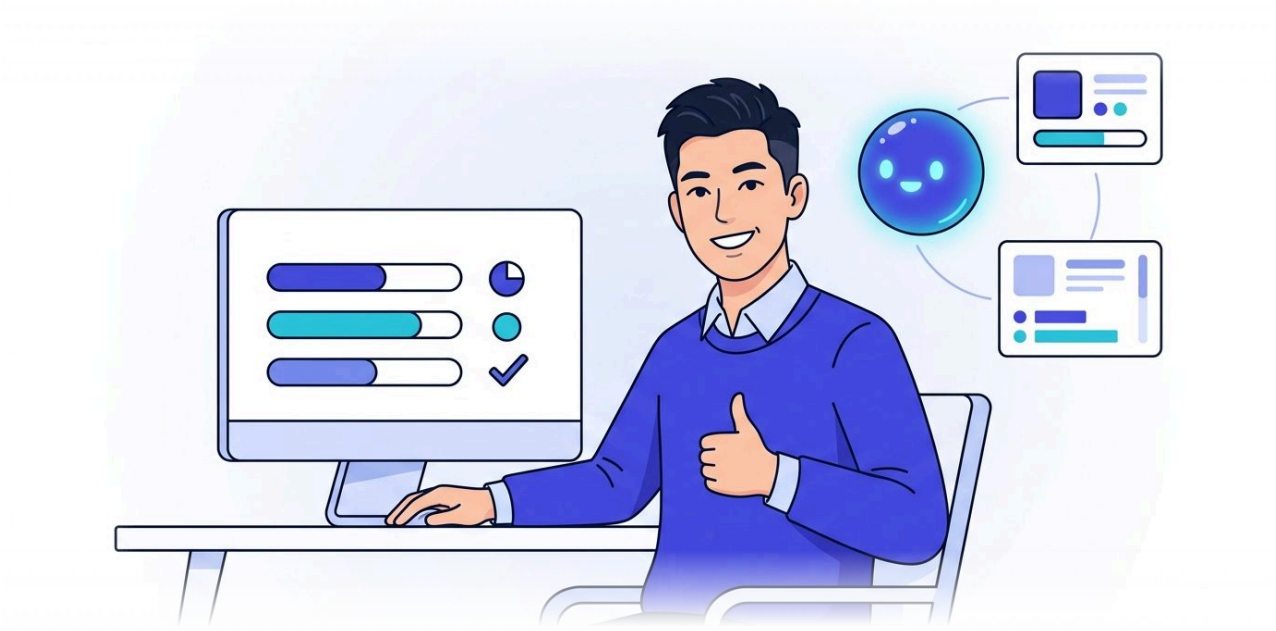
企业智能体落地的十条规矩

不换老系统，把 AI 稳妥接进日常业务——写给企业负责人、业务主管与信息部门的选型、风控与验收指南。



10
条一线工程落地规矩

05
条可写入合同的安全红线

02
张开会打印即用的自查附表

发布机构
诺石数智

版本日期
v3.0 · 2026-11

配套规约
开发规约 v0.1 / 五条红线

官方网站
www.nerss.com

目录与阅读指引

多数企业买完 AI 账号，三个月后只剩写周报。真要进采购、仓储和财务，卡住的不是模型智力，而是权责、老系统、停用兜底与资产归属。

00 **聊天框与受控运营的分水岭**
对照表与三层两核参考架构图

01-02 **选对第一件事 · 人机同岗分清权责**
采购交期前后对比图解与推荐场景

03-04 **动作单据化 · 五级风险硬拦截**
确认单解剖图与 R0–R4 定级对照表

05-06 **四级顺序接老系统 · 影子运行准入**
不改业务库红线与四步准入关口

07-08 **一键停用回原界面 · 只追加审计账本**
双轨切换示意图与不可篡改记账

09 **企业可受控的数字资产与知识底座**
四步建成路径与五类自有导出格式

10 **3–5 年展望与短 / 中 / 长期明码推进**
三阶段演进轨道与四期验收付款

附表 **两张打印即用实战自查表（A / B）**
首场景 10 分筛选表与供应商尽调表

企业负责人 / 分管副总

重点看 **00、01、09、10** 与**附表 A**。5 分钟算清投入、资产与第一步。

业务主管（采购 / 售后 / 财务）

重点看 **02、03、04、07**。看清怎么省跑腿活、守住签字拍板权。

信息部 / 法务与风控

重点看 **04、05、06、08、09** 与**附表 B**。核查不改库、评测与导出。

口径声明：本白皮书所列工程规则均对齐诺石数智现行标准（《企业级智能体开发规约 v0.1》《安全与内控红线》）；文中出现的采购单号、订单号与确认单示例均为**演示数据（模拟示例，不代表真实运营或客户数据）**。

聊天框进不了真实业务，受控执行才可以

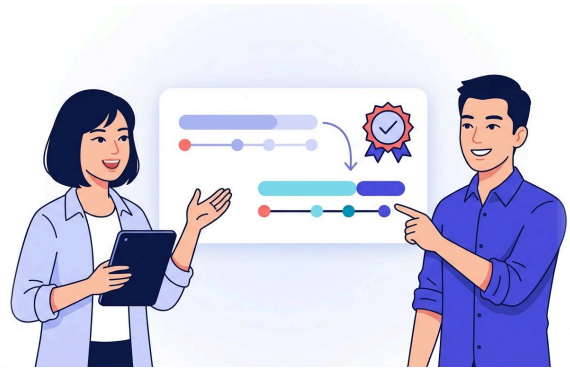
> 企业运营要的不是一段文字建议，而是一次**有制度原文依据、有主管签字、安全写回老系统、事后查得清**的受控办理。

比较项	个人通用对话工具	诺石受控智能运营（人机同岗）
输出形态	一段聊天文字，员工需手工搬进系统	**写清改前改后、附原文的结构化确认单**
审批权责	脱离审批流，出错难定责	**按 R0–R4 事先定级，正式变更主管签字**
老系统写入	未接通，纯靠人工复制	**签字后经官方接口/审批流写回，不改库**
异常停用	回到纯手工翻系统	**一键停用 AI，带齐单号切回原人工表单**
留存家底	散落个人账号，人走断档	**五类数字资产归企业，标准格式全量导出**

图 1 · 诺石三层两核受控运营架构　　支持公有云 / 专属云 / 本地私有化



规矩 01–02：选一件高频实事，让 AI 跑腿、由人拍板



一封供应商延期函，过去折腾五个窗口，现在一张确认单办结

过去：切邮箱、ERP、制度、OA、销售群，耗十几分钟还易漏通知

现在：数十秒核完原单与制度，主管点签字即经接口写回

01

先挑一件高频、跨系统、规则清楚的实事

常见踩坑：一上来建“全公司万能助手”，半年花完预算却没一个部门天天用。

首个场景须同时满足三点：**每月办几百次以上、横跨两套以上老系统、判断口径写得清**。先集中打穿一件事，团队和老板一眼看见实效。

现场追问：「动工前能否用一页纸写清第一件事的边界、涉及系统、签字人与验收口径？」

02

人机同岗：智能体备单跑腿，主管握紧拍板权

常见踩坑：迷信“无人值守”“替代人工”，AI 改错一笔单子，业务主管不敢用也无人担责。

遵循「岗位智能体 + 人类 = 人机同岗」。智能体查多套系统、核制度、起草单据与对外草稿；**同不同意变更、怎么定责补发，始终由原岗位主管拍板**。

现场追问：「改变业务状态的每一步，系统里是不是都对应组织架构里一位明确的签字人？」

首批推荐高频场景	横跨的常见老系统	智能体干什么	谁签字把关
采购交期变更	邮箱 + ERP + OA + 微信群	核订单与制度，出改前/改后确认单	采购主管
订单与售后异常	OMS + WMS + 物流底单	三单自动比对，起草补发/处置单	责任主管（退款只起草）
现场工单调度	报修群 + 工单 + 备件库存	匹配历史排障案例，起草派工单	调度长（绝不控设备）
财务报销/合同预审	费控 + OA + 制度条款库	逐条初筛，标出超标/偏差与原文	财务 / 法务终审

规矩 03–04：拒绝黑盒改数据，确认单与网关硬控

图 2 · 结构化确认单解剖图（六件事一眼核清再签字）　　演示数据 · QR-20261001-0001



04 · 五级风险硬判定

权限边界写死在网关规则里，绝不靠提示词盼着模型“自觉”

每个动作在接入前即由企业制度定死 R0–R4 等级并写进磐枢规则网关。无论对话怎么诱导，高危动作均被硬性拦下。

级别	典型业务动作	网关硬性放行方式	责任归属
R0 只读	查订单、库存、制度条款	按岗位权限自动放行并留痕	经办人本人
R1 草稿	报销 / 合同偏差标注	生成内部草稿，不改业务状态	审核人终审
R2 变更	改交期、补发单、派工单	**强制弹确认单，授权主管签字后写回**	业务主管
R3 高敏	付款申请、合同签发、对外通知	**AI 仅起草，由人核对后自行办理/发出**	财务 / 法务
R4 禁止	直接打款、删库、改权限、控设备	**通道不接入，网关层硬性禁止**	AI 永不触达

规矩 05–06：老系统不动库，真单据测透再写入

图 3 · 上线准入四步关口（拒绝拿演示视频当验收）　　对应《NERSS 实验室评测方法》



05

四级顺序接老系统，任何级别不直改数据库

常见踩坑：直连 ERP 底层写表，绕过原厂校验与事务，导致账实不符且失去原厂维保。

逐个动作按**「L1 官方接口 → L2 原审批流 → L3 只读同步 → L4 有限界面自动化」**顺序优先选用，能用上一级绝不用下一级，严禁申请业务库读写账号。

现场追问：「交付期间是否需要我们信息部开 ERP 或 OA 数据库写账号？」（索要即否决）

06

上线前真单据评测 + 影子运行，失败样例原样交底

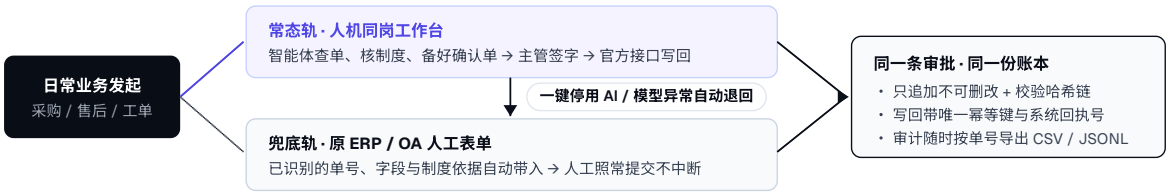
常见踩坑：看几段美化过的演示视频就匆忙上线，一碰真实业务里的奇葩格式和例外就翻车。

上线前把门槛写进验收单，用客户真实历史单据影子跑通、逐笔归因修复，**不达标绝不开放正式写回**。

现场追问：「能否用我们近三个月脱敏真单据先影子跑两周，把所有出错样例交给我们复盘？」

规矩 07–08：离开 AI 照常转完，事后查同一本账

图 4 · 双轨并存与「一键停用 AI」应急退回机制　　两条轨走同一条审批流 · 留同一份账本



07

双轨并存：原操作界面永久保留，上线必做停用演练

常见踩坑：替换掉原有表单，大模型服务一抖动，全公司采购发货和审批跟着瘫痪。

新工作台与老系统表单长期并存。拨动「一键停用 AI」立即切回原界面并自动带入已识别信息；**上线前必须和客户团队现场演练通过**。

现场追问：「如果明早大模型断网两小时，正在办的采购和售后单怎么接着走完？」

08

只追加、可校验的审计账本，每笔写回有来龙去脉

常见踩坑：只有零散聊天记录、没有幂等防重和版本记录，年底内审说不清谁凭哪版制度批的。

意图、条款版本号、确认单、签字时间戳、接口回执五步全记账；**制度升版后旧版留档**，半年后抽查仍准确指向当年依据条款。

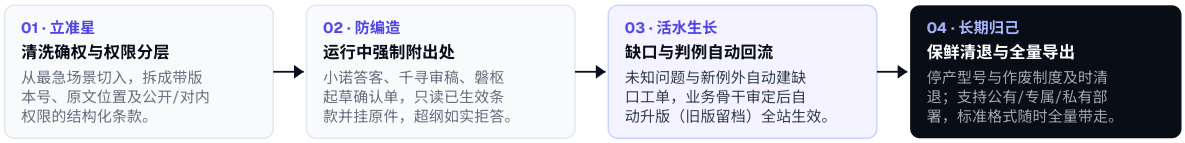
现场追问：「审计能否按单号一键导出从提问、依据版本、签字人到系统回执的完整记录？」

规矩 09：模型会换代，唯有可控数字资产留给企业

把全公司文档一股脑倒进黑盒向量库一定不好用。真正能拉开差距的，是**带版本、带出处、会回流生长、按标准格式归企业自有**的知识与数字资产底座。

图 5 · 企业可受控知识与数字资产底座四步建成路径

在业务运转中越积越厚



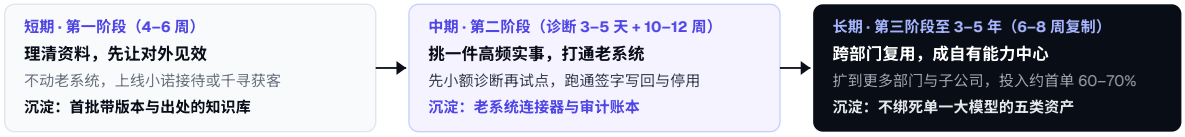
企业自有五类资产	具体包含什么	标准导出格式	沉淀位置
业务知识与经验	产品手册、技术规范、审定后的缺口知识卡	Markdown / JSON	磐石底座
审批与内控规则	交期权限、售后定责、差旅限额、合规词表	JSON / YAML	磐石底座
人工确权业务判例	高频例外处置方案、老师傅排障经验卡	JSON / Markdown	磐石底座
连接器与动作规约	ERP/OA 接口映射、动作清单与确认单结构	OpenAPI / Schema	磐枢中枢
确认单与审计账本	已签字确认单、接口回执与只追加执行流水	CSV / JSONL	磐枢中枢

现场追问：「若两年后不再续约，能否把知识库、规则集、连接器与账本按上述开放格式完整移交，且承诺我司数据绝不用于模型训练？」

规矩 10：3–5 年看方向，短、中、长期明码标价推进

瞄准 3–5 年「人机同岗 + 受控执行 + 企业自有能力中心」的终局，但今天按三阶段逐步落地，每一步可验、可停、明码标价。

图 6 · 短 / 中 / 长期三阶段演进轨道　　可按需切入，前一步攒下的资产后一步直接复用



合作步骤	主站公开报价口径	参考周期	交付物与保障
方案交流	**免费**	线上 1 小时	交付一页纸《场景初判》，工作日 4 小时内响应
对外获客与接待	老站改造 **¥6,800 起** 千寻模块 **¥12,800 起** 知识接待落地 **3–8 万**	4–6 周	不动内部老系统；千寻细分模块与预算测算见 www.nerss.net
对内场景诊断	**¥6,800 起**	3–5 工作日	交接口、风险定级与精确报价三份报告；**90 天签实施全额抵扣**
受控办事试点	**15–25 万元**	10–12 周	以诊断报价为准；含双核底座、1 个业务场景、影子运行与停用演练
推广复制 / 年度运行	复制约首单 **60%–70%** 年服 **20%–30%/年**	6–8 周 / 按年	跨系统年服最低 ¥2 万/年；私有化能力中心按机房环境面谈

受控办事试点四期按验收付款（对公转账 · 开具增值税专用发票）



附表 A：首个跨系统场景 10 分筛选打分表

建议由企业负责人、业务主管与信息部共同花 5 分钟勾选打分，快速决定先从对外轻起步，还是直接进跨系统诊断。

场景适合度打分表　　每行勾选 1 项，累计总分（满分 10 分）

评估维度	0 分	1 分	2 分	3 分
1. 涉及几家厂商系统	☐ 1 家	—	☐ 2 家	☐ 3 家以上
2. 拍板业务主管参与度	☐ 无	☐ 有但未参与	☐ 亲自参与	—
3. 这件事每月办理频次	☐ 不清楚	☐ 几十次	☐ 几百次以上	—
4. 接口或只读视图情况	☐ 全无	☐ 待查明	☐ 明确具备	—
5. 本年 / 明年预算窗口	☐ 暂无	☐ 已列计划	—	—

得分参考：

- **7–10 分：**条件成熟，建议直接进入 3–5 天**场景诊断（¥6,800 起）**，拿接口清单与精确报价（90 天签实施全额抵扣）；
- **4–6 分：**建议先约 **1 小时免费方案交流**，由顾问帮您理清切入点；
- **0–3 分：**暂不急于接老系统，建议先做**资料梳理与官网小诺接待**轻起步。

候选场景名称：

涉及的现有系统（如 ERP / OA / WMS / 邮箱）：

目前最耗工时或最易出错的环节：

本次总分：_____ 分　　**下一步决定：**☐ 约免费交流　☐ 约场景诊断　☐ 先理资料跑接待

附表 B：企业级智能体供应商 10 项尽调自查表

供应商 10 项必问核对清单　　见任何 AI 供应商时逐条核对（包括诺石自己）

序号	必须确认的关键问题	核对结果	要求提供的证据
01	能否先小额诊断给出接口清单与精确报价，再签实施？	☐ 是 ☐ 否	诊断报告样本
02	正式业务变更前，是否强制出确认单并由主管签字？	☐ 是 ☐ 否	确认单演示
03	风险分级是否由规则网关硬控制，而非仅靠提示词？	☐ 是 ☐ 否	网关机制说明
04	是否承诺绝不索要业务库写账号、只经应用层接入？	☐ 是 ☐ 否	写入合同附件
05	打款、删库、改权限、控设备是否网关层硬禁止？	☐ 是 ☐ 否	禁用动作清单
06	上线前能否用历史脱敏单据做影子运行与零漏拦评测？	☐ 是 ☐ 否	评测报告模板
07	一键停用 AI 后，原系统人工表单能否照常办完？	☐ 是 ☐ 否	现场停用演练
08	每笔写回是否留有不可篡改账本、制度版本与回执？	☐ 是 ☐ 否	导出账本样例
09	五类数字资产是否归我司所有并支持标准格式导出？	☐ 是 ☐ 否	导出格式清单
10	是否承诺数据绝不用于训练，且支持私有化部署？	☐ 是 ☐ 否	主权合同条款

评估企业：_____　　评估人 / 部门：_____　　日期：____ 年 __ 月 __ 日

带上您的系统清单，先用 1 小时免费拆清楚第一件事

访问官网预约交流，或获取其余四份公开文件（安全红线 / 开发规约 / 评测方法 / 资产主权规范）。

诺石数智： www.nerss.com
诺石千寻： www.nerss.net
工作日 4 小时内响应