ICS
CCS

T/CASME

团　　体　　标　　准

T/CASME XXX—XXXX

法律智能体设计师能力评价规范

Legal agent designer competence evaluation specification

（征求意见稿）

202X－XX－XX 发布　　202X－XX－XX 实施

中国中小商业企业协会　发 布

目　　次

前　言

本文件按照GB/T 1.1－2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由法天使（北京）科技有限公司提出。

本文件由中国中小商业企业协会归口。

本文件起草单位：法天使（北京）科技有限公司、×××、×××、×××。

本文件主要起草人：×××、×××、×××。

引　　言

随着人工智能（AI）技术，特别是大语言模型（LLM）技术的飞速发展，法律服务行业正经历着从数字化向智能化的深刻转型。在这一过程中，单纯的法律专业人员或单纯的技术开发人员已难以满足行业对“法律AI应用落地”的迫切需求。

技术的应用正在推动法律从业人员能力的分化。市场亟需一种新型复合型专业人才，他们既具备深厚的法律实务功底，又通晓生成式AI的技术原理与边界，能够通过提示词工程、知识库构建和工作流编排，将法律专业知识转化为AI可理解、可执行的“法律智能体”（Legal Agent）。本文件将此类专业人员定义为“法律智能体设计师”（Legal Agent Designer，简称LAD）。

随着LAD需求的增长，建立一套科学、规范的人才评价标准对于行业发展至关重要。为满足企业、法律服务机构和从业者对能力评价的需求，特制定本文件。本文件提供了法律智能体设计师的评价原则和方法，规定了其职业能力要求、评价程序等指导意见。本文件可为企业选用LAD人才提供依据，也可为相关的培训、评价、认证等人才管理工作提供指引。

法律智能体设计师能力评价规范

1 范围

本文件规定了法律智能体设计师（LAD）的术语和定义、能力要素、能力要求、评价方法与程序，以及监督处置机制。

本文件适用于企业、律师事务所、法律科技公司及第三方评价机构对法律智能体设计师进行职业能力评价，也可为相关培训、考核与聘用提供参考。

法律智能体设计师能力考核由中国中小商业企业协会下设管理小组（下称“管理小组”）具体负责。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 1.1-2020 标准化工作导则 第1部分：标准化文件的结构和起草规则

GB/T 41867-2022 信息技术人工智能术语

GB/T 45288.1-2025 人工智能大模型 第1部分：通用要求

SJ/T 11805-2022 人工智能从业人员能力要求

3 术语和定义

下列术语和定义适用于本文件。

3.1 通用术语

3.1.1

人工智能 artificial intelligence; AI

〈学科〉人工智能系统相关机制和应用的研究和开发

[来源:GB/T 41867-2022，3.1.12]。

3.1.2

人工智能系统 artificial intelligence system

针对人类定义的给定目标，产生诸如内容、预测、推荐或决策等输出的一类工程系统。

注1：该工程系统使用人工智能相关的多种技术和方法，开发表征数据、知识、过程等的模型，用于执行任务。

注2：人工智能系统具备不同的自动化级别。

[来源：GB/T 41867-2022，3.1.12]

3.1.3

大语言模型 large language model; LLM

一种利用深度学习在海量数据集上训练的基础模型，能够生成类似人类的文本并执行广泛的自然语言任务。

3.1.4

自然语言处理 natural language processing; NLP

〈系统〉基于自然语言理解和自然语言生成的信息处理。

[来源: GB/T 41867-2022, 3.3.162]

3.2 智能体及其职业相关术语

3.2.1

人工智能体 AI Agent

一种能够感知环境、做出决策并采取行动的智能实体。它可以被看作是一个自主的软件或硬件系统，其目标是在特定的环境中实现某种预定义的目标或任务。

[来源:T/SIA 047-2025, 3.6]

3.2.2

法律智能体

依托大语言模型、法律知识库、业务规则、小模型及工作流编排而构建的、用于执行特定法律任务的可控型AI应用单元。此处可控型AI应用单元的含义比人工智能体的含义更广一些。

3.2.3

法律智能体设计师 Legal Agent Designer (LAD)

具备法律专业知识与实务经验，能够将法律逻辑与AI能力相结合，通过合理的规则、流程与提示词设计，搭建法律智能体，使AI成为可控、可复用的法律助手的复合型法律工作者。

3.3 知识库与数据处理相关术语

3.3.1

语义理解 semantic comprehension

理解数据符号的语义信息,或在具体业务场景下的需求表达,并按照要求输出正确反馈结果的过程。

[来源:GB/T 41867-2022,3.3.12]

3.3.2

语义计算 semantic computing

旨在识别计算内容含义和理解用户意图并以机器可处理的形式表达它们的计算领域。

[来源:GB/T41867-2022,3.3.11]

3.3.3

检索增强生成 Retrieval-Augmented Generation (RAG)

一种通过检索外部知识库获取相关信息，并将其与用户输入合并后提交给大语言模型，以生成更准确、更符合特定领域知识的回答的技术框架。

3.3.4

向量化 vectorization

将文本、图像等非结构化数据转换为数值向量的过程，使得计算机能够理解和处理数据的语义信息。

3.3.5

向量检索 vector search

一种基于向量空间模型的检索技术，通过计算查询向量与数据库中向量的相似度（如余弦相似度），来返回最相关的数据结果。

3.3.6

召回 recall

在信息检索或分类任务中，被正确检索或分类的相关实例数量与数据库中所有相关实例数量的比率。

注：在RAG系统中，通常指检索系统从知识库中成功找到与用户问题相关文档的能力。

3.3.7

数据清洗 data cleaning

系统排查数据集中的错误值、缺失值、不完整与不准确数据、重复内容及无关数据，并加以处理，提升数据质量的过程。

[来源:T/SIA 047-2025, 3.7]

3.4 工作流与交互设计相关术语

3.4.1

提示词工程 Prompt Engineering

向生成式人工智能模型提供输入（文本或图像）以指定和限制模型响应集的学科或过程。

3.4.2

迭代 iteration

针对一批样本，重复地执行系列步骤直至完成训练的过程。

[来源:GB/T 41867-2022, 3.2.5]

3.4.3

思维链 Chain-of-Thought;CoT

一种将复杂任务拆解为多个简单步骤，让大模型逐步进行推理或解释的提示方法 。

3.5 安全与伦理

3.5.1

鲁棒性 robutness

<人工智能>系统在任何情况下都保持其性能水平的特性。

3.5.2

幻觉 hallucination

人工智能系统生成的不仅不准确，而且通常是自信地陈述出的错误信息。

4 要求

LAD能力要素按知识、技能和经验三个维度构成，评价结果为合格或不合格。

4.1 知识体系要求

4.1.1 法律业务与逻辑知识

法律实务基础：具备扎实的部门法理论知识，熟悉合同审查、诉讼策略分析、合规咨询等典型法律业务场景的作业标准。

逻辑结构化能力：能够识别法律文本中的关键要素，并理解法律论证的逻辑，能将非结构化的法律经验转化为结构化的逻辑规则。

4.1.2 AI 与技术通识

a）模型机制与边界认知：

生成机制理解：理解大语言模型（LLM）“基于概率预测下一个Token”的生成本质，知晓模型并不具备人类的主观意识，而是基于统计规律进行文本补全。

能力边界认知：深刻理解模型的幻觉（Hallucination）现象及其成因，了解上下文窗口（Context Window）的长度限制对法律长文本处理的影响，以及温度（Temperature）参数对输出随机性的影响。

b）数据逻辑与交互认知：

数据结构化思维：能够区分非结构化数据（如法律文本、案情描述）与结构化数据（如Excel表格、数据库字段），理解JSON格式在智能体输入输出中的作用。

交互原理理解：理解应用程序编程接口（API）的基本概念，知晓智能体如何通过API与外部系统（如法规库、判例库、企业软件系统）进行数据交换与工具调用。

c）关键技术范式理解：

技术路径区分：理解提示词工程（Prompt Engineering）与检索增强生成（RAG）的区别与适用场景，能在设计时做出正确的技术选型。

向量语义概念：理解向量（Embedding）与向量数据库的基本作用，知晓计算机如何通过计算“语义距离”来实现法律文本的相似度检索，而非传统的关键词匹配。

4.1.3 AI 合规与伦理知识

监管法规：熟悉《生成式人工智能服务管理暂行办法》及国家关于数据安全、个人信息保护的相关法律法规。

风险治理：深刻理解大模型特有的风险，包括幻觉、算法偏见、数据泄露及知识产权侵权风险，并掌握数据脱敏、合规审查等基本的风险治理意识。

4.2 专业技能要求

4.2.1 法律知识工程能力

a）结构化知识整理：具备将自然语言表述的法律文本转化为机器可执行逻辑的能力，并能用markdown语法呈现。能够对非结构化文本进行逻辑解构，精准识别并提取规范构成要件，将其转化为计算机可解析的逻辑规则集合或结构化数据对象，实现法律知识向机器语言的精确映射。

b）基于RAG原理的知识库构建：

数据预处理：能够将非结构化文本转换为计算机可读的结构化格式（如Markdown、JSON），精准保留文档的层级结构（如标题、章节、条款号），为后续的自动化分层与分段奠定基础，确保机器能够理解法律文档的逻辑结构。

语义分段（Chunking）策略：深刻理解检索增强生成（RAG）原理，能够根据法律文本的体裁特点设计适配的分段策略。

索引构建机制：熟练掌握向量检索（Vector Search）、关键词检索（Keyword Search）及混合检索（Hybrid Search）的原理与应用场景。能够根据业务需求选择最优的索引组合方式，在召回率与准确率之间取得平衡。

检索字段优化与匹配具备精细化的检索字段设计能力，能够根据分块内容确定最佳的检索字段。

c）知识库动态维护：建立知识库的更新与版本管理机制，能够根据法律法规的立改废释及时对知识库进行增量更新或版本迭代，确保智能体引用的法律依据真实、有效且具备时效性。

4.2.2 工作流编排与交互设计能力

法律业务流程拆解：能够将复杂的法律业务场景拆解为若干个独立、可执行的子任务，并明确各个子任务之间的逻辑关系。

工作流逻辑编排：能够基于输入数据类型和内容，以及输出的法律效果，设计符合任务场景的工作流。熟练操作可视化流程编排工具或低代码开发平台，通过拖拽组件或编写少量代码，将拆解后的原子任务串联成完整的自动化工作流。

4.2.3 提示词工程（Prompt Engineering）能力

a）理解大模型生成原理：深刻理解大模型的生成机制，懂得如何通过上下文（Context）和约束条件（Constraints）来收窄模型的搜索空间，从而提升输出的准确性。

b）具备分层提示词设计能力：能够区分并设计系统提示词（System Prompt）与用户提示词（User Prompt）。

c）结构化提示词构建：能够设计包含人设、目标、任务要求、约束条件、背景信息、输出格式、输入数据的结构化提示词框架。

d）熟练掌握各类提示词技巧，包括：

零样本提示（Zero-Shot）：直接通过指令引导模型；

单样本提示（One-Shot）：提供一个标准范例供模型模仿；

少样本提示（Few-Shot）：提供多个案例以增强模型的理解；

思维链（CoT）提示：引导模型逐步推理。

4.2.4 代码能力

法律智能体设计师需具备基础的代码理解与应用能力。

a)能够编写并阅读简单脚本，完成字符串处理、文件解析、数据结构操作、异常处理等基础任务；

b）能在工作流中使用代码节点进行数据清洗、参数转换、JSON 结构化输出；

c）理解常见库的基本用法（如re、json、string）；

b）能阅读并修改他人代码以适配业务逻辑。

4.2.5 工具调用能力

平台原生工具运用能力：熟练掌握AI开发平台提供的原生插件与工具组件，能够根据法律业务需求为智能体配置相应的功能模块。

外部接口（API）配置与连接：理解HTTP/HTTPS协议基本原理，能够在低代码平台中配置API的请求方式（GET/POST）、请求头（Header）及鉴权方式（API Key/OAuth），实现与外部数据库的对接。

4.3 职业素养

4.3.1 法律伦理与数据合规（Legal Ethics & Data Compliance）

坚守法律职业底线：严格遵守法律工作者的职业道德，在设计智能体时秉持客观、公正原则，防止算法歧视或误导用户。

数据安全与保密意识：在工作流设计中严格执行“数据最小化”原则，严格保密接触到的法律数据与商业秘密，杜绝因违规使用AI工具导致的数据泄露风险。

4.3.2 持续学习与创新能力

政策法规动态追踪：密切关注人工智能治理政策（如生成式AI管理规定）及相关业务领域法律法规的最新变化，能够及时更新智能体的合规逻辑与知识库内容，确保产品的合法性与时效性。

技术前沿敏感度：保持对大模型技术迭代（如新一代推理模型、多模态能力）的敏锐度，能够及时评估新技术在法律场景落地的可行性与价值。

业务创新思维：不满足于传统法律服务的数字化，能够主动探索AI重构法律业务流程的创新模式。

5 评价方法与程序

5.1 评价方法

LAD能力评价采用“资格审查+理论考试+实务考核”相结合的方式。

a）资格审查（否决项）：申请人需提交普通高等学校法学专业本科及以上毕业证书，或其他符合国家教育行政部门规定的、可予以认定的法学高等教育学历的证明；或提交《中华人民共和国法律职业资格证书》（A类）。不符合基本申报条件者不予评价。

b）理论考试（权重30%）：采用闭卷机考形式，重点考查AI技术通识、提示词工程原理等。

c）实务考核（权重70%）：采用上机操作或方案设计形式。

具体的LAD能力评价要求见附件：《LAD技术考试大纲》。（附件由管理小组负责更新，以最新版本为准）

5.2 评价权重

评价维度	考核内容	权重	合格标准
理论知识	代码能力基础、AI通识基础、RAG原理	30%	单项得分≥60分（总分100分）
实务技能	知识库构建、提示词编写、工作流设计	70%	单项得分≥60分（总分100分）
总计	—	100%	折算总分≥60分

5.3 评价程序

5.3.1 注册申报

申请人登录管理小组的LAD登记管理平台进行注册申报。申请人需上传有效身份证明、学历学位证书（或法律职业资格证书），并签署职业道德承诺书。

5.3.2 形式审查

管理小组对申请人提交的申报材料进行形式审查，重点核验材料的完整性、真实性及是否满足基本的法律专业背景要求。审查通过者获得参加考核资格；材料不全者应在规定时间内补正。

5.3.3 参加考核

审查合格的申请人参加由[指定机构]统一组织的理论知识考试和实务技能考核申请人需在一次评价周期内完成两部分考核。

5.3.4 成绩评定与评审

管理小组对考核试卷与方案进行评分，总成绩达到合格标准（如60分）即视为通过。对于实务考核部分，可视情况组织专家评审委员会进行复核。

5.3.5 证书颁发

经考核合格的申请人，由管理小组统一颁发《法律智能体设计师（LAD）证书》。管理小组应在官方平台公示获得证书的人员名单。

5.3.6 证书有效期与继续教育

LAD证书有效期为两年。鉴于AI技术迭代迅速，持证人员在有效期内，每年应参加累计不少于20学时的继续教育课程，内容涵盖大模型新技术（如多模态、推理模型）及行业最佳实践，以保持能力的有效性。

6 申诉、投诉、监督与处置

6.1 监督

LAD持证人员应接受评价机构及所在行业的监督，严格遵守职业道德与数据合规要求。

6.2 申诉

申请人如对评价结果有异议，可在成绩公布后15日内向评价机构提起书面申诉，并提供相关证明材料。评价机构应建立畅通的申诉渠道并及时反馈处理结果。

6.3 违规处置

有下列情形之一的，评价机构有权视情节轻重给予警告、暂停证书或注销证书的处理，并予以公告：

a) 在评价过程中弄虚作假、舞弊的；
b) 在执业过程中因设计缺陷导致重大法律事故且存在主观过错的；
c) 严重违反职业道德，利用智能体从事违法违规活动的；
d) 未按规定完成继续教育学时的。

附录 A

（资料性）

法律智能体设计师（LAD）技术考试大纲

一、考试目的

评估 LAD 申请人掌握法律智能体设计所必需的技术基础能力，包括 AI 通识理解能力、代码与数据处理能力、提示词工程与规则设计能力、工作流设计、调试与集成能力。

二、考试结构

1.考试方式：理论考试+实操考试
2.计分分布：AI 通识 20%，代码 20%，提示词工程 20%，工作流 40%

三、考试内容大纲

（一）AI通识知识

1.大模型（LLM）工作机制、Transformer 基础原理
2.多模态模型的能力边界（文本、图像、语音、视频）
3.AI 行业“三层结构”：基座模型层/平台系统层/应用层
4.RAG 原理：向量化、相似度检索、召回与重排序
5.小模型（SLM）的定义、能力边界、适用场景
6.智能体输入/输出接口规范、稳定性要求
7.模块化设计理念：松耦合+高内聚
8.AI 数据安全与企业私有化部署场景
9.AI 在法律任务中的典型应用模式
10.幻觉控制与链式推理（CoT）基础机制

（二）代码与数据处理能力

1.字符串基础处理
2.JSON 解析、合并、校验
3.流程图（flowchart/Mermaid）节点与箭头语法
4.API 请求构建（GET/POST、Headers、Auth）
5.对第三方 API 的数据解析/二次封装能力
6.错误处理：缺字段、错误类型、格式错误
7.将 AI 输出二次结构化为标准 JSON
8.编写用于工作流的简易代码（如合并文本、格式校验）

（三）提示词工程与规则设计

1.提示词结构
2.多步骤推理（CoT）与任务拆分
3.审查规则结构化表达：规则表、分值、严重级别

4.RAG场景下的提示词模板
5.提示词的“模块化”构建
6.小模型辅助提示词的编排
7.提示词防幻觉策略
8.输出结构标准化要求
9.提示词调优：参数调整、示例优化
10.典型法律场景提示词

（四）工作流设计

1.根据任务输入和预期输出设计完整工作流
2.根据工作流报错日志修复错误节点
3.正确设置外部接口节点
4.知识库构建：分片策略、索引、embedding配置

参考文献

[1] GB/T 41867-2022 信息技术人工智能术语[S]
[2] GB/T 41867-2022 信息技术人工智能术语
[3] GB/T 45288.1-2025 人工智能大模型 第1部分:通用要求 [S]
[4] SJ/T 11805-2022 人工智能从业人员能力要求