《大型语言模型（LLM）系列产品工具及提示词工程》专业培训大纲

目标学员: 金融行业产品经理、运营人员、技术开发者、数据分析师、风险管理人员、合规专员以及对 LLM 应用感兴趣的相关人员。

培训目标:

- 全面了解主流大型语言模型的特点、能力边界与选型策略。
- 掌握 LLM 的多种使用方式，理解企业级接入与部署的关键考量。
- 精通提示词工程的核心原理、结构与高级技巧。
- 能够针对金融领域的具体场景（分析、客服、风控等）设计、优化和应用高效提示词。
- 理解 LLM 使用的最佳实践、伦理考量与未来趋势。 **先决条件:** 对人工智能和金融业务有基本了解。

模块一：大型语言模型（LLM）概览与选型

- **1.1 主流 LLM 产品深度解析**
    - **核心模型介绍:**
        - **国际代表:**
            - DeepSeek (特点: 开源、代码能力)
            - ChatGPT (特点: 综合能力、插件生态)
            - Claude (特点: 长文本处理、安全与伦理)
            - Gemini (特点: 多模态、Google 生态集成)
        - **国内代表:**
            - 文心一言 (特点: 中文理解、百度生态)
            - 通义千问 (特点: 综合能力、阿里生态)
            - 讯飞星火 (特点: 语音交互、跨领域知识)
        - *(实时更新)* 其他值得关注的新兴模型。
        - **演示:** 对比不同模型对同一通用任务的响应（如摘要、翻译）。

- **开源 vs. 闭源 LLM:**
  - 定义与代表模型。
  - **核心差异:** 成本、定制化潜力、数据隐私控制、更新频率、社区支持。
  - **案例讨论:** 为何某金融科技公司选择基于开源模型微调，而另一家大型银行选择使用闭源模型的 API?

- **1.2 LLM 核心能力维度对比**
  - **语言理解与生成:**
    - 文本摘要、内容创作、翻译、情感分析等能力对比。
    - **实例:** 使用不同模型生成同一主题的营销文案，对比风格和效果。
  - **多模态能力:**
    - 图像理解 (OCR, 图表解读, 图像描述)。
    - 图像生成 (根据描述创作)。
    - 音频处理 (语音识别、语音合成)。
    - **实例:** 使用多模态模型解读财报截图中的图表，或根据语音指令生成会议纪要。
  - **工具使用与代码能力:**
    - Function Calling / Tool Use 机制介绍。
    - 代码生成、解释、调试能力。
    - **演示:** 如何让 LLM 调用外部 API（如实时股价查询）或生成一段 Python 数据分析脚本。
  - **安全性与合规性:**
    - 偏见与歧视风险。
    - 数据泄露风险。
    - "幻觉"现象与事实核查。
    - 不同模型的安全防护机制对比。
    - **讨论:** 金融场景下，哪些安全合规问题最为关键?

- **1.3 如何为您的业务选择合适的 LLM**
    - **选型核心考量因素:**
        - 任务匹配度 (特定能力强项)。
        - 性能指标 (准确率、响应速度)。
        - 集成复杂度 (API 友好度、文档支持)。
        - 供应商可靠性与技术支持。
        - 社区生态与未来发展。
    - **成本效益分析:**
        - API 调用成本 (Token 计费)。
        - 私有化部署成本 (硬件、人力)。
        - 订阅费用。
        - **模板:** 提供一个简单的成本效益分析框架供学员参考。
    - **隐私保护与数据安全:**
        - 数据处理协议 (Data Processing Agreements)。
        - 数据是否用于模型再训练?
        - 数据传输与存储加密。
        - 满足金融监管要求（如 GDPR, CCPA, 国内相关法规）。
        - **案例分析:** 对比不同云服务商提供的 LLM 在数据隐私保护条款上的差异。

模块二：LLM 使用方式与企业级集成

- **2.1 多样化的 LLM 使用方式**
    - **Web/移动端交互:**
        - 官方界面、第三方应用。
        - 优点：易上手、快速验证。缺点：自动化程度低、难以集成。
        - **实操:** 学员现场体验不同模型的官方 Web 界面。
    - **API 调用:**

        - RESTful API 基础。
        - 关键参数 (模型、温度、最大 Token 数等) 解释。
        - **代码示例:** Python 调用主流 LLM API 的基本代码框架。
    - **大型云平台服务 (LLM as a Service):**
        - AWS Bedrock, Azure OpenAI Service, Google Vertex AI 等。
        - 优点：托管服务、易扩展、集成生态。
        - **介绍:** 各大云平台提供的 LLM 服务特点和优势。
- **2.2 企业级 LLM 接入与部署策略**
    - **私有化部署 vs. 云服务:**
        - **对比维度:** 数据控制权、安全性、成本、维护复杂度、性能、合规性。
        - **决策树:** 提供一个简单的决策框架，帮助企业根据自身情况选择。
        - **案例研究:** 分析某证券公司选择私有化部署的动因和挑战。
    - **安全访问与身份认证:**
        - API 密钥管理最佳实践。
        - 身份认证与授权 (IAM, OAuth)。
        - 网络隔离 (VPC, Private Link)。
    - **数据保护与敏感信息处理:**
        - 数据脱敏技术 (假名化、匿名化)。
        - PII (个人身份信息) 检测与过滤。
        - 输入/输出内容监控与审计。
        - **讨论:** 如何在客服场景中应用 LLM，同时确保客户敏感信息不被泄露或滥用?
- **2.3 LLM 应用开发平台与工具**
    - **低代码/无代码平台:**
        - 介绍集成 LLM 能力的平台 (如 Zapier, Make, Coze 等)。
        - **演示:** 如何通过无代码平台快速搭建一个“邮件内容摘要”应用。

- **应用开发框架:**
    - LangChain, LlamaIndex 等核心概念与用途。
    - **简介:** 如何使用框架构建更复杂的 LLM 应用 (如 RAG)。
- **知识库与 LLM 结合 (Retrieval-Augmented Generation - RAG):**
    - 原理：解决 LLM“幻觉”和知识更新问题。
    - 构建流程：数据准备、向量化、检索、生成。
    - **案例:** 如何构建一个基于内部合规文档库的智能问答系统。

模块三：提示词工程（Prompt Engineering）核心原理与技巧

- **3.1 提示词工程导论**
    - **定义:** 什么是提示词 (Prompt)？它为何如此重要？(Garbage In, Garbage Out)。
    - **类比:** 提示词如同与“非常聪明但不了解具体任务的实习生”沟通的指令。
    - **基本原则:** 清晰性 (Clarity)、具体性 (Specificity)、上下文 (Context)、简洁性 (Conciseness)。
    - **好/坏提示词对比:**
        - **实例:** 对比模糊指令与清晰指令产生的巨大差异。
            - *差:* "总结一下市场情况。"
            - *好:* "请扮演一位资深金融分析师，根据过去 24 小时[指定信息源]的主要新闻，为我总结全球股票市场的三个关键动态，并指出每个动态对科技板块可能的影响。使用项目符号列表格式。"
- **3.2 高效提示词的结构化设计 (CRISP/RCIOS 等框架)**
    - **核心要素拆解:**
        - **角色 (Role/Persona):** "你是一位经验丰富的财富顾问..."
        - **指令 (Instruction/Task):** "请分析这份财报..." / "生成一封安抚邮件..."
        - **背景 (Context/Input Data):** "这是客户过去一年的交易记录..." /

"以下是相关的市场新闻..."

- **输出格式 (Output Format):** "请以 JSON 格式返回结果..." / "使用专业的商业信函格式..."
- **补充要素:** 语气 (Tone), 目标受众 (Audience), 约束条件 (Constraints)。

- **模板化:** 提供几种常用场景的提示词模板结构。
- **练习:** 学员分组，针对给定场景，设计结构化的提示词。

- **3.3 实用提示词技巧与高级模式**
  - **任务分解 (Decomposition / Chain of Thought - CoT):**
    - 引导模型"思考步骤"。将复杂任务拆解为子任务。
    - **实例:** 如何让模型先分析原因，再提出解决方案。
  - **思维链提示 (Chain-of-Thought Prompting):**
    - 提供包含推理过程的示例，引导模型模仿。
    - **演示:** 对比标准提示和 CoT 提示在解决逻辑推理问题上的效果。
  - **少量示例学习 (Few-Shot Learning):**
    - 在提示词中提供 1-5 个输入/输出范例。
    - **实例:** 如何通过示例让模型学会特定风格的文本生成或信息提取。
  - **零示例学习 (Zero-Shot Learning):** 依靠模型的泛化能力直接执行任务。
  - **迭代优化:**
    - 测试 -> 分析输出 -> 修改提示词 -> 再测试 的循环过程。
    - 如何根据不理想的输出反推提示词的问题所在。
    - **技巧:** 尝试不同措辞、调整结构、增减上下文、改变温度参数等。
  - **实战演练:** 提供一个不完美的提示词和输出，引导学员进行分析和优化。

模块四：金融场景提示词工程实战应用

- **4.1 金融分析与研究报告类应用**
    - **市场动态分析:**
        - **模板:** 设计用于总结宏观经济指标、行业新闻、竞品动态的提示词。
        - **案例:** 从大量财经新闻中自动提取关键信息，生成每日市场摘要。
    - **财务报告解读:**
        - **模板:** 提取关键财务指标 (营收、利润、增长率)、分析变化原因、识别潜在风险。
        - **案例:** 快速解读上市公司季度财报 PDF，生成关键要点摘要。
    - **投资研究与建议:**
        - **模板:** 结构化生成投资逻辑、风险评估、估值分析框架。 (*注意: 强调 LLM 仅为辅助，不能替代专业判断和合规审查*)
        - **讨论:** 如何设计提示词以生成初步的、平衡风险与收益的投资思路?
- **4.2 客户服务与沟通咨询类应用**
    - **金融产品智能问答:**
        - **模板:** 结合 RAG，基于产品说明书和 FAQ，回答客户关于利率、费用、申请条件的咨询。
        - **案例:** 构建虚拟客服助手，处理常见的银行业务咨询。
    - **客户意图识别与问题分类:**
        - **模板:** 分析客户消息，判断其意图（咨询、投诉、建议）并分配给相应处理流程。
    - **沟通文案生成与润色:**
        - **模板:** 生成标准化的客户通知、营销邮件、投诉回复初稿。
        - **案例:** 辅助客户经理撰写个性化的客户关怀邮件。
    - **角色扮演练习:** 学员扮演客服，使用 LLM 辅助回答模拟的客户刁钻问题。

- **4.3 风险管理与合规审查类应用**
    - **文档合规性检查:**
        - **模板:** 对比合同条款、营销材料与内部合规规则库，识别潜在违规点。
        - **案例:** 初步审查贷款申请材料是否符合银行政策要求。
    - **风险事件识别与预警:**
        - **模板:** 从新闻、社交媒体、监管公告中监测与特定公司或行业相关的负面信息或风险信号。
    - **反洗钱(AML)与欺诈检测辅助:**
        - **模板:** 总结可疑交易模式描述、辅助生成可疑活动报告(SAR)的文本内容（*强调：仅为辅助，需严格遵守法规*）。
        - **讨论:** LLM 在风控合规中的应用边界和潜在风险。
- **4.4 综合实战演练与优化工作坊**
    - **场景设定:** 提供 1-2 个贴近学员工作的金融业务场景（如: "为某基金撰写营销亮点", "分析某股票的近期风险"）。
    - **分组任务:** 学员分组，针对指定场景，合作设计、测试并迭代优化提示词。
    - **成果展示与分享:** 各组展示其最佳提示词和生成结果。
    - **专家点评与最佳实践总结:** 讲师对各组进行点评，总结该场景下的最佳实践和常见陷阱。

模块五：总结、最佳实践与未来展望

- **5.1 核心要点回顾**
    - LLM 选型关键因素。
    - 企业级应用考量。
    - 高效提示词设计的核心原则（角色、指令、上下文、格式）。
    - 关键提示词技巧（CoT, Few-shot，迭代）。
- **5.2 LLM 使用最佳实践与伦理考量**

    - 建立提示词库与版本控制。
    - 持续监控与评估模型输出质量。
    - 人机协同 (Human-in-the-loop) 的重要性。
    - 负责任的 AI：识别与缓解偏见、保护隐私、透明度、可解释性。
    - **讨论:** 在金融领域推动 LLM 应用时，最重要的伦理原则是什么？
- **5.3 未来趋势与展望**
    - 更强的多模态能力。
    - AI Agents 与自主任务执行。
    - 领域专用模型 (Domain-Specific Models) 的发展。
    - 个性化与自适应学习。
- **5.4 互动问答 (Q&A)**
    - 解答学员疑问，深入探讨特定问题。
- **5.5 培训评估与后续资源**
    - 收集反馈。
    - 提供延伸阅读材料、工具链接、社区资源。