经济；给予整改窗；逾期失去预算。把关停解释为保护可规模化场景，才能让收口从「政治斗争」变成「经营纪律」。

【行动建议框 | 收口】

- 季度公布转化/整改/关停三类名单。
- 平台复用次数计入平台 KPI。
- 合规证据包与发版火车同表。

收口结果分布（示意）



来源：本报告综合测算（≤2023-12-31）

洞察：用结构看组合，而不是只看总数。

【图注 4-4】本期关键结构示意。来源：本报告综合测算（≤2023-12-31）。洞察：结构重于总量——用分层指标做决策。

5. 技术演进

5.1 关键节点（展开）

开源可商用权重在 2023 下半年显著扩散，使中型企业也能开展私有化试验；**2023-08-15** 中国生成式暂行办法施行，把标识、评估与公众服务路径从原则写成可检查项；企业版助手与工作区扩展进入采购清单；开发者生态出现更长上下文与助手编排接口；**2023-12** 欧盟 AI 法案政治协议明确风险分级与通用目的模型透明度取向。

产业含义： 供给层选择变多，企业差异化转移到平台层与治理层。任何「只接模型、不建门禁」的试点，在 2024 年预算审查中将处于劣势。

5.2 工程重点（展开）

参考架构应至少覆盖：网关（鉴权、日志、脱敏、配额、路由）、RAG（混合检索、引用强制、权限切片）、评测（黄金集回归、幻觉与安全红队）、成本（场景标签、缓存、小模型分流）、人机签发队列。评测必须成为发布门禁：无回归通过不得升流量。

建议把「平台就绪度」做成内部评分：0-5 分评估网关、检索、评测、成本、权限五项；低于 3 分的组织不应并行超过 2 个生成式试点。

5.3 代理与多模态边界（展开）

工具调用演示增多，生产仍限白名单工具、最大步数、人工确认与完整日志。多模态文档（报销单、合同、图纸）试点升温，须设字段级准确率、脱敏与抽检比例。把代理演示直接写进经营计划，是本期最常见的治理失败前兆。

5.1 关键节点

开源可商用权重扩散；**2023-08-15** 中国生成式暂行办法施行；企业版助手与工作区扩展；开发者生态出现更长上下文与助手编排接口；**2023-12** 欧盟 AI 法案政治协议。

5.2 工程重点

网关（鉴权、日志、脱敏、配额、路由）、RAG（混合检索、引用、权限切片）、评测（黄金集回归、幻觉与安全红队）、成本（场景标签、缓存、小模型分流）、人机签发队列。评测应成为发布门禁：无回归通过不得升流量。

5.3 代理与多模态边界

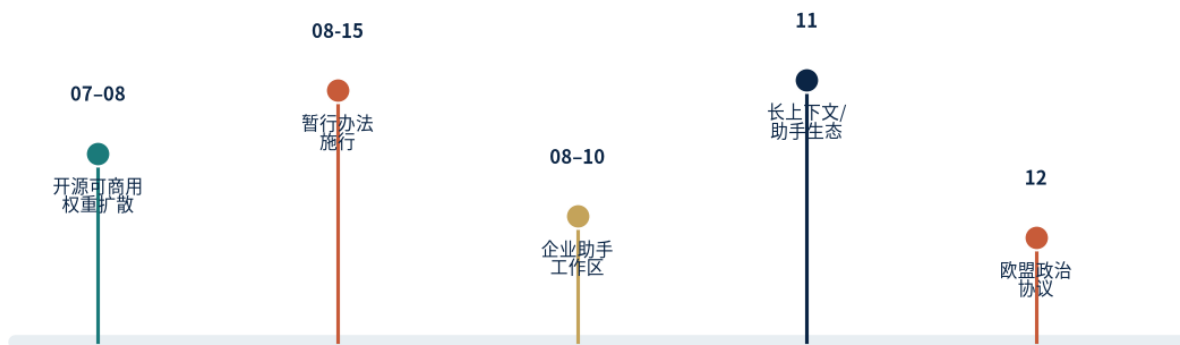
工具调用演示增多，生产仍限白名单工具、最大步数、人工确认与完整日志。多模态文档（报销单、合同、图纸）试点升温，须设字段级准确率、脱敏与抽检比例。

图 5-1 2023年末企业生成式技术栈



来源：公开市场调研综合 / 本报告综合测算（≤2023-12）
洞察：L3平台层成采购中心。

图 5-2 2023下半年关键节点



来源：监管公开文本与公开技术节点（≤2023-12-31）

洞察：合规与能力供给同期叠压。

5.4 数据契约、评测门禁与反馈飞轮

没有数据契约的检索增强会在权限与新鲜度上反复翻车。建议最低限度具备：文档源系统登记、更新SLA、敏感级标签、用户反馈回灌评测集。合成数据可补充长尾，但不能替代真实流量上的影子模式验证。

发布门禁应写死：无黄金集回归通过不得升流量；无成本标签不得调用生产网关；无人工签发策略不得触达客户。评测成为发布门禁；混合检索、权限切片与小模型分流进入参考架构。

5.5 供应韧性 with 多模型路由

企业应准备「采购 / 微调 / 编排 / 自托管」并存策略。路由维度至少包括：任务复杂度、数据敏感度、时延预算、单价上限。核心提示词、检索语料与身份特征默认不出域；开发与低敏试点可用托管API。

【行动建议框 | 工程优先级】

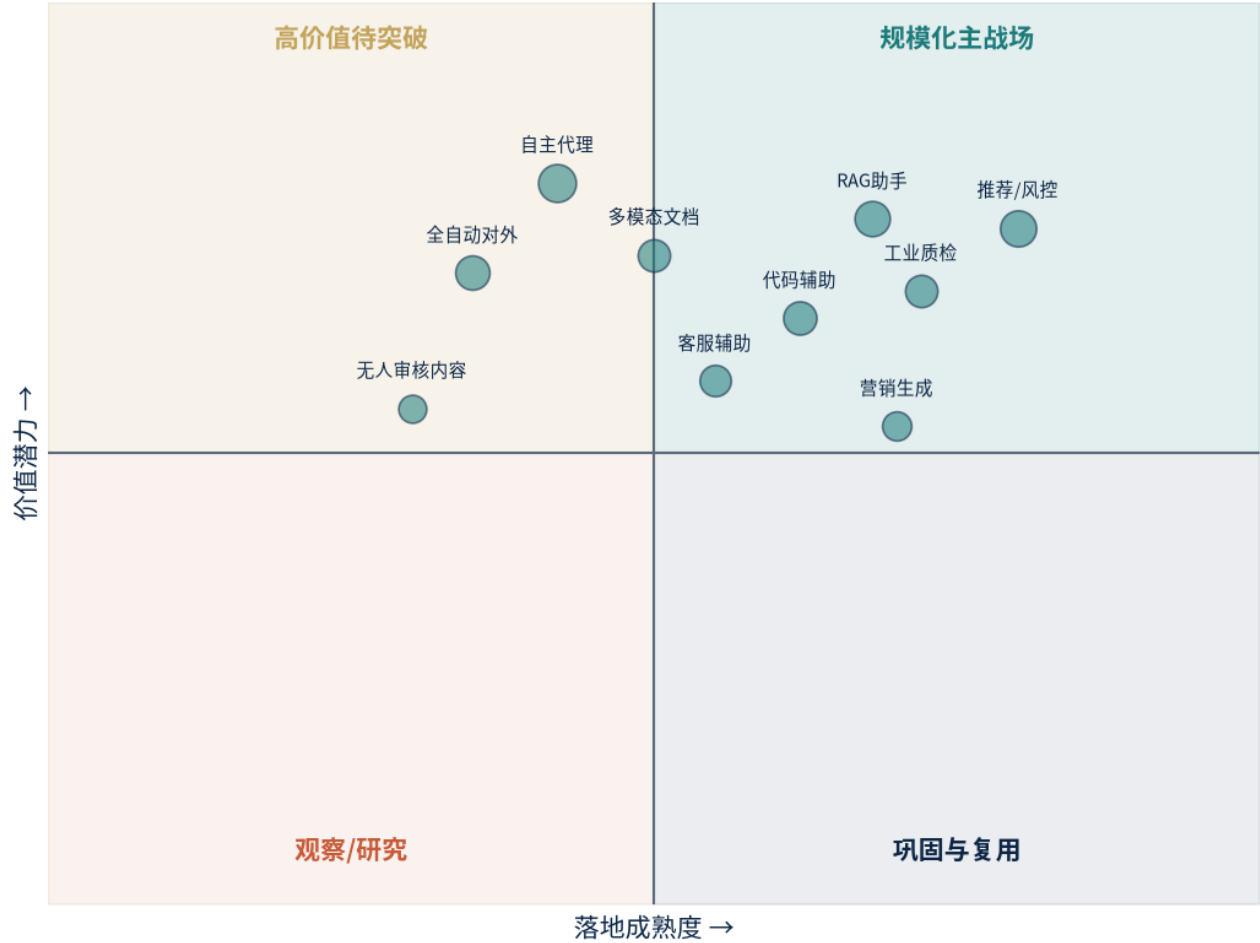
- 先止血：统一网关日志与月度成本看板。
- 再提质：黄金集 + 红队 + 引用强制。
- 后扩面：多场景复用同一平台组件。

6. 跨行业落地：价值池与成熟路径

6.1 总览

结合公开价值池思路与本期产业实践，落地成熟度仍呈「较成熟 / 加速转化 / 早期高风险」三档。生成式抬高了知识与内容类价值预期，但高后果自动决策仍须慢。

图 6-1 价值—成熟度矩阵（2023年末）

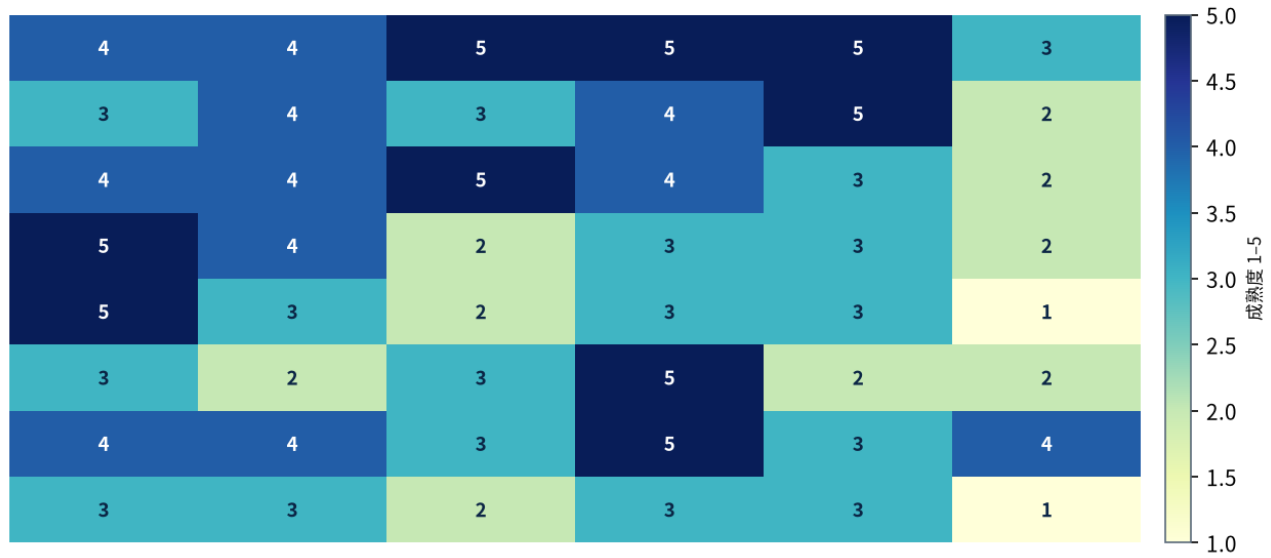


来源：本报告综合测算
洞察：RAG近规模化；代理偏左上。

洞察：对话/RAG抬升；代理仍早期。

来源：本报告综合测算

图 6-2 行业×能力热力（2023年末）



6.2 金融服务

反欺诈、反洗钱、信审辅助与客服仍是预算主力；生成式把「内勤知识、报告初稿、合规问答」推到可快速试点档位。硬约束未变：**模型风险管理（MRM）、可解释性、第三方供应链尽职调查、人机共决策责任划分**。自动拒贷/理赔结论不得因工具热度绕过既有控制。

对经营层而言，金融业 AI 预算的正确切法是「稳态系统 + 受控生成式」双账本：前者按风险加权资产与监管检查节奏维护；后者按评测通过率与引用覆盖率放量。暂行办法施行后，面向公众的生成式服务路径必须可审计。

【案例框 | 银行内勤知识助手（示意）】

- 范围：制度/产品问答，强制引用段落与版本号；禁止直接给客户最终答复。
- 门禁：幻觉抽检 ≤3%、敏感字段不出域、周级回归。
- 90 天目标：客服与运营人均检索时长下降，且零 P1 泄密。

6.3 零售与消费

需求预测、库存与定价仍靠传统预测优化主线；生成式加速商品文案、活动页、导购辅助与售后话术草稿。品牌安全词库、虚假宣传防控与合成内容标识必须前置。极端需求冲击下须保留人工覆盖规则，避免把决策权完全交给黑箱。

领先零售商把「算法建议 + 运营规则 + 人工覆盖」写成决策权责矩阵：促销模型可提议，但库存与价格最终由明确角色签发。内容标识与抽样人工成为上架默认步骤。

【案例框 | 零售内容工厂（示意）】

- 生成 → 品牌词库过滤 → 法务抽样 → 上架；对外素材 100% 可追溯生成批次。
- 成功指标：单篇内容成本、返工率、投诉率，而非「生成条数」。

6.4 制造与供应链

视觉质检、预测性维护、排程优化是 ROI 高地。生成式最佳入口是工艺/维修知识检索与工单摘要。OT/IT 数据融合质量决定上限；港口拥堵、关键器件短缺等系统性冲击，无法单靠局部优化模型对冲——AI 须与多源采购、安全库存与可见性战略绑定。

【案例框 | 工厂维修知识 RAG（示意）】

- 语料：设备手册、历史工单、安全规程；权限按产线切片。
- 禁止：生成结果直接改写 PLC/联锁参数；高风险操作双人确认。
- 价值：平均故障修复时间（MTTR）与一线培训周期可量化。

6.5 医疗与生命科学

影像辅助与研发计算持续吸引投入；生成式可用于文书、病历草稿与文献辅助。诊疗自动结论必须服从注册与临床路径；隐私与责任约束使节奏慢于消费互联网。医院运营类（排班、质控文书）可与临床类分轨推进。

医院知识助手优先服务医务行政，临床结论仍走人审。

6.6 汽车、出行与设备

辅助驾驶与座舱交互继续推进；高等级自动驾驶仍处长周期、高投入。主机厂与科技公司的分层采购、数据回流与安全责任划分是战略变量。生成式在车内助手与售后知识库可试点，但功能安全与信息安全标准不可降级。

6.7 科技、电信、媒体与公共部门

电信反诈与网络优化、媒体内容生产与标识、公共部门效率工具并行。高风险自动化须更高透明度与人工监督；欧洲风险分级思路对此类应用尤为敏感。平台型企业须把标识、内容安全与增长实验一体设计，避免「先放量后整改」。

工作区管控与数据不出域成为买方第一问。

6.8 能源与公用事业

负荷预测、巡检视觉与新能源出力预测是主场景。生成式用于规程检索与工单摘要时，不得绕过安全联锁与双人确认。资产寿命长、安全标准高，使上线周期长于消费互联网——成功项目几乎都绑定可靠传感器与工单数据。

6.9 落地失败共性（本期强化）

1. 场景伪需求或无业务 Owner；
2. 只接模型接口、不建检索与评测；
3. 成本无熔断、账单黑箱；
4. 合规后补，发版与证据包不同表；
5. 代理演示代替验收，无步数与日志约束；
6. 组织孤岛：数据科学 KPI 与业务损益脱节；
7. 发版与证据包不同表：合规后补。

【要点框 | 行业选择启发式】

优先：高频决策、反馈可观测、错误代价可界定、可加引用/可人工签发。条件缺一，留在研究清单，而不是生产清单。

【行动建议框 | 行业组合】

- 每个事业部最多并行 2 个受控试点；超额必须先关停僵尸项。
- 跨部门复用组件（网关/评测/词库）计入平台 KPI，而非仅计业务线。

7. 投融资与产业格局

7.2 中国市场与供应韧性（展开）

产业政策鼓励智能经济与算力建设；暂行办法抬高「可合规创新」门槛。能把增长与标识/评估一并产品化的厂商，更适配 2024–2025 制度环境。对企业采购：评估供应商融资跑道，保留多供应商与数据可迁移性；对开源自托管路径，同步准备补丁与许可证审计。

7.3 产业层重估

基础设施层战略属性强化；平台层（网关、向量库、评测、护栏）成为企业采购新重心；应用层比拼工作流与数据壁垒。「套壳」叙事在尽调中折价。评测与安全治理细分开始获得独立预算科目。

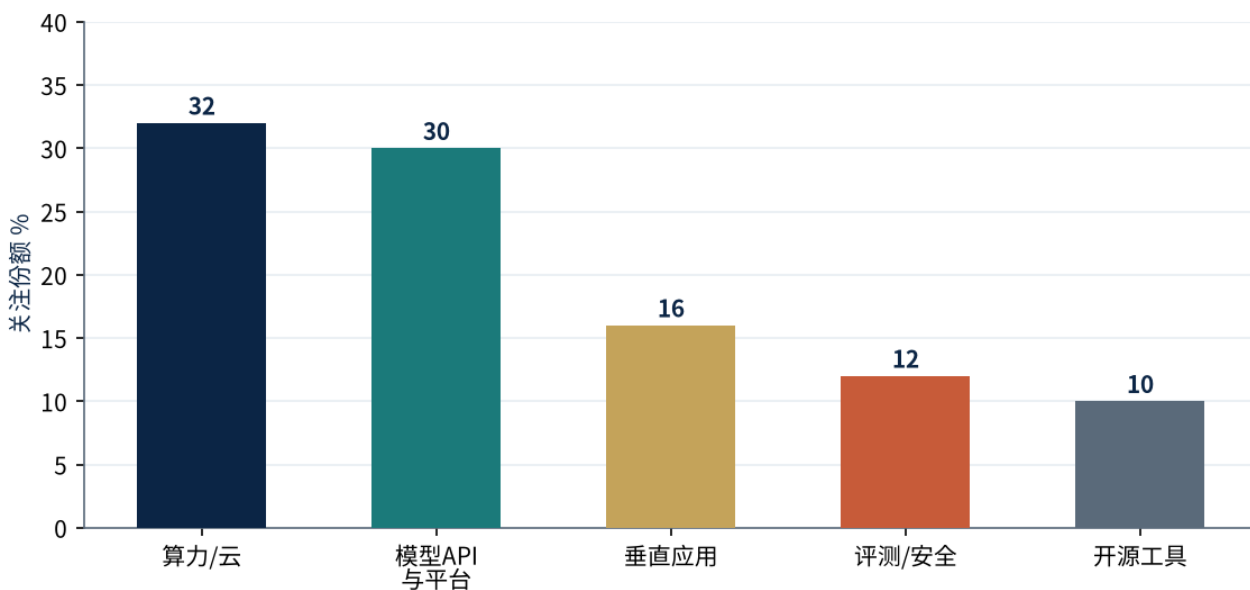
7.1 结构

算力/云与模型 API/平台仍吸金最多；垂直应用须证明工作流嵌入；评测与安全治理份额上升。套壳叙事在尽调中折价。

7.2 中国市场与供应韧性

合规能力成为公众服务准入成本；ToB 平台与行业私有化更契合。维护关键供应商健康度名单：融资、交付、事故响应、区域部署。大型云与行业软件商通过收购补齐 RAG 与护栏。

图 7-1 投融资关注结构 (2023H2)



来源：本报告综合测算

洞察：平台与算力吸金；治理份额上升。

7.4 选型、合同与退出

合同应包含：服务水平、安全事件通知时限、数据删除与导出、模型变更通知、价格调整机制、退出协助。对开放权重自托管，还需明确补丁责任、漏洞响应与许可证合规审计权。

买方尽调清单（更新）：融资跑道、再训练条款、评测透明度、私有化交付、多区域部署、开源成分与许可证、事故响应演练记录。评测、安全与私有化交付能力成为估值支撑点。

【案例框 | 供应商退出演练（示意）】

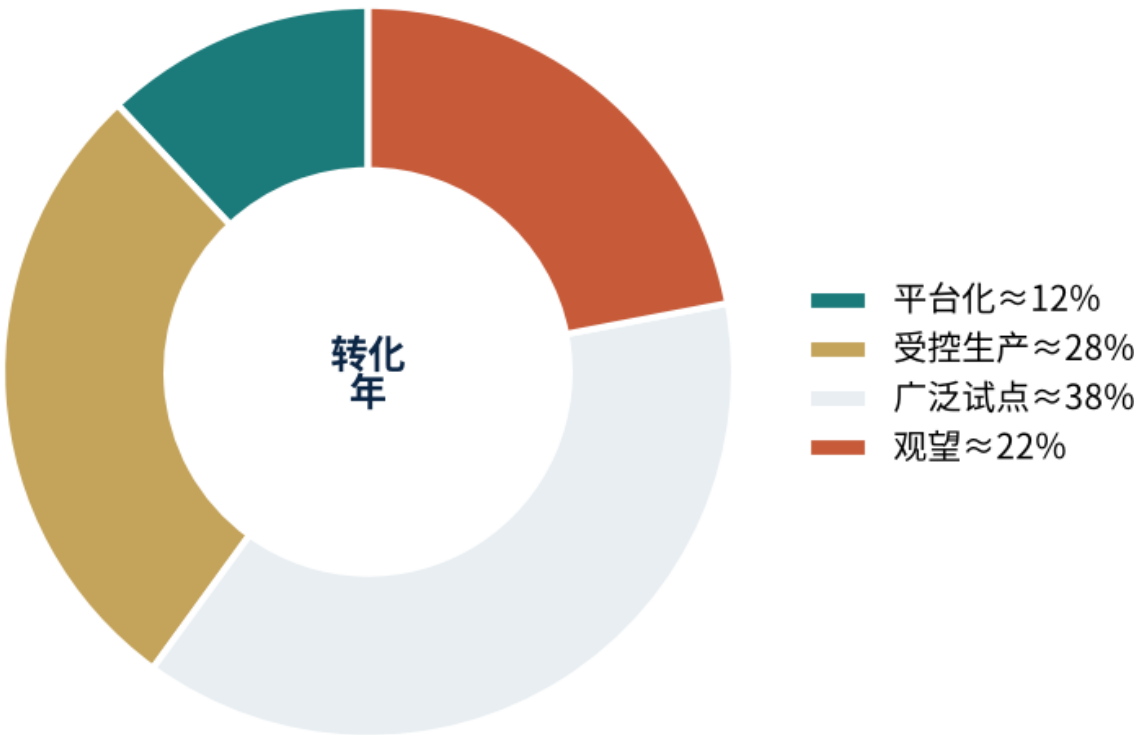
- 每半年一次：在 72 小时内切换备用模型路由，验证检索与评测门禁仍可用。
- 成功标准：主场景可用性不中断；日志与证据包完整。

8. 组织、人才与能力建设

8.1 成熟度画像

组织能力决定转化率。试点膨胀而平台未建，是最危险的错觉。

图 8-1 成熟度分野（2023年末）



来源：本报告综合测算

洞察：进入转化年临界点。

8.2 关键角色

平台产品经理、知识工程师、提示/编排工程师、评测与红队、模型风险官、业务 Owner。缺少 Owner 的试点应关停。翻译官角色（业务↔技术）仍是转化瓶颈。

8.3 培训与素养

从「认识生成式工具」转向：任务说明书、验收标准、保密红线、如何阅读引用与不确定度。管理层培训重点是投资纪律、风险分级与单位经济。

8.4 运营机制

双周转化评审（转化/停损/并入平台）；CoE 提供参考架构与共用组件；业务提供场景与验收。以正式服务目录收编影子 IT，提供合规替代路径而非一刀切禁用。

8.5 变革管理

公布客观门槛（评测、Owner、单位经济）；给予整改窗；逾期失去预算。把关停解释为保护可规模化场景，而非否定创新。

8.6 能力度量与激励

把 AI 相关激励从「立项数/模型数」改为「试点转化率、单位经济性、平台复用次数、高风险清单覆盖率」。对业务 Owner 给予与损益挂钩的阶段性奖励；对平台团队给予稳定性与降本指标。

培训分层：董事会（投资纪律与监管窗口）、经营层（场景选择与停损）、一线（任务说明书、验收、保密红线）。翻译官（业务↔技术）配置不足时，优先于再招「明星科学家」。

【行动建议框 | 组织】

- 公布客观门槛（评测、Owner、单位经济）；给予整改窗；逾期失去预算。
- 把关停解释为保护可规模化场景，而非否定创新。

9. 治理、风险与监管窗口

9.1 中国（展开）

《生成式人工智能服务管理暂行办法》自 2023-08-15 施行，覆盖训练数据、安全评估、标识、面向境内公众服务等取向。深度合成规定与算法推荐规定持续有效。企业内部工具与公众服务路径应分轨设计：前者强调数据分级与网关，后者强调评估与标识证据。

9.2 欧盟（展开）

2023-12 政治协议强化风险分级与通用目的 AI 透明度方向。在欧运营或服务欧洲客户的企业，应启动高风险用例差距预评，并把文档、人工监督与数据治理成本写入 2024 预算。

9.3 最小控制集（展开）

1. 高风险用例清单与上线门禁；
2. 生成式工具政策（允许/限制/禁止）；
3. 数据分级与外部接口阻断；
4. 评测回归与红队；
5. 面向公众内容的标识策略；
6. 第三方尽职调查与退出条款；
7. 事件响应与证据包目录。

9.4 深度伪造与跨境（展开）

伪造成本下降抬升品牌与金融欺诈风险。公共传播与客户材料增加来源核验；跨境场景按数据主权分区训练/微调，核心身份特征不进入公共 API。

9.1 中国

暂行办法已施行，叠加深度合成与算法推荐义务。安全评估、语料合规、标识与公众服务路径进入可检查状态。

9.2 欧盟

政治协议确立风险分级与通用目的 AI 透明度等取向；正式文本与实施细则仍待后续程序。在欧运营企业应启动义务预映射。

9.3 最小控制集

工具白名单与工作区、网关、评测、标识、安全评估证据、高风险登记、第三方尽调、事件响应。风险排序：不准确、泄密、知识产权、有害内容、供应商依赖。

9.4 深度伪造与跨境

公共传播强制来源声明；高影响内容人工签发。数据主权分区微调、推理就近、敏感特征不进公共 API。

图 9-1 监管窗口（2023年末）



来源：监管公开文本

洞察：中国义务可执行；欧洲进入协议后窗口。

【行动建议框】

定风险级别 → 配控制措施 → 再扩流量。合规成本写入业务 case。

9.5 事件响应与证据包

预设场景：幻觉导致对外错误陈述、数据粘贴泄露、深度伪造冒充、代理误操作、版权投诉。演练频率不低于每半年一次；复盘输入评测集与门禁规则。

证据包最小目录：高风险清单、模型/提示版本、评测报告、人工审核抽样、供应商合同关键条款、数据流图、事件时间线。目标：监管或客户尽调到来时，**30 天内可提交**。暂行办法已施行；欧盟政治协议强化跨国企业对标压力。

【行动建议框 | 治理】

- 定风险级别 → 配控制措施 → 再扩流量。
- 把合规成本写入业务 case，而不是让法务事后背锅。

10. 未来12-24个月情景分析

以下情景以 **2023年12月** 为起点，展望至 **2024年末至 2025年末**。均为管理推演，非点预测。

10.1 基准情景（概率重心：中高）

- 多数企业完成 1-3 个场景受控生产转化，平台最小闭环上线；
- 成本标签与熔断成为财务常规要求；
- 中国合规执法与检查案例增加，头部企业证据包标准化；
- 欧洲义务预评进入跨国企业年度计划；
- 资本市场继续分化：有转化与收入质量者 vs 纯叙事者。

企业含义： 2024 年是「平台与转化年」——少追新模型新闻，多建可审计生产线。

10.2 乐观情景

- 检索与评测工具链成熟，使中型企业也能稳定运行多个生成式工作流；
- 单位推理成本下降，知识与客服人效显著改善；
- 出现可复制的行业知识助手产品模块，缩短自建周期。

企业含义： 提前锁定语料合作与人才；用平台化方式捕捉场景扩散，避免部门重复造轮子。

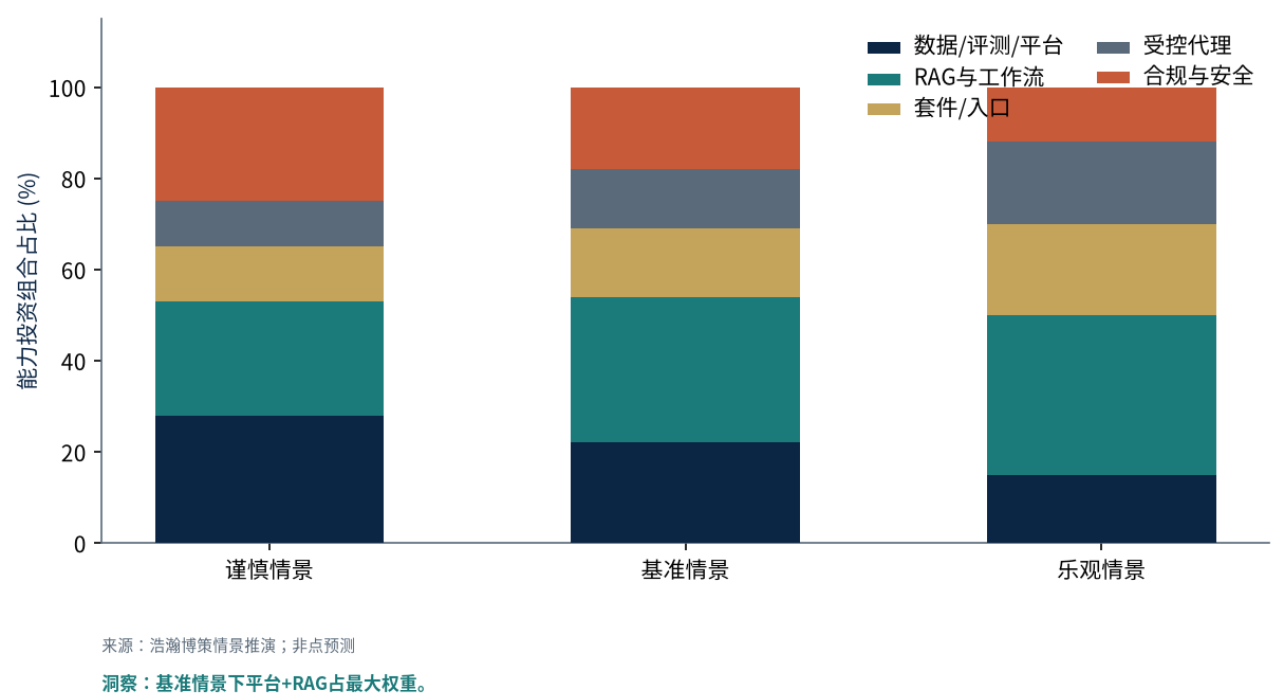
10.3 谨慎情景

- 重大泄密、幻觉事故或合规处罚引发行业性收紧；

- IT 预算冻结，未证明价值的生成式项目首先被砍；
- 算力或合规成本抬高，放慢扩散。

企业含义： 保留停损清单；优先捍卫已贡献现金流的场景；把合规与安全投入视为保命资产。

图 10-1 三情景投资组合（2023-12起点）



10.4 情景触发指标（供战略部跟踪）

建议每季度跟踪下列触发器，以决定从基准情景切换到乐观或谨慎路径（起点 2023年12月）：

触发器	乐观方向信号	谨慎方向信号
试点转化率	连续两季达标	连续两季过低
单位成本	下降或可控	失控或无标签
P1 事故	无	监管关注或重大误判
合规差距	按期关闭	主场景须下线改造
证据包就绪	抽检通过	材料拼凑

战略含义： AI 议程应被管理为 **带期权的投资组合**，而不是一条不可逆的直线路线图。基准情景下仍应以平台能力与受控转化为重心；乐观时扩面，谨慎时捍卫已贡献现金流的场景并加强合规。

11. 企业行动议程（90天 / 12个月）

11.1 未来 90 天

序号	行动	产出
1	压缩试点名录	关停/并入清单
2	平台最小闭环	网关+RAG+评测
3	暂行办法证据包	目录与缺口
4	场景成本熔断	CFO会签
5	对欧义务预评	一页差距

11.2 未来 12 个月

≥3 场景受控生产；平台成默认入口；RAI 覆盖高风险；多供应商预案；单位经济上董事会。

11.2a 转化度量（本期）

建议董事会级仪表盘至少包含：受控生产场景数、试点转化率、单位任务成本、评测通过率、高风险清单覆盖率、P1 事故数、证据包抽检通过率。缺项的组织，先补度量再扩场景。

【行动建议框 | 投资纪律】

每个新试点必须回答：数据是否就绪？上线谁负责？失败如何停损？与现有平台如何复用？四问缺一，不予立项。

11.3 董事会监督问题清单

1. 生产系统与试点转化率如何？
2. 单位成本与熔断是否有效？
3. 高影响自动化决策责任是否清晰？
4. 合规证据包能否在 30 天内提供？
5. 人才缺口在平台工程还是业务 Owner？

11.4 行业定制速览

银行保险：MRM 与解释性优先。零售：内容安全词库。制造：质检+知识RAG。医疗：临床路径不可绕过。软件：代码辅助+保密隔离。平台型：标识与安全与增长同设计。

11.5 投资纪律与停损清单

每个新试点必须回答四问：数据是否就绪？上线谁负责？失败如何停损？与现有平台如何复用？四问缺一，不予立项。季度价值审计公开「转化 / 整改 / 关停」三类结果，避免僵尸项目吞噬云与人力。

结合 2023年12月 节点的 90 天强调： 先完成组合可见性与高风险清单，再扩场景；任何面向公众或客户触达的生成能力，必须同步标识/审核/引用策略。

12 个月强调： 至少 2 个场景完成受控生产转化并公布单位经济；平台最小闭环（网关/检索/评测/成本）上线；高风险生产系统 RAI 控制全覆盖；形成多供应商与退出演练记录。

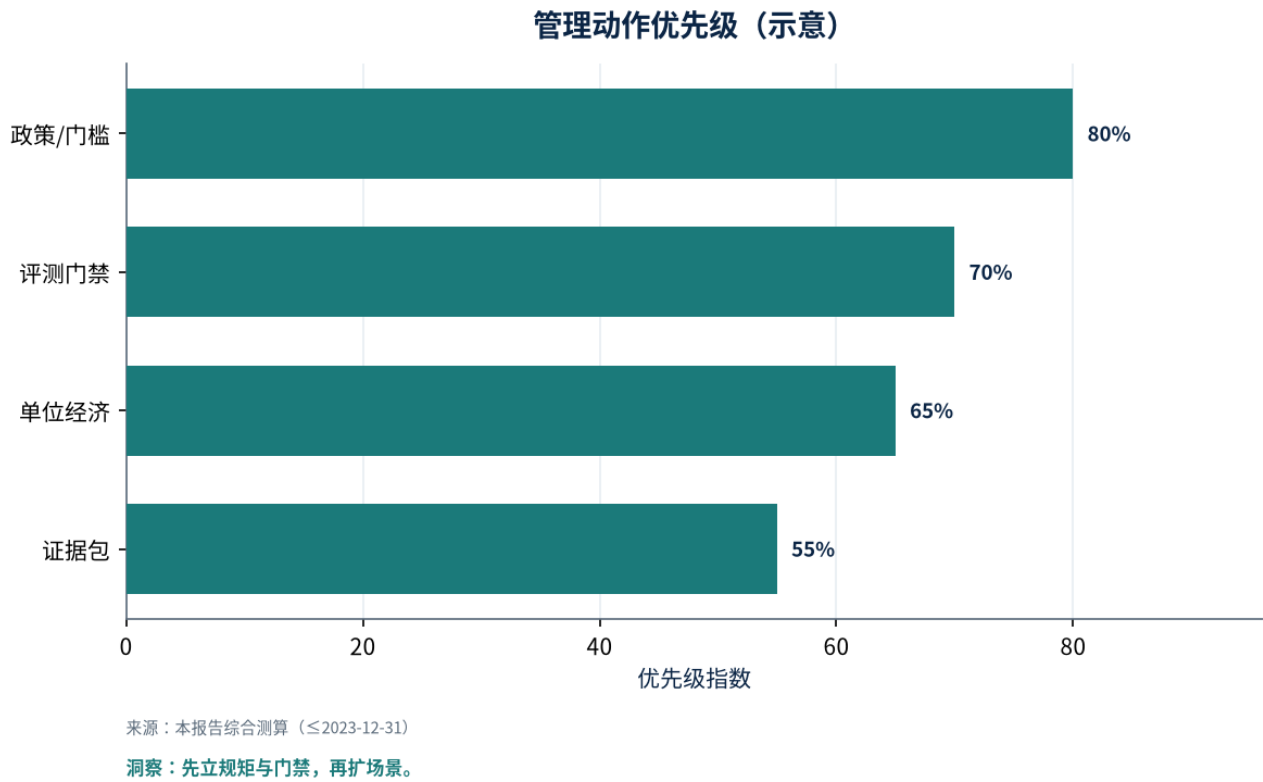
11.6 跨职能协同节奏

节奏	参与方	产出
双周	业务 Owner + 平台	转化/停损决议
月度	CFO + CIO	成本与熔断回顾
季度	经营层	组合雷达与预算重配
半年	董事会风险委	高风险清单与证据包抽检

董事会可追加追问： 上季度关停了哪些僵尸项目？平台复用次数是否上升？若核心供应商断服，72 小时内能否切换？

11.7 行业定制议程（展开）

- **银行保险：** 证据包与暂行办法路径设计同步。
- **零售：** 标识与抽样成为默认上架步骤。
- **制造：** 平台组件复用计入 KPI。
- **医疗：** 医务行政助手优先。
- **公共部门：** 透明度与人工监督优先于自动化率。



【图注 11-1】行动与监督优先级示意。来源：本报告综合测算（≤2023-12-31）。洞察：把度量与门槛写进议程，场景扩张才可控。

12. 附录

附录 0 | 图表索引

编号	说明	主来源（均 ≤2023年12月31日）
图 3-1	核心能力/优先级	公开市场调研综合 / 本报告综合测算
图 4-1~4-4	市场与需求（含结构示意）	公开市场调研 / 本报告综合
图 5-1~5-2	技术栈与时间线	公开技术节点 / 本报告综合
图 6-1~6-2	价值矩阵与热力	本报告综合测算
图 7-1	投融资结构/气氛	行业公开统计 / 本报告综合
图 8-1	成熟度分野	本报告综合测算
图 9-1	监管窗口	监管公开文本
图 10-1	三情景投资组合	本报告情景推演

图表文件目录：[charts-2023-H2/](#)。

附录 A | 术语表（节选）

术语	含义
RAG	检索增强生成
企业AI平台	网关/检索/评测/成本/权限共用层
受控生产	有评测、监控、审核与回滚的正式上线
单位经济性	单次任务成本与业务收益对照
RAI	负责任/可信赖人工智能
模型路由	按任务复杂度/敏感度选择不同模型或缓存

附录 B | 场景优先级评分卡

维度	权重建议	评分 1-5	备注
年度价值潜力	20%		可挂钩 P&L 或明确成本池
数据敏感性（逆向）	20%		高分=更敏感，计算用 6-分
评测可行性	15%		能否建黄金集与回归
人工审核可负担性	15%		审核负荷是否可承受
合规复杂度（逆向）	15%		高分=更复杂
平台复用潜力	15%		组件能否被 2+ 场景复用

计分： 加权总分；逆向维度以 (6-评分) 参与加权。低于内部阈值不得接入生产网关。

附录 C | 高管沟通话术

「AI 已进入经营系统议题。我们用转化率、单位成本与合规证据做决策，而不是用演示张数。模型会迭代，平台与数据资产留在组织。未来 12-24 个月比拼的是可控的规模化，不是热点跟踪速度。」

附录 D | 90 天执行检查清单

周次	检查项	完成标准
W1-2	组合雷达与影子 IT 抽样	一页纸经 CEO/CIO 会签
W3-4	高风险清单与数据分级	法务/安全/业务三方签字
W5-8	受控试点评测集与门禁	黄金集可回归；无门禁不升流量
W9-12	单位经济与停损决议	至少 1 个转化或明确关停

附录 E | 术语补充与评分卡使用说明

术语	含义
黄金集	冻结的真实样本评测集，用于回归门禁
证据包	可提交监管/客户尽调的控制与版本材料目录
快/深路由	按任务复杂度在低成本模型与推理模型间分流
影子采用	未经正式批准的员工自用工具行为
单位经济性	单次任务成本与业务收益对照
停损清单	未达门槛即关停或降级的项目列表

评分卡使用说明： 评分 1–5，加权汇总；「逆向」维度高分表示风险更高，计算时用 (6-评分)。建议由业务 Owner 初评、平台与风控复评；总分低于阈值的项目不得进入生产网关。权重可按行业微调，但「数据敏感性/合规」逆向项不得删除。

附录 F | 高管沟通话术（补充）

向业务团队：

「模型不会自动理解你们的客户与库存。先把决策频率、对错代价和可用数据写清楚，技术团队才能交付可上线的系统。你们是 Owner，模型是工具。」

向董事会风险委员会：

「我们用高风险清单、评测门禁与事件演练证明可控。模型世代会变，证据包与平台资产留在组织。检查到来时，目标是 30 天内交出材料，而不是临时拼凑幻灯片。」

以上附录材料知识截止：2023年12月31日。

附录 G | 场景组合雷达（填写示例）

场景	价值	数据就绪	风险级	成熟度	决策
内勤知识助手	高	中	中	试点	转化
营销文案生成	中	高	中	试点	转化（加词库）
自动对外理赔结论	高	中	高	概念	研究/禁止自动
代码辅助	中	高	中	试点	转化（隔离）
无 Owner 聊天开通	低	—	高	影子	关停或收编

示例为管理模板，数值须替换为本企业评估；知识截止 2023-12-31。

附录 H | 90 天周节奏（展开）

周	焦点	产出物
1	组合盘点	雷达与影子抽样
2	风险与数据	高风险清单、分级表
3-4	门禁	评测集、网关策略
5-6	试点运行	对照实验数据
7-8	单位经济	成本与收益一页纸
9-10	合规证据	证据包目录 v1
11-12	转化/停损	经营层决议

13. 参考文献

1. 公开市场调研综合：2023下半年企业生成式采用、平台化与成本治理口径。

2. 《生成式人工智能服务管理暂行办法》（2023-08-15施行）；深度合成规定；算法推荐规定。

3. 欧盟机构关于 AI 法案政治协议的公开新闻稿（2023-12）。

4. 公开技术节点：开源可商用权重、企业助手与长上下文/开发者接口（≤2023-12）。

5. 本报告综合测算与情景推演（浩瀚博策，2023-12）。

14. 关于浩瀚博策（出品方）

北京浩瀚博策咨询有限公司（品牌：浩瀚博策）聚焦企业数据、商业决策与 AI 商业落地，服务定位可概括为：

让 AI 成为企业的新能力。把 AI 用进业务，把能力留在组织。
从产品创新到销售增长，以 培训 · 咨询 · 持续赋能 帮助企业把商业判断转化为经营行动。

主要服务：

- **AI 商业培训：** 围绕真实业务场景，把工具、方法与实操结合，帮助经营团队建立方向感与行动方法。
- **经营增长咨询：** 从产品、客户与销售流程寻找突破口，用数据辅助判断，推动 AI 进入具体经营动作。
- **组织永久赋能：** 将关键经验沉淀为流程、SOP 与可复用方法，使个人专业能力转化为组织长期资产。

方法主张： 经验沉淀 → 把能力用起来 → 持续验证业务指标，形成可复用、可迭代的组织能力。

官网： <https://www.haohan365.com/>

本报告为浩瀚博策 2023下半年 公开研究观点，供讨论参考，不构成投资建议。 **浩瀚博策 • 2023年 12月** *知识截止：2023年12月31日* © 2023 北京浩瀚博策咨询有限公司