

行业定制与私有化指南

从一件事开始，把AI装进企业

本指南给企业负责人、业务部门、IT与安全、采购与法务一起使用。目标是：
在扩大预算和权限之前，先把一件真实的事做成。

道生 · v3.0 · 2026年9月

十分钟看完

先别买大平台。从一件每周都在重复、做对做错能判断的事开始。

分四步走，每步都能停：

1. 资格评估（30分钟）；
2. 场景验证（用真实样本，先只看不动）；
3. 私有部署（装进你的机房，接入资料和系统）；
4. 长成能力（把做顺的流程沉淀下来，下一件事直接用）。

先问清四件事：资料放在哪、谁能用谁来批、做了什么查得到吗、不想用了怎么撤。

01 这件事适不适合交给AI

条件	适合	先缓一缓
多常发生	每周或每月都在重复	偶尔一次，攒不出样本
结果清不清楚	有人用、有合格样例	只说“提高智能化”
资料有没有	有表格、单据、文档或系统记录	全靠口头经验
对错能不能判断	做对做错可以检查	完全凭感觉，没人签字
风险大不大	可以先只看不动	一上来就要AI自己执行重要动作

任何一项不满足，先补条件，而不是换一个更强的AI。

02 谁必须在场

角色	要提供什么	最终对什么负责
业务负责人	这件事怎么做、合格样例、常见错误	结果能不能用
资料或系统负责人	资料在哪、多久更新、谁有权限	资料和对接稳定
安全与合规	哪些资料敏感、能不能出机房	风险边界
财务与采购	预算、合同、付款与退出	商务条件
项目负责人	节奏、问题、变更	项目按时完成

业务负责人不能只在开头和结尾出现。合格样例和常见错误，必须由业务一起定。

03 装在哪里：三种选择

选择	适合	你要准备
装在企业机房	资料最敏感、要求完全不出门	服务器、网络、管理员；如需本机模型还要显卡
装在你们的私有云	已有私有云或专属云资源	云账号、网络隔离、访问方式
道生代为托管	先快速验证，资料敏感度一般	数据处理约定、访问权限

关键区别：“私网访问”“专属模型”“本地界面”都不等于“完整装在你这里”。选型时要分别问清：软件、资料、资料索引、AI模型、工具、日志、备份各放在哪里。

怎么定：部署方式在资格评估后，按资料敏感度、使用人数和现有机房条件确定。

04 需要什么样的机器（参考）

用法	大致配置	说明
只用云上AI模型	一台普通服务器（8核、32G内存、500G硬盘）	资料和数据生在机房，AI模型在云上
本机跑中小模型	加一块24—48G显存的显卡	敏感资料只给本机模型
本机跑大模型或训练	多卡服务器，按模型大小评估	训练“让模型学会你的做法”时需要

以上仅为规划参考，具体配置在资格评估后按资料量、使用人数和模型选择给出。

05 资料准备清单

- 20到100份真实样本（可以先脱敏），包括正常、特殊和出错的情况；
- 5到20份业务认可的合格成果，以及不合格的反例；
- 资料说明：从哪来、多久更新、谁负责、有没有授权；
- 现在人工怎么做、平均花多久、常见返工原因；
- 要对接的系统：有没有测试环境、能不能只读访问。

资料说不清来源和更新责任的，先不要进入正式使用。

06 建资料库要准备什么

事项	要回答的问题
范围	哪些文件、制度、案例要放进来？哪些绝对不能放？
权限	谁能看哪一类资料？离职、调岗怎么处理？
更新	资料多久更新一次？谁负责？旧版本怎么处理？
出处	回答要引用到哪一级：文件、页码还是段落？
检查	用哪20个常见问题检验资料库答得对不对？

资料库的好坏，七成取决于资料本身是否干净、有没有人负责更新。

07 想让模型学会你的做法，要准备什么

分三步，先易后难：

1. 把规矩写下来：老手的判断口径、术语、常见例外，写成规则和样例。大多数企业做到这一步就能明显见效。
2. 攒纠错记录：业务人员每次修改AI的答案，都会被记录下来。
3. 攒够了再训练：纠错记录达到足够数量（至少300组），再训练模型；训练后要在同一套测试题上比原来好才上线，可以一键退回。

要准备： 一位愿意持续复核的业务老手、一套测试题（常见问题和标准答案）、训练所需的显卡资源（或使用托管训练）。

当前状态： 第一步可演示；训练流程规划中。

08 权限和风险要问清

- 谁能发起任务？谁能看到输入和结果？
- 资料会不会发给外部AI？哪些只给本机模型？
- 哪些动作只看不动，哪些会改系统、会对外发出？
- 谁来批准？批准能不能被程序绕过？
- 操作记录保存多久？人员离职或合同终止后怎样收回权限？

道生默认的规矩：不认识的人拒绝、没登记的能力拒绝、超过用量上限停止、重要动作不经批准不执行。

09 验证怎么做

阶段	目标	什么情况下进入下一阶段
摸底	记录现在人工怎么做、花多久	样本和口径一致
只看不动	AI出结果，不改任何系统	合格率和节省时间达标
并行对照	AI和人同时做，比较差异	严重错误可控
小范围使用	开放少量低风险动作	审批、记录、接管都有效
扩大	增加人员、资料或动作	复盘通过

验证的范围、时间和合格线，要在开始前写进验收表。

10 验收看四类证据

方面	要问的问题	证据
业务效果	结果能不能直接用，省了什么	样本、合格率、节省时间
权限控制	越权和重要动作能不能被拦住	正反测试、审批记录
运行情况	花费、容量、故障是否可控	用量账单、监控、恢复演练
责任与退出	谁签字、谁接手、怎样导出	责任表、服务承诺、导出演练

11 费用怎么拆

费用	怎么算
私有部署授权	按部署规模与使用人数
场景实施	按场景、资料和对接范围，付款跟验收节点走
年度维护	升级、监控、支持时段
AI模型用量	自带账号不收费；由道生统一采购的，按实际用量计费
专家能力	按次或按月
定制开发	按范围报价

具体价格在资格评估后按部署规模、场景范围和支持时段给出，以书面报价为准。

12 问供应商的十二个问题

1. 最终交付给我的是什么结果？
2. 哪些能力已经在用，在什么环境？
3. 资料、AI模型、工具分别在哪里运行？
4. 每个人、每个部门的空间怎样隔开？
5. 哪些动作默认不执行？
6. 人工审批能不能被程序绕过？
7. 用来检验效果的测试题由谁维护？
8. AI模型或工具升级后怎样复查？
9. 花费能不能拆到每件事？
10. 出了事故谁响应？
11. 资料、设置、记录、测试题能不能导出？
12. 不合作了怎样迁走、怎样收回权限？

13 能退出，才敢开始

项目开始时就约定好可以带走的东西：资料、设置、规则和样例、测试题、操作记录、用量记录、成果和人工修改。

退出时要演练：账号撤销、密钥更换、资料归还或销毁、外部系统断开、未完成任务处理、第三方订阅终止。

道生的每一块都能换成别家的——这既是对你的承诺，也是我们对自己的要求。

第一步

准备一件每周都在重复的事、一份合格样例、三条常见错误、现在人工花的时间和涉及的系统。用30分钟做资格评估，结论只有三种：**适合开始、先补资料、暂不适合**。

本指南与《道生产品手册》配套使用。能力状态、价格、部署条件以书面确认为准。