

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

2025年下半年，行业叙事从「冲击与复现」转向「可靠性与运营纪律」。推理能力进入更多生产路径；代理系统在客户支持、研发与内部运营中扩大受控试点；欧盟与中国义务在日常发版中被例行检查。董事会较少追问「是否要做 AI」，更多追问「事故率、单位成本、合规节点是否按期」。

截至 **2025年12月31日**：

第一，推理从专项预算变为能力目录中的一档，与快模型、检索增强并列配置。

第二，代理入轨的关键是可观测性： 工具调用链、回滚、人工接管与业务 KPI 对齐，而不是更炫的自主演示。

第三，可靠性指标（幻觉率、任务成功率、P1 事故、漂移）进入经营仪表盘，与收入并排。

第四，合规成为发布流水线的自动门禁，而非专项运动。

第五，人才结构向「平台 SRE + 业务 Owner + 风险官」三角稳态演化。

【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】

代理围栏、可靠性看板、误操作上限。

1A. 给经营层的「代理放量」对话脚本

当团队展示代理自动完成多步任务时，请追问四句：（1）哪些工具在白名单外？（2）步数与金额上限是多少？（3）副作用评测用例有哪些？（4）一键停用是否演练过？四问答不清，演示停留在实验室。

可靠性竞赛的奖赏属于能把事故 MTTR、评测通过率与可用性放进经营例会的组织。代理不是更聪明的聊天，而是带执行力的自动化——执行力必须配刹车。

对所有读者的共同约束：不把单价、演示或开通数当成成功；成功定义为受控生产、单位经济与证据包三者同时成立。

2. 研究范围、方法与知识截止

2.1 研究问题

1. 截至知识截止日，全球 AI 市场、技术与资本处于何种位置？
2. 哪些行业与职能已显现可规模化价值？
3. 组织、人才与治理如何决定转化率？
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：** 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	2025年12月31日
发布设定	2025年12月（2025下半年报告）
禁止引用	截止日后的新产品世代与未发生监管终局
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 | 可靠性成为竞赛主维度】

可用性、评测通过率、事故 MTTR 进入经营看板；「能演示」不再加分，「能稳态」才加分。

【判断 2 | 代理入轨但必须围栏】

工具调用与多步编排进入更多试点；生产前提是白名单、步数、金额/操作上限与完整轨迹。

【判断 3 | 推理常态化要求成本纪律】

深思不再是新闻，而是可选资源。路由与预算熔断决定毛利。

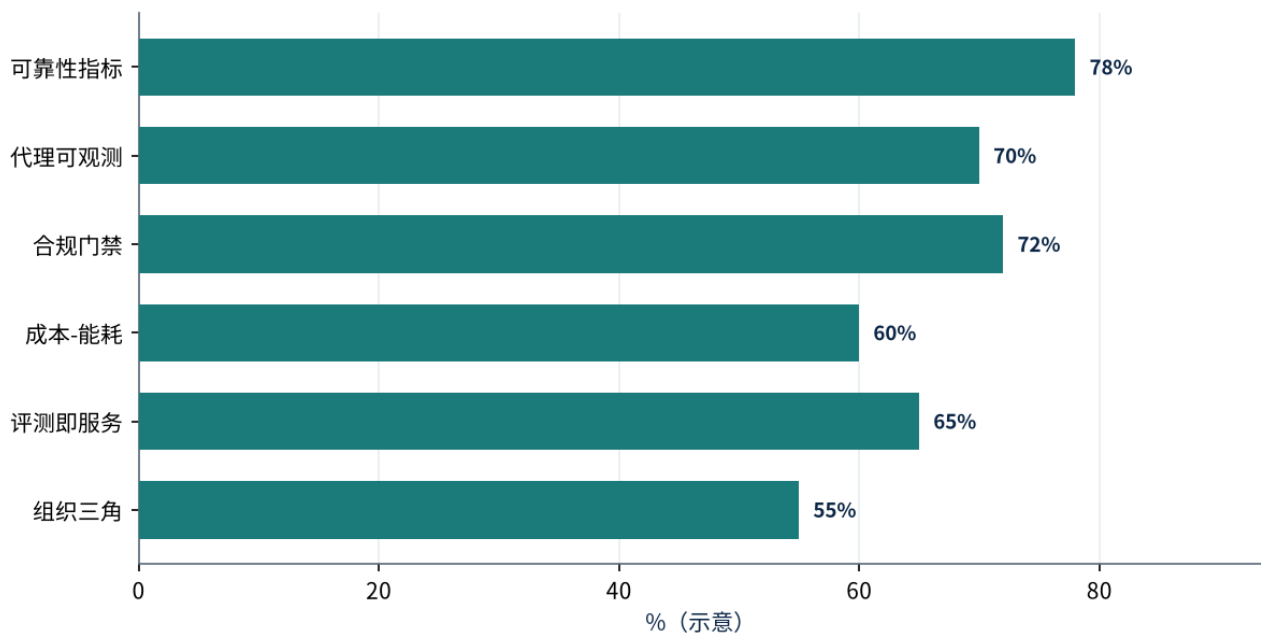
【判断 4 | 误操作风险被低估】

代理一旦可写促销规则、工单或支付指令，损失可瞬时放大。演练与上限必须先于放量。

【判断 5 | 治理证据决定出海与招采】

检查与客户尽调更频繁要求证据包；无变更控制的系统难以进入合格供应商名录。

图 3-1 2025年末优先级



来源：公开市场调研综合 / 本报告综合测算（≤2025-12）

洞察：平台与评测优先于新模型尝鲜。

【图注 3-1】 2025年末可靠性与代理围栏优先级。来源：公开市场调研综合 / 本报告综合测算（≤2025年12月31日）。洞察：稳态指标重于演示指标。

4. 全球市场与需求图景

4.1 采用与规模化

可靠性与代理围栏成为采购评分项；「能演示」不再加分，「能稳态」才加分。
买方关注点转向可验收指标与平台能力，而非单点模型新闻。

4.2 支出结构

基础设施、服务、API/推理、评测与人工审核共同构成 TCO。降价不等于降本。

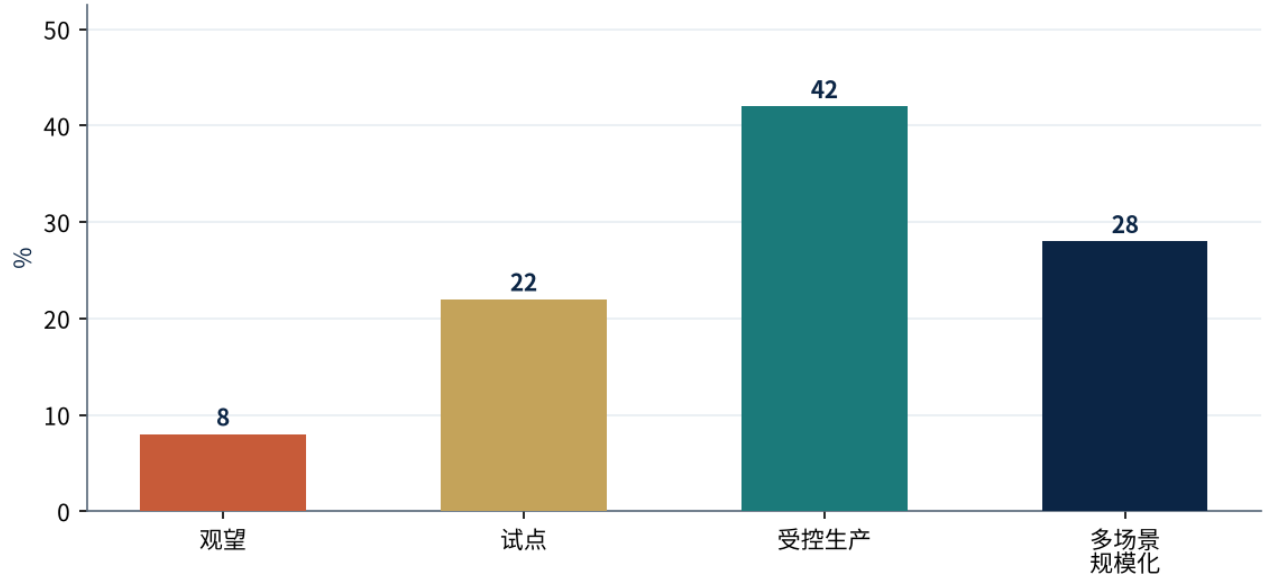
4.3 区域与合规

产品与数据流须按司法辖区拆分；合规证据进入采购评分。

4.4 测量

人效与质量须对照实验；自我报告不足以下预算结论。

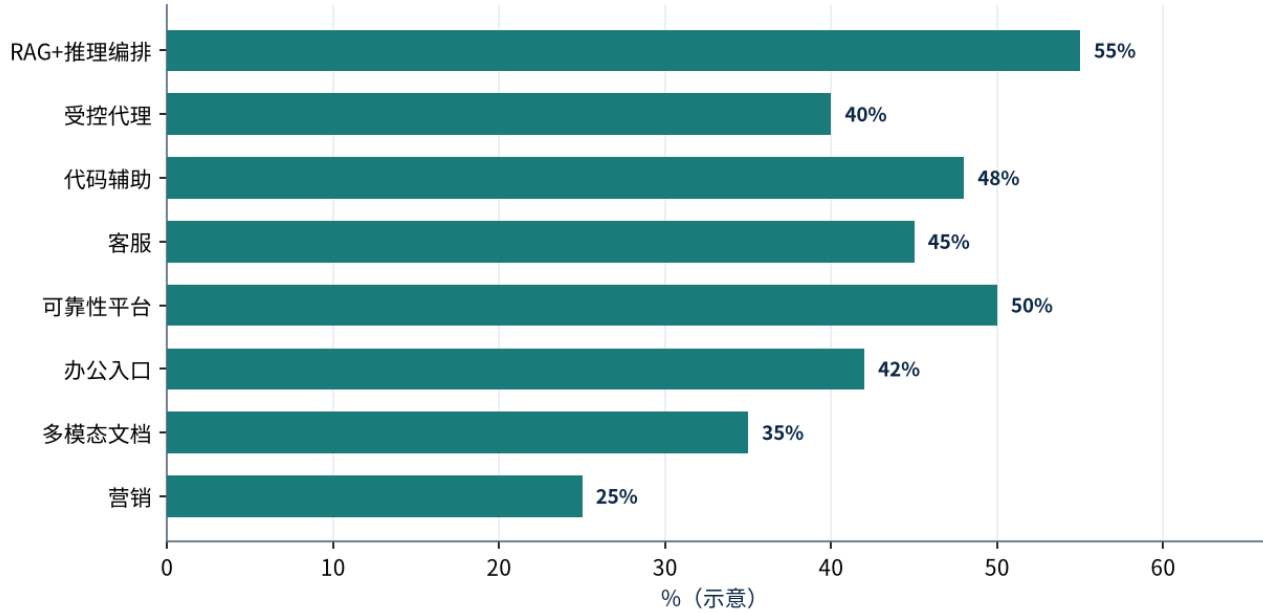
图 4-1 成熟度 (2025年末)



来源：公开市场调研综合 / 本报告综合测算 (≤2025-12)

洞察：受控生产成为中位数目标。

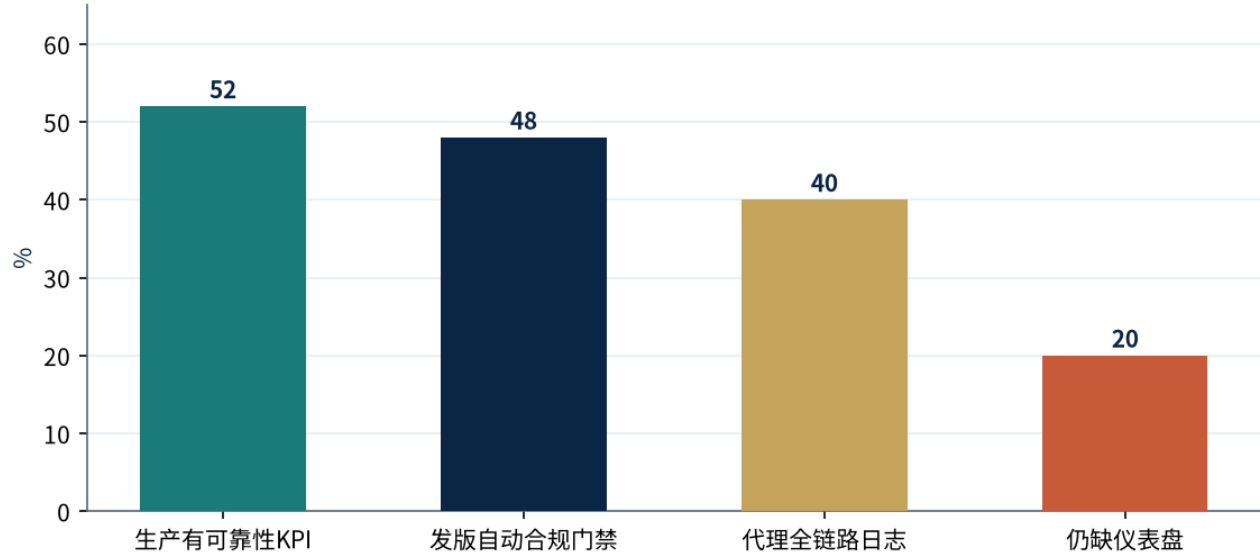
图 4-2 场景热度 (2025H2)



来源：公开市场调研综合 / 本报告综合测算 (≤2025-12)

洞察：RAG与生产力场景居前。

图 4-3 可靠性与门禁覆盖



来源：公开市场调研综合 / 本报告综合测算（≤2025-12）
洞察：三者齐全者仍是少数。

买方采购评分中，可靠性与代理安全权重上升。市场热度从「新模型发布」转向「谁能在真实工单上连续 90 天稳定达标」。影子采用若仍大量存在，说明正式服务目录体验不足——应用体验与治理工具同步投入。

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。

可靠性与代理围栏成为采购评分项；「能演示」不再加分，「能稳态」才加分。

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。

4A. 本期深度洞察：代理入轨与可靠性竞赛

当模型能够调用工具、操作电脑或编排多步任务时，企业 AI 从「生成内容」进入「执行动作」。执行动作的价值更高，失败代价也更高。本期核心命题不是「要不要做代理」，而是「代理的围栏是否先于放量」。

可靠性竞赛的评分表建议如下：

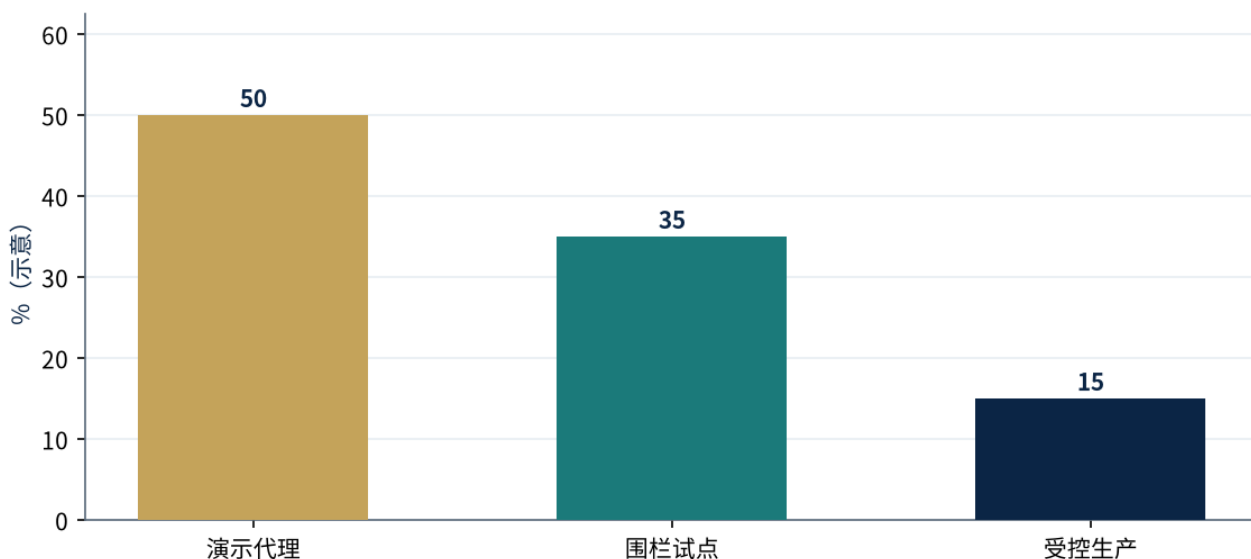
维度	生产门槛（示例）
可用性	关键路径月度可用性目标
评测	代理任务集回归通过
副作用	不可接受副作用用例为零容忍
观测	轨迹、工具、成本、错误全量可得
停用	一键停用开关经演练

【案例框 | 客服退货代理】

- 允许：查询订单、起草回复、创建工单草稿。
- 禁止：直接改价格、直接退款超阈值、绕过风控名单。
- 超金额或改主数据必须人工确认；轨迹保留不少于审计要求天数。

把代理演示直接写进经营计划，而不附带围栏与副作用评测，等于把自动化风险外包给运气。董事会应要求：任何可写生产系统的代理，先看演练记录，再看业务 case。

代理成熟度分野（2025年末示意）



来源：本报告综合测算（≤2025-12-31）

洞察：演示多、生产少——围栏决定能否放量。

【图注 4-4】本期关键结构示意图。来源：本报告综合测算（≤2025-12-31）。洞察：结构重于总量——用分层指标做决策。

5. 技术演进

5.1 技术焦点（展开）

代理框架与计算机操作能力吸引实验；推理调用常态化；观测（轨迹、工具调用、成本、错误类型）成为平台标配。没有观测的代理等于没有刹车的自动化。

5.2 工程与围栏

默认拒绝：未登记工具、超步数、超金额、无人工确认的生产写入。评测集增加「代理任务成功但副作用不可接受」类用例，避免只优化任务完成率。

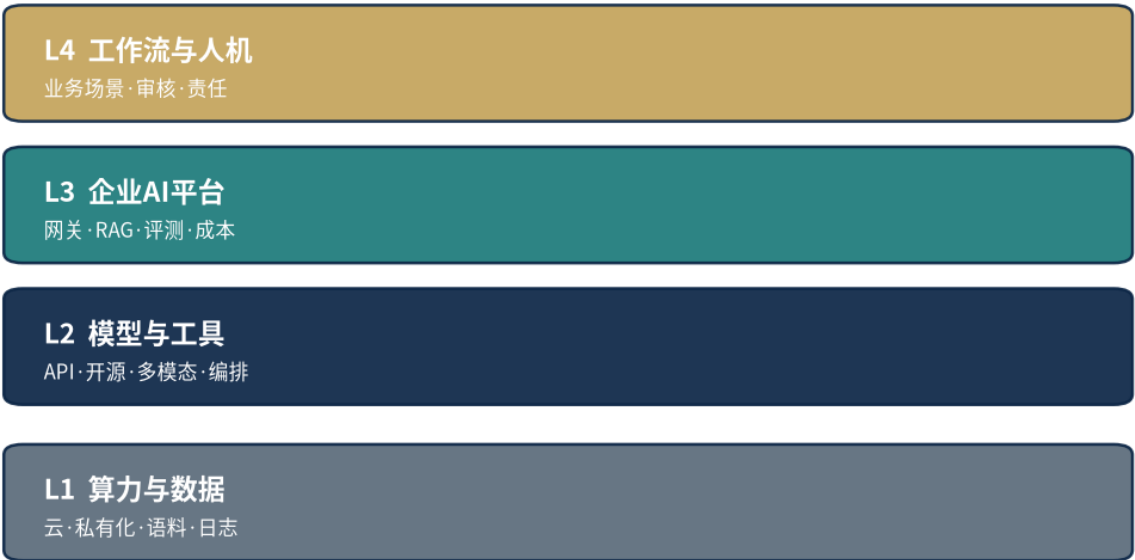
5.3 人机协同

高影响步骤保持人工签发；把人工审核负荷纳入单位经济，而不是假设审核免费。

5.0 本期技术要点摘要

推理、多模态、工具调用与记忆机制在平台中编排。重点工程：端到端追踪、评测即服务、混沌/故障注入、模型卡自动生成、能耗与成本联合优化。学术与产业对推理训练方法的公开讨论升温，但企业采纳以可验证基准为准。

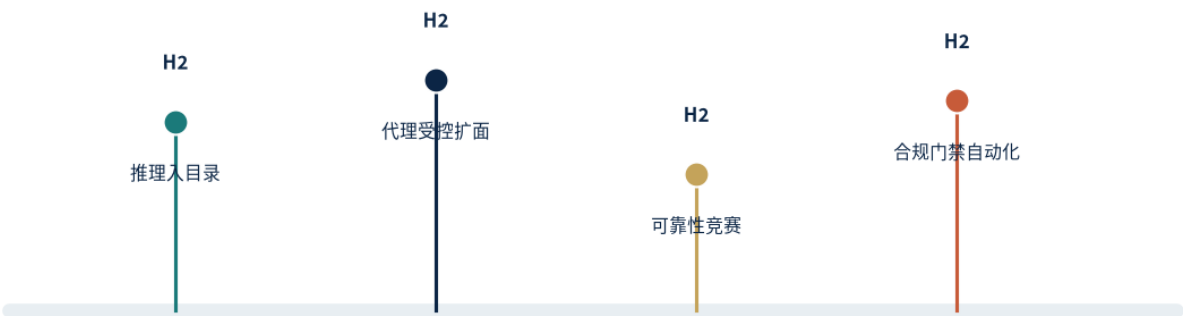
图 5-1 企业AI技术栈



来源：公开市场调研综合 / 本报告综合测算（≤2025-12）

洞察：平台层决定转化率。

图 5-2 2025下半年主题节点



来源：监管公开文本与公开技术节点（≤2025-12-31）

洞察：供给与合规并行。

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。代理步数、工具白名单、金额/操作上限与完整轨迹日志成为生产前提。

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】

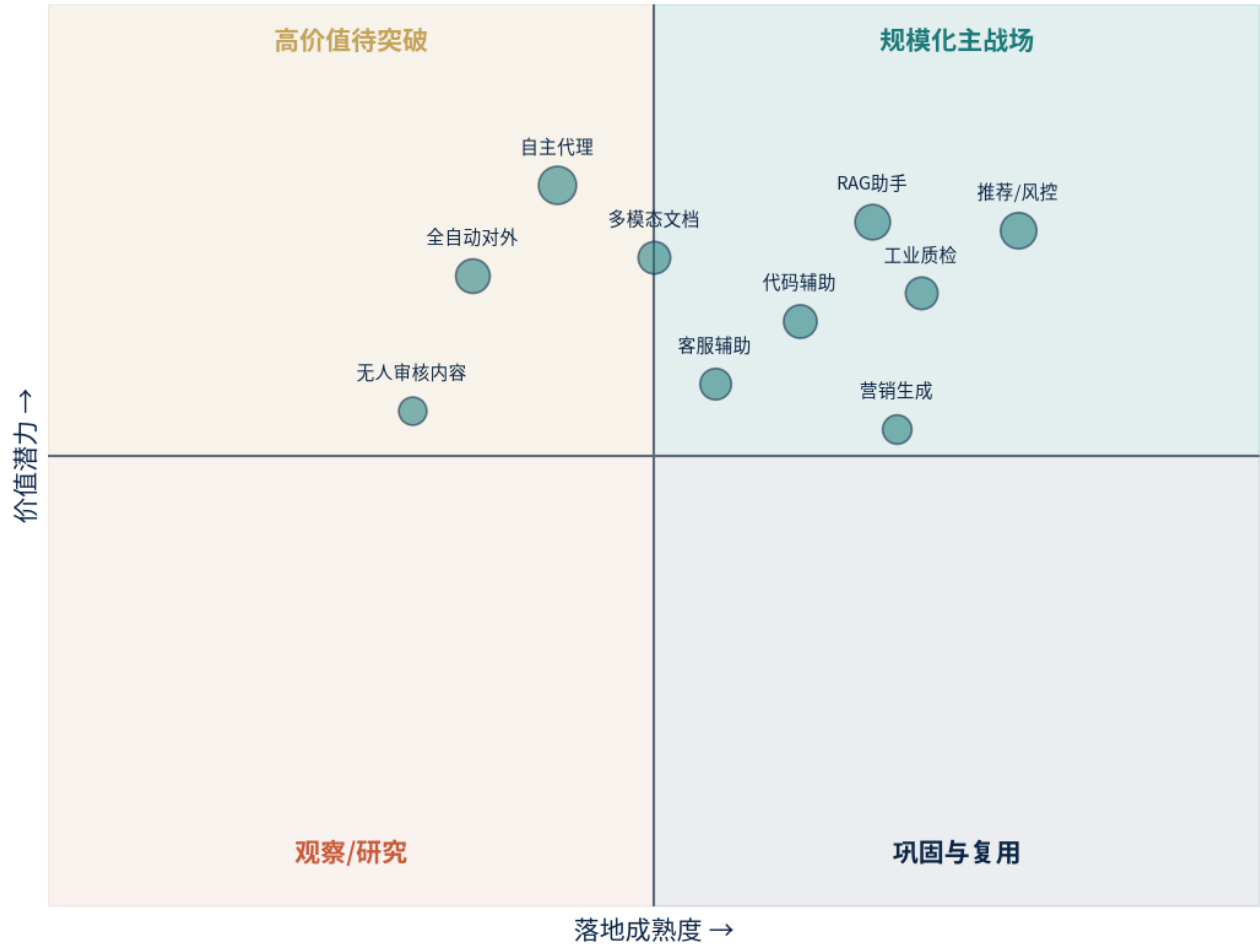
- 先止血：统一网关日志与月度成本看板。
- 再提质：黄金集 + 红队 + 引用强制。
- 后扩面：多场景复用同一平台组件。

6. 跨行业落地：价值池与成熟路径

6.1 总览

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



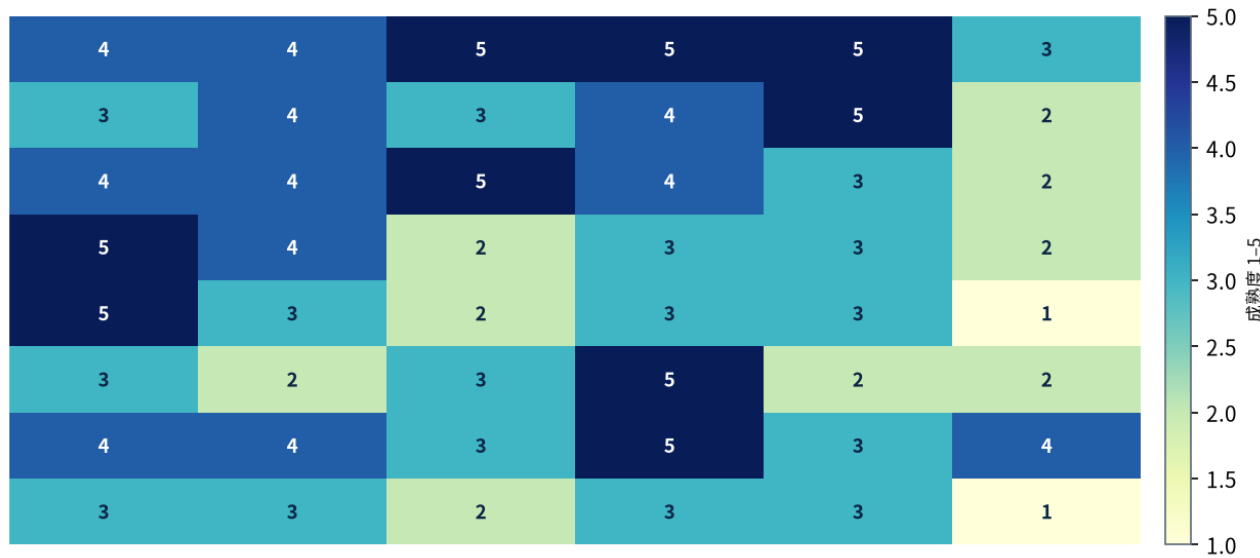
来源：本报告综合测算

洞察：右上象限优先。

洞察：能力组合决定差异化。

来源：本报告综合测算

图 6-2 行业×能力热力



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。代理入轨实验增多，生产坚持白名单工具与人工确认。

【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 $\leq 3\%$ 、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。库存代理若误操作促销规则，损失可瞬时放大——必须步数与金额上限。

【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。

代理编排文献与文书可以，触达医嘱系统必须双重闸门。

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」。

可靠性竞赛：可用性、评测通过率、事故 MTTR 成为看板。

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. 代理演示代替验收。

【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 结构

可靠性与代理安全细分出现融资关注；同质化编排层承压。买方愿为可观测与可回滚付费。

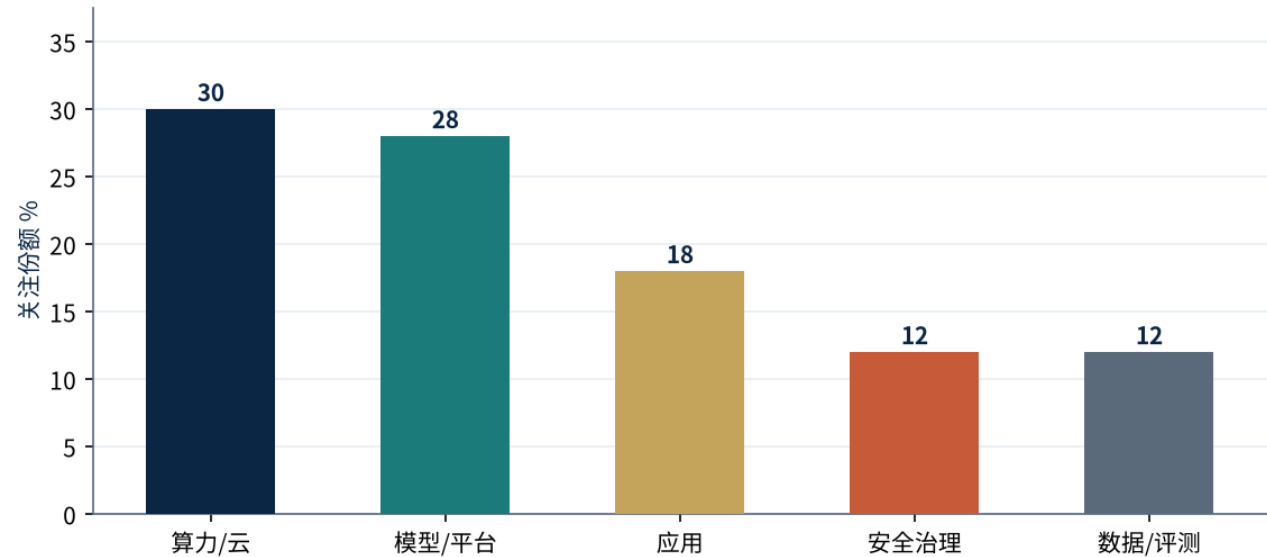
7.3 尽调更新

增加：误操作演练记录、轨迹保留策略、金额上限配置权、紧急停用开关证明。

7.1 结构与气氛

资金流向：可靠性工具、评测、安全、垂直 workflow、高效推理基础设施。纯模型层创业更难独立融资，常走向平台或被收购。

图 7-1 投融资关注结构



来源：本报告综合测算
洞察：基础设施与平台仍居前。

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。可靠性与代理安全创业细分出现；同质化编排层承压。

【案例框 | 供应商退出演练（示意）】

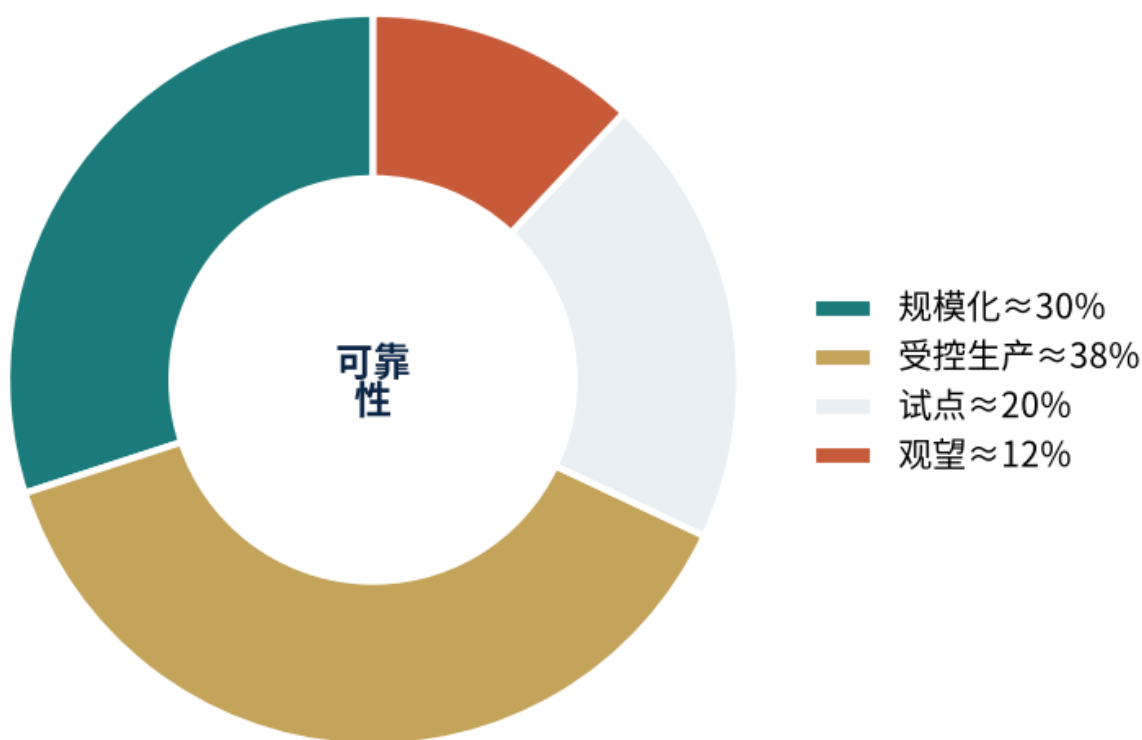
- 每半年一次：在 72 小时内切换备用模型路由，验证检索与评测门禁仍可用。
- 成功标准：主场景可用性不中断；日志与证据包完整。

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（2025年末）



来源：本报告综合测算

洞察：从项目制走向经营化。

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。

8A. 人才与激励：可靠性竞赛中的岗位重估

代理与观测体系需要新型岗位：轨迹分析、工具治理、副作用评测、应急停用值班。传统「提示词工程师」头衔不足以覆盖生产责任。建议在岗位说明书中写明：可写生产系统的代理变更权限、演练频率与事故升级路径。

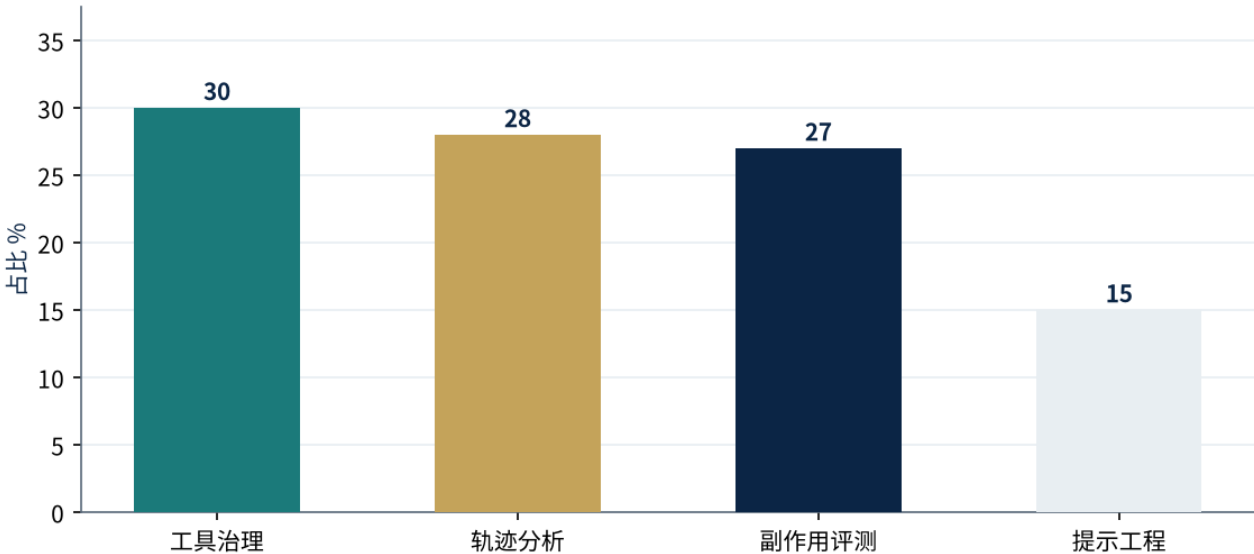
激励上，奖励「稳态运行天数」与「误拦截后的快速恢复」，而不是「代理完成步数」。完成步数可以被刷，稳态与低副作用不能。

【要点框 | 岗位】

- 代理生产须有命名的工具治理 Owner。

- 红队与业务验收分离，避免既当运动员又当裁判。
- 半年至少一次跨部门误操作桌面推演。

代理生产相关岗位权重（示意）



来源：本报告综合测算（≤2025-12-31）

洞察：治理与评测权重大于提示词本身。

【图注 8-2】组织能力结构示意图。来源：本报告综合测算（≤2025-12-31）。洞察：编制与激励必须跟随生产形态变化。

9. 治理、风险与监管窗口

9.2 代理相关义务

自动化决策与代理操作的人工监督证据成为检查重点。预设：幻觉对外错误陈述、数据泄露、深度伪造冒充、代理误操作。

9.3 控制集补充

工具白名单变更审批、步数/金额上限、轨迹日志留存、紧急停用、半年一度误操作演练。

9.1 监管节奏与企业含义

义务例行化：高风险变更控制、日志留存、事件报告演练。跨境产品维持分区拓扑。深度伪造与合成媒体标识在营销与客服全覆盖。

图 9-1 合规运营化窗口



来源：监管公开文本
洞察：合规成为产品节奏约束。

【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**。代理与自动化决策的人工监督证据成为检查重点。

【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 2025年12月。

10.1 基准情景

代理在白名单场景受控生产；可靠性看板进经营例会；推理成本受控；证据包标准化。

10.2 乐观情景

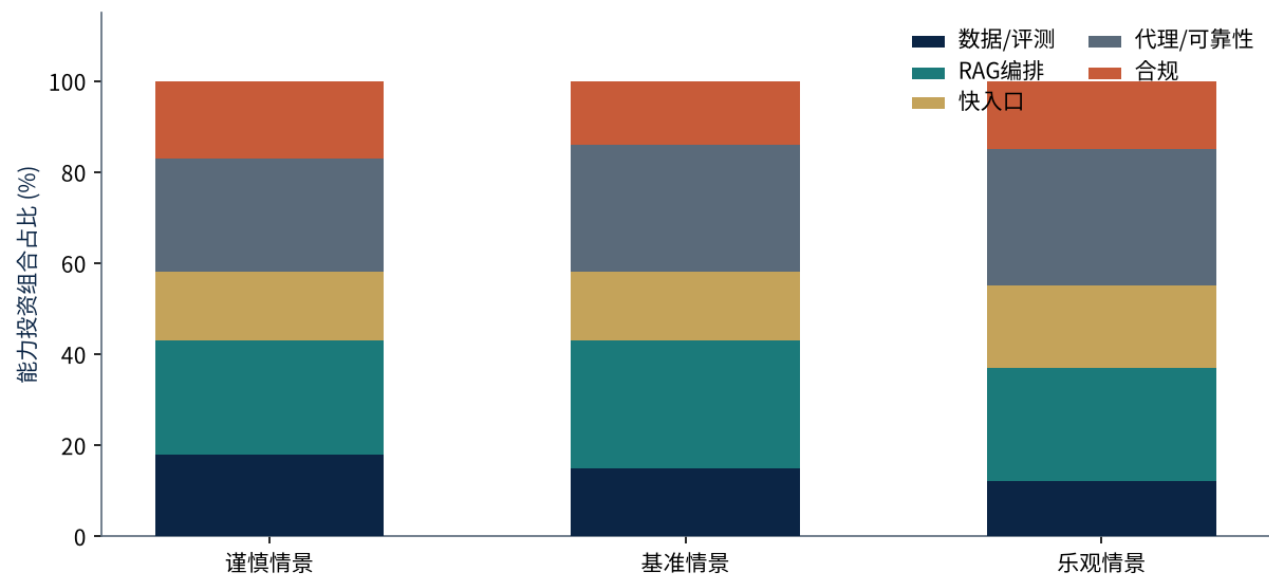
可回滚代理显著降低人工负荷；行业出现可采购的围栏组件；事故率稳中有降。

10.3 谨慎情景

重大误操作引发全面禁用代理；保险与合规成本上升；未建观测的组织被迫回退到纯人工。

企业含义：2026 年是「可靠性年」——先围栏，后放量。

图 10-1 情景（2025-12起点）



来源：浩瀚博策情景推演；非点预测
洞察：基准情景仍以平台与RAG为重心的。

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 2025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
代理误操作	被围栏拦截	造成资金/数据损失

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	可靠性仪表盘	含P1与幻觉
2	代理可观测性	全链路追踪
3	合规自动门禁	接入CI
4	能耗-成本联合看板	财务会签
5	组织三角编制	HR确认

11.2 未来 12 个月

可靠性达标合同化；代理 ≥ 2 场景受控；合规门禁全覆盖生产发版；人才三角到位。

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 2025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。

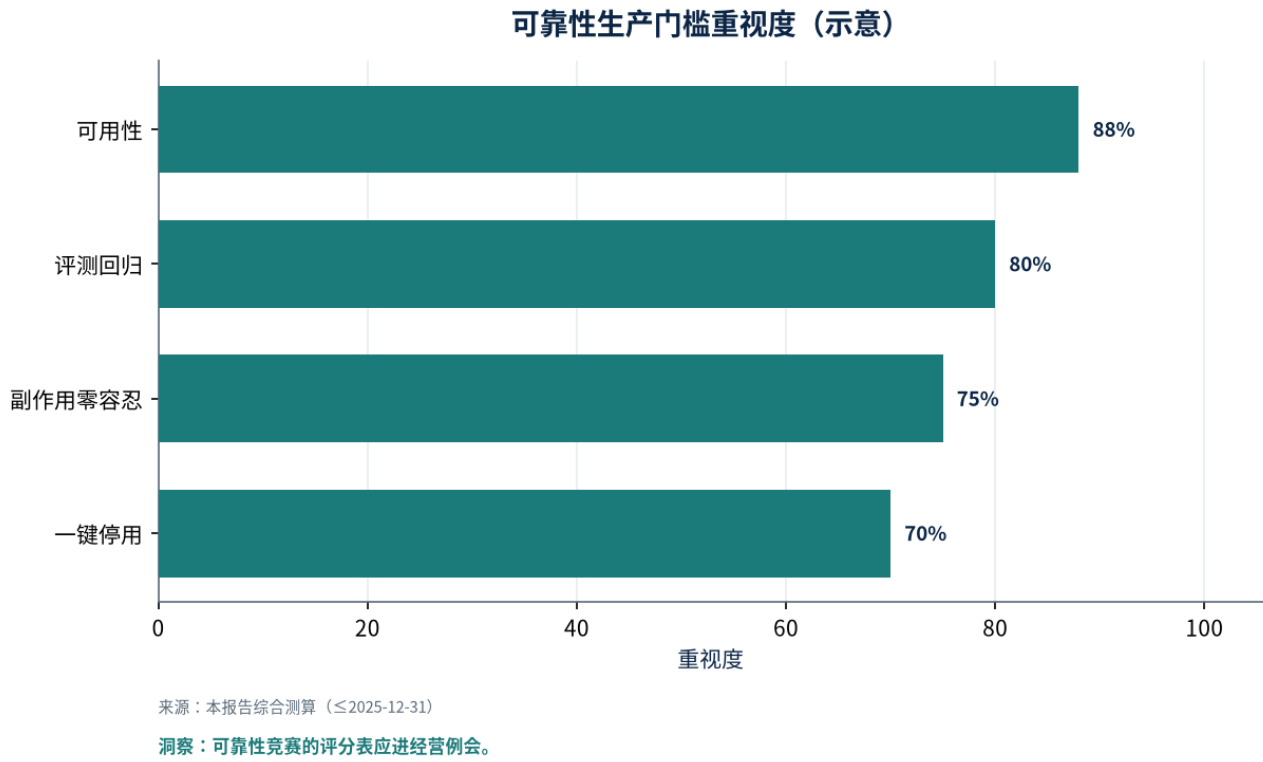
11.6 跨职能协同节奏

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：** 代理白名单与金额上限。
- **零售：** 促销规则变更必须人工确认。
- **制造：** 工单代理步数限制。
- **医疗：** 触达医嘱系统双重闸门。
- **全行业：** 可靠性看板进经营例会。



【图注 11-1】行动与监督优先级示意。来源：本报告综合测算（≤2025-12-31）。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 ≤2025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-2025-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：2025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 2025-12-31。

附录 I | 董事会一页纸模板

栏目	填写
本季转化/关停	
单位成本与熔断	
高风险清单覆盖	
P1 事故与 MTTR	
合规里程碑	
下季三项投资	

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：2025下半年企业AI可靠性、代理与成本口径。

2. 监管公开文本：欧盟分阶段义务与中国生成式等相关规定。

3. 公开技术节点：推理/代理/评测工程实践（≤2025-12）。

4. 组织能力结构示意图（图 8-2）与行动优先级图见正文。本报告综合测算（浩瀚博策，2025-12）。

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 2025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 · 2025年 12月** *知识截止：2025年12月31日* © 2025 北京浩瀚博策咨询有限公司