

ISO 9001:2015 §7.1.6

V2 正式可外审版

SOP-33 AI_Advisor使用管理程序 v2

Lithera 程序文件 v2 — 主责: KC + 全员

文件信息	内容
文件编号	LITHERA-SOP-33-V2-20260429
版次	v2
主责	KC + 全员
对标 ISO 9001:2015	§ 7.1.6 组织的知识
来源	Lithera 自主新增 (5 AI Advisor 系统化管理)
关联	Empryon 第 5 条方法论专利
适用	Lithera 全部 AI Advisor 调用情境
保存期	5 年

文件变更履历表

版序	日期	内容
v1	2026-04-28	框架版
v2	2026-04-29	首版正式可外审版: 完整人在回路 + 异常处置 + 持续优化

1. 目的

本程序规范本公司**5 AI Advisor**（合规 / 采购 / 供应链 / 战略 / 财务）之调用、决策辅助、记录、责任之机制，确保：

1. **AI 辅助决策有效**：85%+ 建议被采纳后效果良好
2. **人在回路（HITL）**：AI 仅辅助，最终决策仍由人类负责
3. **可追溯**：所有 AI 调用 + 回应纪录留存
4. **持续优化**：异常案例回馈 prompt 改进
5. **合规风险可控**：AI 错误不导致法规违反或重大损失
6. **法律风险可控**：明确 AI 仅辅助，不替代专业判断

业内痛点：AI 工具普遍缺乏使用规范，员工容易「**全信 AI 不查证**」或「**完全不用浪费投资**」。本公司透过明确的**调用流程 + 决策准则 + 异常处置**，让 AI 真正成为「**5 人团队作 50 人产能**」的副驾。

2. 适用范围

涵盖：所有员工调用本公司 5 AI Advisor 之情境。

3. 5 AI Advisor 介绍

3.1 5 AI Advisor 列表

Advisor	领域	主要功能	调用情境
Compliance Advisor	法规合规	危化品 / 出口 / SDS / GHS 问题	法规变更 / 合规审查 / 客诉法律风险
Procurement Advisor	采购策略	询价 / 议价 / 双源 / 风险评估	采购规划 / 供应商评估
Supply Chain Advisor	供应链管理	库存 / 物流 / 风险 / 仓储	库存预警 / 危运调度
Strategy Advisor	战略规划	市场 / 客户 / 定价 / 扩张	战略决策 / 客户关系
Finance Advisor	财务 / 税务	报销 / 税务 / 汇率 / 内控	财务决策 / 月结

3.2 技术架构

- 基础模型: Claude Sonnet 4.6 / Opus 4.7 (视复杂度)
 - 调用通道: claude-proxy:8099 (KC OAuth)
 - 系统提示: 每 Advisor 注入 Lithera 业务上下文
 - Memory : Lithera 平台 type=advisor_chat 留档
-

???

????????????

6. 决策辅助原则（核心）

6.1 人在回路（Human-in-the-Loop, HITL）

AI Advisor 仅提供建议，绝不可替代人类决策。

决策等级	AI 建议作用	人类签核
一般操作	参考	员工自决
中风险（RMB 5,000-10 万）	重要参考	主管签核
高风险（≥ RMB 10 万 / 法规 / 客户合约）	必参考但可推翻	KC 签核
极高风险（≥ RMB 100 万 / 战略）	必参考 + 律师审核	KC + Charles + 律师

6.2 5 大不可代替

AI **绝不可** 代替： 1. 法律决策（必律师审核） 2. 重大财务决策（必 KC + Charles） 3. 客户重大承诺（必 KC） 4. 应急救援现场决策（必 Robert + KC 现场） 5. 员工去留决策（必 KC + 王婧）

6.3 可信度判断

员工评估 AI 建议时考虑： - 这个领域 AI 历史准确度 - 信息时效（AI 训练数据可能过期） - 是否涉及本公司专属 know-how（AI 可能不知） - 是否涉及最新法规变更 - 复杂度（越复杂越要查证）

7. 调用纪录

7.1 自动留档

每次调用自动留档： - 调用者 - Advisor 类型 - 时间 - 问题（完整 prompt） - AI 回应（完整 response） - 是否采纳 - 执行结果（如适用） - 后续追踪（如有）

7.2 可追溯性

任何重大决策可追溯到： - AI 建议 - 人类决策 - 执行结果 - 改进措施

8. 异常处置

8.1 异常类型

异常	描述	处置
AI 建议明显错误	与事实 / 法规不符	立即记录 + 通报 KC
AI 输出涉敏感信息	误回客户 / 供应商机密	立即停止 + 通报 KC
AI 服务中断	平台无回应	切换备援（Empryon 团队） / 人工处理
重大决策后 AI 错误暴露	已采纳后发现错误	立即评估损失 + 触发 SOP-08 + 改进 prompt
AI 答非所问	偏离问题	重新提问 + 优化 prompt

8.2 异常通报流程

```
??????  
?????  
[24h ??Lithera ???type=advisor_anomaly ??]  
?????  
?????KC + Empryon ???  
?????  
[KC ??]  
????????????????????  
????????????????????Advisor + Empryon ???  
?????  
[Prompt ?????system message ??]
```

?? ??
?? ?? ?? ??
?? ??
?? ?? ?? ??
?? ??
?? ?? ?? ?? ?? ??

8.3 严重错误标准

发生下列任一即「**严重错误**」，立即触发 § 8.2 流程 + KC 直管： - 法规违规 / 行政处罚 - 重大财务损失 (≥ RMB 10 万) - 客户索赔 - 安全事件 - Know-how 泄漏 (如 AI 误回应客户)

9. 持续优化

9.1 月度评估

KC 每月评估： - 各 Advisor 调用次数 - 采纳率 - 异常率 - 准确度 (事后验证) - 员工满意度

9.2 季度 prompt 重申

KC + Empryon 团队每季： - 检视各 Advisor system prompt - 客户案例反馈纳入 prompt 优化 - 新法规 / 新业务模式纳入

9.3 半年模型升级评估

如 Claude / 其他 AI 模型有重大升级： - 评估升级效益 - 影响测试 - 决定是否升级

10. KPI

KPI	目标
AI 建议采纳后效果良好率	≥ 85%
严重 AI 错误事件	= 0
调用响应时间	< 30 秒
月度调用次数（每员工）	≥ 20 次（鼓励使用）
异常 24h 通报率	100%

11. 法规依据

- ISO 9001:2015 §7.1.6
- 《数据安全法》
- 《个人信息保护法》
- 《生成式人工智能服务管理暂行办法》（2023-08-15）
- Lithera 自主标准：人在回路 5 大不可代替

12. 表单

表单	名称	保存
QEF-33-01	AI Advisor 调用记录（Lithera 平台自动）	5 年
QEF-33-02	AI 异常通报单	5 年
QEF-33-03	Prompt 优化记录	永久
QEF-33-04	月度 AI 使用报告	5 年

13. 关联

所有 SOP 之 AI Advisor 调用 → 本程序规范。

特别关联： | SOP | AI 调用情境 | |----|-----| | SOP-01 采购 | Procurement Advisor | | SOP-02 销售 | Strategy Advisor | | SOP-08 不合格 | Compliance Advisor | | SOP-09 供应商 | Procurement + Supply Chain Advisor | | SOP-15 客户服务 | Strategy + Compliance | | SOP-21 法规 | Compliance Advisor (核心) | | SOP-25 内审 | AI 抽样辅助 | | SOP-30 统计 | AI 关联分析 |

14. 培训

#	课程	时长
1	本程序 + 人在回路原则	4h
2	各 Advisor 调用情境 + 实操	4h
3	Prompt 工程基础	4h
4	AI 异常识别	2h
	合计	14h

每年复训：4h (更新 + 新案例) 。

15. 审批

角色	签字
Miku (AI 副驾自我介绍) + KC	—
Robert + Charles	—

