

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：旗舰模型、开源与工具链
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（含术语、评分卡、高管沟通话术）
13. 参考文献
14. 关于浩瀚博策（出品方）

1. 执行摘要

2023年上半年，人工智能产业完成了一次罕见的「议程压缩」：**公众级对话产品的引爆** → **旗舰多模态模型与办公套件集成公告** → **开源权重进入研究社区** → **中国生成式服务管理征求意见**，几乎叠压在同一财政半年内。对企业而言，问题已从「要不要关注生成式」转为「如何把试点变成可审计的工作流，并在合规征求意见稿的方向上预整改」。

本报告基于截至 **2023年6月30日** 的公开调研、市场信号、技术节点与监管文本，对 2023 上半年全球 AI 态势作出半年度研判。五组并行事实构成管理层决策底座：

第一，生成式从「个人尝鲜」跃迁为「企业立项主题」。 公开市场调研显示，约 **六成** 受访大型组织已采购或计划在当年采购至少一款生成式工具；董事会与高管个人使用显著抬头。与此同时，采用传统（判别式）AI 的组织比例大体平稳——生成式更多是 **叠加层**，尚未自动转化为全公司 AI 成熟度跃迁。

第二，能力供给出现「旗舰 API + 开源权重 + 套件嵌入」三轨并行。 2023年3月前后，多模态旗舰模型、对话助手与办公生产力套件集成相继进入公开议程；2月研究社区获得更具效率的开源权重家族。企业技术委员会必须同时评估调用成本、数据出境、私有化可行性与员工日活入口，而不是押单一供应商故事。

第三，价值证明仍集中在知识、内容、代码与服务辅助。 营销销售、产品开发、服务运营与软件工程是试点最热职能；风控、供应链与人力相对谨慎。检索增强（RAG）知识助手成为「可治理入口」的共识选项；完全自主的多步骤代理仍偏实验。

第四，风险治理落后于采用速度。 公开调研反复提示：组织认为「不准确/幻觉」是最相关风险之一，但采取系统缓解措施的比例显著低于采用意愿。数据泄露担忧（员工粘贴敏感信息）与版权、深度伪造并存。

第五，中国监管从深度合成施行迈向生成式专项征求意见。 《深度合成管理规定》已于 **2023年1月10日** 施行；**2023年4月11日** 生成式人工智能服务管理公开征求意见，对训练数据、安全评估、内容标识与面向公众服务提出明确取向。欧盟 AI 法案提案的风险分级框架仍是在欧运营对标基线。

对经营层的直接含义： 未来 12-24 个月，赢家不是「立项最多」的企业，而是能把 **RAG/评测/权限/成本** 做成共享底座，并完成 2-3 个场景从 PoC 到受控生产转化的企业。2023 下半年的关键 KPI 应是 **试点转化率**，而非账号开通数。

【要点框 | 给 CEO / 董事长的一页纸】

- 冻结公司级生成式策略：三轨（API / 开源私有化 / 套件嵌入）+ 统一治理底座。
- 只允许 3-5 个正式试点进入预算，其余部门实验走沙箱。
- 每个试点必须有：评测集、幻觉红线、数据分级、人工审核、单位成本上限。
- 对照生成式征求意见稿做预整改差距表（即便正式办法尚未公布）。
- 董事会每季审查：转化率、P1 事件、API 账单、合规关闭进度。

读者	读完后 72 小时内可做的事
董事长/CEO	批准「试点名录」与停用僵尸 PoC 清单
CFO	设定生成式云/API 月度熔断线
CIO/CTO	选定企业 RAG 参考架构与模型网关
业务一把手	提交场景宪章（基线人效/质量指标）
法务/合规	映射征求意见稿义务到产品清单
CHRO	上线提示词与保密必修课

【本期研判焦点】

工作流嵌入、企业版管控、人效对照实验与征求意见稿预演。

2. 研究范围、方法与知识截止

2.1 研究问题

1. 截至 2023 年中，生成式与大模型如何改写市场、技术与资本位置？
2. 哪些职能与行业已具备受控生产条件？

3. 组织与治理如何追上采用速度？
4. 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：2022-2023H1 公开市场调研、行业公开统计、监管公开文本与技术节点综述。
- 监管精读：深度合成规定、算法推荐规定、生成式服务管理征求意见稿、欧盟 AI 法案提案、OECD 原则。
- 技术节点交叉验证：官方博客与研究发布（均≤2023-06-30）。
- 咨询式综合：转化为判断、情景与行动项。

2.3 知识截止与表述约定

约定	说明
知识截止	2023年6月30日
发布设定	2023年6月（2023上半年报告）
禁止引用	此后生成式正式办法公布施行、后续开源权重新世代等
时态	「当前（2023年中）」「2023上半年」「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

检索增强（RAG）：以企业知识检索结果约束生成，提升可溯源与可审计性。**受控生产**：有评测、权限、审核、监控与回滚的正式上线。**代理（Agent）**：能多步骤调用工具以追求目标的系统，2023年中多数仍处实验。

3. 五大核心判断

【判断 1 | 立项浪潮已至，转化才是稀缺能力】

采购与试点意愿在 2023 上半年集中释放，但能稳定贡献可审计人效/收入的场景仍少。组织应把「PoC 数量」从 KPI 中降权，把「转化率与单位经济」升权。

【判断 2 | 三轨技术策略成为默认解】

公共 API、开源私有化与办公套件嵌入将长期并存。胜负手是共享的数据分级、网关、评测与成本治理，而非押中单一模型品牌。

【判断 3 | RAG 是企业级「可治理入口」】

相对纯对话，带引用的知识助手更易通过法务与风险审查。营销与代码辅助可并行，但对外自动答复仍须人机共决。

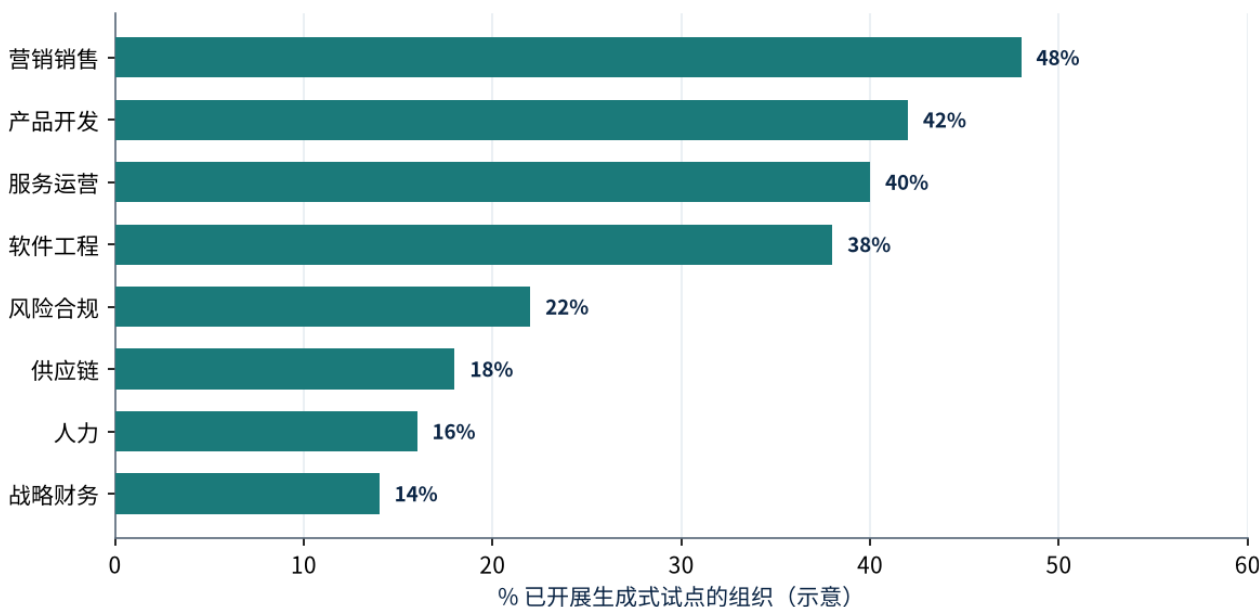
【判断 4 | 算力与平台吸金，应用靠 workflow】

一级市场关注向云推理、模型 API 与平台集中；垂直应用必须证明嵌入现有系统与销售动线，否则估值承压。

【判断 5 | 征求意见稿已具「预整改效力」】

即便正式办法尚未落地，训练数据、安全评估、标识与公众服务路径的取向已足够明确。等待终稿再动手，往往错过产品窗口。

图 3-1 生成式试点渗透：按职能热度（2023上半年）



来源：公开市场调研综合 / 本报告综合测算（企业生成式职能渗透，≤2023-06）

洞察：营销、产品、服务与工程先热——风控与供应链仍偏谨慎。

【图注 3-1】生成式试点渗透：按职能热度（2023上半年）。

来源：公开市场调研综合 / 本报告综合测算（≤2023-06）。

洞察：营销、产品、服务与工程先热；风控与供应链偏谨慎。

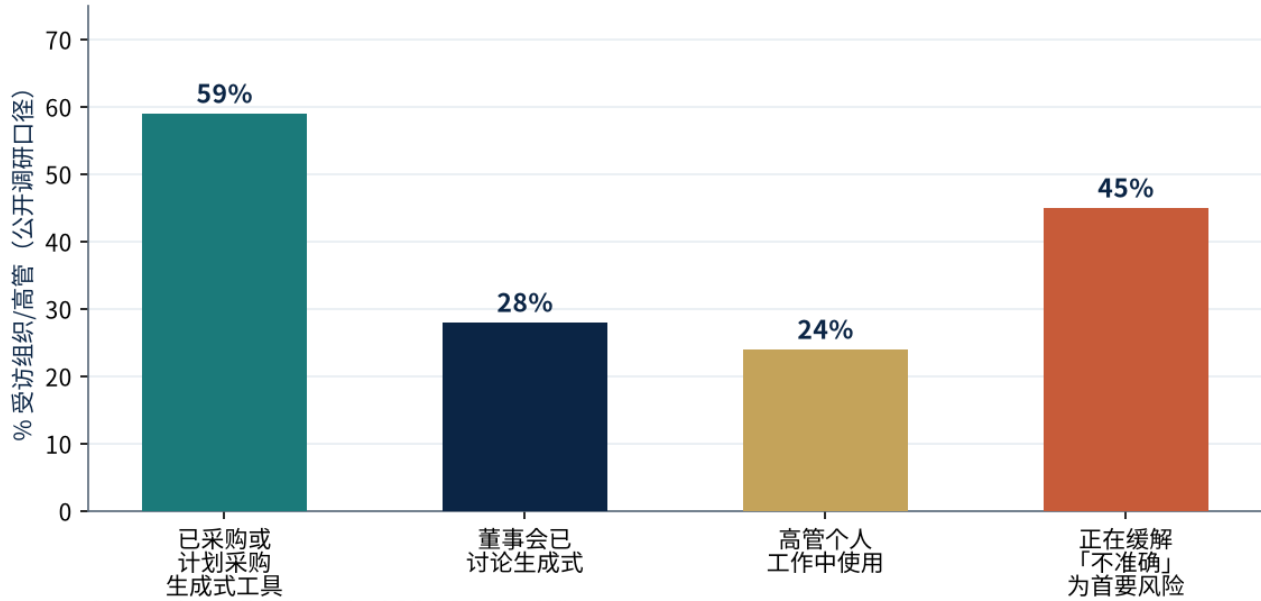
4. 全球市场与需求图景

4.1 采用：生成式叠加，而非替代

公开市场调研在 2023 春夏释放的信号高度一致：生成式工具的试用与采购意向快速上升；部分调研口径显示约 59% 的大型组织已采购或计划采购；董事会讨论与高管个人使用成为新常态。与此同时，传统 AI 采用广度并未同步出现同等幅度跃迁——说明生成式更多改变了 **可见性与优先级**，而不是一夜之间补齐了数据与 MLOps 短板。

对 CFO/CIO 的含义：不要用「生成式立项数」替代「生产模型健康度」报表；两套账要并表。

图 4-1 2023上半年企业生成式态势关键指标



来源：公开市场调研综合（2023年春夏企业生成式采用与风险缓解公开口径，≤2023-06）

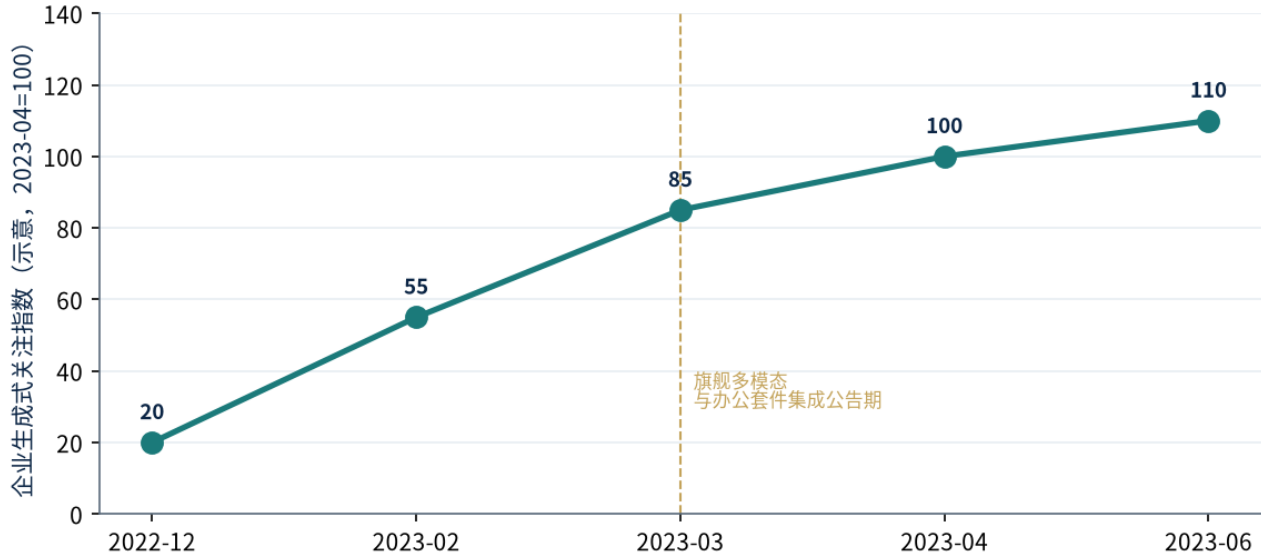
洞察：采购意愿高涨，但风险缓解仍落后于采用——不准确是第一风险。

【图注 4-1】 2023 上半年企业生成式态势关键指标。

来源：公开市场调研综合（≤2023-06）。

洞察：采购意愿高，风险缓解仍落后；不准确是首要风险。

图 4-2 企业生成式关注指数轨迹（2022末-2023中）



来源：本报告综合测算（公开产品节点与媒体/招聘/采购信号交叉）

洞察：2023年一季度完成从「尝鲜」到「立项」的跃迁。

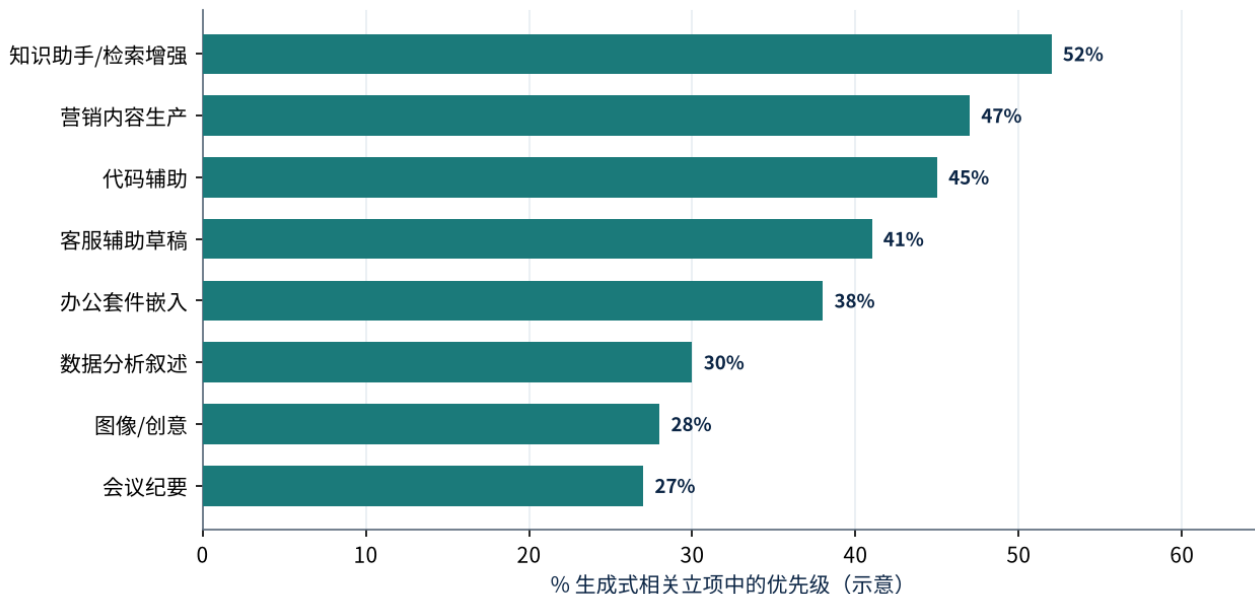
【图注 4-2】 企业生成式关注指数轨迹（2022末-2023中，示意）。

来源：本报告综合测算。洞察：2023Q1 完成从尝鲜到立项的跃迁。

4.2 需求结构：入口场景收敛

企业正式立项呈现收敛趋势：知识助手（RAG）、营销内容、代码辅助、客服草稿、办公套件嵌入居前。图像创意与会议纪要广泛存在于个人生产力层，但进入受控生产的比例较低。

图 4-3 2023上半年企业生成式立项优先级



来源：本报告综合测算（公开用例与采购观察，≤2023-06）

洞察：检索增强知识助手成为「可治理入口」首选。

【图注 4-3】2023 上半年企业生成式立项优先级。

来源：本报告综合测算（≤2023-06）。

洞察：RAG 知识助手成为可治理入口首选。

4.3 支出：总账仍宽，生成式科目单列

2022 年宽口径 AI 支出预测（软+硬+服务约四千亿美元量级）仍提醒管理层：基础设施与服务是大头。2023 上半年新增的是 **推理 API、向量数据库、评测与人工审核** 等科目。建议在预算中单列「生成式运营成本」，并设月度熔断，防止试点账单失控。

4.4 区域：供给竞赛与规制竞赛并行

美国主导旗舰模型产品化与开发者生态；中国应用落地与生成式监管节奏上形成独特约束；欧洲继续推进风险分级立法讨论。跨国企业须按数据主权拆分拓扑：训练/微调分区、推理就近、敏感特征不进公共接口。

4.5 买方行为：从「开通」到「验收」

合同条款继续硬化：不用于再训练、输出知识产权、幻觉责任、审计与退出、私有化选项。内部则出现「AI 采购委员会」或把生成式并入现有 CoE。演示型供应商进一步承压。

4.6 生产力叙事与测量陷阱

厂商与早期用户大量传播「人效提升 50%+」类故事。管理层应要求：

- 1. 基线如何测（任务时长、返工率、客户满意）？
- 2. 是否包含审核与返工时间？
- 3. 是否只在自愿使用者中统计（选择偏差）？
- 4. 质量事故是否入账？

没有对照实验的人效宣传，不应直接写入年度经营计划。

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。

2023 上半年「开通」容易、「验收」困难。人效须对照实验，自愿使用者自我报告不足以写入经营计划。

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。

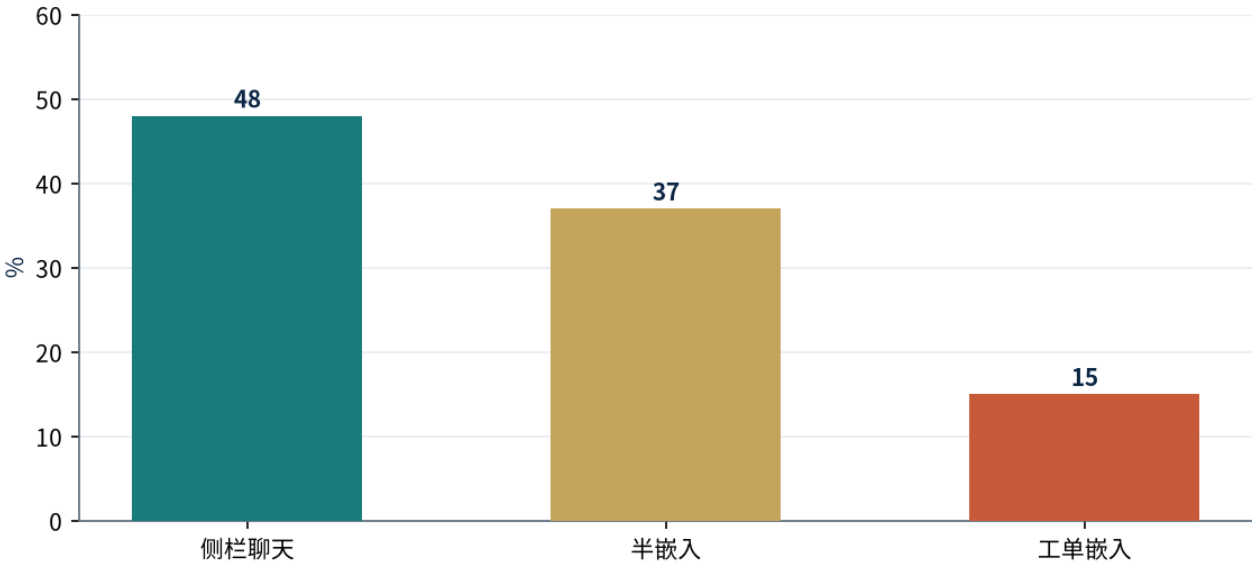
6.0 从对话产品到工作流嵌入

2023 上半年对话产品与办公嵌入降低了试用门槛，也放大了「开通即成功」的错觉。嵌入工作流的标志是：助手出现在工单处理界面、知识权限与业务系统打通、验收指标可对照实验。仍停留在侧栏聊天的组织，应把下半年预算从「座位许可」转向「系统集成与评测」。

【行动建议框 | 嵌入标准】

- 每个试点必须指出被嵌入的系统与被替代的步骤。
- 无对照实验的人效数字，不得写入经营计划。
- 部门自行采购超过阈值必须收编到平台目录。

试点嵌入深度（示意）



来源：本报告综合测算（≤2023-06-30）

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（≤2023-06-30）。洞察：结构重于总量——用分层指标做决策。

5. 技术演进：旗舰模型、开源与工具链

5.1 2023上半年关键节点

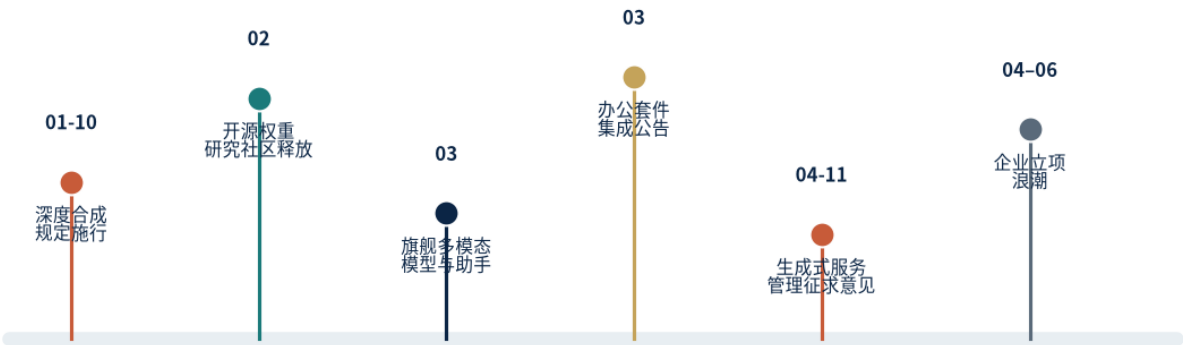
- 2023-01-10：中国深度合成管理规定施行；
- 2023-02：研究社区获得更具参数效率的开源权重家族，私有化试验升温；
- 2023-03：旗舰多模态模型与新一代对话助手进入公开议程；办公生产力套件集成公告点燃员工日活想象；
- 2023-04-11：生成式人工智能服务管理公开征求意见；
- 2023-04至06：企业集中立项，RAG、提示链与简易代理框架在工程社区扩散。

图 5-1 2023年中企业大模型技术策略三轨



【图注 5-1】 2023 年中企业大模型技术策略三轨。
来源： 浩瀚博策综合。洞察： 三轨须共享治理底座。

图 5-2 2023上半年关键节点（公开时间线）



来源：监管公开文本与厂商/研究机构公开博客（均≤2023-06-30）

洞察：能力供给、办公入口与监管征求意见在同一季度叠压。

【图注 5-2】 2023 上半年关键节点。
来源： 监管公开文本与公开技术节点（≤2023-06-30）。

5.2 从「提示词」到「系统」

领先团队不再把竞争力定义为会写提示词，而是：

层级	能力
数据	语料权限、脱敏、更新频率、引用溯源
检索	切片、向量/关键词混合、重排
编排	提示模板版本、工具调用、回退策略
评测	黄金集、幻觉率、安全红队、回归
运行	网关、配额、缓存、成本与延迟看板
人机	审核队列、升级路径、责任归属

5.3 开源与供应韧性

开源权重使中小团队可做私有化 PoC，但也带来许可证、安全补丁、评测与运维责任。务实策略：低敏研发用开源试验；生产默认经网关；高敏数据不出域；保留至少一条备选推理路径。

5.4 代理与工具链：热情与边界

多步骤代理演示在工程社区流行，但 2023 年中企业生产仍应限制在：明确工具白名单、最大步数、人工确认点、完整日志。把代理当「数字员工」写入编制，为时尚早。

5.5 多模态：文档与截图理解升温

旗舰多模态能力使「读图/读文档再 generat」成为新试点方向（报销单、图纸、表单）。准确率与隐私（屏幕含敏感信息）需同步设计。

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。从提示词走向系统：编排、工具调用边界、企业版工作区与日志。

5.5 供应韧性与多模型路由

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】

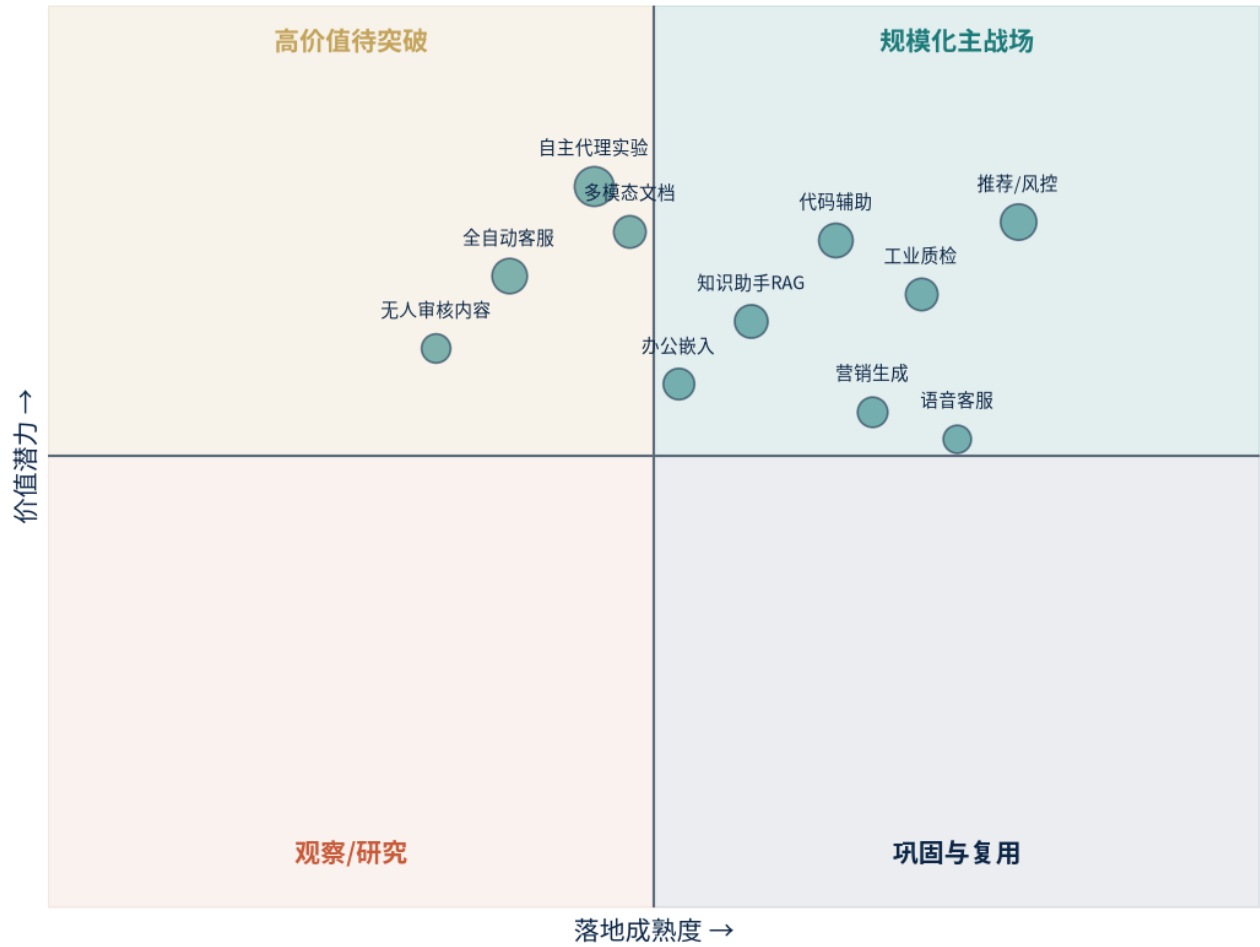
- 先止血：统一网关日志与月度成本看板。
- 再提质：黄金集 + 红队 + 引用强制。
- 后扩面：多场景复用同一平台组件。

6. 跨行业落地：价值池与成熟路径

6.1 总览

档位	场景	特征
较成熟	推荐/风控、工业质检、部分语音	闭环与 ROI 清晰
加速转化	RAG 知识助手、代码辅助、营销生成、办公嵌入	人机共决可快速证明
早期	自主代理、全自动对外答复、无人审核内容分发	责任边界未清

图 6-1 价值—成熟度矩阵（2023年中）



来源：本报告综合测算（公开价值池思路与2023H1产业实践）。

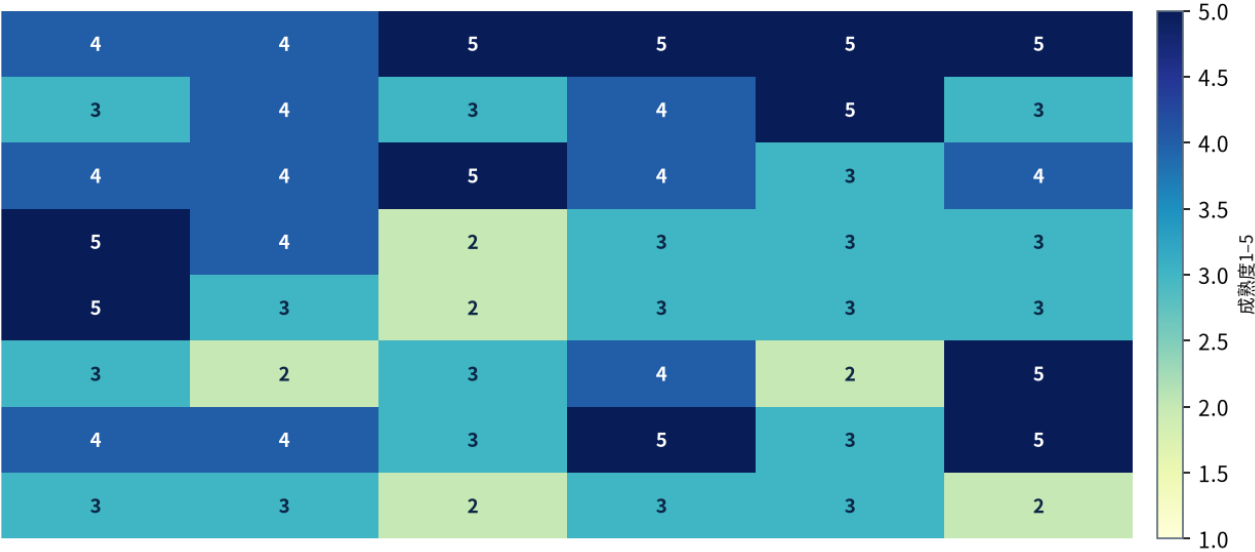
洞察：RAG知识助手进入可规模化边缘；自主代理仍偏左上——先定边界。

【图注 6-1】 价值—成熟度矩阵（2023年中）。来源： 本报告综合测算。

洞察：软件/互联网生成式成熟度跃升；金融仍受MRM与合规约束。

来源：本报告综合测算（≤2023-06）。

图 6-2 行业×能力热力（2023年中，1-5）



【图注 6-2】行业×能力热力（2023年中）。来源：本报告综合测算。

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。2023 上半年办公嵌入与对话产品企业版讨论升温，内勤场景应先于客户触达。

【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。活动页与导购草稿可快试，但广告法合规词库必须前置。

【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。

文书辅助与临床决策分轨；后者不得「先试点后补注册」。

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」。

代码辅助几乎成为标配讨论；客户代码隔离是采购关键条款。

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. 百花齐放无收口：各部门各买各的，无法复用。

【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】

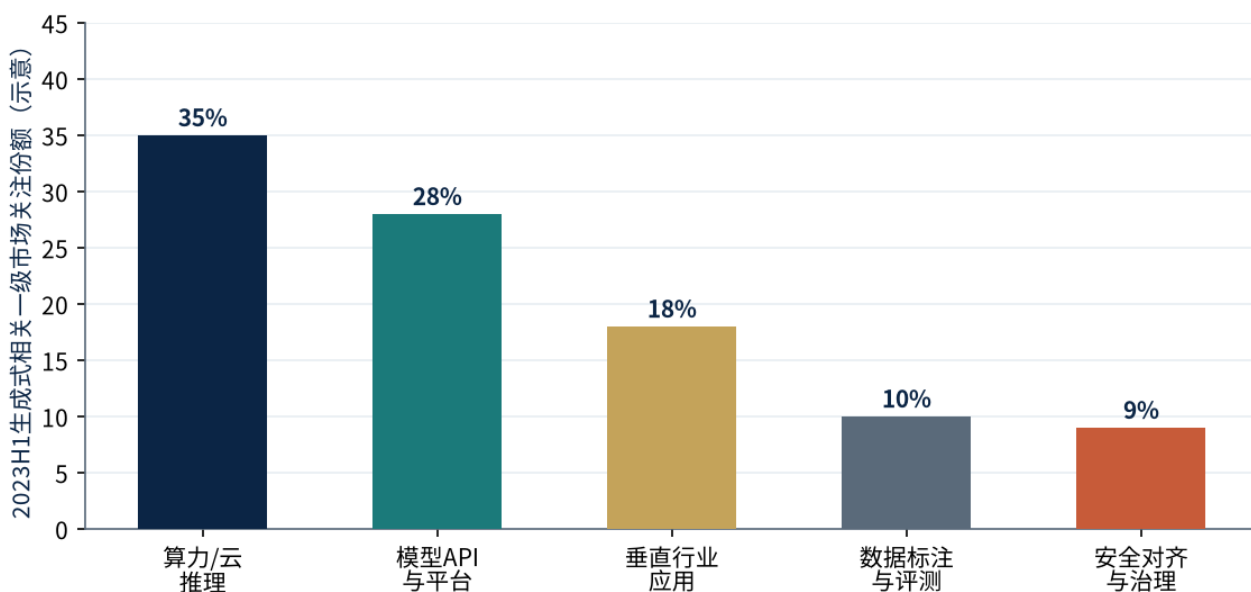
- 每个事业部最多并行 2 个受控试点；超额必须先关停僵尸项。
- 跨部门复用组件（网关/评测/词库）计入平台 KPI，而非仅计业务线。

7. 投融资与产业格局

7.1 结构：算力与平台为重心

2023 上半年生成式相关一级市场关注高度集中于算力/云推理与模型 API/平台；垂直应用、评测与安全治理份额上升但仍次之。

图 7-1 生成式投融资关注结构（2023上半年）



来源：本报告综合测算（公开融资事件与赛道热度，≤2023-06）

洞察：算力与API吸金最多——应用层必须证明工作流嵌入。

【图注 7-1】生成式投融资关注结构（2023H1示意）。来源：本报告综合测算。

7.2 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。

7.3 中国市场

大模型创业与云计算投入并行；生成式征求意见稿抬高公众服务门槛。ToB 知识助手与行业私有化更契合制度环境。

7.4 买方尽调清单（更新）

融资跑道、再训练条款、评测透明度、私有化交付能力、事故响应、多区域部署、开源成分与许可证。

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。算力与平台获关注；垂直应用比拼工作流与数据壁垒。

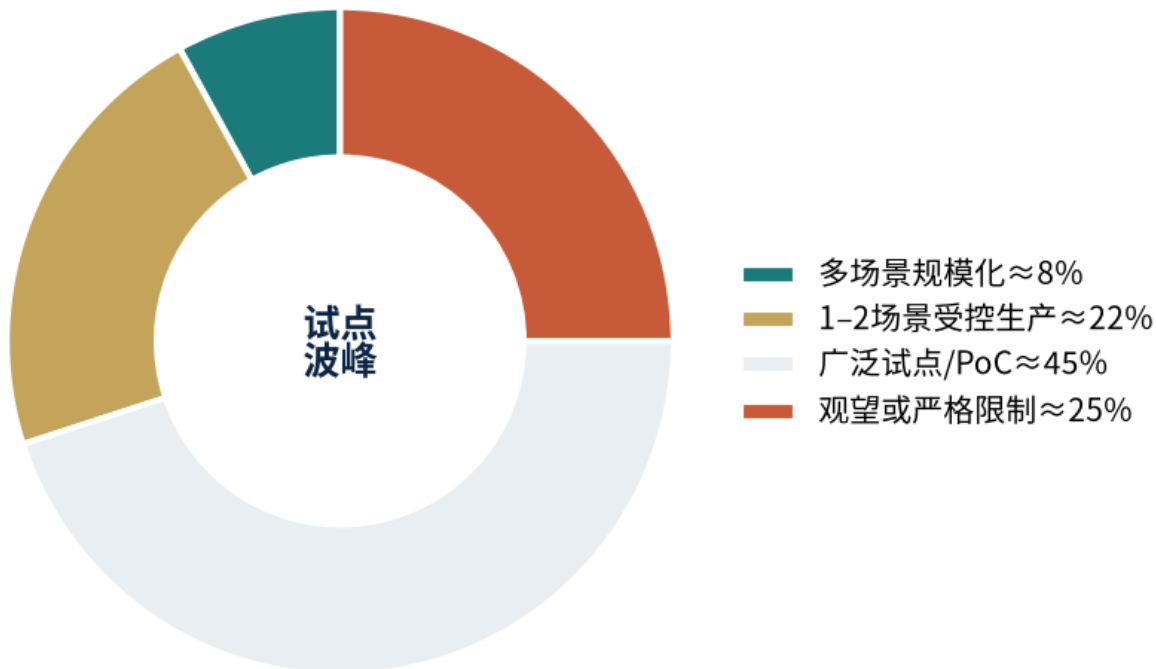
【案例框 | 供应商退出演练（示意）】

- 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：PoC 波峰

图 8-1 企业生成式成熟度分野（2023年中）



来源：本报告综合测算（公开采用调研与产业实践延伸）。

洞察：PoC波峰已现——2023下半年比拼转化而非立项数量。

【图注 8-1】企业生成式成熟度分野（2023年中）。来源：本报告综合测算。

洞察：下半年比拼转化而非立项数。

8.2 角色

新增或强化：提示/编排工程师、知识工程师、评测与红队、模型风险官、AI 产品经理。业务 Owner 仍是转化关键——没有 Owner 的试点应关停。

8.3 培训

从「认识 Chat」转向：任务说明书、验收标准、保密红线、如何读引用。管理层培训重点是投资纪律与风险分级。

8.4 运营机制

建议设立双周试点评审：转化/停损/并入平台。CoE 提供参考架构与共用组件，业务部门提供场景与验收。

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】

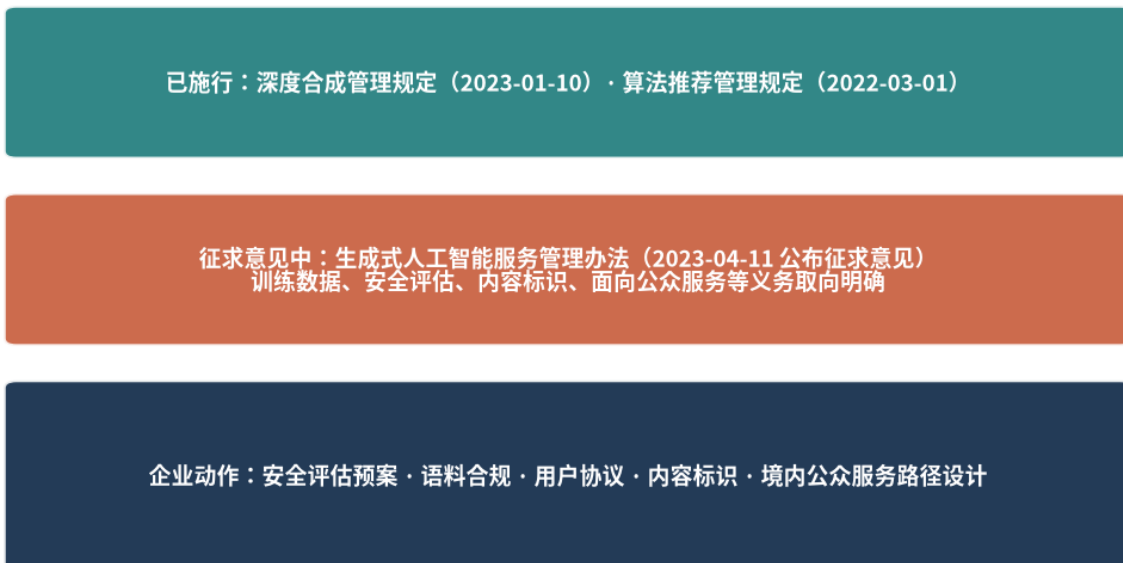
- 公布客观门槛（评测、Owner、单位经济）；给予整改窗；逾期失去预算。
- 把关停解释为保护可规模化场景，而非否定创新。

9. 治理、风险与监管窗口

9.1 中国合规节奏（截至2023-06）

深度合成规定已施行；生成式服务管理处于征求意见阶段，取向覆盖训练数据、安全评估、标识、面向境内公众服务等。算法推荐规定持续有效。

图 9-1 中国生成式合规节奏（截至2023-06）



来源：监管公开文本（网信办等）。欧盟AI法案提案风险分级仍为在欧对标基线。

洞察：正式办法尚未落地，但征求意见稿已足够驱动产品与法务预整改。

【图注 9-1】中国生成式合规节奏（截至2023-06）。来源：监管公开文本。

9.2 风险优先级

公开调研与产业实践共同指向：不准确/幻觉、数据泄露、知识产权、有害内容、供应商依赖。缓解顺序建议：数据分级与网关 → 评测与引用 → 人工审核 → 合同条款 → 红队。

9.3 最小控制集（2023年中）

1. 公司级三轨策略与工具白名单；
2. 模型网关（鉴权、日志、脱敏、配额）；
3. 高影响输出人工签发；
4. 面向公众内容标识策略；
5. 征求意见稿预整改差距表；
6. 第三方尽职调查与退出演练。

【行动建议框】

采用速度可以快，但风险缓解必须「同表」。先扩后治的纠错成本在生成式时代更高。

9.4 跨境与数据主权

公共 API 默认视为潜在出境路径。核心身份、客户隐私、未公开财报、源代码不得粘贴。分区部署与专有实例应进入架构标准。

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**。生成式管理处于征求意见阶段，取向覆盖训练数据、评估与标识——按终稿可能方向预演。

【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

起点：2023年6月；展望至 2024中至 2025中。管理推演，非点预测。

10.1 基准情景（中高概率）

- RAG 与办公嵌入成为主流生产形态；代理保持实验；
- 生成式正式监管文本落地预期升温，预整改企业更从容；
- API 价格竞争加剧，但评测与治理投入上升；
- PoC 大浪淘沙，转化率成为预算门槛。

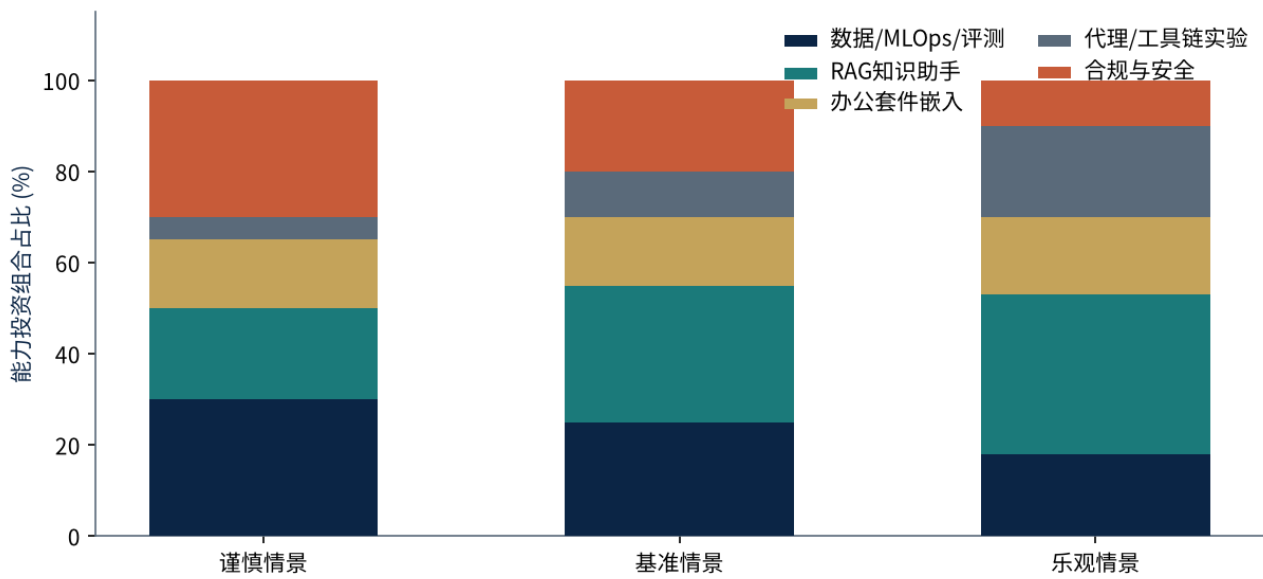
10.2 乐观情景

- 单位成本显著下降，中型企业维持多条生产工作流；
- 行业可复制模块（合同、客服、知识）出现；
- 多模态文档理解进入规模化。

10.3 谨慎情景

- 重大幻觉/泄密事件引发收紧；
- 预算冻结，仅保留证明 ROI 的场景；
- 算力或合规成本抬高，放慢私有化。

图 10-1 三情景投资组合（2023-06起点）



来源：浩瀚博策情景推演（2023-06起点）；非点预测。
洞察：基准情景下，RAG与评测底座应占最大权重。

【图注 10-1】三情景投资组合（2023-06起点）。来源：浩瀚博策情景推演。

10.4 触发指标

触发器	乐观	谨慎
试点转化率	连续两季>40%	连续两季<15%
P1 事件	无	监管关注或重大误导
API 单位成本	下降>25%	账单失控
合规差距	按期关闭	主场景须下线

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6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
API 账单	熔断有效	创新预算被吞噬

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（至约 2023年9月）

序号	行动	产出
1	公布三轨策略与白名单	架构一页纸
2	压缩试点名录至 3-5 个	宪章+评测集
3	上线模型网关最小版	日志与配额
4	征求意见稿预整改	差距表
5	设定 API 熔断线	CFO 会签

11.2 未来 12 个月（至约 2024年中）

- ≥2 场景完成受控生产并公布单位经济；
- 企业 RAG 平台与提示词登记成为默认；
- 高风险用例全覆盖 RAI 控制；
- 业务团队完成验收素养培训；
- 多供应商与私有化预案就绪。

11.3 董事会问题清单

- 本季转化率与关停了哪些僵尸 PoC？
- 幻觉与泄密事件态势如何？
- API/推理成本是否在熔断线内？
- 预整改差距关闭进度？
- 人才缺口在工程师还是业务 Owner？

11.4 行业定制

- **银行保险**：RAG 内勤优先；MRM 覆盖生成式。
- **零售**：文案+词库；禁止无审对外。
- **制造**：维修知识 RAG；质检主线不变。
- **医疗**：文书试点；诊疗严循路径。
- **软件**：代码辅助+保密隔离。
- **平台**：标识与内容安全与增长同设计。

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6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。

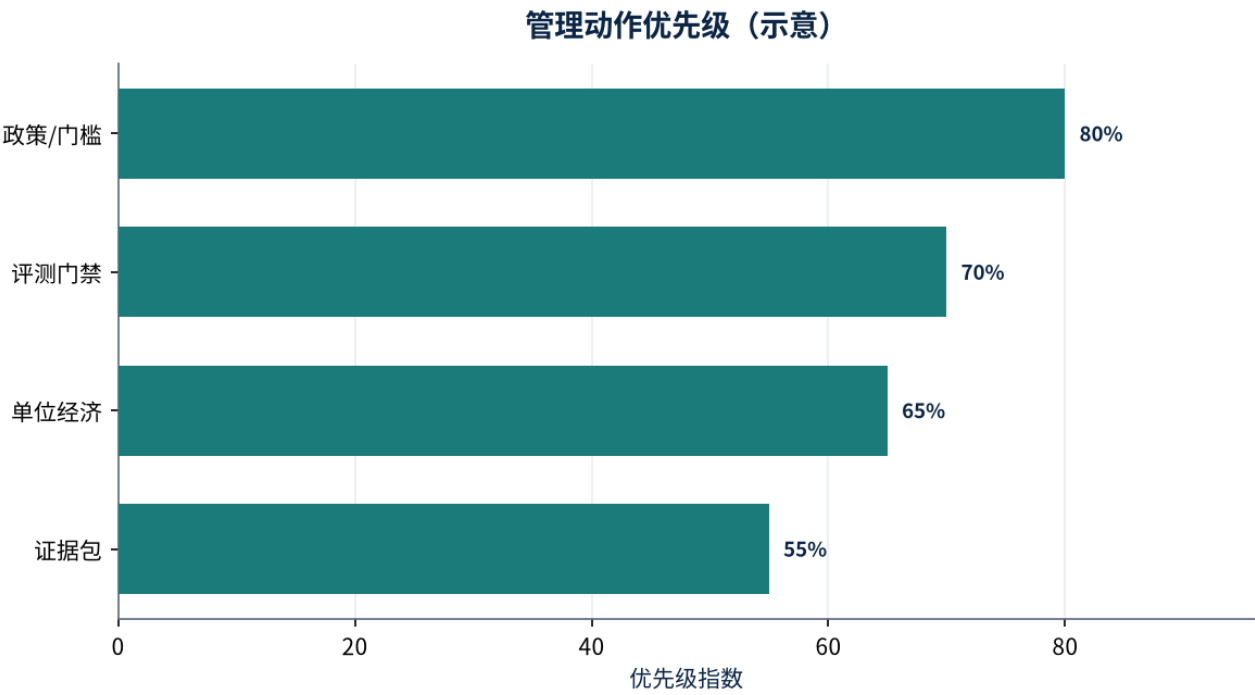
11.6 跨职能协同节奏

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：** 企业版工作区 + 引用强制；自动决策不放宽。
- **零售：** 导购草稿快试，广告法词库前置。
- **制造：** 工艺 RAG + 质检；禁止生成改写控制参数。
- **医疗：** 文书与临床分轨。
- **软件：** 代码辅助 + 客户代码隔离与许可证扫描。



来源：本报告综合测算（≤2023-06-30）

洞察：先立规矩与门禁，再扩场景。

【图注 11-1】 行动与监督优先级示意。**来源：**本报告综合测算（≤2023-06-30）。**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	标题	主来源（≤2023-06-30）
图 3-1	职能渗透	公开市场调研综合
图 4-1	企业态势指标	公开市场调研综合
图 4-2	关注指数	本报告综合测算
图 4-3	立项优先级	本报告综合测算
图 5-1	三轨策略	本报告综合测算
图 5-2	时间线	监管公开文本/公开技术节点
图 6-1	价值矩阵	本报告综合测算
图 6-2	热力图	本报告综合测算
图 7-1	投融资结构	本报告综合测算
图 8-1	成熟度	本报告综合测算
图 9-1	监管节奏	监管公开文本
图 10-1	情景组合	本报告情景推演

附录 A | 术语表

术语	含义
RAG	检索增强生成
模型网关	统一鉴权、日志、脱敏、配额的推理入口
旗舰多模态	支持图像+文本等输入的高性能模型
代理	多步骤工具调用系统
预整改	依据征求意见稿提前补齐义务

附录 B | 场景评分卡

维度	权重
价值潜力	20%
数据敏感性（逆向）	20%
评测可行性	15%
审核可负担	15%
合规复杂度（逆向）	15%
平台复用	15%

附录 C | 高管话术

「生成式已经从新闻变成预算科目。我们不追求人人有账号，而追求少数场景在评测、成本与合规上可审计地贡献人效。三轨技术可以并行，但治理底座只有一套。下半年看转化率。」

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6月30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 2023-06-30。

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 春夏企业生成式采购意向、董事会讨论、风险缓解等公开口径（含约 59% 已采购或计划采购等）。
2. 公开技术节点：开源权重研究社区释放、旗舰多模态与对话助手、办公套件集成公告等（均 ≤2023-06）。
3. 国家互联网信息办公室等.《互联网信息服务深度合成管理规定》（2023-01-10 施行）。
4. 国家互联网信息办公室.《生成式人工智能服务管理办法（征求意见稿）》（2023-04-11）。
5. 国家互联网信息办公室等.《互联网信息服务算法推荐管理规定》（2022-03-01 施行）。
6. European Commission. AI Act 提案（2021-04）及后续立法进程公开信息（至2023-06）。
7. OECD AI Principles（2019）。
8. 本报告综合测算与情景推演（浩瀚博策，2023-06）。

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 上半年公开研究观点，供讨论参考，不构成投资建议。***浩瀚博策 · 2023年6月** *知识截止：2023年6月30日* © 2023 北京浩瀚博策咨询有限公司