超级个体和组织 Harness

AI 原生 IT 组织实践分享

宣讲人：王海涛（CTO @ CBNB）

个体 4×，组织 34%

4×

部门最优秀的员工

用上大模型后，单任务提效

VS

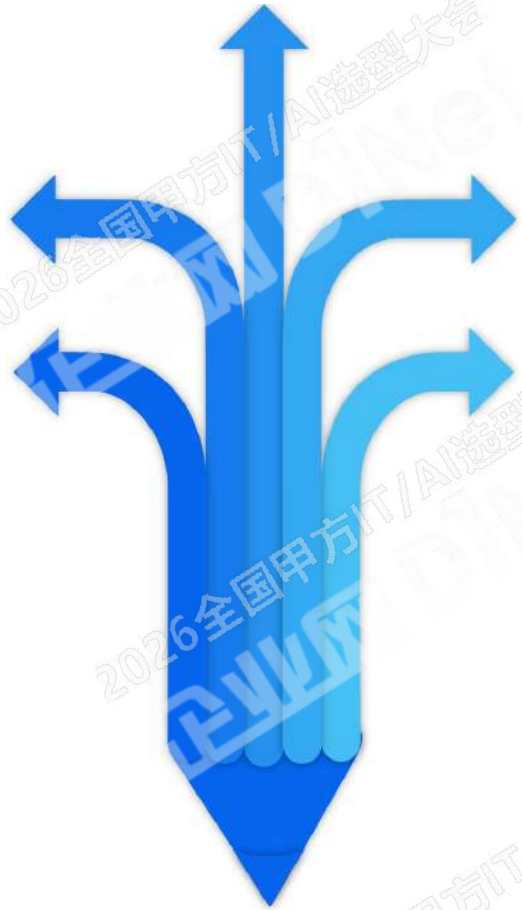
34%

同一个部门整体

全部岗位加总后的提效

AI 个人能力赋能后的爆炸和组织提效的不协调，暴露的是——「AI 可复制」还没做到。

模型 → Agent → Harness → 超级个体 → ? → AI Native组织



从内向外，一层层推开

内核 · AI Harness

规约金字塔 · Manifest · 门禁 · 幂等退化 · 成熟度

超级个体

会用大模型的人 = 新物种，一人 4×

重塑组织能力

个体强 ≠ 组织强（4× vs 34%）

AI Native 组织

不只是能力，更是思想的冲击

目录

Contents

01 超级个体
能力富集

02 组织 Harness
驾驭能力

03 AI Native 组织
能力回归

04 FDE × 本体
能力外推



超级个体

问题：会用好大模型的人，正在成为新物种。
快，却不可复制？

一个人，正在变成一支团队

过去 · 一个人 = 一个岗位

- 写代码、查资料、改文档、跑流程，各占一段
- 想清楚 → 排期 → 找人做，链条长
- 效率取决于岗位，不取决于个人

现在 · 一个人 = 一支团队

- 一个人闭环：想、写、查、改、交付
- LLM 当外脑，当天把想法做成能用
- 单任务提效 4×——已经发生



一个人闭环的四件事

想 · 写 · 查 · 改 —— 过去要四个人接力，现在一个人当天闭环。

它的本质是换了工作方式。
追求效率的机制情况是个人“清空”团队，这样真的好吗？

很强，却不可复制

01

依赖个人悟性

不是人人一点就会

02

方法没外化

提示词锁在个人手里

03

经验锁在人脑

组织拿不到就放不大

问题不在能力强弱，在能力能不能被组织接住。



组织级 AI Harness

把规约从服务个人到组织，
而不是锁在个人手里。

部署热，盈利冷



已部署 Gen AI 的企业
全行业样本

报告「无实质盈利贡献」
同一批企业的自评

超八成

高价值垂直场景困在试点

走不出 POC，规模化停在 PPT 里

两条几乎一样长的条——
部署与失望同步发生。

McKinsey 称之为 gen AI paradox：
部署热、盈利冷。

来源：McKinsey《Seizing the agentic AI advantage》

不是人的问题，是结构的问题

横向工具铺得快

Copilot、聊天机器人遍地都是，
但收益稀薄。

垂直场景卡试点

90% 走不出 POC，
项目碎片化。



数据缺口 + AI 孤岛

团队各干各的，
经验不互通。

文化与组织惯性

流程没为「AI 协作」
重设计。

个体的能力长在 AI 上，组织的能力还没长在 AI 上。

五层规约，把个人能力变成组织能力



01	战略层	为什么做、边界在哪
02	架构层	系统怎么切、接口怎么定
03	契约层	数据与交付的显式约定
04	门禁层	检查先于代码
05	实现层	AI 在此自由发挥

组织级 AI Harness——不让组织学超体的手速，而让组织拥有超体的闭环。

开工前，先回答六个问题

WHAT

要做什么

目标与范围，一句话说清

WHY

为什么做

动机与背景，防止跑偏

APPROACH

打算怎么做

路径与思路，先想后做

FILES

会动哪些文件

改动清单，先声明再动手

SUCCESS

怎样算成功

验收标准，可检查不靠感觉

STOP

何时必须停

止损红线，越界即停

Pre-Execution Manifest——把「个人怎么干活」外化成一张可审阅的开工单。

让检查先于代码

G0	G1	G2	G3	G4	G5	G6
基线	风格	结构	事实	一致性	独立评审	签发放行
约束齐了吗	AI 味过滤	与约束一致	引用可溯源	改 A 查 B	不自卖自夸	人确认上线

门禁层做的事：
约束写「应该怎样」，门禁证明「确实这样」。

AI 没有自我怀疑——让一个不怀疑自己的执行者给自己打分，分数永远是满分。



把一个人的 4×，变成整个部门的快

01

超级个体

4×

一个人的闭环，
但锁在个人手上。

02

组织级 AI Harness

契约 · 门禁 · 幂等

把闭环翻译成体系，
拆掉「经验锁在人脑」那道墙。

03

组织

可复制的快

≈ 34% → 持续增长，
个体跑得快，组织接得住。

这也是全场的捷径——不让组织去练超体的手速，
而是让组织长出超体的闭环。

AI 挂了，业务不停

正常
大多数时候

故障
超时 / 幻觉 / 失败

降级
切备用路径

幂等可重放

同一操作重复执行，
结果一致。

自动识别

异常被拦下，
不静默、不放过。

人工兜底

切换备用路径，
业务继续跑。





状态色约定：绿 = 稳 · 红 = 停 · 琥珀 = 兜底

trust is earned in drops, lost in buckets——信任靠工程化兑现。

幂等、识别、兜底三件事做完，组织才敢把业务交给 AI 跑。

02 2.6 实现层 · 幂

AI 挂了，业务

正常
大多数时候

幂等可重放

同一操作重复执行，
结果一致。

自

异
不

状态色约定：绿 = 稳 · 红 = 停

trust is earned in drops,

幂等、识别、兜底三件事做完，



把组织的闭环，装进一个仓库

01

一个仓库 · Derekcoding Framework

queue → worker → 状态迁移：流水线跑在一个可克隆的仓库里。

02

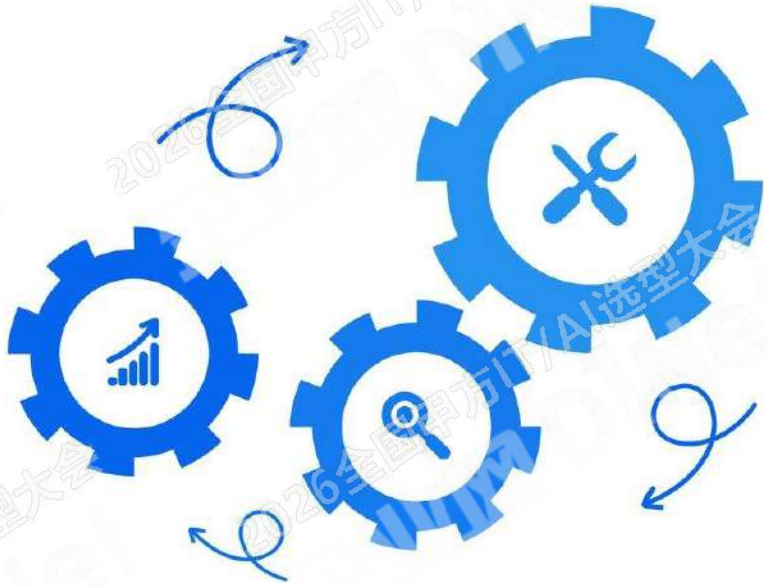
一套纪律

先读再写 · 涟漪 · 门禁 · 回写——每一条都写成了命令。

03

一个闭环

契约 · 门禁 · 幂等，写进可克隆的脚本 + 文档，人人可拉取接手。



从个人作坊到军工厂——个体强是运气，体系强才是组织。

三轨并行，四门把关

每条轨道都可查询、每道门都可执行、每份记忆都可校验。

三轨三线

三条轨道各自可回卷

WBS
做什么

Issue
出什么问题

TestCase
做对没有

四门把关

每道门都是可执行命令，过不去就修

01 提交门
交单之前全绿

02 涟漪门
改 A 必查 B

03 产出门
红灯即升级

04 总闸
人签字放行

三种身份：开发 · 复盘 · 治理——同一个身份，同一条纪律链。

冷启动 A1–A11：判断身份 → 复制框架 → 密钥治理 → 最小闭环 → 过门禁 → 独立验证 → 自检归档。

确定性逐级上升——这正是组织敢让 AI 跑起来的底气。

DCF 自己会成长

01

个人经验

个体在任务中产生的教训与灵感，过门禁后沉淀、写入团队记忆——
个人的一次，变成组织的一条。

02

Team Memory

可查询 · 可校验 · fail-closed：记住教训、淘汰过时、自我改写，
用一次，就长一次。

03

反哺 · 再进化

下次任务自动召回相关记忆，使用中再造新经验、再次回写——
回路闭合，框架随之成长。



一条经验 → 一条记忆 → 一次召回 → 更新经验；回路每转一圈，DCF 就长一圈。

CTRM

01

02 AI Coding

spec

03 452 97.8%

SQL CI

完

4 21 -- 9 30

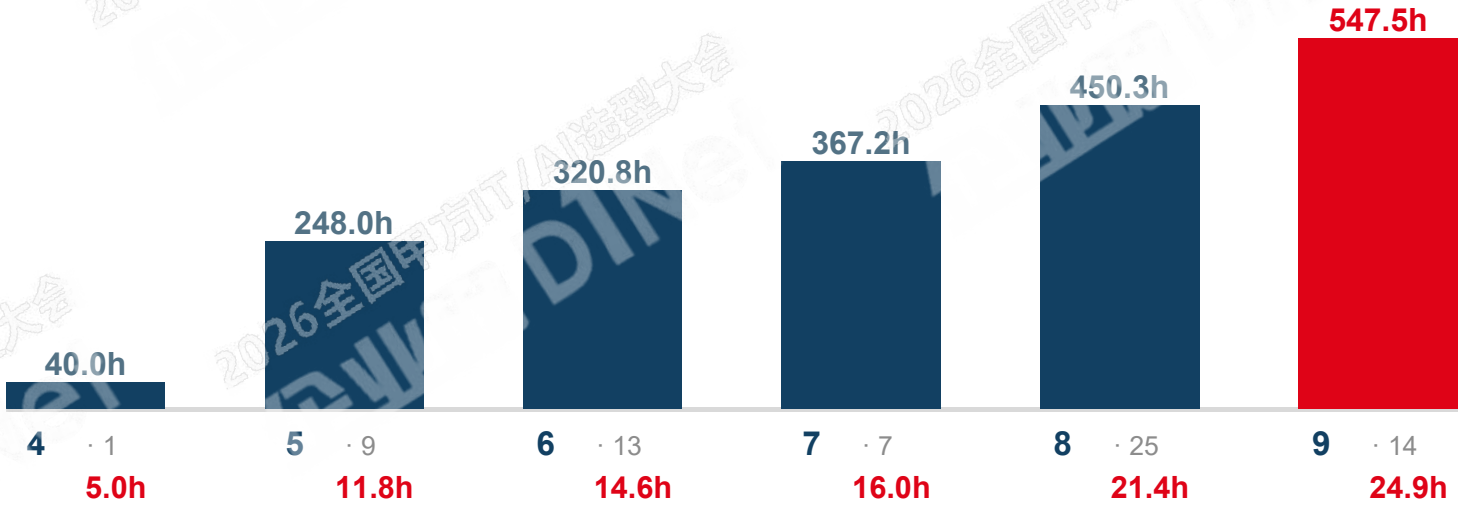
73

完

1973.75 h

完

16.9 h



从个人效果，到组织能力

01

个人作坊

快，但锁在人脑 · 4×

02

写进组织的体系

契约 · 门禁 · 幂等

把个人的闭环，写进组织。

03

AI Native 组织

可复制的快 ≈ 34% → 持续增长

能力与思想，一起被改写

超级个体 + DCF = AI Native组织?

不让组织去练超体的手速，而让组织长出一套超体的闭环。



AI Native 组织

改变的不只是能力，
更是组织的默认值。

AI Native 迭代的是“软件时代”的默认值

旧默认值 · 软件时代	新默认值 · AI Native
招人写代码 代码是稀缺产能，人越贵，交付越慢	**团队的高度一致性** 人从产出者变监督者：定义问题、把住边界
追求效率 同一件事，花更少的钱做完	**速度 - 质量 - 资源，三角重构** 约 3/4 高绩效企业调整技术支出换取数字化回报
个人英雄 组织强不强，看几个强人	**精英和精英组织** 记忆与知识层让系统自己进化，组织自己诊断

麦肯锡 CIO 报告：技术负责人正从「守门人」转向「战略架构师」。

当执行被接管，人剩下什么

以前看重的指标，正在被 AI 追平

~~熟练度：会更多工具~~

~~记忆力：知道更多答案~~

~~执行力：更快完成任务~~

~~经验值：踩过更多坑~~

AI 在这些维度已经接近或超过人

唯一无法被替代、也不该被替代的

好奇心&管理

它是提问的能力：

为什么这事值得做？还能怎么做？

边界有没有划对？

我要规划到那个层面，再动手实施？

会不会提问，决定了你是被 AI 替代的人，还是驾驭 AI 的人。

剩下的方法论，组织级的 Harness 都替你兜住了。

技术 Leader 的Agent 相处之道

1 守门人 → 架构师

近 2/3 高绩效企业，技术负责人深度参与战略制定

2 项目 → 平台战略

约 1/10 高绩效企业已全面平台化运营，普及率 4 倍于他者

3 效率 → 速度

约 3/4 高绩效企业调整技术支出结构，换取数字化回报

4 外包 → 自研

约 40% 高绩效企业计划提高内部自研比例

5 管理代码 → 管理信任

真正的挑战是让人用起来、信起来、接住它



一句话结论：技术部是 AI 落地的主战场——**以 19.6% 的账号贡献 53.0% 的消费，人均强度是全公司的 2.70 倍**，且单价与全公司持平，用法健康；同时技术部深度参与了 **86.9%** 的缺陷生命周期（引入 41 个、协助修复 23 条）。**缺陷数量的决定因素是交付/改动强度（修复量 vs 引入量 r = +0.88），而非 AI 用量**——后者在剔除极值后相关性归零。

不再是「技术团队的头」，而是「企业的架构师 + 信任的守门人」。

来源：McKinsey《The new CIO mandate》× AI Harness 方法

CIO：从花钱的，到投资的

过去的 CIO 定位

技术支出的执行者

按预算把系统交付完，向 CFO 交代成本

与业务隔一层

理解需求、排期、交付，不参与方向

被动的服务方

业务提需求，IT 接需求、控成本

当下的 CIO 转身

内部资源的投资者

把 AI / 平台 / 数据当作「资本」去配置，而非成本去压缩

与 CEO 高度同频

对齐公司战略，决定技术资源投在哪、投多少

主动的价值引擎

用约束体系承接技术资产，隔一层的 IT 变成并肩的合伙人

CIO 不再是「花技术钱的」，而是「拿技术钱去投资业务的」。

组织级 AI Harness，正是这笔投资要落地的底座。

成熟度不看 AI 多先进，看交付多确定

确定性逐级上升



季度增长趋势（Q1 → Q2 → Q3）

连续两季环比均 >40%，且增长性质发生根本变化。

季度	可比成员工时合计	工作日	人均日完成工时	环比	增长性质
Q1	3,392.1 h	60 天	6.28 h	—	基线
Q2	4,985.4 h	63 天	8.79 h	+39.9%	量的增长 靠加人、含外包补位
Q3	7,200.6 h	65 天	12.31 h	+40.0%	质的增长 去除外包红利后的真实内生提效

M0 自由发挥

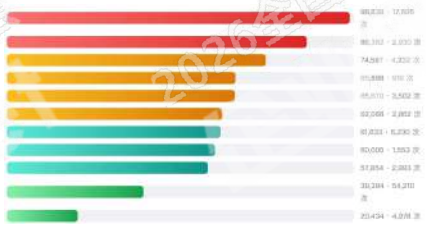
约束缺位，AI 全凭个人救火

M1 有方向

战略与架构：知道为什么、边界在哪

M2 可预期

契约与门禁：不合格被拦在半路

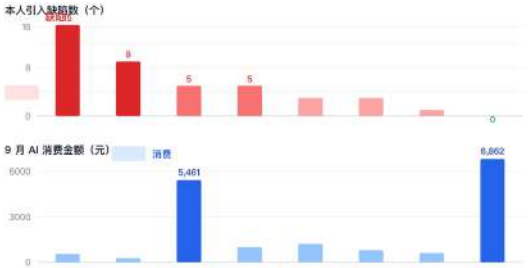


M3 扛得住

幂等与退化：出错时业务不停摆

M4 会进化

记忆 · 归因 · 测试：教训自沉淀、体系自诊断



AI Native 的一个公式

一个不同时间一定有不同答案的猜测：定义 AI Native。

超级个体

会提问、会被 LLM
放大的人

+

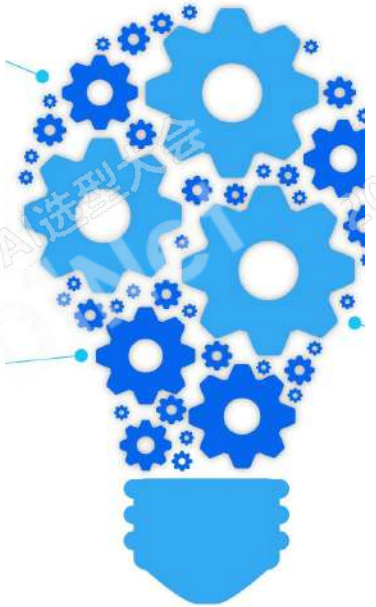
组织级 AI Harness

把个人的闭环，
写进组织的体系

=

AI Native 组织

能力与思想，
一起被改写



一个人强，叫运气；

一套体系能复制强，才叫组织。

FDE：长在客户现场的技术角色

01

源头 · Palantir 发明

2000 年代末确立并推广；内部曾称 Delta，约 2011 年前后正式化。

02

名字 · 借军事术语

「forward deployed」来自 forward-deployed forces，最早的客户就是情报机构。

03

真实前线案例

Mark Scianna 部署到美国陆军旅级指挥所：装服务器、做数据集成、
训练情报分析员使用 Palantir。

「这些洞察，在加利福尼亚的
办公室里永远得不到。」

——前出部署的意义

四位一体

工程 现场 求解 共情

长在客户一侧，但根子是软件工程：先工程师，再业务。

澄清一个事实：FDE 是「深入业务的技术角色」

提倡它的人常常只讲「贴近业务」，但它的底色仍是技术——贴近业务是手段，技术交付才是本。

来源：decode talent · gtmengineering · Palantir 公开资料



FDE × 本体

把超级个体放到客户现场：
FDE 交付问题，本体沉淀事实。

本体：把「能看、可连、可做」显式化

治理层 · 可审计 / 可回收 / 分级授权

OBJECTS

实体

管什么数据：被抽象成对象，统一接入。

订单 / 客户　仓库 / 生产
配送　医疗设备 / 病患

RELATIONS

关系

谁和谁可连——每条都是加密传输 + 授权边界。

订单 / 客户　配送 / 病患
每条关系都带授权边界

ACTIONS

行动

决策 / 动作：调度 · 审批 · 预警，同样受治理、留痕可查。

调度 · 审批 · 预警
同样受治理、留痕可查

对象管数据、关系管连接、动作管执行——三层都在治理之下显式化。

同一套做法，从深水区走进运营层

2008–2016

经典 · 深水区治理

情报 · 国防 · 金融反欺诈；
FDE × 本体管最敏感的数据。

2024–

当下 · LLM 赋能的超级个体

Anthropic / OpenAI / Sierra
大规模采用 FDE：一人即一队，
单点倍数放大。

FDE（前出部署的人） × 本体（可治理的数据）
× Harness（工程约束） = AI Native 组织

26.09 -- FDE 初步实践报告

把部门每周重复做的事，变成“乐安 X1”的一条指令，面向 Daily 频率优先部署企业 Agent

IT运维部

工单自动化，46 项指令；
晨检、日报、巡检等
8 个自动任务天天跑。

商务部

发一条报单，出合同草稿
邮件也能发报单，
模板自动找、自动复用。

运营部

交易报表放进指定文件夹，
30 秒内自动转成
结果推回群，全程没人管。

资金部

自动筛出可闭卷信用证
办完回一句「闭卷完成」，
系统状态自动改已注销。

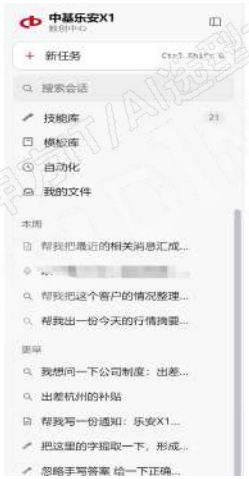
信审部

机器人识别带审查公司，翻邮箱、去重、
打包成 zip，
进度实时推群。

业务部

DP到单后自动生成付款单
也能乐安 X1一句话
手动触发，不用等定时。

46 项对话指令 | 8 个自动任务 | 6 条业务线专属群 | 全部自研





与君共勉，谢谢

宣讲人：王海涛　公司：中基宁波集团（CBNB）

AI Harness 工程方法系列 · 2026

