

AI 应用赋能实践域（AIE）

AI 应用赋能实践域（AIE）概述

必须的实践域信息

意图

在保障企业信息安全与知识产权的前提下，系统化应用大语言模型（LLM）等 AI 技术，提升工程活动的效率与质量，并构建可持续、受控的赋能体系。

价值

通过 AI 辅助减少重复劳动、加速知识流转、增强决策一致性，从而提升工程效能、降低成本，并推动组织向智能化工程模式演进。

解释性实践域信息

实践摘要

第 1 级

AIE 1.1 在工程活动中尝试应用 LLM 工具辅助任务执行。

第 2 级

AIE 2.1 识别并选择适合 LLM 辅助的工程活动场景。

AIE 2.2 在局部流程中集成 LLM 工具并收集使用反馈。

AIE 2.3 专注于初步的风险识别与控制。

第 3 级

AIE 3.1 根据组织定义的流程，在工程活动中应用 LLM 辅助解决方案。

AIE 3.2 为 LLM 应用设计提示词模板与集成工具链。

AIE 3.3 开展人员培训与技能评估。

AIE 3.4 收集并分析 LLM 应用前后的效能数据。

AIE 3.5 建立 LLM 解决方案的持续优化机制。

AIE 3.6, 专注于建立系统化的安全治理流程。

第 4 级

AIE 4.1 使用统计与量化方法分析 LLM 应用对过程性能的影响。

AIE 4.2 基于数据驱动优化 LLM 提示词、模型选型与集成策略。

第 5 级

AIE 5.1 将已验证的 LLM 应用模式推广至组织全流程, 并通过制度与文化变革固化赋能效果。

AI 应用赋能 (AIE) 旨在将 LLM 等 AI 技术系统化融入软件工程实践, 其核心活动包括:

- ☐ 识别可应用 LLM 提升效率与质量的工程场景
- ☐ 构建集成的 LLM 工具链与提示词管理体系
- ☐ 实施人员培训与能力评估
- ☐ 通过数据对比验证局部与整体效能提升
- ☐ 建立持续优化机制并推广有效实践
- ☐ 调整流程、模板、检查项与度量体系
- ☐ 设立专职团队负责推广与优化, 并向高层定期汇报
- ☐ 识别 LLM 应用场景中的信息安全与知识产权风险。
- ☐ 建立数据分类、输入输出审查、API 安全管控等治理措施。

负责 LLM 应用推广的专职团队 (如 AI 赋能中心), **必须配备或紧密联动信息安全专家。**

其职责包括:

- ☐ **维护和更新 AI 安全治理规范。**
- ☐ **调查与响应所有与 LLM 使用相关的安全事件。**
- ☐ **定期向高层汇报效能提升与安全状态 (双轨汇报) 。**

AIE 强调领导关注、集成方案、人员训练、数据验证、专人负责、持续优化、全员推广，并最终推动文化、流程、制度、职责、能力与绩效的系统性变革。所有 AI 赋能活动均不得以牺牲安全性为代价追求效率。

关联实践域

- 组织级培训 (OT)
- 过程管理 (PCM)
- 决策分析与解决 (DAR)
- 性能管理与度量 (MPM)

上下文相关

敏捷开发

上下文标签敏捷开发

上下文说明在迭代周期内集成 LLM 辅助活动，提升敏捷协作与交付效率。

敏捷团队可在站会、迭代规划、评审与回顾中应用 LLM 辅助。例如：

- ☐ 使用 LLM 自动生成用户故事验收条件
- ☐ 在回顾会中分析迭代瓶颈的根因
- ☐ 辅助代码评审与测试用例生成
- ☐ LLM 工具应嵌入敏捷工具链（如 Jira、Confluence），并与持续集成流水线结合。

DevSecOps

上下文标签DevSecOps

上下文说明在 CI/CD 流水线中集成 LLM，提升安全与运维自动化水平。

DevSecOps 团队可利用 LLM：

- ☐ 自动化安全漏洞分析
- ☐ 辅助日志异常检测与根因定位
- ☐ 生成部署检查清单与运维响应脚本

- ☐ 需注意 LLM 输出的安全合规校验，并建立人工审核机制。
- ☐ LLM 辅助安全代码审查时，其自身生成的代码必须经过与人工代码相同的安全流水线扫描。
- ☐ 用于分析日志和事件的 LLM 提示词及输出，必须纳入安全事件与事故管理 (SIEM) 系统的监控范围。
- ☐ 在快速迭代中，应将“LLM 使用安全审查”作为 CI/CD 流水线中的一个可选或强制关卡。

第 1 级

AIE 1.1

必须的实践信息

实践陈述

在工程活动中尝试应用 LLM 工具辅助任务执行

价值

初步体验 AI 辅助潜能，激发团队兴趣与探索意识。

解释信息

初期可聚焦于低风险、高重复性任务，如文档摘要、代码注释生成、会议纪要整理等。

示例活动

在编写技术文档时使用 LLM 辅助草拟内容

在代码开发中使用 IDE 插件实现自动补全

尝试使用 LLM 分析简单的问题日志

示例工作产品

LLM 试用记录

初步效果反馈表

第 2 级

AIE 2.1

必须的实践信息

实践陈述

识别并选择适合 LLM 辅助的工程活动场景。

价值

聚焦于高回报场景，确保资源投入产生最大效能提升。

补充解释信息

选择标准可包括：任务频率、自动化潜力、对质量/效率的影响度、实施成本与安全风险。

示例活动

调研各工程环节中的痛点与重复劳动

使用价值流图识别 LLM 可优化的等待与转换环节

评估不同场景的 LLM 适用性与集成复杂度

示例工作产品

LLM 适用场景分析报告

优先级排序清单

AIE 2.2

必须的实践信息

实践陈述

在局部流程中集成 LLM 工具并收集使用反馈。

价值

通过小范围验证降低风险，快速迭代解决方案。

示例活动

在某个项目组部署 LLM 辅助代码评审工具

设计并试用提示词模板库

收集用户满意度与问题反馈

示例工作产品

试点项目总结报告

用户反馈日志

AIE 2.3

必须的实践信息

实践陈述

识别 LLM 应用中的信息安全与知识产权风险，并实施基本管控。

价值

建立初始安全边界，防止在试点阶段发生重大数据泄露。

解释信息

在引入任何 LLM 工具前，应对其数据处理政策（如是否用于训练）进行评估，并对拟输入的数据进行敏感度分级。

示例活动

制定《LLM 使用初步安全守则》，明确禁止输入公司核心代码、客户数据、未公开战略等。

为团队提供公开模型与私有化部署模型的风险对比培训。

在试用反馈表中增加“是否涉及敏感信息”字段。

示例工作产品

《LLM 应用场景风险初步评估表》

员工安全知晓确认记录

第 3 级

AIE 3.1

必须的实践信息

实践陈述

根据组织定义的流程，在工程活动中应用 LLM 辅助解决方案。

价值

确保 LLM 应用符合组织规范，支持规模化推广。

示例活动

制定《LLM 应用实施指南》

在需求分析、设计、编码、测试、运维中嵌入 LLM 辅助步骤

执行 LLM 输出结果的人工验证流程

示例工作产品

LLM 应用流程图

集成工具清单

AIE 3.2

必须的实践信息

实践陈述

为 LLM 应用设计提示词模板与集成工具链。

价值

提升 LLM 输出稳定性与可用性，降低使用门槛。

示例活动

建立组织级提示词库，按场景分类管理

开发或集成 LLM API 中间件，实现统一调用与审计

将 LLM 功能嵌入 IDE、项目管理平台与 CI/CD 流水线

示例工作产品

提示词模板手册

工具链集成架构图

AIE 3.3

必须的实践信息

实践陈述

开展人员培训与技能评估。

价值

确保员工具备必要的 AI 应用能力，提升工具采纳率。

示例活动

设计分层培训课程（基础、进阶、专家）

组织提示词编写工作坊与实战演练

实施能力认证考试，并将 AI 技能纳入职级体系

示例工作产品

培训课程材料

人员技能矩阵与认证记录

AIE 3.4

必须的实践信息

实践陈述

收集并分析 LLM 应用前后的效能数据。

价值

量化 LLM 应用成效，为优化与推广提供依据。

示例活动

定义效能度量元（如任务耗时、缺陷率、用户满意度）

在试点组与对照组之间进行对比分析

编制效能分析报告，展示局部与整体影响

示例工作产品

效能对比分析报告

度量数据仪表盘

AIE 3.5

必须的实践信息

实践陈述

建立 LLM 解决方案的持续优化机制。

价值

确保 LLM 应用随技术发展与业务需求持续演进。

示例活动

设立定期评估会议，评审提示词效果与工具性能

建立反馈渠道，收集用户改进建议

跟踪业界 LLM 技术进展，评估引入新模型的可行性

示例工作产品

优化迭代计划

技术雷达扫描报告

AIE 3.6

必须的实践信息

实践陈述

遵循组织安全流程，实施系统的 LLM 安全治理。

价值

构建制度化的 AI 安全防线，使规模化应用具备合规基础。

解释信息

治理措施应覆盖数据全生命周期：输入前、处理中、输出后。

示例活动

输入管控：

与信息安全部门共同定义数据分类级别（公开、内部、机密、绝密）。

在集成的工具链中部署预检过滤器，自动拦截或脱敏高密级数据。

强制要求对提示词进行安全审查，避免“提示词注入”泄露指令逻辑。

处理与审计：

优先采用私有化部署模型或具有数据隔离承诺的商用 API。

所有 LLM API 调用必须记录完整的审计日志（时间、用户、输入/输出哈希、模型）。

建立定期安全审计机制。

输出管控：

对关键业务领域的 LLM 输出（如法律条款、安全代码）建立强制人工复核流程。

在 CI/CD 管道中集成 AI 生成代码的安全扫描工具。

示例工作产品

《企业 LLM 应用安全治理规范》

数据分类与脱敏规则清单

LLM API 调用审计日志系统

安全审查清单与复核记录

第 4 级

AIE 4.1

必须的实践信息

实践陈述

使用统计与量化方法分析 LLM 应用对过程性能的影响。

价值

深入理解 LLM 对工程效能的作用机制，支持精准优化。

示例活动

使用控制图、回归分析等方法量化 LLM 贡献度

分析不同团队、不同场景下的效果差异

建立预测模型，预估新场景引入 LLM 的潜在收益

示例工作产品

统计分析报告

性能预测模型

AIE 4.2

必须的实践信息

实践陈述

基于数据驱动优化 LLM 提示词、模型选型与集成策略。

价值

提升 LLM 输出的准确性、稳定性与业务契合度。

示例活动

A/B 测试不同提示词模板的效果

评估不同模型在特定任务上的性能

优化 API 调用策略以平衡成本与响应速度

示例工作产品

提示词版本管理库

模型选型评估报告

第 5 级

AIE 5.1

必须的实践信息

实践陈述

将已验证的 LLM 应用模式推广至组织全流程，并通过制度与文化变革固化赋能效果。

价值

实现 AI 赋能的全员覆盖与深度融入，推动组织智能化转型。

示例活动

制定组织级 AI 应用推广路线图

将 AI 效能指标纳入团队与个人绩效考核

设立“AI 创新奖”，鼓励最佳实践分享

在组织文化中强调数据驱动与人机协同

示例工作产品

AI 应用推广计划

更新后的岗位职责与绩效合同

文化变革沟通材料