



CHINA AI MARKETING / ECOSYSTEM ATLAS

中国 AI 营销 产业生态图谱

沿经营价值流识别能力层、供给角色、连接接口与治理边界，帮助企业组合一套可运营、可观察、可替换的 AI 营销行动系统。

[阅读完整报告 ↓](#)

[下载 PDF 版本](#)

看清生态的真实主轴

不按厂商清单采购，按经营价值流识别能力

划清平台与工具边界

区分模型、SaaS、Agent、工作流与营销 OS

验证演示之外的能力

用真实接口、异常、成本和退出检验 PoC

形成可替换的组合

把企业控制层与外部能力层分离

竹势 AI 营销智库出品

shichangbu.ai

出版说明

本报告面向企业董事会、经营层、营销与数字化负责人，以及营销技术采购、产业投资和生态合作负责人。报告把“中国 AI 营销产业”定义为：围绕市场感知、客户理解、策略决策、内容与创意、渠道与广告、客户运营、AI 搜索可见性、执行编排、效果反馈和治理控制，提供模型、数据、软件、平台、媒体能力、专业服务与基础设施的供给网络。

本报告不采用“工具大全”或静态厂商名单口径。许多企业同时承担模型提供者、云平台、媒体平台、数据平台、SaaS 与实施服务等多种角色；分类仅用于解释其在特定价值链位置上的主要能力。所有厂商与产品均为非穷尽的公开实例，不构成排名、背书或采购推荐。

报告区分三类证据：法律法规与国家标准；政府、监管机构、企业官方产品资料和公开披露；公开案例与行业研究。平台自述只能证明其宣称的能力范围，不能替代企业在自身数据、流程、权限和风险环境中的 PoC 验证。没有可靠公开证据的市场份额、客户效果、商业关系或性能数字不予估算。

截至时间为 2026 年 7 月。由于模型、接口、平台政策和监管要求变化较快，企业在采购和上线前应复核最新条款、备案状态、数据处理安排与内容标识要求。

阅读地图

表 1 读者决策地图

读者	优先阅读章节	需要形成的决策
董事会/CEO	执行摘要、第1、8、11、12章	投资边界、风险偏好、阶段目标与退出机制
CMO/增长负责人	第2–7、10–12章	场景组合、业务闭环、供应商组合与运营机制
CIO/数字化负责人	第3、6、7、9、11章	架构、接口、身份权限、可观测性和替换策略
采购/法务	第8、9、12章及附录	尽调、PoC、合同、SLA、数据可携带与责任边界
产业投资/生态合作	第1、3、5、6章	供给角色、价值池、互补关系与平台锁定风险

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

执行摘要：生态选择的核心是经营闭环，不是功能数量

经营判断

生态选择的核心不是功能数量，而是企业能否把目标、状态、决策、行动与反馈接成一条可治理、可替换的经营闭环。

企业采购 AI 营销能力的最小单位，应由“可观察的业务闭环”替代“软件账号”或“模型调用量”。

中国 AI 营销生态正在经历三重合流：通用大模型降低了内容、分析与软件构建成本；媒体与商业平台把 AI 嵌入广告、内容、电商和客户触点；企业软件与智能体平台开始把模型能力连接到知识、流程、权限和业务对象。结果是，传统按“内容工具、投放工具、CRM 工具”逐项采购的 MarTech 清单越来越难描述真实价值，也更容易制造重复能力、数据断点和供应商锁定。

董事会需要把 AI 营销视为一套经营控制系统：目标被转译为可追踪状态，状态触发决策，决策形成行动，行动写回业务系统，结果进入反馈与知识沉淀。模型只是推理与生成能力，不能独自承担业务状态、权限、审批、日志、数据治理和责任归属。单点 SaaS 可以快速解决局部问题，Agent 平台可以编排跨工具动作，营销 OS 承担目标、状态与运营控制，数据平台和媒体平台提供事实与触点，咨询实施服务负责把组织规则变成可运行系统。

企业最常见的失败并非模型“不聪明”，而是演示中的理想输入、人工补数和临时操作没有进入真实流程；输出停留在聊天气本，未形成结构化业务状态；外部动作缺少审批、幂等、回滚和审计；评价停留在“生成得像不像”，没有连接线索、商机、转化、成本或品牌风险。供应商尽调必须从产品功能转向状态模型、接口、日志、权限、可观测性和退出能力。

中国监管边界要求企业把生成式 AI、个人信息、重要数据、算法、深度合成与生成合成内容标识纳入同一治理体系。《人工智能生成合成内容标识办法》及配套国家标准自 2025 年 9 月 1 日起施行；面向境内公众提供生成式人工智能服务还涉及备案、安全与内容治理要求。企业内部使用与对公众提供服务的法律适用不同，但采购合同、数据处理协议、内容审批与供应商管理都应提前预留合规门。

建议企业用 90 天完成生态盘点、场景排序、最小可行组合和首个闭环，用 365 天建立统一身份权限、数据与知识底座、模型路由、接口目录、日志与成本观测、供应商组合管理以及年度替换演练。第一阶段不追求全域自动化，而应选择一个目标明确、数据可得、风险可控、反馈周期短的场景，证明“目标—状态—决策—行动—反馈”能够连续运行。

表 2 十项核心判断

序号	核心判断	论证要点	管理动作
1	传统 MarTech 清单失效	AI 能力跨越原有软件边界；同一模型可用于研究、内容、客服、销售和分析，单一厂商也可能横跨云、模型、媒体、数据和应用。	以价值闭环和接口责任采购。
2	模型不是系统	模型负责理解、推理与生成，不负责长期业务状态、组织权限、审批、幂等、回滚和责任归属。	把模型置于可治理的执行框架内。
3	业务状态是分水岭	演示通常展示输出，生产系统必须保存任务阶段、输入输出、责任人、审批、异常、版本和结果。	验收“状态写回”和可观察执行。
4	组合优于单押	通用模型、垂直 SaaS、Agent 平台、营销 OS、数据平台和专业服务各有边界。	按核心/可替换/外围三层组合。
5	媒体平台不可替代	广告、社媒、电商和搜索平台掌握真实触点、账户和反馈，但不应成为企业唯一知识与状态系统。	触点能力与企业控制层解耦。
6	GEO 是新接口层	AI 搜索可见性依赖可抓取内容、实体一致性、可信来源和结构化事实，不等同于传统 SEO 或批量写稿。	纳入内容治理和品牌事实体系。
7	PoC 必须使用真实约束	理想数据与人工补链无法证明生产价值。	用真实权限、真实异常、真实成本与退出测试。
8	治理门应嵌入流程	合规不能只靠上线前法务审查。	按风险等级配置自动、抽检、审批和禁止动作。
9	TCO 的大头在连接与运营	软件许可只是成本的一部分，数据清洗、集成、模型调用、运维、人工审核和变更管理往往更重要。	用 3 年 TCO 与单位业务结果评估。
10	可替换性本身是资产	模型和平台快速变化，锁定会把技术进步变成迁移成本。	合同化数据可携带、接口、日志与退出演练。

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

来源提示：国家互联网信息办公室《生成式人工智能服务管理暂行办法》（2023-07-13）；《人工智能生成合成内容标识办法》（2025-03-14，2025-09-01施行）；GB 45438-2025《网络安全技术 人工智能生成合成内容标识方法》。

第一章 产业边界正在改变：传统 MarTech 清单无法表达 AI 时代的价值创造

AI 把“能力”从固定软件模块中解耦，企业必须改用价值流、业务状态和接口责任描述生态。

1.1 五股结构性力量同时作用

结论 | 大模型商品化、媒介平台 AI 化、企业数据资产化、智能体执行化和监管制度化，正在共同改写营销技术供给。

证据 | 国内云与模型厂商持续提供模型 API、知识检索、工作流、智能体与多模态服务；媒体平台把生成、投放和经营反馈嵌入自身账户体系；监管已形成生成式 AI、算法、个人信息和内容标识等多层规则。

经营含义 | 同一业务能力可能由多个供给角色提供，原有“一个品类对应一个软件”的采购逻辑会出现重复采购和责任空白。

行动 | 先定义业务目标、状态对象和控制点，再确定由哪类供给角色承担。

表 3 生态重构的五股力量

结构性力量	变化	对企业采购的影响
模型能力普及	文本、图像、音视频、代码与推理能力通过 API 或私有部署快速获得	模型性能差距会变化，合同应避免把全部业务状态绑定单一模型
媒体平台 AI 化	平台内生成、投放、推荐、客服和经营分析一体化	触点效率高，但账户、数据和规则受平台约束
企业知识与数据资产化	RAG、知识库、CDP、CRM 与数据仓库成为 AI 事实基础	数据质量、权限和主数据比指令模板更决定生产效果
智能体执行化	AI 从回答问题扩展到调用工具、更新系统和推进任务	需要身份、审批、幂等、回滚、日志和异常处理
监管制度化	内容、数据、个人信息、算法和生成标识要求持续细化	合规能力必须进入产品架构、流程和合同

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

1.2 生态的最小分析单位是“可观察闭环”

结论 | 任何 AI 营销采购都应能回答：目标是什么、状态在哪里、谁作决策、执行写回哪里、结果如何反馈。

证据 | 单点生成工具通常只覆盖一个动作；企业级场景还需要数据输入、审批、发布、客户状态、结果回流和知识沉淀。

经营含义 | 无法形成状态闭环的能力只能算生产力插件，不能被当作经营系统。

行动 | 为每个场景绘制目标—状态—决策—行动—反馈链，并指定系统记录源。

表 4 传统采购与闭环采购对比

维度	传统 MarTech 清单	AI 经营闭环
采购对象	功能模块与席位	业务结果、状态对象与控制点
验收	功能可用、页面可见	真实流程可运行、状态可追踪、异常可处理
数据	各系统局部保存	明确系统记录源与跨系统回写
AI	附加功能或助手	可替换的推理/生成能力
治理	上线前审查	嵌入身份、权限、审批、日志和内容责任
成本	许可费	许可+模型+数据+集成+运营+迁移的TCO

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

1.3 供给数量增长会放大选择成本，价值重心正在离开模型本身

数据 | 国家网信办公告显示，截至 2025 年 12 月 31 日，境内累计有 748 款生成式人工智能服务完成备案，435 款通过 API 等方式调用已备案模型的应用或功能完成登记；2025 年内分别新增 446 款和 330 款。[S17] 国新办 2026 年 1 月发布会援引有关机构测算称，2025 年我国人工智能企业超过 6,000 家，核心产业规模预计突破 1.2 万亿元。[S18] 后一口径覆盖整个 AI 核心产业，不能等同于 AI 营销市场规模，却足以说明企业面对的供给层正在快速扩张。

机制 | 当模型、应用和行业方案持续增加，买方首先要回答相似能力如何归并、状态由谁持有、接口如何替换、结果怎样验收。供应商越多，重复采购、数据复制、身份分裂、合同冲突与退出困难越容易被低估。功能清单只能记录供给，无法解释这些供给如何共同完成一个客户任务。

经典思想 | 罗纳德·科斯在《企业的性质》中用交易成本解释企业边界：当搜寻、谈判、协调和监督外部交易的成本高于内部组织成本，活动会被纳入企业；反之则交给市场。[S36] AI 降低了部分生产与调用成本，却可能提高验证、集成、监督和切换成本。企业边界不能按“模型便宜”决定，而要计算整个交易与治理成本。

边界 | 备案数量不是活跃产品数，也不代表商业成功、营销适用性或技术独立性；核心产业规模来自有关机构测算，且统计边界宽于本报告。两组数字只用于判断供给复杂度和治理义务，不能据此推导厂商份额或市场增长率。

管理动作 | 生态盘点时新增三列：同类能力重叠度、跨系统协调成本、十二个月内可替换性。采购委员会先决定哪些业务状态必须由企业持有，再判断哪些能力适合外购；不要先选厂商，再倒推企业应该怎样工作。

第二章 完整价值链必须围绕“目标—状态—决策—行动—反馈”运行

经营价值闭环

每一层供给都必须服务同一业务状态。

01
目标
定义结果与约束

02
状态
连接实时业务事实

03
决策
用证据判断下一步

04
行动
在授权边界内执行

05
反馈
结果回流并更新状态

营销 AI 只有穿过五个连续环节，才会从内容产能转化为经营结果。

2.1 五环价值闭环定义

结论 | 目标提供方向，状态提供事实，决策选择动作，行动改变现实，反馈用于校正；任何断点都会使 AI 退化为孤立助手。

证据 | 企业常见断点包括：目标未量化、状态散落在聊天与表格、决策没有版本、行动未写回平台、结果与内容或客户无法关联。

经营含义 | 闭环设计决定了系统能否持续运营，也决定供应商之间的接口责任。

行动 | 为每个环节确定输入、输出、责任角色、系统记录源、SLA 和治理门。

表 5 五环价值闭环

环节	核心问题	关键对象	典型系统	控制点
目标	要改变什么经营结果？	OKR、预算、受众、战役、约束	营销 OS、项目管理、预算系统	目标批准、预算边界、风险偏好
状态	当前事实与阶段是什么？	客户、内容、素材、账户、任务、审批、成本	CRM/CDP/CMS/广告平台/数据平台	主数据、权限、时间戳、版本
决策	下一步做什么以及为什么？	策略、优先级、分群、创意、渠道、出价建议	模型、分析平台、Agent、规则引擎	证据、置信度、可解释、人工复核
行动	谁在何处执行？	发布、触达、更新、投放、工单、任务	媒体平台、CRM、SCRM、自动化工具	身份、审批、幂等、限额、回滚
反馈	结果如何回流并改变下一轮？	曝光、互动、线索、商机、转化、品牌风险、成本	BI、数据仓库、归因、知识库	口径、归因、异常、知识版本

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

2.2 经营价值流包含九个能力层

结论 | 从市场感知到经营复盘，能力层之间通过数据、事件、内容资产、客户状态和执行指令连接。

证据 | 公开产品资料显示，市场供给已经覆盖模型、RAG、工作流、多智能体、智能营销、客户旅程、内容创意和广告分析等，但很少有单一产品在所有层均具备最佳能力。

经营含义 | 生态架构应允许专业能力接入，同时由企业控制层保持目标、身份、状态与日志的一致性。

行动 | 采用“企业控制层 + 可插拔能力层 + 外部触点层”的三层架构。

表 6 经营价值流九层

能力层	主要任务	核心输入	核心输出	不可缺少的接口
1 市场感知	趋势、舆情、竞品、客户声音	公开信息、平台数据、内部反馈	信号、证据、机会清单	搜索/采集接口、证据引用
2 客户与数据	身份、标签、分群、同意、行为	CRM/CDP/交易/触点数据	客户状态与可用受众	主数据、同意状态、数据血缘
3 策略与规划	目标拆解、预算、战役、内容支柱	目标、约束、历史表现	计划、Brief、优先级	版本、审批、预算
4 内容与创意	文案、视觉、视频、素材变体	Brief、品牌知识、渠道规格	可审核内容资产	资产ID、版权、生成标识
5 渠道与广告	发布、投放、推荐、触达	内容、受众、预算、规则	平台动作与回执	账户权限、API、回执、限额
6 社媒与内容运营	排期、互动、社区、达人协作	内容资产、日历、互动信号	发布状态、互动任务	平台规则、人工接管
7 CRM与客户运营	线索评分、培育、销售协同、服务	客户状态、内容、销售反馈	任务、旅程阶段、商机状态	CRM写回、SLA、同意
8 AI搜索/GEO	品牌实体、可信答案、可抓取内容	事实库、站点、媒体与结构化数据	AI搜索可见性与引用线索	发布、结构化标记、监测
9 分析复盘与知识	归因、复盘、规则和经验沉淀	全链路事件、成本、结果	洞察、Playbook、下一轮输入	统一口径、知识版本

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

2.3 案例：百胜中国把 AI 助手接入自有会员与交易状态

案例 | 百胜中国 2025 年年报及投资者材料披露，肯德基与必胜客会员总数超过 5.9 亿，过去十二个月有交易的活跃会员超过 2.65 亿，数字点单约占公司销售的 94%，全年数字销售额约 104 亿美元。2025 年 7 月开始试运行、随后向肯德基超级 App 用户开放的“小 K 点餐”，截至 2026 年 1 月底已有超过 200 万会员使用。[S24]

机制 | 点餐智能体并非独立聊天工具。它位于企业自有 App 中，必须连接菜单、门店、库存可售、价格、会员权益、订单和履约状态，才能把自然语言需求转成真实交易。百胜中国还在门店侧试点 Q-Smart，让店长通过可穿戴设备查询排班、库存和食品安全任务，并由系统提出或执行后续动作。[S25] 客户入口与门店运行因共享交易状态而成为同一价值链的两端。

结果与边界 | 200 万使用者证明入口获得初步采用，94% 数字点单和 5.9 亿会员则是 AI 上线前已积累的数字基础，不能归因于“小 K”。公司没有公开该助手对客单价、转化、复购、错误订单或人工服务成本的独立增量。可迁移之处在于：先拥有会员、菜单、交易和履约对象，再让 AI 进入确定流程。

经典思想 | 迈克尔·波特强调，竞争优势来自相互强化的活动系统，而非单个活动的最佳化。[S38] 对餐饮企业而言，推荐、点单、会员、门店执行和反馈若各自采用最优工具但无法共享状态，整体体验仍会断裂。AI 生态的价值要在活动之间的适配度上衡量。

管理动作 | 绘制客户任务时，不只列触点，还要列每次行动所需的权威状态和失败回路。凡是供应商只能输出建议、却不能读取或写回关键对象的环节，都应按“辅助能力”估值，不按闭环系统估值。

第三章 生态全景图的主轴是价值流，纵轴是接口与治理

生态地图：六层供给围绕一条经营价值流

分类是决策工具，不是永久厂商标签。



企业应把生态视为多角色协作网络，并保留重叠角色与动态变化。

3.1 十类供给角色各有明确边界

结论 | 大模型、数据与知识、内容与创意、广告与渠道、社媒运营、CRM、GEO、Agent/工作流、营销 OS、咨询治理共同组成供给网络。

证据 | 市场公开产品表明，腾讯云智能体开发平台提供 LLM+RAG、Workflow 和 Multi-agent；火山引擎提供豆包模型及 Agent 开发部署；腾讯企点等产品覆盖客户数据、旅程与营销自动化。此类实例说明供给角色正在交叉，但不意味着单一平台可覆盖全部生产责任。

经营含义 | 企业要按“主要责任”而非品牌名称归类，并明确每一类不解决的问题。

行动 | 建立能力域×场景×供给角色矩阵，并在采购文件中写明责任边界。

表 7 十类供给角色的能力边界

供给角色	主要解决	通常不解决	典型锁定点
通用/行业大模型	理解、推理、生成、多模态	业务状态、流程责任、数据质量、真实执行	专有API、提示与微调资产、价格与限流
数据与知识平台	事实汇聚、检索、身份、标签、血缘	最终业务动作和营销策略	数据模型、主键、查询语言、存储格式
内容与创意 SaaS	快速生成、协作、审核、资产管理	跨链路客户状态和经营归因	模板、素材库、项目文件格式
广告与媒体平台	触点、流量、账户、投放、回执	企业跨平台统一状态与长期知识	账户数据、归因口径、平台规则
社媒与内容运营平台	排期、发布、互动、账号运营	完整客户生命周期与企业数据治理	账号授权、接口可用性、内容历史
CRM/SCRM/客户运营	客户主数据、线索、旅程、销售协同	上游创意生产和媒体触点全部能力	客户数据模型、自动化流程、生态插件
GEO/AI搜索服务	实体一致性、内容可发现性、引用监测	保证模型回答或替代品牌基础设施建设	监测口径、平台可见性、内容网络
Agent/工作流平台	工具调用、流程编排、事件触发、审批	天然拥有营销方法、业务主数据和组织运营	工作流定义、插件协议、运行时与日志
营销 OS/行动系统	目标、状态、角色、任务、日历、控制与复盘	底层模型、所有外部触点和专业深度能力	统一数据模型、组织流程、连接器
咨询实施与治理服务	场景设计、集成、变更、治理、持续优化	替代企业责任人和长期运营所有权	交付文档、定制代码、人员依赖

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

表 8 能力域 × 场景 × 供给角色矩阵

场景	主责供给	关键协同	企业保留控制
新品上市战役	营销OS/战役管理	模型、创意SaaS、媒体平台、数据平台、咨询	目标、预算、品牌审批、资产与复盘
B2B线索增长	CRM/营销自动化	内容、广告、GEO、Agent、数据平台	客户主数据、评分规则、销售SLA
社媒矩阵运营	社媒运营平台	内容创意、模型、Agent、媒体平台	账号权限、内容责任、日历和品牌规则
广告优化	媒体平台/广告技术	数据平台、创意SaaS、Agent、咨询	预算限额、账户权限、归因口径
私域客户运营	SCRM/CRM	模型、知识库、工作流、客服渠道	同意、客户状态、人工接管
AI搜索可见性	企业内容与GEO服务	CMS、媒体、公关、结构化数据、模型监测	事实库、实体规范、内容责任
市场情报与舆情	数据/情报平台	搜索、模型、知识库、工作流	信号阈值、证据和升级流程
营销管理驾驶舱	营销OS/BI	CRM、广告、社媒、财务、数据平台	指标口径、责任归属、决策节奏

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

来源提示：非穷尽公开实例包括：腾讯云智能体开发平台、腾讯混元、腾讯企点营销云、火山引擎豆包大模型与火山方舟等官方产品资料。实例仅用于说明能力类型。

3.2 案例：淘宝天猫的生态价值来自多方围绕同一商品与交易状态协作

案例 | 阿里巴巴披露，2025 年“双 11”把生成式 AI 接入超过 20 亿件商品的语义索引，并覆盖搜索、推荐、广告、商家内容、经营分析和客服。公司称，复杂查询相关性获得两位数改善，部分推荐场景点击率获得两位数提升；AI 生意顾问自 10 月以来生成超过 500 万份分析报告，店小蜜在大促期间处理 3 亿次咨询。[S21][S22]

机制 | 这是一种平台型生态：模型提供理解与生成，商品目录提供事实，搜索和推荐分配注意力，广告系统连接预算，商家工具形成行动，交易与客服回流结果。价值并非来自某个“万能 AI”，而是平台拥有共同对象、统一触点和高频反馈，第三方商家能够在同一经营语境下调用多种能力。

詹姆斯·穆尔提出“商业生态系统”时，关注企业如何与客户、供应商、竞争者及其他利益相关者共同演化；伊安西蒂与莱维恩进一步用生产力、稳健性和利基创造衡量生态健康。[S39][S40] 平台若只提高自身抽成或强化锁定，不能算健康生态；它还要让参与者更高效、在冲击下继续经营，并允许新的专业角色成长。

边界 | 以上结果均为平台自报，大促同时伴随补贴、流量投入、商家策略和季节性需求，无法把增长单独归因于 AI。分析报告数量与咨询量说明规模，不自动等于商家利润。该案例用于解释平台生态机制，不用于预测任一品牌的 ROI。

管理动作 | 企业评价平台合作时，同时看三项：平台给了什么增量能力，企业保留了什么客户与交易资产，离开平台时还能带走什么知识和内容。短期转化提升若以长期失去客户识别、实验历史或内容资产为代价，应在组合评审中计入依赖成本。

第四章 大模型提供认知能力，但不能替代数据、状态和责任系统

选模型应看任务适配、可治理性和替换成本，而非把模型品牌等同于营销解决方案。

4.1 模型选型应采用任务组合而非单一冠军

结论 | 不同营销任务对中文表达、长上下文、多模态、工具调用、延迟、成本和私有化要求不同。

证据 | 主流模型平台公开提供文本、多模态、联网、知识和 API 能力，但产品能力、价格、上下文、服务条款和备案状态会持续变化。

经营含义 | 企业单押模型会放大价格、限流、质量波动和迁移风险；多模型路由也会增加评测和治理复杂度。

行动 | 建立任务基准集、路由策略、降级策略和季度复测机制。

表 9 模型任务适配评分维度

维度	验证问题	测试方法	最低证据
质量	是否满足品牌、事实、结构和行业要求？	真实任务盲测与人工双评	样本、评分规则、失败案例
工具调用	能否稳定生成合法参数并处理失败？	API沙箱、异常注入、重试测试	调用日志、错误码、幂等策略
长上下文/RAG	能否正确引用企业知识并避免越权？	权限分组文档与冲突事实测试	引用片段、召回日志、权限证明
多模态	是否满足图像/音视频理解与生成要求？	品牌素材与复杂场景测试	输入输出版权与安全说明
延迟与吞吐	峰值是否满足业务SLA？	并发压测与超时降级	P50/P95、限流策略
成本	单位闭环成本是否可控？	按实际token、图片、视频和调用量核算	价格表、用量日志、预算告警
部署与合规	数据是否跨境、是否支持私有/专有环境？	架构与数据流审查	数据处理协议、部署说明
替换性	提示、工具、评测集能否迁移？	双模型切换演练	抽象层、导出格式、回归结果

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

4.2 RAG、微调和提示工程解决不同问题

结论 | 企业事实优先使用可治理知识检索；稳定风格和分类可考虑提示模板或微调；实时业务状态必须来自系统接口。

证据 | 把实时价格、库存、客户状态写入模型参数会迅速过期；只用指令模板又难以保证事实、权限和引用。

经营含义 | “把所有资料喂给模型”不是知识治理，可能造成越权、冲突事实和版本混乱。

行动 | 建立知识对象、权限、版本、有效期、引用和冲突处理规则。

表 10 知识与模型适配

手段	适合	不适合	治理要求
提示模板	任务结构、语气、格式、决策步骤	大量动态事实与权限隔离	版本、测试、变更记录
RAG/知识库	企业事实、制度、产品、案例、可引用资料	强实时交易状态、复杂计算	权限、来源、版本、有效期、引用
微调	稳定分类、风格、领域表达、工具行为	频繁变化事实、少量样本	训练数据合法性、回归、回滚
实时API/数据库	价格、库存、客户、账户、预算、任务状态	开放式推理本身	认证、限流、幂等、数据最小化
规则引擎	硬约束、禁区、阈值、审批	模糊判断和创意生成	责任人、版本、例外管理

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

4.3 模型成本快速下降，架构选择却不会自动变简单

数据 | 斯坦福 HAI《2025 AI Index》显示，在 MMLU 上达到 GPT-3.5 水平的模型推理价格，从 2022 年 11 月每百万 Token 约 20 美元降至 2024 年 10 月约 0.07 美元，约下降 280 倍；部分开源权重模型与闭源模型的基准差距也明显收窄。[S19] 模型能力更便宜、更可得，会削弱仅靠单一模型访问形成的差异化。

机制 | 模型价格下降会推动更多应用出现，但企业总成本还包括数据准备、知识维护、系统集成、评测、人工复核、监控、权限和错误恢复。模型可以被替换，业务状态、评测样本和运行经验却会累积。架构应让任务能在质量、时延、成本和风险之间路由，并保证模型替换不破坏业务语义。

4.4 案例：携程把 AI 放进旅行产品，同时在年报中保留风险判断

案例 | 携程集团在 2025 年第三季度业绩材料中称，旅行智能体 TripGenie 已在 200 多个国家和地区使用，2025 年上半年用户数同比增长超过 200%；2025 年度 20-F 又说明问道、TripGenie 与 Trip.Planner 被用于行程规划、信息收集和用户互动，并已就相关产品完成部分备案或登记。[S26][S27]

结果与边界 | 用户增长反映跨市场采用速度，不代表预订转化、利润、准确率或长期留存。公司在同一份监管文件中明确提示：AI 产品需要持续的模型设计、测试、监测、更新、专业人才和显著投入，也可能不被用户采用或无法产生足够回报。把增长数据与风险披露并读，比只看产品发布更接近董事会应有的判断。

管理动作 | 模型层采购采用“任务评测集 + 路由 + 可替换合同”。每季度用真实任务复测质量、延迟、成本与安全；任何模型升级都不得绕过回归测试。供应商不能导出评测记录、调用日志和业务对象映射时，即使单价更低，也应把迁移风险计入 TCO。

第五章 单点 SaaS 的价值在快速落地，边界在跨链路状态与复盘

专业工具应成为可插拔能力，而不应自动获得企业控制层地位。

5.1 内容、创意与社媒工具适合高频可标准化任务

结论 | 模板化内容、图片、视频、排期和协作能够快速释放产能。

证据 | 生成式内容工具和平台内创作能力已广泛存在，但品牌事实、版权、审批、生成标识、渠道回执和经营效果仍需跨系统协同。

经营含义 | 单点工具的 ROI 取决于是否被嵌入 Brief、资产、审批、发布和反馈链，而非单次生成速度。

行动 | 要求工具支持资产ID、版本、导出、API、审核状态和用量日志。

表 11 内容与创意能力边界

能力域	解决问题	必须外接	常见误判
文案生成	初稿、改写、摘要、多版本	品牌知识、事实校验、审批、发布	把“生成量”当成营销成果
视觉生成	概念图、素材变体、尺寸适配	版权、品牌规范、资产管理、渠道规格	忽略可编辑性和源文件
视频生成/剪辑	脚本、分镜、配音、剪辑加速	肖像/声音授权、审核、平台规则	把展示片段当成稳定批量生产
社媒排期	日历、草稿、协作、发布	账号权限、平台接口、异常回执	忽略平台接口变化与人工接管
互动回复	分类、建议、草稿、部分自动回复	客户同意、风险分级、人工接管	默认所有互动都适合自动化

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

5.2 广告与渠道平台拥有不可替代的触点能力

- 结论** | 媒体平台掌握流量、账户、竞价、推荐和真实回执，是行动层的重要组成。
- 证据** | 平台内 AI 可用于素材、受众、投放与分析，但其数据口径、接口、归因和规则由平台控制。
- 经营含义** | 企业不能绕开媒体平台，也不应让平台成为唯一客户知识、内容资产和跨平台归因系统。
- 行动** | 把预算、资产、客户主数据和复盘口径保留在企业控制层；通过受控连接器调用平台。

表 12 媒体平台连接控制点

控制点	企业要求	验收证据
账户与身份	最小权限、子账户、双人审批、高风险动作限制	权限矩阵、操作日志
预算与出价	预算上限、日限额、异常停机、dry-run	规则配置、模拟执行、回滚记录
素材与版本	资产ID、版本、审核状态、来源与授权	素材清单、发布回执
数据回流	原始回执、时间戳、维度、口径和延迟	API样例、字段字典、数据对账
归因	平台归因与企业归因并存，明确窗口和去重	归因说明、样例计算
接口变化	变更通知、兼容期、降级流程	SLA、变更记录、应急预案

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

5.3 案例：京东 618 展示了单点工具如何嵌入平台经营链

- 案例** | 京东在 2026 年 618 前 52 小时的官方披露中称，数字人直播方案 JoyStreamer 已服务超过 8 万商家、累计直播超过 80 万小时，相关成交额超过 2.4 亿元；JoyMarketing 覆盖获客、转化和会员运营等 100 多个场景，活动期记录超过 1.35 亿次互动。[S23]
- 机制** | 数字人、互动营销、商家客服、库存诊断和物流不是同一种产品，却通过平台的商品、流量、会员、订单和履约对象连接。单点工具的价值由平台状态放大：内容能够直接进入触点，互动能够形成受众和订单信号，履约结果又可用于下一轮运营。离开这些连接，同样的生成能力只能产出孤立素材。

结果与边界 | 以上均为京东活动期自报数据。成交额没有披露对照、商家分布和全部成本；“最高提升”类转化数字不能代表平均效果，互动次数也不是独立客户数。可迁移判断是：平台型单点工具应按它能读取和写回的业务对象估值，不能只按生成质量估值。

管理动作 | 采购内容、直播或广告 SaaS 时，增加“闭环距离”指标：输出离真实触点有几次人工搬运，离订单或线索状态有几次系统交接，结果多久能回流。距离越远，越应按局部生产力工具部署，并控制长期合同与数据依赖。

第六章 Agent、工作流与营销 OS 的差异在“谁拥有状态与运营责任”

边界由状态所有权与运营责任决定

单点 SaaS 完成明确功能	工作流 连接确定步骤
Agent 在约束内判断与行动	营销 OS 持有目标、状态、协同与治理

工作流负责把动作连起来，营销 OS 负责让目标、角色、状态、节奏和复盘持续运行。

6.1 Agent 平台的价值是编排与执行

结论 | Agent 平台通常提供模型、知识、工具、工作流、多智能体和发布渠道，适合作为能力构建与集成层。

证据 | 腾讯云 ADP 官方资料明确提供 LLM+RAG、Workflow、Multi-agent 和 API/SDK 接入；火山引擎公开提供从 Agent 开发到部署的服务。

经营含义 | 平台能降低构建门槛，但营销方法、业务对象、组织权限和长期运营仍需企业设计。

行动 | 把 Agent 平台放在企业架构的执行与编排层，避免把聊天记录当业务数据库。

6.2 营销 OS 的判定标准是持续经营能力

结论 | 营销 OS 不以功能数量定义，而以是否统一目标、状态、角色、节奏、审批、日志、成本和复盘定义。

证据 | 很多“AI 营销平台”会覆盖多个功能，但企业应验证其是否拥有结构化状态对象、跨应用事件、责任人、SLA、监控和数据可携带。

经营含义 | 没有状态和运营机制的平台，本质上仍是功能集合；有状态但无法开放接口的平台可能形成更深锁定。

行动 | 采用最小可行营销 OS：目标、任务、日历、资产、客户/线索引用、审批、事件、日志、成本与复盘。

表 13 通用模型、SaaS、Agent 平台与营销 OS 对比

类型	主要价值	状态能力	执行能力	适用阶段	主要风险
通用模型	快速认知与生成	弱，通常会话级	依赖工具调用	探索、个人与局部任务	事实、权限、持续状态不足
单点SaaS	专业任务快速落地	局部业务状态	局部或平台内执行	明确高频场景	数据孤岛、接口与导出限制
Agent/工作流平台	跨工具编排与自动化	流程运行状态	强，取决于连接器	集成与流程自动化	运行时、插件、日志锁定
营销OS	经营目标与跨场景控制	组织级状态	通过编排层和连接器	规模化运营	统一数据模型与平台锁定
数据平台	事实、身份、分析与口径	数据状态	通常不直接执行营销动作	数据基础成熟企业	建设周期、模型复杂度
咨询实施	场景、架构、变更与治理	文档/项目状态	依赖客户与技术平台	复杂转型与关键场景	人员依赖、交付不可复用

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

表 14 最小可行营销 OS 对象模型

对象	必须字段	系统记录源	关键事件
目标/KR	责任人、指标、基线、目标、周期、预算	营销OS/绩效系统	创建、批准、偏差、完成
场景/战役	阶段、受众、渠道、风险、预算、资产	营销OS	启动、阶段切换、暂停、复盘
任务/工作流	输入、状态、负责人、截止、重试、异常	工作流/任务系统	触发、审批、失败、完成
内容资产	版本、来源、授权、品牌审核、生成标识	DAM/CMS	生成、审核、发布、撤回
客户/线索引用	客户ID、同意、阶段、来源、评分	CRM/CDP	新建、评分、移交、转化
决策记录	证据、模型/规则版本、建议、批准人	营销OS/决策日志	建议、批准、覆盖、复核
执行日志	身份、工具、参数、结果、时间、错误	可观测平台	调用、回执、回滚
成本记录	模型、平台、人工、媒体、集成成本	FinOps/营销OS	预算告警、月结、异常

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

6.3 案例：WPP 内容引擎的竞争力来自互补者组合，而非单一模型

案例 | WPP 与 NVIDIA 自 2023 年开始构建生成式内容引擎，把 Omniverse 的 3D 工作流与 Adobe 的创意工具、Getty Images 的授权内容及客户产品数据连接，用于生成品牌一致的图片、视频和交互式 3D 体验；2024 年又把方案扩展到零售和消费品场景。[S29][S30]

机制 | 汽车、包装和耐用消费品的营销内容需要精确保持产品几何、材质、标识和版本。模型负责生成变化，3D 产品资产提供事实，创意软件承载人工编辑，授权内容控制知识产权，代理商负责客户流程与交付。任何一层都无法独立完成品牌级生产，竞争优势来自互补资产被编排成可重复流程。

马克·里德把这一合作视为 WPP 的差异化能力，黄仁勋则强调 3D 与生成式 AI 结合能够提高内容规模和个性化；这些是合作方的战略判断，不是独立效果证据。[S29] 公布材料未披露客户覆盖、全成本、平均生产周期或销售增量，因此本报告只把它计为“架构案例”，不计为“价值已证实案例”。

经典思想 | 赫伯特·西蒙把复杂系统描述为近似可分解的层级：模块内部关系更强，模块之间通过有限接口协作；鲍德温与克拉克则指出，模块化的价值依赖清晰的设计规则。[S41][S42] 企业控制层就是设计规则的持有者：对象、接口、版本、身份和验收必须稳定，外部模块才可能真正替换。

管理动作 | 组合架构评审不问“是否开放 API”，而问五件事：对象语义是否一致、版本变化是否通知、调用失败如何恢复、内容与日志能否导出、替换后历史是否连续。只有接口、数据和运行责任同时可迁移，模块化才不是架构图上的假象。

第七章 组合架构应把企业控制层与可替换能力层分离

把企业控制层与可替换能力层分开

数据、权限和业务状态留在企业控制域。

企业控制层：目标 · 身份 · 状态 · 规则 · 日志 · 价值口径		
模型	内容	渠道
CRM	GEO	Agent

最优架构不是购买最多，而是把不可外包的控制权留在企业，把快速变化的能力做成可插拔模块。

7.1 三层组合架构降低重复与锁定

结论 | 企业控制层管理身份、目标、主数据、状态、策略、日志与成本；能力层提供模型、创意、分析和 Agent；触点层连接媒体、CRM、社媒和外部系统。

证据 | 模型与平台变化快，而客户、品牌、流程、决策与历史结果具有长期价值。

经营含义 | 把长期资产绑定短周期技术，会增加迁移成本；反之，完全自建会放大实施和运维负担。

行动 | 用开放接口、事件总线、统一ID和可导出格式建立松耦合组合。

表 15 供应商组合架构

层级	企业应控制	可采购/替换	设计原则
企业控制层	组织身份、目标、预算、客户与品牌主数据、状态、审批、日志、指标口径	营销OS、IAM、数据平台可采购但需可携带	系统记录源明确，数据和配置可导出
能力编排层	工具目录、策略、评测集、路由与风险规则	Agent平台、工作流、模型网关	协议抽象、模型路由、错误与重试统一
专业能力层	品牌规则、验收标准	模型、内容创意、舆情、GEO、分析、翻译等	按任务替换，保留输入输出与版本
业务系统层	客户/交易/资产主键与责任人	CRM、CDP、CMS、DAM、BI	主数据一致，事件可订阅，写回可审计
外部触点层	账户治理、预算边界、发布责任	广告、社媒、电商、搜索、消息平台	最小权限、回执、限额、人工接管

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

7.2 可替换性需要在设计和合同中同时实现

结论 | 技术抽象层只能减少代码依赖，真正迁移还需要数据、配置、日志、模型行为和运营流程可带走。

证据 | 常见锁定来自专有工作流格式、不可导出的向量库、平台内客户ID、缺失原始日志、模型版本不透明和定制代码无权利。

经营含义 | 没有退出机制的低价合同可能形成高额未来迁移成本。

行动 | 对核心供应商进行年度替换演练，并设置分层退出RTO/RPO。

表 16 可替换性设计清单

对象	可替换要求	最低交付
模型	统一调用协议、提示与工具schema独立、评测集可复用	模型清单、路由配置、基准结果
知识库	、元数据、权限、切块与向量可重建	文档包、元数据、权限映射、索引说明
工作流	定义可导出、节点输入输出明确、外部凭证独立	流程JSON/BPMN或等价格式、字段字典
业务数据	稳定主键、全量与增量导出、删除证明	数据字典、导出样例、迁移工具
日志	原始调用、决策、审批、执行和错误日志	标准格式、保留周期、查询/导出接口
内容资产	源文件、可编辑文件、版本、授权与标签	资产包、版权/授权记录
定制成果	源代码、配置、部署说明、第三方依赖清单	代码仓、SBOM、部署文档、测试
运营知识	SOP、异常手册、评测标准和复盘	运行手册、培训材料、交接记录

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

7.3 案例：欧莱雅用企业控制层连接多家技术伙伴

案例 | 欧莱雅 2025 年年报披露，集团以 One Intelligence 维护消费者知识，以 CreAltech 生产品牌内容，以 BETiq 支持媒体决策，并通过 NEO 统一跨地区数据与流程。CreAltech 约有 4,500 名用户、每月生产超过 49.5 万项资产；BETiq 已在 8 个市场部署；集团有 6.5 万余名员工完成生成式 AI 责任使用培训。[S28]

机制 | 这一架构没有把企业交给单一供应商。Google、Adobe、NVIDIA 以及媒体平台承担不同能力，品牌、消费者知识、流程规则和人才体系由企业控制。内容、洞察和媒体决策可以共享事实，却保持不同的风险、更新频率和责任人；外部能力变化时，企业仍保有经营语境。

结果与边界 | 用户数、资产数、市场覆盖和培训人数证明运营规模，不直接证明增量收入或利润；年报也未披露各伙伴的完整 TCO、替换时间和资产采用率。案例支持的是“企业控制层 + 多伙伴”的组织方式，不能据此判断所有大型企业都应自建同等平台。

经典思想 | 奥利弗·威廉姆森把资产专用性、不确定性和交易频率作为治理结构的重要变量。[S37] 品牌知识、客户身份和实验历史专用性高、使用频繁、错误代价大，适合由企业控制；通用模型与可标准化创意能力变化快、可比较，适合保持市场竞争。自建或采购应逐层决定，不能给整套系统贴一个标签。

管理动作 | 三年 TCO 增加“专用资产暴露”与“替换成本”两栏：哪些知识只能在供应商内使用，哪些流程依赖私有对象，退出需要重新标注多少数据、重做多少审核、培训多少岗位。混合模式的价值，正是把高专用性资产留在企业，把易变化能力保持可竞争。

第八章 自建、采购、集成或混合模式取决于差异化、风险与TCO

四种供给方式没有固定优劣			
自建 差异化高、控制要求高		采购 标准能力、时间优先	
集成 跨系统闭环、接口可控		混合 核心状态自持、外围能力可换	

企业不应按“技术能力强弱”二分，而应按资产战略价值、变化速度、监管风险和运营能力逐项决策。

8.1 决策树从业务资产和风险开始

结论 | 核心客户数据、关键决策规则和差异化流程更适合企业控制；通用生成、基础工具和标准触点更适合采购。

证据 | 自建并不等于自研模型，采购也不等于交出数据与状态控制。多数企业适合混合模式。

经营含义 | 过度自建会拖慢价值，过度采购会形成碎片和锁定。

行动 | 对每个能力域进行五维评分：差异化、数据敏感、变化频率、可标准化、内部运营能力。

表 17 自建/采购/集成/混合决策树

判断问题	是	否
该能力是否形成核心竞争差异或包含关键决策规则？	优先自建控制层或混合	进入下一问
是否处理高敏感个人信息、重要业务数据或高风险外部动作？	私有/专有部署+严格集成治理	进入下一问
市场是否已有成熟标准产品且接口开放？	采购并集成	进入下一问
需求是否快速变化、需要多供应商能力？	采用Agent/工作流集成与可替换架构	进入下一问
企业是否有持续产品运营和工程能力？	可自建应用与控制层	采购+实施服务
是否能在12个月内形成可证明价值？	进入PoC与阶段建设	缩小范围或放弃

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

表 18 四种模式适用条件

模式	适用条件	优势	风险	治理重点
自建	高度差异化、强数据控制、具备产品工程团队	控制权与定制性高	周期、人才、运维和机会成本	产品负责人、架构标准、长期预算
采购	需求标准、成熟产品、快速上线	速度快、责任相对清晰	功能重叠、数据锁定、续费变化	合同、数据可携带、SLA
集成	已有系统较多、需跨链路闭环	保护既有投资、灵活组合	接口脆弱、责任边界复杂	API管理、事件、监控、变更管理
混合	核心控制自有、专业能力外购	平衡速度、控制与创新	架构治理要求高	企业控制层、供应商组合管理

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

8.2 TCO 必须按三年和单位业务结果核算

结论 | 许可、模型调用、数据、集成、运维、人工审核、培训、合规与迁移共同构成总拥有成本。

证据 | 低价模型或SaaS可能因大量人工补链、数据清理和异常处理而成本更高；高自动化也可能增加审核和风险成本。

经营含义 | 只比采购价格会系统性低估运营和退出成本。

行动 | 建立单位合格内容、单位有效线索、单位受控动作和单位闭环成本。

表 19 三年 TCO 构成

成本项	一次性	持续性	常被漏算
软件与平台	实施、初始化	订阅、席位、增值模块	最低承诺、超量、环境费
模型与生成	评测、提示/微调	Token、图片、视频、搜索、存储	重试、低质量废稿、多模型冗余
数据与知识	清洗、迁移、主数据治理	更新、质量、权限维护	版权、过期信息、数据对账
集成与工程	API、连接器、定制开发	接口变更、监控、故障处理	沙箱、回归测试、版本兼容
人工运营	培训、流程设计	审核、异常、复盘、供应商管理	关键人员依赖、轮班与高峰
安全与合规	评估、合同、技术改造	审计、备案/复核、事件响应	内容标识、删除请求、取证
退出与迁移	迁移工具、双跑	年度演练、数据归档	停机、重建索引、重新培训

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

8.3 自建与采购的决策单位应是能力层，而不是整套平台

判断 | 同一个场景可以同时包含企业自建的客户状态、采购的模型、集成商搭建的工作流、媒体平台触点和内部审批。把“自建还是采购”当成单选题，会迫使企业在控制力与速度之间做虚假二选一。正确问题是：每一层的差异化、专用性、变化速度和失败后果分别是什么。

科斯与威廉姆森的共同启示是，市场与企业并非固定边界，而是不同协调机制。[S36][S37] 当供应商接口成熟、绩效可测、替代充分时，外购可以降低生产成本；当知识难以合同化、跨方协调频繁、结果难以验收时，内部控制可以降低交易风险。AI 让能力更可调用，却没有消除责任不完备与合同不完全。

管理动作 | 把现有决策树改为逐层判定：业务状态、身份权限、知识资产、工作流编排、模型、内容工具、触点和专业服务分别评分。任何单项高风险都不必否决整套合作，但必须改变控制位置、合同条款和退出演练。

第九章 供应商尽调必须穿透演示，验证真实流程、状态和异常

PoC 六道证据门

演示通过不等于经营可用。

真实输入	真实接口
真实异常	真实人工接管
真实成本	真实退出

PoC 的目标不是证明“能做”，而是证明在真实约束下可运营、可观察、可治理、可退出。

9.1 演示能力与生产能力存在七个断层

结论 | 演示通常使用理想数据、单用户、人工补链和成功路径；生产环境包含权限差异、脏数据、并发、接口失败、模型波动和责任追踪。

证据 | 企业 AI 项目最容易在数据接入、业务状态、权限、异常处理、成本和变更管理处失效。

经营含义 | 只评输出质量会买到“会表演的工具”，而非可运营系统。

行动 | PoC 必须注入真实异常、真实审批、真实回写和退出测试。

表 20 演示到生产的七个断层

断层	演示表现	生产验证
数据	精选样例、人工整理	脏数据、缺失、冲突、权限隔离、增量更新
身份权限	管理员账号	多角色、最小权限、离职回收、服务账号
业务状态	一次性输出	阶段、责任人、版本、审批、超时、重试、完成条件
外部执行	手工点击或模拟	真实API、回执、幂等、限额、回滚、人工接管
模型稳定性	最佳提示和成功案例	批量样本、随机波动、模型升级、降级策略
可观测性	结果页面	调用链、成本、日志、错误、证据、审计
退出	不展示	全量导出、迁移、停服、删除证明、替代供应商双跑

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

表 21 供应商尽调评分卡

维度	权重	关键问题	淘汰条件
业务闭环	20	是否覆盖目标、状态、决策、行动和反馈？	输出无法进入真实业务状态
数据与知识	15	权限、血缘、版本、更新、删除如何实现？	无法证明数据隔离或导出
执行可靠性	15	幂等、重试、回滚、限额、人工接管？	高风险动作无审批/回滚
质量与评测	12	是否有真实基准、失败率和版本回归？	只提供精选案例
安全合规	12	数据流、供应链、内容责任和标识？	拒绝提供必要协议或审计材料
开放与替换	10	API、日志、配置、数据和模型能否迁移？	核心数据或流程不可导出
可观测与SLA	8	延迟、可用性、错误、成本是否可监控？	无原始日志与事件通知
TCO与商业条款	8	三年成本、涨价、超量和退出成本？	价格机制不透明或无限责任转嫁

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

9.2 PoC 要用业务验收而非功能清单

结论 | PoC 需要明确样本、基线、成功阈值、失败类型、人工投入、风险事件和退出交付。

证据 | 同一产品在不同企业的数据、品牌和流程环境中表现可能显著不同。

经营含义 | PoC 成功也只证明限定范围可行，不等于可直接规模化。

行动 | 采用“真实数据小范围、影子运行、受控上线、阶段扩容”四步法。

表 22 PoC 验收模板

模块	必须定义	示例口径
范围	场景、用户、渠道、数据、周期、排除项	单一产品线、一个渠道、限定客户分群
基线	现有周期、成本、质量、风险、转化	人工处理时长、返工率、响应SLA
成功指标	业务、效率、质量、风险、采用率	合格率、人工分钟、状态写回率、异常闭环率
样本	正常、边界、对抗、权限、缺失和冲突样本	至少覆盖高频失败模式
人工投入	审核、补数、纠错、配置和运维	按角色记录分钟和次数
异常测试	API失败、超时、重复、权限、模型降级	验证重试、幂等、回滚与告警
退出测试	导出、停服、替换、删除	迁移到备用模型/流程并核对数据

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

9.3 案例：卡夫亨氏用一个具体问题检验平台，而不是先购买宏大愿景

案例 | 卡夫亨氏与 Google Cloud 合作建设 TasteMaker 时，先从一名营销人员的具体内容瓶颈出发，把品牌指南、产品资料、消费者洞察和生成能力接入专用工作流。供应商案例称，新产品概念内容准备由 8 周缩短至 8 小时，平台内产品开发与营销用户采用率约 70%，相关流程节省数千小时。[S32]

机制 | PoC 没有要求员工反复编写复杂指令，而是把品牌知识、数据入口和步骤封装进任务界面。它检验的是一条真实工作流能否使用现有资产、按品牌要求产出并被团队采用。具体问题缩小了集成范围，也使周期、采用和质量能够在同一场景内观察。

结果与边界 | 结果由技术供应商发布，未披露对照组、全部成本、上线资产比例和消费者反应；8 周到 8 小时衡量概念内容准备，不等于产品上市周期整体缩短。案例可以支持 PoC 的设计方法，不能直接支持预算回报承诺。

管理动作 | 供应商 PoC 必须包含一条“反宣传路径”：用脏数据、权限冲突、缺失字段、模型超时、品牌例外和人工拒绝测试系统。演示成功证明能力存在；异常可恢复、日志可解释、结果被业务采用，才证明能力可进入生产。

第十章 治理应按风险分级嵌入 Human-in-the-Loop，而非一律人工或一律自动

风险越高，授权越窄，证据越完整

R1 自动执行	R2 抽检复核
R3 先审后发	R4 双人批准
R5 禁止自动	

风险等级决定自动化权限；治理门必须与数据、内容、客户和外部动作的后果相匹配。

10.1 中国监管边界要求多制度联动

结论 | AI营销可能同时涉及个人信息处理、数据安全、生成式AI服务、算法推荐、深度合成、生成合成内容标识、广告与知识产权等规则。

证据 | 《生成式人工智能服务管理暂行办法》适用于向境内公众提供生成式AI服务；《人工智能生成合成内容标识办法》及GB 45438-2025自2025年9月1日起施行，规定显式和隐式标识等要求。

经营含义 | 企业内部工具、对外内容、客户交互和平台服务的适用边界不同，不能用单一“合规认证”替代场景分析。

行动 | 建立数据流与内容流双台账，由法务、数据安全、业务和产品共同评审。

来源提示：法规依据包括：《个人信息保护法》《数据安全法》《网络安全法》《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》《人工智能生成合成内容标识办法》及GB 45438-2025。

表 23 风险分级与 Human-in-the-Loop 治理门

等级	典型场景	自动化权限	人工要求	技术控制
R1 低风险	内部摘要、格式转换、无敏感数据草稿	可自动执行	抽检	基础日志、版本、访问控制
R2 中低风险	内部分析、公开信息研究、非对外内容	自动生成与建议	发布/关键决策前审核	引用、事实校验、权限、成本限额
R3 中风险	品牌内容、社媒回复草稿、客户分群建议	可生成，不自动外发或写关键状态	业务负责人审批	内容审核、敏感词、证据、回滚
R4 高风险	客户自动触达、线索评分影响权益、广告预算调整	仅受控执行或dry-run	双人审批/人工接管	同意状态、限额、幂等、审计、异常停机
R5 禁止/极高风险	未经授权敏感数据处理、欺骗性内容、绕过平台或法律要求	禁止自动化	法务与高管专项决策	技术阻断、黑名单、事件响应

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

表 24 治理门的八个检查点

检查点	必须回答	责任角色
目的与合法性	为什么处理，是否必要，是否符合合同与告知？	业务+法务/隐私
数据最小化	哪些字段不可进入模型或供应商环境？	数据负责人+CIO
模型与供应链	使用何模型、区域、分包商、版本和备案信息？	CIO+采购+法务
内容责任	事实、版权、肖像、声音、广告表述和标识谁负责？	CMO+法务
客户权益	是否影响分群、报价、服务和人工申诉？	业务+法务
外部动作	是否可限额、审批、回滚和人工接管？	业务系统负责人
日志与取证	能否复现输入、模型/规则、审批和执行结果？	安全+内审
事件响应	错误内容、泄露、越权、平台封禁如何停机和通报？	安全+业务+法务

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

10.2 案例：Klarna 的规模化说明效率与例外负荷必须同时管理

案例 | Klarna 与 OpenAI 在 2024 年披露，客户服务助手上线首月完成 230 万次对话，约占客服聊天三分之二；重复咨询下降 25%，平均解决时间由 11 分钟降至不足 2 分钟，可处理退款、退货等任务并覆盖 35 种以上语言。
[S33]

机制 | 助手连接客户账户、订单与服务动作，因此能改变等待和解决，而不仅是生成回复。规模化同时改变了人工队列：常规任务被系统吸收后，留给人的往往是权益、情绪、欺诈、例外和多系统冲突。自动化率越高，人工案例平均难度可能越高。

利泽恩·班布里奇在《自动化的讽刺》中指出，自动系统接管常规操作后，人类却要在技能最少练习、信息最不完整时处理异常。[S44] NIST 生成式 AI 风险管理框架则要求组织把风险识别、测量、管理与治理贯穿生命周期，而非上线前做一次合规检查。[S34] 二者共同支持“风险越高，授权越窄；系统越自动，接管能力越要练习”的原则。

边界 | Klarna 数字来自合作方与企业自报，首月观察、人员工作量等价和利润估算都不是长期独立审计；不能据此断言客户服务应全面无人化。案例证明标准任务可快速规模化，也提醒企业同步度量人工接管等待、上下文完整率、投诉升级和恢复成本。

管理动作 | 每个风险等级同时规定自动动作、复核比例、人工权限、响应时限和演练频率。治理评审不只查“有没有人工”，还要查人工是否得到完整上下文、是否有权停止或补偿、是否保有处理罕见事件的能力。

第十一章 90 天应证明最小可行组合，365 天应形成可治理的企业系统

验证先于扩张

每一阶段都设置证据门和退出条件。

0-14 天 盘点生态与依赖	15-30 天 定义场景与状态
31-90 天 跑通最小组合	91-180 天 扩展接口与治理
181-365 天 组合运营与替换演练	

路线图要以闭环和运营能力递进，避免先建设“大而全平台”再寻找场景。

11.1 90 天路线的目标是首个闭环与采购基线

结论 | 企业应在三个月内完成生态盘点、场景排序、架构边界、PoC和受控上线。

证据 | 短周期可以暴露数据、接口、权限和人工运营的真实成本，也为年度投资提供证据。

经营含义 | 90天不追求全渠道和全自动，而追求一个结果明确、反馈周期短的闭环。

行动 | 按0-14、15-30、31-60、61-90天推进。

表 25 90 天路线图

阶段	关键任务	主要产出	决策门
0–14天 盘点与定界	系统/供应商/数据/接口盘点；选3–5场景；风险分级	生态台账、价值流图、数据流图、场景评分	确定首个PoC与不做清单
15–30天 设计最小组合	确定系统记录源、状态对象、角色、接口、基线与合同PoC条款	最小架构、PoC计划、评测集、权限矩阵	数据与权限是否可得
31–60天 影子运行	真实数据小范围运行；人工审核；异常注入；记录人工成本	结果对比、失败分类、日志与TCO初版	是否达到业务与风险阈值
61–75天 受控上线	限定用户/渠道；SLA；告警；人工接管；供应商整改	上线手册、应急预案、验收报告	是否扩大范围
76–90天 复盘与组合决策	价值评估、合同谈判、退出测试、下一场景排序	投资建议、供应商组合、365天蓝图	继续/替换/停止

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

11.2 365 天路线的目标是企业级可运营与可替换

结论 | 年度建设应把统一身份、数据与知识、模型路由、状态、可观测、供应商治理和人才机制逐步固化。

证据 | 规模化之后，主要风险从单次质量转向复杂依赖、成本漂移、权限扩大和模型/接口变更。

经营含义 | 没有运营团队和季度复测，系统会快速退化。

行动 | 设立AI营销产品负责人和跨职能治理委员会，按季度扩展场景。

表 26 365 天路线图

周期	建设重点	场景扩展	治理与组织
Q1 证明	首个闭环、最小控制层、PoC和上线	1个核心场景	跨职能小组、周复盘
Q2 连接	统一ID、知识、事件、模型网关、日志与成本	扩展至相邻2-3场景	接口标准、风险分级、月度供应商评审
Q3 规模化	复用工作流、资产、客户状态和评测集	跨渠道/跨团队	SLA、容量、FinOps、审计与培训
Q4 可替换与优化	双供应商/备用模型、退出演练、年度价值复盘	淘汰低价值场景，深化高价值闭环	年度合同、迁移演练、董事会投资复核

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

表 27 场景优先级评分

维度	权重建议	高分条件
经营价值	25	直接影响收入、客户、成本或重大品牌风险
数据可得	15	数据质量可接受、权限清晰、更新及时
反馈速度	15	2–8周内能观察结果并迭代
流程标准化	12	步骤、输入输出和异常可描述
风险可控	12	可限定范围、可人工接管、后果可逆
集成复杂度	10	接口稳定、系统记录源明确
组织准备度	6	有负责人、使用者和运营资源
可复用性	5	可扩展到多产品、渠道或团队

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

11.3 90 天验证闭环，365 天验证组合是否能持续运营

数据 | 麦肯锡 2025 年全球调查覆盖 105 个国家的 1,993 名受访者。88% 表示组织已在至少一个职能经常使用 AI，但只有约三分之一开始企业级规模化；39% 报告 AI 对企业 EBIT 有影响，而且多数低于 5%。[S20] 使用扩张与经营价值之间仍有明显距离，原因通常不在“再买一个工具”，而在 workflow、数据、领导责任、反馈和价值衡量没有共同推进。

实证 | 布林约尔松、李和雷蒙德对 5,172 名客户支持人员的分阶段部署研究显示，生成式 AI 助手使每小时解决问题数平均提高约 15%，经验较少者收益更大，最有经验者的速度收益较小。[S35] 同一能力对不同岗位产生不同结果，组织设计、知识质量与任务分层必须成为路线图的一部分。

经典思想 | 詹姆斯·马奇区分探索与利用：前者产生变异和新知识，后者追求执行与复用。[S45] 90 天的最小组合用于探索并形成可否证证据；365 天则要把已验证对象、接口、评测和治理沉淀为复用能力。只有探索会形成试点堆积，过早只做利用则会把第一版供应商和流程永久固化。

管理动作 | 季度组合评审把项目分为“探索假设、验证闭环、规模复用、退出迁移”四类，分别看证据产出、业务结果、复用率和退出完成度。项目数量增加而迁移率下降，说明组织在生产演示，不是在建设生态能力。

第十二章 组织、合同与验收决定生态能否长期创造价值

董事会设边界，CMO负责业务结果，CIO负责架构与运行，采购与法务把可替换性和责任写入合同。

12.1 决策权必须匹配风险与系统责任

结论 | AI营销跨越业务、数据、技术、采购和法律，任何单一部门都无法独立负责。

证据 | 业务部门知道价值和内容责任，CIO掌握架构与安全，采购掌握商业条款，法务判断监管与责任，董事会决定风险偏好和投资边界。

经营含义 | 职责不清会造成“业务认为技术负责结果、技术认为供应商负责合规、供应商认为客户负责内容”的责任空洞。

行动 | 建立RACI并把关键审批写入系统。

表 28 关键角色 RACI

决策/活动	董事会/CEO	CMO	CIO/数据	采购	法务/隐私	业务团队
AI营销投资与风险偏好	A	R	C	C	C	I
场景与业务指标	I	A	C	I	C	R
架构、身份、接口与运行	I	C	A/R	C	C	I
供应商尽调与商业谈判	I	C	C	A/R	C	I
数据、内容与合规评估	I	C	C	I	A/R	R
PoC与验收	I	A	R	C	C	R
上线运营与复盘	I	A	R	I	C	R
退出与迁移	I	C	R	A	C	I

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

12.2 合同必须覆盖变化、失败和退出

结论 | 模型、接口、价格和监管都会变化，合同不能只描述正常服务。

证据 | 生产事故通常涉及数据归属不清、日志缺失、模型升级未通知、分包商变化、内容责任转嫁和退出支持不足。

经营含义 | 合同是架构治理的延伸；没有技术可验证性，条款难执行。

行动 | 将数据、接口、日志、模型变更、内容责任、SLA、退出与迁移列为核心附件。

表 29 关键合同与验收条款

条款	最低要求	验收/证据
数据归属与使用限制	客户数据、提示、输出、反馈和衍生数据归属；不得用于训练/营销除非明确授权	数据处理协议、配置与审计
数据位置与分包商	处理区域、跨境、子处理者清单与变更通知	数据流图、分包商列表
接口与可用性	API范围、限流、版本、兼容期、变更通知	接口文档、沙箱、变更记录
日志与审计	原始调用、审批、执行、错误、管理员操作可查询导出	日志样例、保留周期、导出测试
模型变更	模型名称/版本、替换条件、质量回归、重大变更通知	版本台账、回归报告、回滚方案
内容责任	事实、版权、肖像/声音、广告、标识和审核责任分配	内容流程、授权记录、标识测试
安全与事件	安全措施、通知时限、配合取证、补救与责任	演练、事件模板、审计报告
SLA与支持	可用性、延迟、故障等级、响应恢复、服务抵扣	监控报表、工单记录
价格与成本	计费单位、超量、涨价、最低承诺、停用和预算告警	账单样例、用量对账
知识产权与定制	定制代码、配置、工作流、模板、第三方组件权利	交付清单、代码/配置仓
退出与迁移	导出格式、迁移支持、双跑、停服期、删除与证明	迁移演练、删除证明
验收与持续评测	样本、阈值、失败类型、模型升级后复测	评测集、验收报告、季度回归

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

12.3 案例：Defender 的沉浸式营销需要品牌、代理商与基础设施共同负责

案例 | 2024 年，Accenture Song 与 NVIDIA 为 Defender 展示面向豪华汽车客户体验的生成式内容与实时 3D 方案，把 JLR 的产品与品牌资产、代理商的全球营销运营、Omniverse 平台和生成模型连接起来，用于内容生产、对话式体验和个性化展示。[S31]

机制 | 高价值产品的数字体验不能由一个生成模型独立交付。品牌方定义产品事实和合规边界，代理商持有创意与运营流程，平台提供 3D 与算力，前端触点承担客户互动。合同需要分别约定资产权属、模型与素材来源、输出审核、数据处理、服务等级和退出交接。

结果与边界 | 公开材料描述了方案与合作关系，没有披露生产周期、客户采用、销售转化或全成本，因此只能证明生态编排方式，不能证明财务效果。未披露结果并不使案例无用；它要求采购方把价值验证留给自己的试点，而不是用合作伙伴名单替代证据。

经典思想 | 戴明强调，质量主要是系统设计与管理责任的结果。[S43] 多供应商场景发生错误时，如果合同只规定每家组件的可用率，却没有端到端结果负责人，企业会得到一组“各自合格、整体失败”的服务。验收必须覆盖客户任务，而不只覆盖组件。

管理动作 | 合同附件增加端到端责任图：每个业务对象由谁创建、谁可修改、谁审批、谁监测、谁恢复；跨方事件由谁统筹；替换任一伙伴时谁负责数据、配置、评测和历史迁移。责任图无法闭合时，不进入长期合同。

管理者工具：把生态选择转化为可执行决策

以下清单用于董事会审议、采购立项、PoC验收和年度复盘。

表 30 董事会检查清单

检查项	通过标准
经营目标	至少一个可量化经营结果和明确基线
投资边界	明确90天、365天预算与停止条件
风险偏好	定义可自动、需审批和禁止场景
核心资产	客户、品牌、知识、状态和日志归属清楚
组合策略	不存在单一供应商不可替代的关键依赖，或已有接受理由
价值复盘	按季度报告价值、成本、风险和采用率
退出机制	关键平台有迁移方案和年度演练

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

表 31 CMO 检查清单

检查项	关键问题
场景	是否连接目标、客户、内容、渠道和结果？
品牌	事实、语气、视觉、禁区和审批是否系统化？
内容资产	版本、授权、生成标识和发布回执是否可追踪？
客户运营	线索与客户状态是否写回CRM并有销售SLA？
指标	是否避免只看生成量和曝光量？
人工协同	谁审核、谁接管、谁处理异常？
复盘	结果是否进入下一轮策略和知识库？

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

表 32 CIO/数字化检查清单

检查项	关键问题
架构	企业控制层、能力层和触点层是否分离？
身份权限	人、Agent、服务账号是否统一治理？
数据	主键、血缘、权限、版本、删除和导出是否明确？
接口	API、事件、幂等、限流、重试、回滚是否验证？
可观测	调用链、成本、错误、模型版本和决策日志是否齐全？
韧性	备用模型、降级、停机和灾备是否可用？
替换	模型、知识、流程和数据能否迁移？

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

表 33 采购与法务检查清单

检查项	关键问题
证据	供应商自述、客户案例和独立验证是否区分？
商业	三年TCO、超量、涨价与最低承诺是否透明？
数据	用途、训练、跨境、分包商和删除是否约定？
模型	版本、备案、变更、质量回归和替换是否约定？
内容	版权、肖像、声音、广告与生成标识责任是否明确？
SLA	监控口径、故障等级、恢复和赔偿是否可执行？
退出	导出、迁移、交接、停服和删除证明是否可验收？

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

工具 5：生态依赖穿透卡

使用方法 | 对每个关键场景逐项填写：①客户任务；②权威业务对象；③企业控制层；④外部能力层；⑤跨系统接口；⑥结果与成本口径；⑦人工接管；⑧供应商替换；⑨数据与内容可携带；⑩停机后的最低可运行方案。每项必须写明责任人和可验证证据。

判定规则 | 若业务对象只能在供应商内部识别、结果只能由供应商计算、日志无法导出、人工无权停止、替换后历史中断，任一项成立即标记为高依赖。高依赖并非一定拒绝采购，但必须缩短合同、提高证据门、设置价格与迁移保护，并每年至少完成一次退出演练。

董事会使用 | 穿透卡用于经营连续性判断。它让管理层看见：当某个模型、媒体接口、SaaS 或服务商发生涨价、停服、政策变化或质量退化时，哪些客户承诺和收入流程会先受影响，以及企业需要多少时间恢复。

附录 A：代表性生态角色与公开实例（非穷尽）

实例用于说明供给角色重叠与能力边界，不构成排名、背书或采购推荐。

表 34 代表性生态角色与公开实例

角色类别	公开实例	公开能力线索	使用边界
基础模型/云AI	阿里云通义、腾讯混元/腾讯云、百度智能云文心、火山引擎豆包/方舟、华为云盘古、科大讯飞星火、智谱、月之暗面、MiniMax、DeepSeek等	模型API、多模态、知识、推理、开发与部署	能力、价格、区域、备案和条款需按最新官方资料核验
Agent/工作流	腾讯云ADP、百度千帆、阿里云百炼、火山方舟及企业自动化/低代码平台等	RAG、Workflow、插件、Multi-agent、API/SDK	营销方法、业务状态与治理需企业配置
广告/媒体/商业平台	巨量引擎、腾讯广告、百度营销、阿里妈妈、京东营销、小红书商业、快手磁力引擎等	账户、流量、投放、素材、平台数据与回执	平台规则、归因和接口受平台控制
CRM/客户运营	腾讯企点、销售易、纷享销客、用友、金蝶及各类SCRM/CDP/营销自动化产品	客户主数据、线索、旅程、销售与服务协同	需验证AI能力是否写回真实客户状态
内容/创意/音视频	剪映/即梦、可灵、通义万相、腾讯混元多模态、美图设计室、稿定设计等	图文、图像、视频、设计与素材生产	版权、可编辑性、品牌与标识需独立治理
营销智能/综合平台	迈富时Marketingforce、珍岛相关产品、腾讯企点营销云等公开方案	营销、销售、客户与Agent等综合能力	以企业真实PoC验证跨链路能力，不依据宣传口径排名
数据/分析/情报	云数据平台、CDP、BI、舆情与市场情报服务商	数据汇聚、分析、标签、监测与洞察	数据合法性、口径、实时性和导出能力关键
GEO/AI搜索	传统SEO/内容技术服务商、AI搜索监测与品牌内容服务商、新兴GEO产品	实体、内容可发现性、引用与答案监测	行业仍快速变化，不能承诺控制第三方模型答案
咨询实施/治理	咨询公司、数字化服务商、云生态伙伴、律师与安全评估机构	战略、架构、实施、集成、变更和合规	需防范交付人员依赖和定制成果不可迁移

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

分类口径说明

同一企业可同时出现在多个类别。例如云厂商可能同时提供模型、数据、Agent、营销应用和生态实施；媒体平台可能同时提供内容生成、广告、商业数据与客户触点。

本图谱按企业采购时承担的“主要责任”分类，而非按公司永久身份分类。产品版本、组织调整和生态合作会改变角色。

公开产品页面只能证明供应商宣称的能力，不证明其在特定企业环境中的效果、稳定性、合规性或可替换性。

对外部平台的自动发布、预算变更、客户触达等能力，必须以真实授权、API状态、平台政策和企业审批为准。

附录 B：来源索引（纯文本）

以下仅列机构、文件/页面名称、日期与使用口径，不含第三方可点击链接。

1. 国家互联网信息办公室等：《生成式人工智能服务管理暂行办法》，2023年7月13日；用于生成式人工智能服务适用范围、提供与使用规范。
2. 国家互联网信息办公室：《国家互联网信息办公室有关负责人就〈生成式人工智能服务管理暂行办法〉答记者问》，2023年7月13日；用于制度目标与适用边界说明。
3. 国家互联网信息办公室：《生成式人工智能服务已备案信息公告》及后续附件，2024–2025年更新；用于备案与应用公示要求口径。
4. 国家互联网信息办公室、工业和信息化部、公安部、国家广播电视总局：《人工智能生成合成内容标识办法》，2025年3月14日发布，2025年9月1日起施行；用于显式、隐式标识与平台责任。
5. 国家市场监督管理总局、国家标准化管理委员会：GB 45438–2025《网络安全技术 人工智能生成合成内容标识方法》，2025年2月28日发布，2025年9月1日实施；用于生成合成内容标识技术方法。
6. 全国人民代表大会常务委员会：《中华人民共和国个人信息保护法》，2021年；用于个人信息处理、委托处理、自动化决策与跨境等基础要求。
7. 全国人民代表大会常务委员会：《中华人民共和国数据安全法》，2021年；用于数据分类分级、安全管理与风险处置。
8. 全国人民代表大会常务委员会：《中华人民共和国网络安全法》及相关修订；用于网络运营安全与个人信息保护基础要求。
9. 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》，2021年发布、2022年施行；用于算法推荐服务治理。
10. 国家互联网信息办公室、工业和信息化部、公安部：《互联网信息服务深度合成管理规定》，2022年发布、2023年施行；用于深度合成服务与内容标识相关责任。
11. 腾讯云：《腾讯云智能体开发平台产品概述》及产品文档，更新至2026年6月；用于LLM+RAG、Workflow、Multi-agent、API/SDK、企业安全与可观测能力的公开自述。
12. 腾讯云：《腾讯混元大模型》产品页面，访问口径截至2026年7月；用于文本、多模态、联网与API能力的公开自述。
13. 腾讯企点：《腾讯企点营销云/客户运营相关产品页面》，访问口径截至2026年7月；用于客户数据、增长分析、旅程编排与营销自动化能力的公开自述。

14. 火山引擎：《豆包大模型》《火山方舟》《智能营销Agent》等产品页面，访问口径截至2026年7月；用于模型、多模态、Agent开发部署与营销能力的公开自述。
15. 迈富时Marketingforce：企业官网公开产品与解决方案页面，访问口径截至2026年7月；用于综合型AI应用与营销智能体角色示例，不用于独立效果验证。
16. 竹势 AI 营销智库：企业级AI营销智能体平台、营销行动系统、知识/状态/工作流与服务体系内部产品素材，2026年；用于本报告框架设计与企业需求映射，不作为外部市场事实证明。

术语表

表 35 术语表

术语	本报告定义
业务状态	营销对象在流程中的结构化事实，包括阶段、责任人、版本、审批、错误和结果。
系统记录源	对某类事实具有最终权威的系统，例如CRM对客户阶段、DAM对资产版本。
营销OS	统一目标、状态、角色、节奏、审批、日志、成本和复盘的经营控制层。
Agent	能够感知输入、调用模型与工具、根据规则或计划执行动作的人工智能软件实体。
Human-in-the-Loop	在关键判断、审批、异常或高风险动作中保留人工参与和责任。
GEO	面向生成式搜索/AI答案环境的品牌事实、内容可发现性、实体一致性和引用监测实践。
可替换性	在可接受时间和成本内替换模型、平台或供应商，并保留数据、流程、日志和业务连续性。
TCO	许可、模型、数据、集成、运营、合规和退出等全生命周期总拥有成本。

注：本表为决策框架，需结合企业具体行业、数据和流程验证。

V1.1 新增来源索引

- S17 | 国家互联网信息办公室：《关于发布2025年生成式人工智能服务已备案信息的公告》，2026-01-09。截至2025年末的备案与登记数量。
- S18 | 国务院新闻办公室：《2025年工业和信息化发展成效新闻发布会文字实录》，2026-01-21。人工智能企业数量与核心产业规模为有关机构测算，口径宽于AI营销。
- S19 | Stanford Institute for Human-Centered AI, AI Index Report 2025, 2025. GPT-3.5水平模型推理价格变化与开源/闭源模型差距。
- S20 | McKinsey & Company / QuantumBlack, The State of AI in 2025: Agents, Innovation, and Transformation, 2025-11-05. 全球调查覆盖105个国家的1,993名受访者；结果为自报。
- S21 | Alibaba Group, AI Powers Large-scale Applications at the World's Largest Shopping Festival, 2025-10-16. 商品语义索引、搜索推荐、商家内容、广告和客服的企业自报结果。
- S22 | Alibaba Group, Taobao and Tmall's 11.11 Shopping Festival Delivers Solid Growth for Brands, 2025-11-15. AI生意顾问和店小蜜的大促运营规模。
- S23 | JD.com, 618 Grand Promotion Kicks Off with Record Customer Participation and Strong Omnichannel Growth in First 52 Hours, 2026-06-02. JoyStreamer与JoyMarketing活动期企业自报数据。
- S24 | Yum China Holdings, 2025 Form 10-K and 4Q25/Investor Day materials, published 2026. 会员、数字点单、数字销售与Smart K使用数据。
- S25 | Yum China Holdings, Yum China Launches AI Assistant for Store Managers, 2025-06-20. Q-Smart门店运营试点的企业披露。
- S26 | Trip.com Group, 2025 Annual Report on Form 20-F, filed 2026-04-28. AI旅行产品、投入、采用、风险与备案边界。
- S27 | Trip.com Group, 2025 Third Quarter Earnings Materials, 2025. TripGenie覆盖地区与用户增长的企业自报数据。
- S28 | L'Oréal, 2025 Universal Registration Document / Annual Report, filed 2026-03-18. NEO、One Intelligence、CreAltech、BETiq、伙伴生态和培训数据。
- S29 | NVIDIA / WPP, WPP Partners With NVIDIA to Build Generative AI-Enabled Content Engine for Digital Advertising, 2023-05-29. 多方内容引擎架构与合作方观点。
- S30 | NVIDIA, Omniverse Cloud APIs to Power Wave of Industrial Digital Twin Software Tools, 2024-03-18. WPP与Media.Monks内容 workflow 扩展。
- S31 | Accenture, Accenture Teams with NVIDIA to Showcase AI-Powered Immersive Client Experiences for Defender, 2024-03-18. 品牌方、代理商和技术平台协同案例。

- S32 | Google Cloud Customer Story, Kraft Heinz Is Using Data and AI to Create the Products and Content Consumers Crave, accessed 2026-07-20. TasteMaker供应商案例及企业自报结果。
- S33 | OpenAI / Klarna, Klarna's AI Assistant Does the Work of 700 Full-Time Agents, 2024. 合作方披露的首月客服运营数据与利润估计。
- S34 | National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST AI 600-1, 2024. 生成式AI全生命周期风险管理。
- S35 | Erik Brynjolfsson, Danielle Li & Lindsey Raymond, Generative AI at Work, The Quarterly Journal of Economics, 2025. 5,172名客户支持人员的分阶段部署研究。
- S36 | Ronald H. Coase, The Nature of the Firm, Economica, 1937. 交易成本与企业边界的经典论文。
- S37 | Oliver E. Williamson, The Economic Institutions of Capitalism, 1985. 资产专用性、不确定性、频率与治理结构。
- S38 | Michael E. Porter, What Is Strategy?, Harvard Business Review, 1996. 战略取舍、活动系统与适配。
- S39 | James F. Moore, Predators and Prey: A New Ecology of Competition, Harvard Business Review, 1993. 商业生态共同演化框架。
- S40 | Marco Iansiti & Roy Levien, Strategy as Ecology, Harvard Business Review, 2004. 生态生产力、稳健性与利基创造。
- S41 | Herbert A. Simon, The Architecture of Complexity, Proceedings of the American Philosophical Society, 1962. 近似可分解系统与层级复杂性。
- S42 | Carliss Y. Baldwin & Kim B. Clark, Design Rules, Volume 1: The Power of Modularity, 2000. 模块化设计规则与选择价值。
- S43 | W. Edwards Deming, Out of the Crisis, 1986. 系统质量、过程管理与管理责任。
- S44 | Lisanne Bainbridge, Ironies of Automation, Automatica, 1983. 自动化后人工监督、技能保持与异常接管。
- S45 | James G. March, Exploration and Exploitation in Organizational Learning, Organization Science, 1991. 探索、复用与组织长期适应。
- S46 | Adobe / NVIDIA, Strategic Partnership for Firefly Models, Creative, Marketing and Agentic Workflows, 2026-03-16. 创意、3D、模型与营销工作流的伙伴架构；未作为效果证据。

结语：生态能力只有进入企业控制系统，才会成为长期资产

企业的目标不是拥有更多 AI 工具，而是拥有一套能持续发现机会、作出决策、执行动作、控制风险并沉淀经验的营销经营系统。

中国 AI 营销生态的供给会继续扩张、交叉和重组。模型性能会迭代，平台接口会变化，新的内容和搜索形态会出现。稳定的并不是某个工具名称，而是企业对目标、客户、品牌、知识、业务状态、审批和责任的控制。

因此，最具长期价值的投资不是一次性选出“最佳厂商”，而是建立可组合、可观察、可治理、可替换的能力体系。企业应让专业供应商在其优势位置创造价值，同时确保关键数据和经营状态可以持续积累、迁移和复用。

当目标—状态—决策—行动—反馈闭环能够稳定运行，AI才真正进入营销经营；当供应商退出、模型替换和接口变化不会破坏这一闭环，企业才真正拥有AI营销能力。

附录 C：生态盘点工作底稿

生态盘点的目的不是统计软件数量，而是识别每项能力承担的业务责任、数据依赖、接口依赖、风险与退出难度。

企业通常会低估“影子 AI”与重复能力：员工个人订阅的通用模型、部门自行采购的内容工具、媒体平台内置 AI、CRM 插件、自动化脚本和外包服务可能同时处理同一类数据。盘点必须覆盖正式采购、免费试用、个人账号、外包交付、平台内置功能和定制脚本。

每一项能力都应映射到价值闭环中的一个或多个环节，并标明系统记录源。若多个系统同时声称保存客户阶段、内容版本或投放结果，应明确哪一个是权威源、谁负责对账、冲突如何处理。

盘点结果应形成四类动作：保留并深化、保留但降级为外围能力、整合或替换、停止使用并迁移。停止动作必须包含数据导出、账号关闭、凭证回收、知识和工作流迁移以及供应商删除证明。

表 36 生态资产盘点字段

字段组	必填字段	判定用途
基本信息	产品/服务、供应商、业务负责人、技术负责人、合同期限、费用	识别所有权与续约窗口
价值位置	场景、五环位置、主要用户、业务结果、使用频率	判断是否真正进入经营闭环
数据	输入数据、敏感等级、系统记录源、处理区域、保留期	识别合规与数据锁定
技术	模型、API、连接器、认证、部署方式、依赖系统	识别架构耦合和运行风险
运营	活跃用户、人工审核、异常处理、SLA、支持机制	识别真实运营成本
输出	数据、内容、工作流、日志、配置能否导出	评估可携带性
风险	内容、客户、预算、账户、个人信息、供应链风险	确定治理等级
退出	替代方案、迁移周期、停机影响、删除要求	形成退出计划

附录 D：场景定义卡与状态设计模板

场景定义卡把业务语言转化为可实施的状态、事件、接口与责任，是供应商沟通和PoC的统一基线。

场景名称应描述一个可验证的经营过程，例如“新线索在15分钟内完成资格判断并分配销售”，而不是“AI线索助手”。业务结果必须同时包含正向指标和风险护栏；例如提高响应覆盖率的同时，不得未经同意自动触达，不得把低置信度判断直接写入客户永久标签。

状态设计要避免用聊天记录替代业务状态。每个对象需要稳定ID、阶段枚举、责任人、时间戳、输入输出版本、审批和异常字段。状态变化由事件触发，事件应能被审计并支持重复消息的幂等处理。

对于外部动作，必须描述dry-run、审批、执行、回执、失败、重试、撤回和人工接管。只有建议而无回写的场景，应明确其是“决策支持”而非“自主执行”。

表 37 场景定义卡

模块	填写内容	示例
经营目标	结果、基线、目标、周期、预算	缩短合格线索首次响应时间
对象与状态	对象ID、阶段、责任人、完成条件	lead_id; new/qualified/assigned/contacted
输入	数据源、字段、权限、时效	CRM线索、官网表单、活动来源
决策	模型/规则、证据、置信度、覆盖方式	规则先行，模型补充意图判断
行动	系统、动作、限额、审批、回滚	创建任务，不直接外发；高分线索人工确认
反馈	结果字段、时间窗、归因方式	是否联系、是否接受、是否进入商机
风险门	数据、内容、客户权益、外部动作等级	R4，需人工确认与同意状态
异常	缺失、冲突、超时、接口失败、重复	进入人工队列并保留原始事件
验收	业务、质量、效率、风险、成本指标	状态写回率、误分率、人工分钟、单位线索成本

附录 E：接口与数据可携带性验收规程

接口验收不能止于“有 API”，还要验证权限、语义、稳定性、变更、日志和迁移。

供应商常用“支持 API”描述开放性，但 API 可能只读、仅覆盖部分对象、缺少增量同步、无法导出历史版本或受高额调用限制。验收应按具体业务对象逐项确认创建、读取、更新、删除、查询、批量、事件订阅和错误处理能力。

数据可携带性应覆盖原始数据、派生字段、标签、向量索引所需元数据、工作流定义、提示模板、评测集、审批历史和日志。仅导出最终报表或PDF不构成可携带。

变更管理应规定版本策略、弃用期、沙箱、测试环境、通知方式和兼容承诺。对于媒体与社交平台接口，企业还需要准备接口不可用时的人工降级流程。

表 38 接口验收用例

类别	测试用例	通过标准
认证与权限	不同角色、服务账号、凭证轮换、离职回收	最小权限生效，凭证可独立撤销
对象完整性	创建/读取/更新/删除/查询/批量	覆盖承诺对象，字段语义一致
事件	新增、更新、审批、失败、撤回事件	事件可订阅，有唯一ID与时间戳
可靠性	超时、重复、乱序、部分失败	幂等、重试、死信与对账机制有效
限流与容量	峰值并发、批量导入、长期运行	达到SLA，超限有明确错误和降级
日志	请求、响应、身份、版本、耗时、错误	企业可查询和导出原始日志
版本变更	旧版弃用、字段新增/删除、模型切换	有兼容期、通知、沙箱和回归
迁移	全量导出、增量追平、双跑、切换	在约定RTO内完成并核对一致性

附录 F：SLA、可观测性与运行值班模板

AI 营销系统的 SLA 必须覆盖模型、数据、工作流和外部平台，不应只写一个总体可用性百分比。

端到端服务由多个依赖组成：模型、知识检索、身份认证、业务系统、工作流、媒体平台和人工审批。单一供应商可用不代表业务闭环可用。企业应建立场景级SLO，并将故障定位到具体依赖和责任方。

可观测性至少包含：调用链、模型与提示版本、知识引用、工具参数、审批、外部回执、错误、重试、人工接管、用量和成本。对于自动决策或客户触达，还应记录触发依据和覆盖决定。

运行值班需要业务和技术共同参与。技术故障可能表现为接口失败，业务故障可能表现为事实错误、品牌风险、客户投诉或转化异常。两类故障都需要停机开关和升级路径。

表 39 场景级 SLA 模板

指标	定义	建议处理
端到端成功率	从事件进入到状态正确写回的比例	按场景和失败类型统计，不只看API 200
处理延迟	事件到建议/审批/执行/回执的P50/P95	区分模型、人工审批和外部平台耗时
状态一致性	企业记录源与外部平台对账一致率	设置自动对账与差异工单
人工接管率	进入人工队列的比例及原因	区分设计性接管和系统失败
质量失败率	事实、品牌、格式、政策和业务规则失败	按模型/版本/场景做回归
风险事件	越权、错误外发、预算异常、客户投诉	零容忍项即时停机和通报
单位成本	每个合格结果的模型、平台与人工成本	设置预算阈值和异常告警
恢复时间	从发现到恢复或降级的时间	按P1-P4故障等级约定

附录 G：模型与供应商变更管理

模型升级可能改善总体能力，也可能破坏特定品牌、格式、工具调用和合规行为，因此必须作为生产变更管理。

供应商应披露模型或关键组件的重大变化，包括模型名称或版本、上下文、工具调用协议、安全策略、价格、限流和数据处理安排。企业应保留接受、延期、切换备用模型或终止的权利。

每次重大变更都应运行回归评测集。评测集由真实任务、边界样本、权限样本、对抗样本和历史失败样本组成，并覆盖输出质量、工具参数、引用、成本和延迟。

对高风险场景，变更应采用影子流量、灰度、双跑和回滚。模型升级不应自动改变客户分群、预算、发布权限或内容责任。

表 40 变更评审清单

变更类型	必做评估	发布控制
模型版本	质量、工具调用、幻觉、偏差、成本、延迟	影子测试、灰度、回滚
提示/规则	任务质量、边界、例外、责任人	版本审批、A/B或分组验证
知识库	来源、权限、冲突、过期、索引重建	增量验证、引用抽检
连接器/API	字段、认证、限流、错误、事件	沙箱、兼容期、对账
供应商子处理器	数据区域、用途、安全与合同	法务评审、用户/客户通知（如需）
价格与套餐	单位成本、最低承诺、超量、预算	财务评审、路由或替代方案
监管要求	适用范围、流程、标识、记录	法律意见、产品改造、培训

附录 H：年度供应商组合评审

供应商评审应同时看价值贡献、运行质量、风险、开放性和未来适配，而不是只看续费折扣。

年度评审应把供应商分为战略核心、专业能力、基础设施和可替代外围四类。战略核心数量应受控，并要求更严格的数据可携带、SLA、审计和退出演练。

价值评估应扣除人工补链、废稿、异常处理、重复系统和迁移准备等成本。对于未能进入真实流程的“活跃使用”，不应按生产价值计入。

供应商路线图只能作为参考。企业的年度决策应以已交付能力、真实运行证据和合同保障为基础，不以尚未上线的承诺替代验收。

表 41 年度组合评审矩阵

维度	评审问题	可能动作
业务价值	是否持续改善经营指标，还是仅提高局部产量？	深化、缩小、停止
采用与运营	目标用户是否稳定使用，人工负担是否可接受？	培训、流程改造、替换
质量与可靠性	失败是否可预测、可恢复，SLA是否兑现？	整改、赔偿、双供应商
成本	单位结果和三年TCO是否优于替代方案？	议价、路由、合并
安全合规	审计、事件、分包商和监管变化是否满足？	补充条款、限制使用、退出
开放与迁移	数据、配置、日志和工作流是否可带走？	迁移演练、整改、降低依赖
路线适配	产品方向是否仍与企业架构一致？	战略合作或替代
集中度	单一供应商故障或涨价影响是否可承受？	建立备份、分拆能力

附录 I：退出与迁移演练手册

退出能力只有经过演练才可信。关键供应商至少每年进行一次桌面演练，核心平台应进行技术双跑。

退出触发包括合同到期、价格显著变化、服务质量长期不达标、重大安全或合规事件、产品停止、接口关闭、并购后策略变化以及企业主动架构调整。合同应允许企业在触发条件下获得合理迁移期和供应商协助。

迁移顺序通常为：冻结范围、导出并校验、重建身份和权限、迁移知识与配置、接入业务系统、双跑对账、切换、归档和删除。对于客户触达和广告投放，应避免在高峰期切换，并准备人工运行方案。

删除证明应覆盖主数据、备份、日志、向量索引、训练或缓存副本以及子处理者。法律或审计要求必须保留的记录，应明确保留范围、隔离和删除时间。

表 42 退出演练步骤

步骤	责任	完成证据
触发与治理	业务/采购/法务	退出决定、范围、时间表、沟通计划
资产清单	业务+CIO	数据、知识、工作流、日志、代码、凭证清单
导出与校验	供应商+CIO	全量导出、哈希/数量/字段一致性
替代环境	CIO+新供应商	身份、权限、接口、监控和容量就绪
双跑与对账	业务+CIO	结果、状态、成本和异常对比
切换与降级	业务负责人	切换窗口、人工预案、回滚点
关闭与回收	采购+安全	账号、凭证、网络、子处理者访问关闭
删除与归档	法务+安全	删除证明、依法保留清单、审计记录

附录J： 董事会年度价值报告模板

年度报告应把技术活动翻译为经营价值、风险暴露、组织能力和下一年度资本配置。

董事会不需要查看模型调用次数或指令模板数量，而需要知道哪些业务闭环已经稳定运行、形成了什么可验证结果、承担了什么风险、是否具备替换能力以及下一阶段投资的边际回报。

价值报告应区分：直接财务价值、效率价值、风险减少、能力资产和战略期权。尚不能可靠归因的收益应标注为相关性或潜在价值，不以估算数字包装确定性。

报告还应披露失败与停止项目。及时停止低价值场景是组合管理成果，而非负面指标；关键在于是否形成可复用的评测、接口、数据和治理经验。

表 43 董事会年度报告结构

部分	核心内容	证据
组合概览	核心供应商、能力层、场景与集中度	生态图、合同与依赖台账
价值结果	收入、线索、客户、效率、风险和资产	基线、对照、财务/业务系统记录
运行质量	SLA、失败、人工接管、成本、采用率	日志、工单、用量、用户数据
风险与合规	事件、审计、数据、内容、供应链变化	事件报告、审计与整改
可替换性	备用模型、迁移演练、数据可携带	演练报告与RTO
组织能力	产品负责人、运营、数据、工程与培训	岗位、流程、成熟度评估
下一年度投资	扩展、整合、替换、停止和预算	场景优先级、TCO、风险评估

PUBLISHER

关于竹势 AI 营销智库

竹势 AI 营销智库出品

竹势 AI 营销智库关注企业增长、营销组织变革、智能体运营与 AI 治理，帮助企业老板、CEO、CMO 和数字化管理者把复杂技术议题转化为可讨论、可比较、可执行的经营决策。

本报告的生态地图、组合架构和管理者工具，旨在帮助企业沿经营价值流识别能力边界，并形成可治理、可观察、可替换的 AI 营销行动系统。