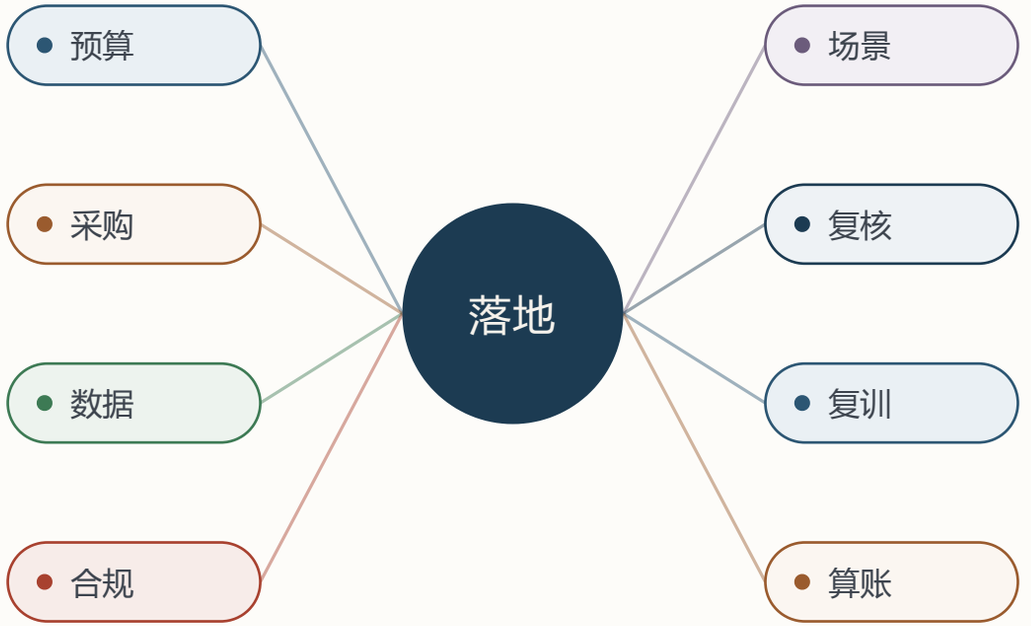
COURSE 08 · AI ENTERPRISE

AI 企业落地课

不谈哪个模型更强，只谈公司怎么把它用起来



AI 教学课件工厂 · 系列课程 08

企业负责人与 IT 主管 / 约 70 分钟

个人版够用，但不能拿来跑业务

员工自己花钱开个账号试试，没问题。把客户资料贴进去，问题就来了。

01 个人订阅的条款是给个人看的，数据怎么用由服务方说了算

02 席位挂在个人名下，人一离职，账号和历史对话都带不走

03 发票主体、合同、付款流程对不上，财务这一关就过不去

04 企业版贵的不只是功能，是数据条款和责任边界

个人版：自己花钱自己用	公司用：卡在三件事
功能基本齐全	合同与发票主体
按月订阅，随时能停	数据归属与训练条款
数据条款按个人算	离职交接与审计

试用随便用个人号，业务数据进去之前先把合同签了。

订阅和 API 是两笔钱，别混着算

同一个模型，两条计费线互不相通。企业版席位再多，也不能拿来跑程序。

01 订阅管人：按席位包月，谁在用、用多少，账面上看不出来

02 API 管程序：按 token 计费，输入和输出单价不一样，跑一次算一次

03 程序上线前先把预算上限和告警设好，别等月底账单

04 对内要能分账：哪个部门、哪个应用花了多少，得拆得开

订阅	按人 · 包月	给人用
API	按量 · 按 token	给程序用
缓存	命中后单价更低	重复的提示词
预算	上限 + 告警	先设再跑

订阅管人，API 管程序，两笔预算分开设。

账单不是用多了，是每次都在重读同一段

同一个问题问一百遍，如果每次都把两万字资料重新贴进去，那就是一百次全价。

01 上下文越长，每一轮都要重算，长文档一贴，单价翻几倍

02 输出比输入贵，让它写长文和让它答一句，不是一个价

03 失败重试、自动循环、批量任务，一次没算对就是成倍的钱

04 把固定的系统提示词和资料做成缓存，是最直接的一刀



先看重复，再看用量。多数账单问题出在重复。

什么数据不能进云端模型

判断标准不是「重不重要」，是「泄露了谁承担」。

01 公开信息、行业常识、通用知识，直接用

02 内部文档和代码，要先确认服务方承诺不用于训练

03 客户个人信息、身份证、手机号、病历，默认不进

04 涉密信息、未公开的财务与并购材料，一律不进，离线处理

可以
公开信息、行业常识
直接用

看合同
内部文档、代码
确认不训练

默认不进
个人信息、客户数据
先脱敏

一律不进
涉密、未公开财务
离线处理

分不清属于哪一档的，按最严的那一档处理。

脱敏不是把名字改成「某先生」

名字去掉了，单位、岗位、时间、金额还留在句子里，凑起来照样能定位到人。

01 真正要去掉的是组合：单位 + 岗位 + 时间 + 金额，四条凑一起就唯一

02 能在本地做的先在本地做，只把结论送出去

03 换完再读一遍，用陌生人的眼睛看还能不能认出是谁

04 留一份脱敏前后的对照，出了问题才查得回去



脱敏看的是「还能不能认出是谁」，不是「名字有没有出现」。

备案、标识、留痕

三条都不是技术难题，是流程里必须有人认领的活。

01 面向公众提供生成式 AI 服务要走备案，纯内部自用不走这条

02 AI 生成的文字、图片、音视频，对外发布要带标识

03 日志要留得住：谁问的、什么时候、用的哪个模型、返回了什么

04 内部自用和对外服务是两套要求，别拿内部经验去对外

01	备案	对外服务才需要
02	标识	AI 生成要标注
03	留痕	日志可追溯

先问一句「这个服务是给谁用的」，再决定走哪套流程。

私有化买的是「数据不出门」

如果只是想省钱，私有化几乎从来算不过来。

01 数据一步都不能出内网——这条成立，才谈私有化

02 有稳定的使用量，长期租算力才可能比买卡便宜

03 有能维护的人：模型更新、显存、并发，出问题得有人管

04 三条缺一条，先用云上的专有实例过渡，别急着买卡

三条都成立才做

- 数据不能出内网
- 用量长期稳定
- 有人负责运维

缺一条就先别急

- 只是偶尔用用
- 没人管显存和并发
- 主要目的是省钱

私有化解决的是数据边界，不是成本问题。

账号发下去没人用，问题不在工具

缺的不是培训，是「这件事以后就按这个做」的那句话。

01 账号发下去，没人知道拿它干什么，一周后就不再登录

02 培训讲完就散，第二天回到原来的做法，等于没培训

03 先挑一件每周都要做、做完还要检查的活，把它改掉

04 让做这件事的人自己提需求，从上面派下来的通常推不动



工具发下去只是开始，流程改掉才算落地。

三个筛子，筛完只剩一半

列场景的时候容易什么都想试，真能做的没几个。

01 高频：一周至少做几次，低频的学会了也忘

02 有明确对错：能判断结果好不好，才敢交出去

03 出错代价可控：错了能发现、能改回来

04 三条都过，再谈用什么模型、要不要私有化



三条筛下来，能做的场景通常不到你列的一半。

人工复核放在哪一步

复核不是不信任模型，是给流程留一个刹车。

01 对外发出的内容，发之前必须有人看，不能是发完再看

02 涉及钱、合同、对外承诺的，人签字才算数

03 内部参考用的，抽检就够，但要留下样本备查

04 复核位要写进流程和岗位职责，不能靠「大家自觉」

逐条看
对外发布的内容
人签字

抽检
内部参考
留样本

不用看
格式转换、初稿
出错能发现

复核位写不进流程，等于没有复核。

一年后，这笔钱怎么算

算省下来的时间，不算「用了多少次」。

01 时间要折成钱：谁的时间、什么单价，写清楚

02 成本要把订阅、API、算力、维护、复核人工全算进去

03 复核人工最容易被漏算，它往往占掉省下来的一半

04 算下来不划算的场景，就该停掉，不用觉得可惜

收益
省下的时间 × 单价
折成钱

成本
订阅 + API + 算力
全算进

漏算
复核与维护人工
补上

结论
不划算就停
别硬撑

算不出钱的场景，通常不是没效果，是没人真的在用。

这门课之后

你不一定马上能算出回报，但应该清楚钱花在哪、数据能去哪、出了事谁签字。

下一步：挑一件每周都做的活，用三个筛子过一遍。

