



020 / SELECTION DOSSIER

ENTERPRISE AI MARKETING /
SELECTION DOSSIER

企业AI营销 选型指南

从功能演示回到经营责任：比较工具、平台、营销 OS 与服务商，
建立可验证、可运营、可退出的选型案卷。

先定义经营任务

结果—任务—能力—功能—非功能要求逐层追溯

用真实任务生成证据

盲测、失败注入、治理闸门与人工基线

分清四类方案责任

工具、平台、OS 与服务不按同一功能表排名

把退出写进签约

三年 TCO、知识转移、资产导出与替换演练

BOARD BRIEF 01

出版信息

竹势 AI 营销智库出品

项目	内容
题名	企业AI营销选型指南：工具、平台、OS与服务商怎么选
出品方	竹势 AI 营销智库
版本	2026 年 7 月
适用读者	企业董事长、CEO、CMO、CIO/CDO、采购、法务与安全、营销运营、业务单元及 AI 项目负责人
品牌主页	https://shichangbu.ai/
使用说明	本报告用于建立企业级选型、采购、PoC、治理、合同与持续运营的共同决策语言。示例权重与阈值均须由企业依据风险偏好、业务基线与法域要求校准。

版权说明：未经书面许可，不得将本报告整体或主要框架用于商业转售。企业可在内部采购、架构评审、治理审查和供应商管理中引用并改编。

证据说明：报告中的公司结果以企业披露、供应商案例或项目口径标注；公开材料未给出可归因结果时，明确写为“未披露”。法规与标准按其法域、适用对象及自愿或强制属性分别解读。

执行摘要

竹势 AI 营销智库出品

BOARD SELECTION RULE / 董事会选型原则

不要购买功能最多的产品；选择一套能在本企业约束下持续承担经营任务、留下证据并允许退出的责任系统。

任务可追溯

架构可连接

结果可验收

风险可降级

资产可带走

核心判断 企业 AI 营销选型的采购对象不是一组功能，也不是一次演示，而是一套责任系统：它必须在企业约束下持续完成明确经营任务，保留可审计证据，清楚分配产品方、服务商和企业内部责任，并在成本、风险或战略变化时能够替换和退出。

AI 营销采购之所以容易失败，根源通常不在模型能力不足，而在需求定义、架构连接、责任边界、质量证据、成本归集和退出设计彼此脱节。管理层常在演示阶段看到“生成得快”，却没有确认真实业务里的身份、权限、知识、工作流、渠道、记录系统、日志和审批是否连通；在合同阶段购买了许可，却没有购买数据迁移、知识转移、运行保障和终止支持；在上线阶段统计使用量，却没有验证经营结果和风险暴露。

十条可证伪的经营结论

1. 任何无法追溯到经营结果、业务任务和责任人的功能需求，都不应进入强制采购项。若上线后仍无法说明该功能减少了哪类失败、缩短了哪段周期或改善了哪项决策，它就是待删除需求。
2. 单点工具适合边界清楚、可独立交付、替换成本低的任务；横向平台适合跨部门复用的模型、知识、工作流和治理能力；AI 营销 OS 适合需要长期管理目标、任务、数据对象、权限、审批和复盘的营销行动系统。三者不是成熟度排名，而是责任范围不同。
3. 架构适配优先于功能丰富。供应商若不能在企业身份体系、记录系统和审计链上留下完整证据，功能越多，影子流程和责任空洞越大。
4. 买、建、组装与混合的分界由资产专用性、差异化价值、变更频率、控制要求和人才供给共同决定。高差异化且高变更的决策逻辑宜由企业控制；通用底座和低差异化能力宜采购或托管。

5. PoC 必须使用真实任务、人工基线、盲测样本、失败注入和退出阈值。仅验证“能否生成”不构成采购证据；至少要验证质量、稳定性、可恢复性、单位成本、风险事件和人工复核负荷。
6. 权限、隐私、内容责任、日志、人工复核、供应链和适用法域是采购主闸门，不是中标后的整改项。高风险缺口应触发否决、封顶或限定场景，而不是用平均分抵消。
7. 三年 TCO 的主要不确定性常来自集成、人工复核、数据治理、变更、评测和退出，而非首年许可费。任何只比较订阅价格的决策都可能系统性低估成本。
8. 产品能力与服务商能力必须分开评分。优秀产品可因实施团队薄弱而失败；优秀顾问也无法补救不可审计、不可导出、无法满足安全要求的产品。
9. 合同必须把数据权利、知识资产、配置导出、组件替换、最低消费、终止支持、审计和退出演练写成可验收义务。没有退出义务的采购，等于接受未来议价权转移。
10. 选型结束只是运营治理开始。月度运行看任务与异常，季度复评看价值、风险与成本，年度替换看战略适配和可替换性；未持续复评的系统会因模型、价格、法规和组织变化迅速失配。

董事会问题	必须取得的证据	不能接受的替代品
为什么买	经营结果、目标任务、人工基线、失败成本	行业热度、供应商路线图、同行都在用
买什么	责任边界、架构连接、数据与审批链	功能数量、模型榜单、演示观感
为什么是它	真实任务 PoC、风险闸门、三年 TCO、服务能力	通用案例、未经复核的 ROI、最低报价
如何控制	RACI、SLA、审计、预算、变更与停止机制	口头承诺、售后响应群、无限制制
如何退出	导出格式、迁移窗口、终止支持、退出演练	“数据归客户所有”的原则性条款

第一章 选型对象：从功能产品转向责任系统

竹势 AI 营销智库出品

责任系统六构件

任何一项缺失，都可能把供应商能力变成企业责任真空

01

经营任务

对象、情境、结果

02

数据与知识

权利、质量、边界

03

模型与工具

能力、版本、限制

04

流程与权限

触发、审批、接管

05

证据与控制

评测、日志、追责

06

运营与退出

变更、迁移、终止

1.1 为什么功能清单会制造错误确定性

功能清单把复杂经营问题切成大量可勾选条目，方便比较，却隐去了四类关键差异：任务发生的上下文、输入数据的质量、失败时的责任、以及能力离开演示环境后的持续运行条件。两个产品都可以标注“内容生成、客户洞察、自动发布”，但一个只能在独立工作台输出草稿，另一个能继承企业身份、读取经授权知识、进入审批、写回记录系统并保留日志。两者承担的经营责任并不

相同。

Drucker 在《管理：任务、责任、实践》中把管理的起点放在任务和结果，而非工具占有。用于 AI 选型时，管理转译是：先确定必须完成的经营任务、结果标准和责任人，再决定资源组合。其当代修正是，AI 的输出并非最终结果，任务定义还要包含数据来源、自动化权限、人工复核、异常处理和证据留存。

1.2 责任系统的六个构件

构件	管理问题	采购证据
经营任务	系统具体承担哪段工作，成功与失败如何定义	任务说明、基线、输入输出、责任人、周期与边界
能力组合	需要生成、检索、判断、执行、监控还是协同	能力映射、依赖、限制、可替代组件
技术与连接	如何接入身份、数据、知识、流程、渠道和记录系统	架构图、接口清单、数据流、写回机制
治理控制	谁能做什么，哪些动作必须审批，如何停止与追溯	RBAC/ABAC、审批流、日志、告警、回滚、保留策略
运营责任	产品方、服务商、企业内部如何分工	RACI、SLA、升级路径、问题管理、知识转移
经济与退出	三年成本、变更成本、迁移成本和替换条件是什么	TCO 模型、导出验证、终止支持、退出演练

1.3 有限理性与“可比较证据”

Herbert Simon 的有限理性说明，决策者在信息不完备、时间受限和认知负荷高的情况下，往往寻求“足够好”的方案。企业软件采购因此容易把可见、易懂、可展示的功能当作质量代理。AI 进一步放大这一问题：语言输出流畅会形成能力错觉，单次成功会掩盖稳定性，厂商准备充分的样例会替代真实业务证据。采购机制必须把注意力从演示转向可重复测试，把供应商叙述转为企业可验证的证据包。

管理含义 任何选型材料都应回答三个问题：该能力承担什么任务；失败由谁发现、处理和承担；停止或替换时企业能带走什么。答不清的能力不进入核心架构。

第二章 需求定义：经营结果—任务—能力—功能—非功能要求

竹势 AI 营销智库出品



2.1 需求追溯树

需求追溯树把“想要什么功能”改写为五层可验证链条。最上层是经营结果，例如降低获客成本、缩短内容周转、提高销售响应、减少合规事件；第二层是业务任务；第三层是需要的能力；第四层才是技术功能；第五层是非功能要求，包括安全、可用性、性能、可解释、可审计、可移植和成本。任何功能都必须能向上追溯到任务和结果，向下落到验收证据。

层级	示例问题	示例证据
经营结果	哪个财务、客户、流程或风险结果要改变	基线、目标区间、观察周期、影响边界
业务任务	由谁在什么触发条件下完成什么工作	任务流程、输入、输出、时限、责任人
能力	系统需要识别、检索、生成、决策、执行还是监控	能力分解、人工与机器分工、异常路径
技术功能	哪些功能或接口支撑能力	功能规格、API、连接器、工作流节点
非功能要求	在何种安全、性能、稳定和成本约束下运行	SLO、权限、日志、数据驻留、恢复、导出、预算

2.2 Jobs to Be Done：把购买理由写成进步任务

Christensen 等人提出的 Jobs to Be Done 强调客户“雇用”产品来完成特定情境中的进步。用于企业 AI 营销，任务不能写成“采购一个内容平台”，而应写成：“当新品上市且渠道素材需求在两周内集中爆发时，市场团队需要在品牌和法规边界内生成、审校、适配并发布多渠道素材，同时保留版本、依据和审批记录，以避免延期、返工和违规。”这一写法同时揭示功能、非功能要求与组织责任。

2.3 需求分级与否决逻辑

等级	定义	处理规则
经营必要	缺失将使目标无法达成或风险不可接受	进入必选项；必须有验收证据
架构必要	缺失会造成身份、数据、记录或审计断裂	作为架构闸门；不能由平均分抵消
优化价值	能改善效率、体验或单位成本，但可分阶段上线	进入加分项或路线图
探索能力	价值尚未验证或依赖未来组件	限定预算与期限，用实物期权管理
展示性需求	无法追溯到结果，或只是为了“看起来先进”	删除或放入非采购观察项

2.4 需求追溯模板

编号	经营结果	任务与责任人	能力	功能/接口	非功能要求	验收证据	退出条件
RT-01	示例：内容周转周期缩短	品牌运营负责人完成多渠道适配与审批	知识检索、生成、规则检查、工作流	品牌库、审批、版本、渠道导出	权限隔离、日志完整、峰值时延	盲测质量、周期、返工率、日志抽查	连续两季未达阈值或迁移不可接受
RT-02	企业自行填写	企业自行填写	企业自行填写	企业自行填写	企业自行填写	企业自行填写	企业自行填写

第三章 四类方案边界：工具、平台、OS与服务

竹势 AI 营销智库出品

TOOL

单点工具

承担一个窄任务
企业负责拼接运营

PLATFORM

横向平台

提供复用能力
企业定义业务对象

OS

营销 OS

连接对象与流程
共同承担持续运营

SERVICE

实施 / 运营服务

交付项目或结果
必须锁定知识转移

3.1 边界不是产品名称，而是承担责任的范围

市场中的“平台”“OS”“智能体平台”命名并不稳定，采购方不能按厂商自称分类。更可靠的方法是观察其管理对象和责任边界：单点工具通常管理一个任务或产物；横向平台管理可复用的模型、知识、工作流和治理能力；AI 营销 OS 管理营销目标、业务对象、任务状态、权限、审批、渠道执行和持续复盘；咨询实施与运营服务管理设计、集成、变更、能力转移和日常运行。

类型	主要对象	最适场景	关键依赖	主要风险	退出重点
单点工具	一个任务、素材或局部流程	任务边界清楚、独立价值高、替换频繁	人工衔接、文件交换、基础账号治理	工具堆叠、数据散落、责任停在草稿	标准格式导出、账号与资产回收
横向平台	模型、知识、工作流、智能体、治理组件	多个部门复用共同底座并需统一控制	企业架构、平台团队、连接器和治理制度	平台过度建设、场景价值不足、开发积压	API、配置导出、模型与组件替换
AI 营销 OS	目标、营销对象、任务、渠道、审批、运营节奏	需要端到端经营闭环和长期运营	记录系统、组织权限、数据治理、运营责任	业务绑定深、迁移复杂、供应商锁定	业务对象、历史状态、规则、知识和日志迁移
咨询/集成/运营服务	需求、方案、交付、变更和运行	组织能力不足、系统复杂、需跨部门推进	清晰 RACI、方法资产、客户投入和管理赞助	对个人依赖、知识不转移、无限定制	文档、代码、配置、培训和替代服务商交接

3.2 Porter 的取舍：拒绝“既要全部又要立即”

Porter 的战略取舍提醒管理者，系统价值来自一致的活动组合，而不是无限增加功能。企业选型时必须选择优先责任范围：是先解决内容供应链、线索运营、投放优化，还是建立全域营销行动系统。试图一次覆盖所有渠道、所有业务单元、所有数据，会增加集成面和治理面，使试点变成平台建设。取舍应围绕价值闭环、风险边界和可复制性，而不是围绕厂商模块完整度。

3.3 四类方案组合原则

用单点工具验证高频、低耦合任务；成功后通过标准接口纳入平台或 OS，而不是让文件和个人账号成为长期集成方式。

把共性的身份、权限、知识、评测、日志、模型路由和成本控制放在横向平台，避免每个场景重复建设。

只有当企业需要管理跨周期目标、工作状态、业务对象和执行闭环时，才引入 OS 级责任；否则可能形成重平台、轻价值。

服务商不替代企业责任。企业必须保留产品负责人、数据责任人、风险责任人和业务验收人。

BOARD BRIEF 06

第四章 企业架构适配：连接决定能力能否进入经营现场

竹势 AI 营销智库出品



4.1 八类连接

连接域	必须回答的问题	最低证据
身份	是否继承企业 SSO、组织、角色、离职与外部协作身份	身份流程、角色映射、禁用时效、特权账号清单
数据	数据从哪里来、到哪里去、是否跨境、如何删除和保留	数据流图、分类分级、驻留、加密、删除证明
知识	知识如何授权、更新、引用、过期和撤回	知识目录、权限继承、版本、来源与删除机制
工作流	任务状态、审批、异常、重试和回滚如何管理	状态机、审批矩阵、失败路径、人工接管
渠道	外部发布、触达、广告和客户互动使用何种权限	渠道授权、发送策略、频控、撤回与证据
记录系统	CRM、内容库、工单、主数据谁是最终记录	系统主责、写回规则、冲突处理、幂等机制
日志	能否重建谁在何时基于何数据做了何动作	日志字段、保留期、不可篡改、检索与导出
审批	哪些决策和动作必须由何角色批准	风险分级、审批 SLA、替代审批、紧急停止

4.2 模块化理论与可替换性

Baldwin 与 Clark 的模块化理论指出，清晰接口可以降低系统内部依赖并创造替换选择。对 AI 营销架构，模块化不等于微服务数量多，而是关键对象和接口稳定：模型层可替换，知识层保留来源和权限，工作流层保存状态和审批，渠道层使用受控连接器，记录系统保持权威数据。若厂商把模型、知识、流程、业务状态和日志封装为不可导出的专有对象，所谓“一体化”会转化为高迁移成本。

4.3 企业架构适配图（文字版）

层级	核心对象	企业控制点	供应商可承担
经营与治理层	目标、预算、政策、风险偏好、责任	董事会/管理层批准，业务负责人验收	提供指标、证据和运营建议
业务运行层	活动、内容、线索、客户、商机、任务、审批	业务规则、关键决策、最终记录	工作流、协同、自动化与监控
智能能力层	模型、知识检索、评测、规则、智能体	模型准入、知识权限、质量门槛	模型路由、检索、生成、评测工具
集成与数据层	身份、API、事件、主数据、日志	架构标准、数据分类、记录系统	连接器、编排、日志采集
基础设施层	云、本地、算力、密钥、网络、备份	部署边界、密钥与恢复策略	托管、运维、容量与可用性

4.4 架构适配的否决项

无法继承企业身份与及时撤销权限，却需要访问敏感数据或执行外部动作。

无法说明权威记录系统，多个系统可同时修改客户、预算或发布状态。

关键日志不可导出、字段不足以重建操作，或日志由普通管理员可随意删除。

知识权限与源系统权限脱节，导致检索结果越权暴露。

模型、组件、配置或业务对象只能通过人工截图和复制迁移。

BOARD BRIEF 07

第五章 买、建、组装或混合：用交易成本与实物期权决策

竹势 AI 营销智库出品

任务是否构成持续差异化？
低
购买标准能力 以速度和可替换性为先
高
数据、规则和反馈是否可控？ 不可控则先补底座
可控
组装或自建核心 外购模型与通用组件
所有路径都必须提交三年 TCO、运营责任与退出卡

5.1 决策变量

变量	偏向采购	偏向自建/控制	管理解释
差异化	行业通用、客户不可感知	直接决定竞争优势或专有流程	差异化逻辑应由企业掌握
速度	需要快速上线验证	可接受建设周期并有稳定团队	先采购可作为学习期权
资产专用性	标准数据与通用接口	专有数据、规则、渠道或流程高度耦合	专用性越高，受制于供应商风险越大
控制与合规	低敏感、外部托管可接受	高监管、关键决策、数据边界严格	控制要求决定部署和审计深度
变更频率	能力成熟、变化可由厂商吸收	业务规则高频变化且需快速发布	高频变化要求内部产品能力
人才与运营	内部缺少平台和运维能力	有产品、架构、数据与风险团队	自建不是开发一次，而是长期产品责任
锁定成本	标准导出、替代供应充分	专有对象、最低消费、迁移复杂	合同与架构共同决定锁定

5.2 Coase/Williamson：边界取决于交易成本和资产专用性

Coase 解释企业与市场边界时强调交易成本，Williamson 进一步讨论资产专用性、不确定性和交易频率。对应 AI 选型：采购价格只是市场交易成本的一部分，需求澄清、供应商监督、变更谈判、接口协调、质量争议和退出迁移同样构成成本。若营销规则、知识和数据高度专有，且变更频繁，完全外包会产生持续谈判和依赖；若能力通用且供应充分，自建则可能承担不必要的固定成本。

5.3 买/建/组装决策树

- 该任务是否直接形成企业差异化，且业务规则高频变化？若“否”，优先采购成熟能力；若“是”，进入下一问。
- 是否涉及高敏感数据、关键客户决策或监管责任，需要企业直接控制？若“是”，保留核心逻辑、数据和审计控制。
- 企业是否具备持续产品、架构、评测、运维与治理团队？若“否”，采用混合模式：企业掌握规则与数据，供应商提供底座和交付。
- 市场是否有标准接口和可替代供应？若“是”，采用组装；若“否”，把退出和替代成本纳入三年 TCO。
- 价值与技术路径是否仍高度不确定？若“是”，采用小额、分阶段、可停止的实物期权，而非一次性长期承诺。

5.4 实物期权：把不确定性转成分段投资

实物期权思想的价值不是延迟决策，而是设计保留选择权的投资结构。企业可以先购买时间受限、范围受限的试点权；通过真实任务证据决定扩展、暂停、替换或内建。合同应避免试点自动转长期最低消费，技术上应避免在证据不足时把关键业务对象迁入专有结构。每一阶段都要有继续投资的证据门和停止条件。

第六章 把演示改造成真实任务 PoC

竹势 AI 营销智库出品

01

真实任务包

常态、边界、异常、攻击

02

盲测与基线

同输入、人工基线、统一评分

03

失败注入

断连、越权、脏数据、版本变更

04

运营观察

延迟、成本、接管、恢复

05

证据决议

通过、限用、返工、退出

6.1 PoC 的目标是减少决策不确定性

PoC 不是缩小版上线，也不是供应商展示。它要回答：在本企业数据、人员、流程、风险和成本约束下，该方案能否稳定承担特定任务；失败是否可发现、可恢复；人工复核负荷是否可接受；证据是否足以支持下一阶段投资。为避免供应商对样例过拟合，测试包应包含公开任务、盲测任务、边界任务和失败注入。

6.2 真实任务 PoC 测试包

测试域	设计要求	建议指标（企业校准）	证据
任务成功	使用真实输入和真实交付格式，覆盖常规与复杂任务	任务完成率、一次通过率、周期、返工	样本、输出、评审记录
人工基线	同一任务由现有团队完成，保持质量要求一致	质量差异、周期差异、人工时、错误类型	基线工单、时间记录、盲评
盲测质量	评审者不知道产出来源，采用统一量表	准确、完整、品牌一致、可执行、风险	评分表、分歧与复核
稳定性	重复执行、并发、峰值和长周期任务	波动、超时、失败率、恢复时间	运行日志、重试记录
失败注入	缺失数据、错误权限、接口中断、冲突指令	发现率、停止行为、降级、恢复	故障脚本、告警、恢复证据
风险与治理	越权请求、敏感数据、违规内容、未经批准外发	阻断率、误阻断、日志完整、审批覆盖	红队样本、审批与日志
成本	统计许可、模型、算力、人工复核和支持	单位任务成本、波动、峰值预算	计量报表、人工记录
退出	导出配置、知识、业务对象和日志并在替代环境重建	导出完整、重建时间、数据损失	导出包、重建演示

6.3 Deming：质量是系统属性，不是末端检验

Deming 的质量思想强调稳定过程、统计理解和持续改进。用于 AI PoC，管理重点不是挑出几条漂亮样例，而是理解输出分布和失败模式：同类任务是否稳定；错误是否集中在特定数据、语言、渠道或权限场景；人工复核是否真正降低风险，还是把成本转移给员工；改进能否通过知识、规则、工作流和模型组合沉淀，而不是依赖个别操作者技巧。

6.4 PoC 通过、限用与退出阈值

结论	触发条件	后续动作
通过	经营价值、质量、稳定、治理和成本同时达到预设门槛	进入受控试点或规模化；固化基线与 SLO
限用	价值成立，但在敏感数据、外部动作或复杂任务存在缺口	限定场景、权限、数据和人工复核；设整改期限
补测	关键样本不足、接口或数据准备不完整，结论不确定	只补足影响结论的测试，不扩大范围
退出	主闸门失败、单位成本不可接受、迁移不可行或供应商拒绝关键义务	停止采购；执行数据清理和经验复盘

BOARD BRIEF 09

第七章 治理与安全闸门：合规不是平均分项目

竹势 AI 营销智库出品

G1

合法与适用范围

G2

数据权利与最小化

G3

身份权限与隔离

G4

内容责任与标识

G5

评测日志与追溯

G6

人工审批与接管

G7

供应链与退出

风险分级决定闸门强度；认证和合规声明不能替代本企业任务验证。

7.1 中国规则与国际框架的边界

中国《生成式人工智能服务管理暂行办法》面向向境内公众提供生成式人工智能服务的情形，企业内部使用是否直接落入适用范围，需要结合服务对象、提供方式和具体业务判断。自 2025 年 9 月 1 日起施行的《人工智能生成合成内容标识办法》及配套强制性国家标准 GB 45438-2025《网络安全技术 人工智能生成合成内容标识方法》，强化了生成合成内容显式与隐式标识、传播平台核验和服务提供者责任。企业采购时应确认产品在内容生成、文件元数据、发布链路和平台接口中的标识能力，但不能把公众服务规则机械等同于所有内部系统要求。

NIST AI RMF 1.0 以 Govern、Map、Measure、Manage 组织风险活动，属于自愿框架；ISO/IEC 42001 规定 AI 管理体系要求，可用于组织建立治理制度和接受认证。二者可以帮助企业构建跨产品的治理方法，但不替代具体法域的法律义务。采购文件应把“遵守法律”“符合框架”“取得认证”和“通过企业控制测试”区分开。

7.2 七道治理与安全闸门

闸门	核心问题	处理规则
身份与权限	最小权限、特权访问、离职撤销、机器身份是否可控	高风险缺口否决；低风险限期整改
隐私与数据	目的、最小化、驻留、跨境、保留、删除、训练使用	无法限制二次使用或删除时否决
内容责任	事实、版权、品牌、广告、标识、外部发布责任	关键内容必须有规则、证据和审批
日志与审计	能否重建输入、知识、模型、工具、审批和外部动作	关键链日志不完整时不得自动执行
人工复核	复核点是否按风险设置，人员是否有时间和能力	人工复核负荷纳入成本和产能
供应链	模型、插件、开源组件、云和分包商是否透明	建立组件清单、变更通知和替代方案
韧性 & 停止	异常发现、降级、回滚、密钥吊销、业务连续性	必须通过失败注入与停止演练

7.3 NIST、ISO 与监管视角的管理转译

机构/专家视角	原始上下文	本报告转译	边界
NIST AI RMF	组织识别、衡量和管理 AI 风险的自愿框架	RFP 要求供应商提供风险映射、测量方法、控制证据与剩余风险	不是法规合规证明
ISO/IEC 42001	AI 管理体系要求	评估供应商是否有职责、风险、生命周期、事件与持续改进机制	认证不等于具体产品安全
中国网信等部门	生成式 AI 服务和生成合成内容治理	核对适用范围、内容标识、数据与服务责任，落到产品和发布链	不同业务、法域需单独法律判断
OWASP GenAI Security Project	大模型应用常见安全风险与测试实践	用于设计越权、检索污染、工具滥用、敏感信息和供应链测试	社区项目，不替代企业威胁建模

BOARD BRIEF 10

第八章 三年 TCO：把隐藏成本和波动成本放进同一模型

竹势 AI 营销智库出品



8.1 十一类成本账户

成本账户	包含内容	常见遗漏
许可/订阅	席位、模块、环境、API、存储、支持等级	测试环境、只读用户、外部协作账号
模型与算力	调用量、上下文、推理、向量、图像/视频、峰值容量	重试、失败调用、评测和批处理
数据	清洗、标注、权限、迁移、保留、删除	知识过期维护、主数据对齐
集成	接口、连接器、事件、主数据、身份、渠道	版本升级、接口限流、异常补偿
评测	测试集、盲评、红队、回归、监控	新模型或规则变更后的重新评测
人工复核	审核、纠错、升级、抽检和高风险批准	复核拥堵、培训和机会成本
培训与变革	角色培训、流程重构、沟通、激励和采用支持	管理者时间、岗位重新设计
运维	监控、SLA、事件、容量、备份、密钥和发布	夜间支持、跨供应商协调
变更	需求、规则、知识、模型、接口、法务和流程变更	小变更累积、供应商变更单
治理	隐私、安全、审计、法务、风险委员会和记录	内部控制证据、外部审计
退出迁移	导出、转换、并行运行、验证、终止支持和数据销毁	业务中断、知识重建、最低消费

8.2 三年 TCO 模型（示例口径，由企业自行校准）

年度 TCO = 固定许可与基础设施 + 用量成本 + 数据与集成摊销 + 评测与治理 + 人工复核 + 培训与变革 + 运维与变更 + 风险准备金。三年 TCO 还应加入扩张情景、价格变化、模型替换和退出迁移。模型必须同时展示基准、增长和压力情景，避免用单点预测掩盖波动。

变量	基准情景输入	增长情景输入	压力情景输入	责任人
业务量	任务数、用户数、渠道数	规模扩张与新场景	峰值、重试和低质量数据	业务负责人
单位用量	每任务调用、存储、检索	更复杂任务与更长上下文	模型价格、汇率或算力变化	技术/财务
人工复核	复核比例与时长	高风险场景比例上升	质量波动导致返工	业务/风险
集成变更	计划内接口与升级	新增系统和业务单元	核心接口重构或厂商停服	架构负责人
退出迁移	计划性演练与导出验证	并行运行与替代组件	紧急终止、数据转换和业务恢复	采购/架构/法务

8.3 单位经济性与预算控制

采购团队应把“每席位价格”改写为“每个合格任务、每个获批资产、每个有效线索或每个受控工作流周期的全成本”。单位成本需要包含失败任务和人工复核。预算控制应设置调用上限、模型路由、异常告警、场景预算和停机阈值；成本下降不能以质量、审计或风险转移为代价。

第九章 产品与服务商双评分：能力与交付不能互相代偿

竹势 AI 营销智库出品



9.1 产品评分矩阵

维度	评价重点	证据形式	主闸门
任务能力	真实任务质量、稳定性、边界和恢复	PoC 样本、日志、盲评、失败注入	是
架构适配	身份、数据、知识、流程、渠道、记录、日志	架构评审、接口验证、数据流	是
治理安全	权限、隐私、内容、审计、供应链、停止	控制测试、报告、清单、演练	是
经济性	三年 TCO、用量透明、扩张与退出成本	报价结构、计量、情景模型	否，但需封顶
可替换性	导出、标准接口、模型与组件替换	导出测试、替代演示、合同义务	是
产品路线	版本治理、兼容、弃用、客户影响	发布记录、路线图、变更政策	否

9.2 服务商评分矩阵

维度	评价重点	证据形式
行业理解	能否识别价值链、渠道、监管和任务边界	情境案例、方案样稿、关键假设
交付方法	需求、架构、数据、评测、上线与变更是否有方法	交付计划、模板、质量门
RACI 与团队	关键角色是否明确，是否依赖单一明星顾问	实名团队、投入比例、替补机制
SLA 与运营	事件分级、响应、恢复、问题管理和报告	SLA、历史服务数据、运营样报
知识转移	企业能否接管配置、规则、评测和运营	培训计划、文档、代码与配置交付
持续改进	是否按运行证据优化，而非无限追加需求	月报、季度复评、变更治理
财务与供应稳定	现金流、关键人员、分包、保险和业务连续性	财务材料、分包清单、连续性计划
退出协作	是否支持替代服务商、数据迁移和并行运行	终止支持方案、退出演练

9.3 RFI/RFP 评分卡（示例权重，由企业自行校准）

评分卡不应先给出行业通用权重。企业应先按场景风险确定否决项和封顶项，再对剩余可比较项设权重。评分必须引用证据编号，并记录不确定性和前提。

编号	要求	类型	供应商答复	证据编号	采购方评分	风险/前提
RFP-01	真实任务 PoC 达到企业门槛	主闸门				
RFP-02	支持企业身份、权限与离职撤销	主闸门				
RFP-03	业务对象、知识、配置与日志可导出	主闸门				
RFP-04	三年 TCO 与用量计量透明	评分/封顶				
RFP-05	实施团队、RACI、SLA 与知识转移	评分				
RFP-06	路线图与弃用政策	评分				

第十章 企业与实证案例：选型机制比技术标签更重要

竹势 AI 营销智库出品

九个案例只回答一个问题：什么机制允许能力在真实约束下持续交付？

企业披露、供应商材料与现场实验按不同证据等级使用；没有公开财务归因时不反推 ROI。

以下案例用于说明选型机制，不构成对任何供应商或产品的推荐。公司披露和供应商案例均可能存在选择性披露；未公开的数据明确标注“未披露”。

案例一：摩根士丹利财富管理与 OpenAI（2023—2024）

主体与情境：摩根士丹利财富管理业务需要让顾问更快检索内部研究与知识，同时保持合规和客户责任。具体动作：公司与 OpenAI 合作构建内部知识助手，先在受控顾问群体中测试，再扩大使用；系统强调从内部批准内容中检索，并把最终客户沟通责任留给顾问。公开结果：公司披露了广泛采用和知识访问改善，但未披露可独立归因的收入或利润结果。机制：以高价值知识任务切入，限定数据源和用户，保留人工责任。归因限制：企业自报，缺少公开对照组。边界：适合知识密集、合规要求高且拥有高质量内部内容的组织。管理启示：高监管行业的首个场景应优先选择可控检索和辅助决策，不宜直接授权外部承诺。[S19][S20]

案例二：JPMorgan Chase 的 LLM Suite（2024）

主体与情境：JPMorgan Chase 面向员工推出内部生成式 AI 能力，需要在大型金融机构的安全、数据和合规体系内提供通用生产力。具体动作：公司建立内部受控入口，把多类模型能力放在企业治理、权限和数据控制之下，并逐步扩展用户。公开结果：公司披露员工覆盖规模和使用方向，未披露独立财务回报。机制：企业控制入口、策略和数据边界，模型可作为组件演进。归因限制：公开信息主要来自公司管理层和媒体转述。边界：适合拥有成熟平台、安全和运营团队的大型企业。管理启示：当模型变化快、组织规模大时，控制面和统一入口可能比锁定单一模型更有长期价值。[S21]

案例三：Klarna 客服 AI 与人工服务再平衡（2024—2025）

主体与情境：Klarna 在高频客户服务中使用 AI 助手，目标是降低响应时间和运营成本。具体动作：公司将 AI 接入大量客服对话，并披露处理量、响应时长和等效工作量；随后管理层公开强调需要保持高质量人工服务和选择权。公开结果：早期结果为公司披露口径，包含约三分之二客服对话等指标；后续对人工服务的再平衡说明质量和客户体验不能只由自动化率代表。归因限制：缺少独立审计，业务和成本变化可能受其他因素影响。边界：适合标准化问题，但复杂、情绪化和高价值交互需要人工接管。管理启示：采购阈值必须同时包含效率、质量、升级率和客户结果；规模化后仍要允许策略回撤。[S22][S23]

案例四：P&G 与 Harvard Business School “The Cybernetic Teammate”现场实验（2024）

主体与情境：研究在 P&G 的 791 名专业人员中测试生成式 AI 对产品创新任务和团队协作的影响。具体动作：参与者随机进入个人/团队及有无 AI 的条件，完成真实风格的创新任务。公开结果：研究报告显示 AI 可提高任务质量并缩短时间，个人配合 AI 的表现可接近传统团队；不同职能之间的信息边界也有所缩小。归因限制：任务、组织和工具环境特定，不能直接外推到长期经营结果或所有营销工作。边界：适合结构化、可评审的知识创作任务。管理启示：选型应评估任务重构和团队边界变化，而非只计算单人节时。[S24]

案例五：联合利华 Desire at Scale 与 AI 内容运营（2024—2026）

主体与情境：联合利华推进 social-first demand generation，需要在多品牌、多市场环境下提高内容速度、适配和学习。具体动作：公司披露将 AI、数据和内容能力纳入营销转型，并通过品牌、平台和运营机制推动规模化；关键品牌保持人工创意与品牌责任。公开结果：公司披露战略进展和部分运营指标，但不同材料口径不一，无法把整体增长归因于某一 AI 工具。归因限制：企业转型包含品牌组合、媒体、组织和成本项目。边界：适合拥有全球品牌治理、内容供应链和大量可复用资产的企业。管理启示：平台价值来自运营体系和品牌规则，不是批量生成本身。[S25][S26]

案例六：中国平安的 AI 销售与客户服务体系（2023—2025）

主体与情境：中国平安在金融、保险和健康服务中长期建设 AI 能力，营销相关任务涉及客户服务、销售支持、风险管理和运营。具体动作：公司通过自建技术平台、数据治理和业务系统集成，把 AI 嵌入销售与服务流程，并在人机协同与风险控制下运行。公开结果：年报披露 AI 坐席、服务量、覆盖和效率等多类指标，具体年份和口径随业务变化；不能把集团经营结果单独归因于 AI。归因限制：公司自报，且多业务、多技术共同作用。边界：适合数据规模大、流程标准化、内部技术和治理能力强的企业。管理启示：高专用性、长期积累的客户与风险能力更适合企业控制核心数据、规则 and 平台，外部产品作为组件。[S27][S28]

案例七：阿里国际 Accio 与商家营销/采购辅助（2024—2026）

主体与情境：阿里国际面向跨境商家提供 AI 驱动搜索、采购和商业辅助能力，商家需要在多语言、多市场和复杂商品信息中完成研究与决策。具体动作：平台把模型能力与商品、供应链和交易数据结合，提供商业搜索和辅助 workflow。公开结果：公司披露用户增长和产品使用，但未披露可独立验证的商家利润提升。归因限制：平台披露，且跨境贸易结果受需求、物流、汇率和运营能力影响。边界：适合依赖平台数据和跨境知识的商家任务。管理启示：平台优势来自专有数据和交易连接；企业采购时应评估数据可移植性、平台依赖和外部规则变化。[S29][S30]

案例八：联想的混合式 AI 与全球营销运营（2024—2026）

主体与情境：联想同时是全球品牌、硬件与企业技术提供者，需要在多市场运营中使用 AI，并强调公共云、私有环境和端侧的混合架构。具体动作：公司在年度报告和技术披露中把混合式 AI 作为战略方向，营销与客户运营可使用企业知识、生成内容和分析能力，但具体单一营销系统结果未披露。公开结果：公司披露整体 AI 战略、产品与服务进展，无法把营销表现归因于某一工具。归因限制：公司同时作为供应商和使用者，披露带有战略传播属性。边界：适合多法域、多数据边界和既有基础设施复杂的企业。管理启示：混合模式的关键不是部署地点数量，而是统一身份、策略、数据和运营证据。[S31][S32]

案例九：海尔智家的数字化客户运营与平台化能力（2023—2025）

主体与情境：海尔智家在多品牌、零售与服务网络中推进数字化运营，客户触点、内容、销售和服务需要跨渠道协同。具体动作：公司通过自有数字平台、用户运营和生态协同沉淀业务数据，并逐步引入智能能力。公开结果：年报披露数字化运营、用户和效率相关进展，但没有把经营结果独立归因于某个 AI 营销产品。归因限制：渠道改革、品牌、供应链和组织机制共同作用。边界：适合有广泛渠道和长期用户运营能力的消费企业。管理启示：OS 级能力应建立在业务对象和记录系统之上；单独采购生成工具无法替代客户与渠道基础。[S33]

第十一章 管理思想与当代专家视角：建立共同决策语言

竹势 AI 营销智库出品

思想和专家观点只有在能改变一项选型决议时才进入案卷

每项观点均说明原始语境、管理转译和不可外推的边界。

11.1 七个经典思想的选型转译

思想	原始问题	选型连接	当代修正
Drucker：任务与责任	组织如何围绕结果配置资源	先定义经营任务、责任和结果，再选工具	AI 任务还需数据、权限、复核和证据
Christensen：Jobs to Be Done	客户为何在特定情境“雇用”产品	把采购需求写成情境、进步和阻碍	企业任务涉及多角色、合规与系统依赖
Simon：有限理性	决策者如何在约束下做满意化选择	用标准证据降低演示偏差和信息负荷	需要处理模型不确定性与快速变化
Coase/Williamson：交易成本	何时通过市场，何时在组织内部完成	把协调、监督、变更和退出纳入买建决策	软件即服务使依赖持续存在，不能只看签约成本
模块化理论	如何通过接口分解复杂系统	稳定对象和接口，保留组件替换权	AI 的模型、知识、工作流和状态需分层
Porter：取舍	战略为何需要选择不同活动组合	明确优先责任范围，拒绝全功能冲动	平台生态会诱导范围扩张，需证据门
Deming：质量系统	如何减少过程波动并持续改进	测试分布、失败模式和过程控制	生成结果概率化，需持续评测与人工反馈
实物期权/双环学习	如何在不确定性中保留选择并修正假设	分段投资、可停止、复评任务定义	不仅优化参数，还要质疑场景、流程和责任设计

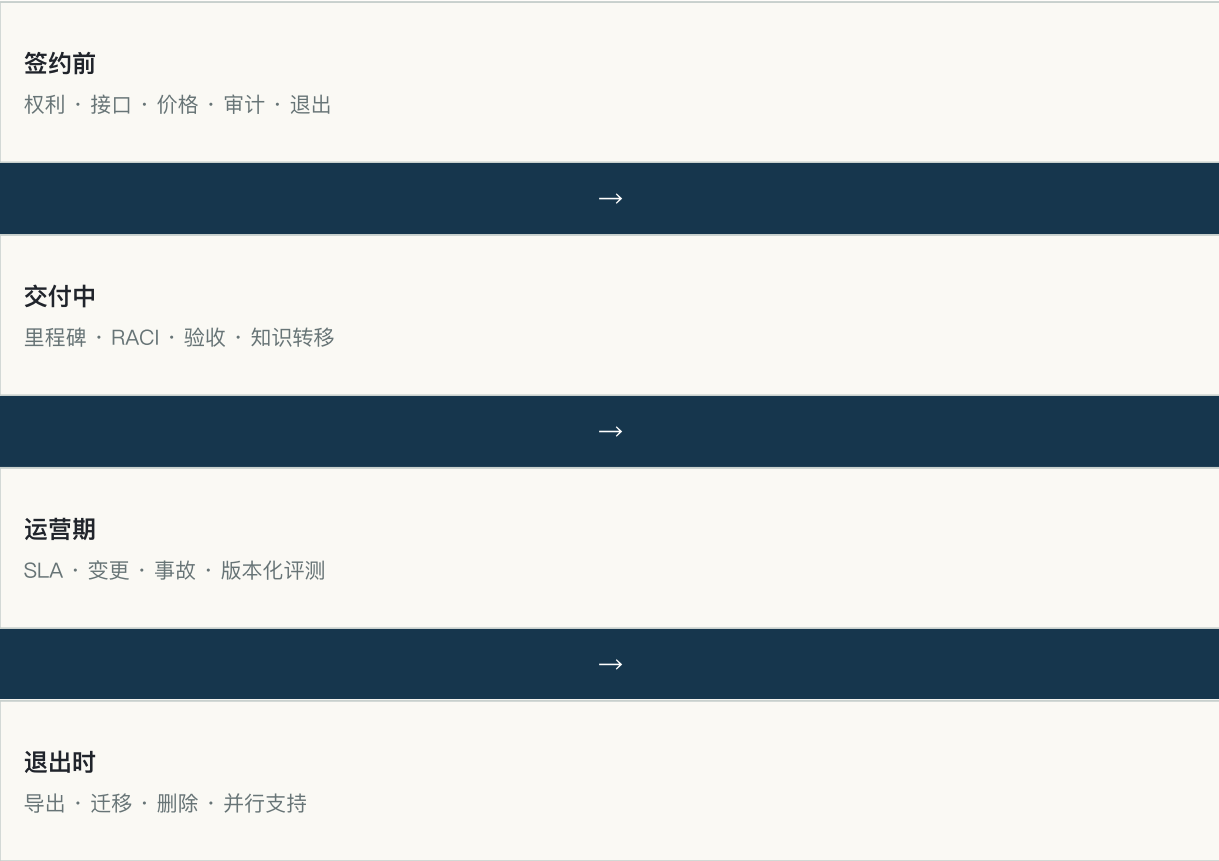
11.2 当代专家与机构视角

专家/机构	正式出处与上下文	与选型的连接	适用边界
Andrew Ng	关于数据中心化 AI 与迭代开发的课程、演讲和企业实践	场景质量依赖数据和快速迭代，采购应评估数据闭环和评测能力	不等于所有场景都适合自建
Ethan Mollick	《Co-Intelligence》及组织实验讨论	AI 使用会改变任务分工，PoC 应评估工作设计而非只评输出	面向知识工作的一般框架
Erik Brynjolfsson 等	呼叫中心生成式 AI 现场研究	收益可能集中在经验较少员工，需观察分布效应和组织学习	特定客服环境，不能直接外推营销 ROI
NIST	AI RMF 1.0 与生成式 AI 配置文件	把治理、映射、测量和管理写入生命周期证据	自愿框架
ISO/IEC	ISO/IEC 42001 AI 管理体系	评估供应商治理职责、风险和持续改进机制	认证不是产品性能或合规保证
Gartner	企业架构、组合管理和“组合式企业”研究	用模块化和组合能力避免巨型套件锁定	商业研究需结合企业实际，不作事实标准
Martin Fowler	演进式架构、持续交付与技术债务著作	接口、可测试性和变更能力决定长期适配	软件工程视角，需叠加业务治理
Bruce Schneier	安全、信任和系统性风险著作	不要把安全等同于功能清单，需威胁模型、失败设计和激励分析	不替代具体技术测试
World Federation of Advertisers	Responsible AI in Marketing 指引与行业治理讨论	营销责任需覆盖品牌、消费者、内容、数据和代理商链	行业自律，不替代法律
IAPP	AI 治理、隐私与组织角色研究	采购应明确数据角色、评估、记录和跨职能责任	专业机构资料需按法域落地

BOARD BRIEF 14

第十二章 合同、交付与退出：把原则写成可验收义务

竹势 AI 营销智库出品



12.1 合同与退出清单

条款域	必须明确	验收/触发
数据权利	控制者/处理者角色、目的、范围、驻留、分包、删除、训练使用	数据流确认、删除证明、分包变更通知
知识产权	企业资料、检索索引、规则、评测集、改进成果的权属和使用权	导出与重建测试
配置与业务对象	工作流、角色、规则、模板、状态、历史和日志的导出格式	定期导出、样本恢复
模型/组件替换	替换模型、云、插件、连接器时的兼容和支持	替换演练、回归测试
最低消费与价格	用量口径、阶梯、涨价、闲置、峰值、汇率和税费	账单核对、预算告警
SLA 与事件	可用性、响应、恢复、数据事件、根因和赔偿	月报、事件报告、服务抵扣
变更与弃用	接口、模型、功能、数据政策和分包变化的通知期	影响评估、迁移窗口
审计	企业审计权、第三方报告、控制证据和整改	年度审查、重大事件专项审计
终止支持	并行期、导出、转换、培训、数据删除和人员支持	终止计划、里程碑和责任
退出演练	频率、范围、成功标准和问题整改	至少覆盖关键对象与日志

12.2 交付 RACI

活动	业务负责人	CIO/CDO/架构	安全法务	采购	供应商产品方	实施/运营服务商
经营目标与任务	A/R	C	C	I	C	C
架构与集成	C	A/R	C	I	C	R
数据与权限	C	R	A/R	I	C	R
PoC 设计与验收	A/R	R	R	C	C	R
合同与商业条款	C	C	R	A/R	C	C
上线与变更	A	R	C	I	C	R
月度运营	A/R	R	C	I	C	R
季度复评	A/R	R	R	R	C	C
退出与迁移	A	R	R	R	C	R

A=最终负责，R=执行负责，C=协商参与，I=知会。企业应按自身治理调整；任何关键活动都必须有企业内部 A，不能把最终责任外包给供应商。

12.3 持续运营机制

周期	关注对象	会议输入	必须输出
每月	任务量、质量、异常、人工复核、成本、SLA	运行报表、事件、用户反馈、预算	问题清单、规则/知识/流程变更、责任与期限
每季度	经营价值、风险趋势、架构债务、供应商表现	基线对比、TCO 更新、控制测试	继续、限用、扩展、整改或替换决定
每年	战略适配、市场替代、合同与退出能力	年度价值、风险、价格、路线图、退出演练	续约、重新竞争、架构调整或退出
重大变更	模型、法务、数据、供应链、接口或业务范围	影响评估、回归测试、法律与安全意见	批准、限制、回滚或停止

第十三章 30/60/90 天采购路线与董事会签字清单

竹势 AI 营销智库出品

0-30 定义任务与证据 基线 · 追溯树 · 否决项 · 真实任务包
31-60 完成 PoC 与比较 架构 · 治理 · TCO · 双评分 · 尽调
61-90 签约与受控上线 RACI · 验收 · 接管 · 退出演练

13.1 30 天：定义任务与证据

时间	关键动作	交付物	证据门
第 1—10 天	确认经营结果、任务、责任人、基线、风险和法域	需求追溯树、现状流程、数据与系统清单	功能需求全部可追溯
第 11—20 天	划分工具/平台/OS/服务边界，确定买建组装假设	目标架构、责任边界、长名单、主闸门	架构与治理否决项明确
第 21—30 天	发布 RFI，收集证据并缩短名单	RFI 比较、风险假设、PoC 设计	仅保留愿意接受真实任务测试者

13.2 60 天：完成 PoC 与商业比较

时间	关键动作	交付物	证据门
第 31—40 天	准备真实样本、人工基线、盲评和失败注入	PoC 测试包、评分规则、数据授权	样本代表性与风险批准
第 41—52 天	并行测试产品、服务团队和退出能力	运行证据、盲评、日志、导出包	主闸门通过或明确限用
第 53—60 天	形成三年 TCO、合同红线和推荐方案	产品/服务双评分、TCO 情景、谈判清单	方案对不确定性和退出负责

13.3 90 天：签约、受控上线与运营接管

时间	关键动作	交付物	证据门
第 61—70 天	完成合同、RACI、SLA、数据与退出条款	合同附件、实施计划、控制矩阵	关键义务可验收
第 71—82 天	受控上线、培训、监控和事件演练	上线清单、权限、日志、恢复与停止演练	业务、技术和风险共同签字
第 83—90 天	建立月度运营、季度复评和年度替换机制	运营看板、会议节奏、复评模板、退出日历	企业内部完成能力接管

13.4 董事会/经营层签字清单

签字问题	是/否	证据编号	责任人
采购对象是否被定义为明确经营任务和责任系统，而非功能集合？			
是否有人工基线、真实任务 PoC、失败注入和退出测试？			
身份、数据、知识、 workflow、渠道、记录系统、日志和审批是否适配？			
治理与安全主闸门是否全部通过，限用条件是否写入系统和合同？			
三年 TCO 是否包含人工复核、集成、评测、变更、治理和退出？			
产品与服务商是否分开评价，关键团队与替补是否确定？			
数据、知识、配置、日志、模型/组件替换和终止支持是否可验收？			
月度、季度、年度复评和停止机制是否已指定内部负责人？			
最坏情景下，企业能否在可接受时间和成本内停止、迁移并恢复业务？			

BOARD BRIEF 16

第十四章 常见失误、受限条件与决策复盘

竹势 AI 营销智库出品

单环改进

调整提示、流程、接口、阈值和责任



双环重审

任务是否仍值得做？边界和采购假设是否成立？

月度运营观察 · 季度供应商复评 · 年度替换与组合重置

14.1 八类选型失误及其纠偏

失误	表面现象	真实机制	纠偏动作
把演示当能力	样例流畅、现场回答快	供应商控制输入、知识和操作路径，未暴露异常与持续运行	改用采购方样本、盲测、重复执行和失败注入
把采用率当价值	登录和调用增长	员工可能把系统用于低价值任务，或增加复核和协调负担	按合格任务、周期、客户和风险结果评价
把一体化当集成	模块都在同一产品界面	身份、主数据、记录系统和审批仍然断裂	以数据流、状态写回和审计链验收
把认证当安全	供应商展示认证证书	认证覆盖范围、时间和系统边界可能与采购对象不同	核对适用范围并执行企业控制测试
把私有部署当控制	系统部署在企业网络	模型、组件、遥测、密钥、运维和升级仍可能受外部控制	核对供应链、管理面、远程访问与替换权
把人工复核当免责	所有输出要求人审	复核者时间不足、缺少依据或形成橡皮图章	按风险设置复核点，提供证据、培训和抽检
把定制当适配	需求都可开发	定制增加升级冲突、服务依赖和迁移成本	优先配置与标准接口，定制须有资产交付和退出方案
把低价当经济性	首年报价最低	后续用量、集成、变更、治理和退出成本被推迟	使用三年情景 TCO 和单位任务全成本

14.2 受限条件：什么时候不应启动大规模采购

企业在以下条件下不宜直接启动平台或 OS 级采购：经营问题尚未形成可验证任务；关键数据没有权威来源和责任人；业务流程频繁变化但没有产品负责人；高风险动作没有审批和停止机制；现有系统无法提供身份、记录或日志连接；管理层希望以软件替代组织决策；预算只覆盖许可而不覆盖集成、复核、运营和变更。此时更合适的动作是缩小场景、修复基础控制、建立人工基线，并以可停止的小额试验获取证据。

暂停采购并不等于放弃 AI。有限范围的单点工具、离线分析、内部知识检索和模拟环境可以作为学习工具，但必须明确其不会自动升级为生产系统。采购方应保留试验记录：哪些假设成立，哪些输入不足，哪些风险尚不可接受，哪些能力应由组织和数据改造解决。

14.3 双环学习：既优化系统，也重审任务

Argyris 与 Schön 的双环学习区分了在既定目标和规则内纠错，以及重新审视目标、规则和假设。AI 营销系统上线后，单环改进包括更新知识、调整 workflow、替换模型和优化审批；双环复评则追问：这个任务是否仍值得自动化，指标是否诱导错误行为，责任边界是否合理，客户是否接受该交互方式，组织是否把判断能力过度外包。季度复评必须至少保留一个议程，用于挑战最初的采购假设。

14.4 决策复盘模板

复盘项	核心问题	记录要求
原始假设	当时认为价值、成本、风险和采用会如何变化	保留基线、假设范围和证据强度
实际结果	哪些指标改变，哪些没有，分布和时间滞后如何	区分公司披露、系统数据和管理判断
意外后果	是否增加复核、影子流程、权限风险或客户摩擦	记录受影响角色和处置成本
供应商表现	产品、实施、运营和商务承诺分别是否兑现	引用 SLA、问题单、变更单和交付物
可替换性	导出、替换和退出演练暴露了什么	记录重建时间、数据损失和依赖项
下一步决定	继续、扩展、限用、重构、重新竞争或退出	明确责任、预算、期限和新证据门

最终决策还应记录剩余风险，而不是只记录中标理由。剩余风险包括尚未覆盖的任务、依赖人工判断的环节、供应链不可见部分、数据质量缺口、法规解释不确定性、价格和容量波动、关键人员依赖以及退出演练中未解决的问题。每项剩余风险应指定所有者、观察指标、复评日期和触发动作。只有当管理层明确知道自己接受了什么，并为风险变化准备了限制、补救或停止手段，采购批准才具有经营意义。

采购决策必须允许出现“不采购”结论。当真实任务价值不足、风险无法被控制、架构代价高于收益，或组织尚无能力接管运行时，停止项目本身就是有效的资本配置。企业应把节省的预算转向数据修复、流程标准化、人才和治理基础，以便在条件成熟后重新评估。

BOARD BRIEF 17

结语：把可退出性当作采购质量的最终检验

竹势 AI 营销智库出品

AI 营销选型的长期质量，最终体现为企业是否保有选择权。能持续承担任务、留下证据、明确责任且可以退出的系统，才值得进入核心经营流程。相反，依靠演示、个人经验、专有对象和口头承诺形成的“快速上线”，会把短期速度转换为长期锁定。

董事会不需要决定每个模型和连接器，但必须决定责任边界、风险偏好、资本承诺和退出条件。业务、技术、采购、法务与安全共同使用同一套需求追溯、PoC、TCO、双评分和合同退出机制，才能把技术选型变成可治理的经营决策。

shichangbu.ai

专题中心 · 返回顶部 ↑

附录 A 采购工作底稿索引

竹势 AI 营销智库出品

工具	主要用途	本报告位置
需求追溯树	把经营结果、任务、能力、功能和非功能要求连接	第二章
四类方案边界图	界定工具、平台、OS 与服务责任范围	第三章
企业架构适配图	检查八类连接和五层控制	第四章
买/建/组装决策树	依据差异化、控制、人才和锁定决策	第五章
RFI/RFP 评分卡	统一证据、否决项、评分和前提	第九章
真实任务 PoC 测试包	验证质量、稳定、风险、成本和退出	第六章
治理与安全闸门	实施否决、封顶和限用规则	第七章
三年 TCO 模型	计算十一类成本与情景波动	第八章
产品与服务商双评分	避免产品和交付能力互相代偿	第九章
交付 RACI	明确企业与供应商责任	第十二章
合同与退出清单	把权利和终止支持写成验收义务	第十二章
持续运营机制	月度运行、季度复评、年度替换	第十二章
30/60/90 天路线	组织采购、PoC、签约和接管	第十三章
董事会签字清单	形成最终资本与风险决策	第十三章

附录 B 供应商问询题库

竹势 AI 营销智库出品

请逐项说明产品在本场景中读取、生成、修改、发送和删除的对象，以及每项动作的默认权限。

请提交完整数据流、分包商、模型与开源组件清单，并说明变更通知机制。

请现场演示用户离职、权限撤销、知识源删除和密钥吊销后的系统行为。

请说明业务对象、工作流、知识、配置、评测集、日志和审批记录的导出格式，并完成样本导出。

请说明模型或组件替换时，哪些功能、质量、成本和合同条款会变化。

请提供过去十二个月重大服务事件、根因、修复和客户通知的汇总口径；无法披露时说明替代证据。

请列出实施团队、投入比例、关键角色替补和分包安排，并说明人员变更对交付的影响。

请把三年报价拆分为许可、用量、环境、支持、集成、培训、评测、运维、变更和退出。

请说明哪些产品路线图能力尚未正式可用，采购方不将其计入当前评分。

请接受由采购方提供的盲测、失败注入和退出测试，并允许采购方保留测试证据。

附录 C 验收证据字典

竹势 AI 营销智库出品

证据字典用于防止供应商用同一份材料回答不同问题。采购方应为每项证据指定编号、所有者、生成日期、适用版本、覆盖范围和复核结论。截图只能证明某一时点界面存在，不能单独证明持续能力；政策文件只能证明制度设计，不能单独证明控制有效；客户案例只能证明在特定客户环境发生过，不证明本企业适用。

证据类型	可以证明	不能单独证明	最低复核动作
产品文档	正式功能、配置项、接口和限制的书面说明	功能在本企业环境可用或稳定	核对版本、许可层级并现场验证
架构与数据流	组件、边界、数据流向和依赖关系	实际权限、日志和删除行为符合设计	抽查配置、网络、账号和数据样本
第三方认证/报告	特定范围、期间和控制的独立检查	采购场景全部合规或产品无风险	核对范围、例外、有效期和分包
PoC 运行日志	特定任务的调用、状态、错误和时延	长期规模化效果	复现样本、核对完整性和时间同步
盲评记录	在统一量表下的相对质量判断	最终客户结果或长期品牌影响	分析评审一致性、分歧和样本覆盖
SLA 历史数据	过去期间可用性、事件和恢复表现	未来一定达到相同水平	核对口径、排除项和客户环境差异
导出包	特定对象可被导出	替代系统能够完整重建	在隔离环境执行恢复和核对
合同承诺	供应商承担的法律和商业义务	技术上已经具备能力	把义务连接到验收、补救和终止权
客户案例	某主体在特定情境采取过相关行动	本企业 ROI、风险或适配性	核对主体、时间、口径、边界和归因
运营报告	运行量、质量、成本、风险和问题趋势	指标定义合理或数据无偏	抽样回溯到原始任务、账单和事件

附录 D 采购档案最小集合

竹势 AI 营销智库出品

最终采购档案应形成可由内审、后续管理者和替代供应商理解的完整链条。至少包括：经批准的经营问题与基线；需求追溯树及变更记录；数据分类、法域判断和系统清单；目标架构与八类连接评审；RFI/RFP、供应商答复及证据索引；PoC 样本、人工基线、盲评、失败注入、成本和退出测试；产品与服务商双评分；三年 TCO 及情景假设；风险接受、限用条件和主闸门结论；合同正文及数据、SLA、实施、价格、审计、终止和退出附件；上线验收、权限清单、运营看板、事件演练和培训记录；月度、季度与年度复评结论。

档案保留的目的不是增加审批文书，而是降低人员变化后的决策失忆。AI 产品、模型、价格和接口变化速度较快，若企业无法重建当初为何选择、依据何在、接受了什么风险、如何退出，后续续约和扩展将重新依赖供应商叙述。采购档案应与配置、日志和合同版本同步更新，并由企业内部角色负责。

附录 E 来源索引

竹势 AI 营销智库出品

[S1] Peter F. Drucker, Management: Tasks, Responsibilities, Practices, 1973.

[S2] Clayton M. Christensen, Taddy Hall, Karen Dillon, David S. Duncan, Competing Against Luck, 2016.

[S3] Herbert A. Simon, Administrative Behavior, 1947; later editions.

[S4] Ronald H. Coase, The Nature of the Firm, Economica, 1937.

[S5] Oliver E. Williamson, The Economic Institutions of Capitalism, 1985.

[S6] Carliss Y. Baldwin and Kim B. Clark, Design Rules: The Power of Modularity, 2000.

[S7] Michael E. Porter, What Is Strategy?, Harvard Business Review, 1996.

[S8] W. Edwards Deming, Out of the Crisis, 1982.

[S9] NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), 2023.

[S10] NIST, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, 2024.

[S11] ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system.

[S12] 国家互联网信息办公室等七部门,《生成式人工智能服务管理暂行办法》, 2023 年 7 月发布, 2023 年 8 月施行。

[S13] 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 月发布, 2025 年 9 月 1 日施行。

[S14] 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。

[S15] OWASP Foundation, OWASP Top 10 for Large Language Model Applications / Generative AI Security Project, current editions.

[S16] World Federation of Advertisers, Responsible AI in Marketing related guidance, 2023—2025.

[S17] International Association of Privacy Professionals, AI Governance research and professional guidance, 2023—2026.

[S18] Erik Brynjolfsson, Danielle Li, Lindsey R. Raymond, Generative AI at Work, Quarterly Journal of Economics, 2025; working paper versions earlier.

- [S19] Morgan Stanley, company announcements on AI knowledge assistant for wealth management, 2023.
- [S20] OpenAI, Morgan Stanley wealth management deployment case material, 2023—2024; supplier case.
- [S21] JPMorgan Chase, management disclosures and company communications on LLM Suite, 2024.
- [S22] Klarna, company disclosure on AI assistant in customer service, February 2024; company-reported metrics.
- [S23] Klarna management public comments on maintaining and expanding human customer service options, 2025.
- [S24] Fabrizio Dell’Acqua and coauthors, The Cybernetic Teammate: A Field Experiment on Generative AI Reshaping Teamwork and Expertise, Harvard Business School working paper, 2024; sample 791 P&G professionals.
- [S25] Unilever, Annual Report and Accounts 2025; marketing transformation and Desire at Scale disclosures.
- [S26] Unilever, 2025 full-year results and investor presentations; company-reported strategic and operating context.
- [S27] 中国平安保险（集团）股份有限公司，2023—2025 年年度报告；人工智能、销售、客服与运营披露。
- [S28] 中国平安，科技与业务运营相关公司公告和正式披露，2023—2025 年。
- [S29] 阿里巴巴集团，2025 财年及后续年度报告、投资者材料；阿里国际与 AI 业务披露。
- [S30] Alibaba International, Accio product announcements and company disclosures, 2024—2026; company-reported usage.
- [S31] Lenovo Group, Annual Reports 2024/25 and 2025/26; hybrid AI strategy and business disclosures.
- [S32] Lenovo, official hybrid AI technology and enterprise solution materials, 2024—2026.
- [S33] 海尔智家股份有限公司，2023—2025 年年度报告；数字化运营、用户与渠道相关披露。
- [S34] Andrew Ng, Machine Learning Yearning and public lectures on data-centric and iterative AI development.
- [S35] Ethan Mollick, Co-Intelligence: Living and Working with AI, 2024.
- [S36] Martin Fowler, writings on evolutionary architecture, continuous delivery and technical debt.
- [S37] Bruce Schneier, writings on security, trust and systemic risk, including A Hacker’s Mind, 2023.
- [S38] Gartner, research on composable enterprise, enterprise architecture and AI platform governance, relevant editions.
- [S39] 竹势 AI 营销智库，企业级 AI 营销产品与服务定位材料，2026 年 7 月；用于报告的场景边界与企业责任系统框架。
- [S40] 竹势 AI 营销智库，中小民营企业老板 AI 营销需求与 GTM 研究，2026 年 4 月；用于理解采购决策语言与实施阻力。

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。

本报告的需求追溯、架构适配、真实任务 PoC、双评分与退出工具，旨在帮助管理团队把供应商能力转化为可审计、可运营、可替换的企业责任系统。

shichangbu.ai

专题中心 · 返回顶部 ↑