FDE 驻场交付白皮书：让 AI 员工进入真实流程并完成资产移交

以业务现场为起点，把流程、知识、工具、权限和验收组织成可复用交付资产

在线技术白皮书

6 分钟阅读

发布日期 / 更新日期
2026-11-22

适合读者

企业项目负责人、业务 owner、IT 与安全团队、交付经理和采购人员

核心结论 / DIRECT ANSWER

FDE 的核心价值是把通用 AI 能力转化为企业现场可验收的工作系统。驻场不是长期替代客户团队，也不是无限定制；它通过共同诊断、短周期原型、真实数据联调、分阶段验收和资产移交，缩短“能演示”与“能使用”之间的距离。

01 / KEY QUESTIONS

本白皮书回答的关键问题

Q1

FDE 与传统软件实施有什么差别？

FDE 同时处理业务流程、模型行为、知识、工具与权限，需要用真实任务持续校准，而不是只安装配置既定功能。

Q2

驻场是否意味着无限开发？

不是。项目必须约定任务范围、变更机制、验收标准与退出条件，优先沉淀可复用资产，避免不可维护的个人化脚本。

Q3

交付结束应留下什么？

应留下版本化应用、接口与权限清单、评价集、运行手册、培训记录、已知限制和回滚路径，而不仅是一个可运行环境。

02 / 正文

01

为什么 AI 员工需要现场工程

企业难点通常不在单次模型调用，而在隐性流程、脏数据、系统权限和责任交接。

通用演示往往假设输入干净、目标明确、接口可用且结果有人检查。真实现场则包含非标准文档、口径冲突、历史系统、账号权限、审批链和例外处理。FDE 通过业务与工程共同工作，把这些隐性条件转化为可设计、可测试的任务契约。

中国信通院智能原生研究强调企业转型需要组织、流程、数据与技术协同。FDE 可作为这种协同的执行机制，但不能替代企业管理层的流程决策，也不能承诺自动解决所有历史系统问题。

- ✓ 业务侧提供真实任务、例外和验收标准。
- ✓ 工程侧处理运行时、知识、接口、权限与可观测性。
- ✓ 安全与合规在方案阶段介入，而不是上线前补审。
- ✓ 项目 owner 对范围、资源、变更和最终采用负责。

本章来源 [1] [2] [4]

02

现场诊断：找到值得交付的首条任务链

优先级不只看“最想做什么”，还看价值、可行性、风险和可复制性。

诊断阶段应观察工作如何真正发生：跟随任务从发起到验收，采集样例、时间、角色、系统、返工和异常，而非只依赖访谈中的理想流程。涉及敏感数据时使用经授权的最小样例，避免为调研复制无关资料。

候选任务可按业务频率、人工基线、输入可得性、输出可检查性、动作可逆性、系统接入成本和推广价值评分。评分是决策辅助，不是虚构的 ROI 承诺。优先选择能在一个交付周期内形成闭环证据的任务。

诊断维度	现场问题	交付决策
任务价值	频率、等待、返工发生在哪里?	是否值得优先试点
数据与知识	来源、 owner、质量和权限是否清楚?	能否合法、稳定接入
系统与动作	接口可用吗，错误是否可逆?	自动化深度与人工节点
验收与复制	谁验收，能否跨团队复用?	范围与后续扩展路径

本章来源 [1] [4] [3]

03

原型共创与系统接入：小闭环优先

原型不是界面演示，而是用真实约束验证任务能否端到端完成。

先用小但真实的评价集建立任务契约，再接入必要知识与只读工具，最后逐步开放有副作用的动作。每次增量只改变有限变量，使质量或延迟变化能够归因。原型环境应记录模型、应用、Skill、知识和接口版本，避免“昨天还能用”的不可复现状态。

VROS Agent 可承接应用、事件、记忆、空间和 Worker 执行的组织；AIBotStore 提供角色与任务配置入口。FDE 则把这些能力映射到企业账号、知识源、业务系统、审批与算力环境。VR Lang、连山及具体连接器的可用范围以交付版本和项目适配为准。

- ✓ 先只读验证知识与检索，再验证写入和外部动作。
- ✓ 每个接口明确身份、字段、超时、重试、限流和错误语义。
- ✓ 网页、文档和工具返回值按不可信输入处理。
- ✓ 为关键动作建立模拟环境、审批与回滚，不直接以生产试错。

本章来源 [1] [8] [2]

04

联调与验收：把质量、异常和责任一起测

验收不只证明“成功过一次”，还要证明在约定条件下能重复、能停止、能恢复。

测试应覆盖正常任务、边界样本、缺失数据、权限不足、接口超时、模型异常和人工接管。结果按任务阶段记录，质量由业务验收，权限与日志由 IT 和安全复核，性能由真实模型服务与算力环境测量。若测试使用脱敏或模拟数据，应明确其与生产差异。

验收阈值、样本范围、版本、责任人和原始证据共同构成结论。未经验证的目标人效、交付周期、拒绝率或硬件指标不能写成项目事实。对未达标项，应形成限制使用、补充开发、重新测试或终止的明确处置。

验收层	测试内容	签署证据
业务质量	真实任务、困难样本与交付标准	评价集结果与业务签署
技术运行	重复执行、超时、恢复与长稳	事件、日志与资源记录
安全权限	越权、注入、审批与数据边界	安全测试与整改记录
组织操作	培训、接管、停用与升级	演练记录与责任人确认

本章来源 [6] [5] [2]

05

资产移交：让客户团队能够接续运营

交付的终点不是专家离开，而是企业获得可理解、可维护、可审计的工作资产。

移交清单至少包括 VR Lang 或其他应用资产、提示词与 Skill、知识和接口清单、权限矩阵、评价集、监控指标、运行手册、培训与已知限制。每项资产需要 owner、版本、依赖、存储位置和变更方式，避免只交付个人电脑上的脚本或不可追踪的配置。

ISO/IEC 42001 的管理体系思路可用于明确职责、风险、运行与持续改进，但参考该标准不代表 AIBotStore 或客户项目已获得认证。对甲方而言，资产归属、第三方许可、保密、退出和后续支持应在合同与移交清单中分别约定。

- ✓ 应用资产：版本、用途、依赖、发布和回滚。
- ✓ 数据资产：来源、权限、质量、更新和删除责任。
- ✓ 评价资产：样本、基线、阈值、失败与复测方法。

- ✓ 运营资产：监控、告警、接管、培训和变更流程。

本章来源 [7] [4] [6]

06

变更与持续服务：防止驻场变成依赖

FDE 应逐步提升客户自主运营能力，而不是形成不可替代的人工黑盒。

项目可设置联合例会和变更看板，按业务价值、风险与依赖审查新增需求。模型、工具、知识、权限或业务流程变化触发影响分析和必要复测。高频共性问题优先沉淀为产品化配置、标准连接器或通用 Playbook，减少重复定制。

部署后监测需要与客户支持、安全和资产管理衔接。受控自进化如进入项目，只可作为候选经验与改进流程，经过沙箱验证、人工审批和版本化后受控发布；具体能力以交付版本和验收为准。高风险动作始终保留人工负责。

- ✓ 约定服务边界、响应机制、变更分类和费用原则。
- ✓ 把重复问题转化为文档、测试与可复用组件。
- ✓ 以阶段验收决定扩大、维持、缩减或退出。
- ✓ 在运行中持续复核质量、安全、成本与人员接管能力。

本章来源 [6] [7] [1]

---

03 / CHECKLIST

项目启动前检查清单

可将以下项目转化为 PoC 计划、采购问题或验收清单。

01	现场观察真实任务并采集经授权的代表性样例
02	按价值、可行性、风险和复制性选择首条任务链

03 从只读原型逐步接入工具与有副作用动作

04 验收覆盖质量、重复运行、异常、安全与人工接管

05 移交版本化应用、接口、权限、评价集和运行手册

06 建立变更、复测、支持、退出与客户自主运营机制

04 / FAQ

常见问题与直接回答

01 FDE 必须长期驻场吗?

不必然。驻场强度取决于诊断、联调和验收需要，可采用现场与远程结合。关键是现场信息真实、责任清楚和资产可移交，而非固定驻场时长。

02 FDE 与普通定制开发如何避免混淆?

在立项时明确任务链、模型与知识行为、复用资产和验收方法。传统功能开发可以包含其中，但 FDE 还必须验证 AI 任务质量、异常和人机责任。

03 能否在 PoC 前承诺交付周期缩短或人效倍数?

不应把目标写成事实。周期和人效需要基于客户基线、范围和真实验收评估，结果受数据、接口、流程与组织条件影响。

04 项目结束后客户能否独立维护?

应以此作为移交目标，通过版本化资产、文档、培训、演练和权限移交实现；具体自主维护范围取决于合同约定与团队能力。

05 / REFERENCES

参考文献与公开来源

中文按 GB/T 7714 风格编排，英文按 APA 风格编排。访问日期：2026-11-22。外部资料用于行业与技术方法参考，不代表 AIBotStore 获得其背书或认证。

[1] 中国信息通信研究院人工智能研究所. 智能原生（AI Native）研究报告（1.0）：企业智能原生转型框架与实践[R/OL]. (2026-10)[2026-11-22].
https://www.caict.ac.cn/kxyj/qwfb/ztbg/202610/P020261022558735347833.pdf →

[2] 中国信息通信研究院政策与经济研究所, 中国政法大学人工智能法研究院. 智能体治理研究报告（2026年）[R/OL]. (2026-09)[2026-11-22].
https://www.caict.ac.cn/kxyj/qwfb/ztbg/202609/P020260916574260931247.pdf →

[3] 中国信息通信研究院. 人工智能安全治理蓝皮书（2025年）[R/OL]. (2026-01)[2026-11-22].
https://www.caict.ac.cn/kxyj/qwfb/bps/202601/P020260109784447548497.pdf →

[4] National Institute of Standards and Technology. AI Risk Management Framework（AI RMF 1.0）[EB/OL]. (2023-01-26)[2026-11-22].
https://www.nist.gov/itl/ai-risk-management-framework →

[5] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile（NIST AI 600-1）[R/OL]. (2024-07-26)[2026-11-22].
https://doi.org/10.6028/NIST.AI.600-1 →

[6] Rao A, Keller A, Kalra N, 等. Challenges to the Monitoring of Deployed AI Systems（NIST AI 800-4）[R/OL]. (2026-03)[2026-11-22].
https://doi.org/10.6028/NIST.AI.800-4 →

[7] International Organization for Standardization. ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system[S/OL]. (2023-12)[2026-11-22].
https://www.iso.org/standard/42001 →

[8] OWASP GenAI Security Project. Agentic AI—Threats and Mitigations[EB/OL]. (2025-04-28)[2026-11-22]. https://genai.owasp.org/resource/agentic-ai-threats-and-mitigations/ →

范围说明

本白皮书用于技术选型与项目规划参考，不构成法律、合规、安全或投资专业意见。VROS Agent、AIBotStore、硬件适配和受控自进化的实际范围以交付版本、项目合同与验收为准。行业任务示例不代表已交付客户或已实现成效。