

团 体 标 准

T/ISC XXX—XXXX

可信智能体 智能体应用场景能力要求

Trusted agent capability requirements for intelligent agent application scenarios

（征求意见稿）

2025-09-23

XXXX—XX—XX 发布

XXXX—XX—XX 实施

中 国 互 联 网 协 会 发 布

目 次

前 言	III
可信智能体 智能体应用场景能力要求	1
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
3.1 智能体 ai agent	1
3.2 大模型 large-scale model	1
3.3 强化学习 reinforcement learning	1
3.4 自然语言理解 natural language understanding	2
3.5 自然语言处理 natural language processing	2
3.6 自然语言生成 natural language generation	2
4 符号和缩略语	2
5 能力概述	2
6 模型接管层	3
7 核心能力层	3
7.1 知识接入	3
7.2 任务规划	4
7.3 任务执行	4
7.4 工具插件	4
7.5 记忆能力	4
7.6 学习能力	4
7.7 通信协议（可选）	5
8 认知交互层	5
8.1 对话能力	5
8.2 理解能力	5
8.3 生成能力	5
8.4 推理能力	6
9 应用场景层（可选）	6
9.1 知识智能体	6
9.2 分析智能体	6
9.3 风控智能体	7
9.4 客服智能体	7
9.5 营销智能体（消费侧）	7
9.6 营销智能体（企业侧）	8
9.7 办公智能体	8
9.8 财务智能体	9
9.9 人力智能体	9

9.10 研运智能体	9
10 安全服务层	9
10.1 服务能力	9
10.2 安全能力	10

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。

本文件由中国互联网协会提出并归口。

本文件起草单位：中国信息通信研究院、中移信息技术有限公司、中国移动集团有限公司、天翼云科技有限公司、中国移动通信集团江苏有限公司、中国移动通信集团浙江有限公司、中国第一汽车集团有限公司、中电信数智科技有限公司、中国联合网络通信有限公司软件研究院、中原银行股份有限公司。

本文件主要起草人：刘思颖、崔晨星、罗欧、郭艺娟、古英杰、张迪、谭俊、马景耀、卢辰、蔡丹丹、张晓京、杨德志、郑少斌、张巍、张瑞、李文伟、李睿、杨林、殷娇、王上淇、沈豪、章坚、杨德志、傅成彦、周琪山、余涛、蒋汉卿、魏旭、奚天奇、武沛多、杨经纬、陈利明、邢驰、叶剑、赵新、全飞、冼宜亮、高翔、白阳、刘亚坤。

可信智能体 智能体应用场景能力要求

1 范围

本文件规定了基于可信智能体应用场景能力要求，包括模型接管层、核心能力层、认知交互层、应用场景层、安全服务层等方面内容。

本文件适用于指导企业级用户规划实施并运维运营可信智能体应用使用，以及指导服务提供方设计、研发此类产品，也可作为第三方测评机构评估使用。

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。

- [1] GB/T 41867-2022 信息技术 人工智能 术语
- [2] GB/T 5271.28-2023 信息技术词汇 第28部分：人工智能
- [3] GB/T 45288.1—2025 人工智能 大模型 第1部分：通用要求

3 术语和定义

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

3.1

智能体 ai agent

是一种能够感知其环境并采取行动以影响该环境的实体，具备感知认知、记忆、规划、执行等能力，它可以通过学习、推理等方式来执行任务，表现出一定程度的自主性和智能性。

3.2

大模型 large-scale model

大规模深度学习模型 large-scale deep learning model

基于大量数据训练得到，具有复杂计算架构，能处理复杂任务，且具备一定泛化性的深度学习模型。

注：大模型的参数有其功能和模态决定，一般不低于1亿规模。大模型训练使用的数据总量受参数量的影响，达到收敛的大模型的参数量的对数与其训练数据总量的对数成正比。

[来源：GB/T 45288.1—2025，3.1]

3.3

强化学习 reinforcement learning

一种通过与环境交互，学习最佳行动序列，使回报最大化的机器学习方法。

[来源：GB/T 41867—2022，3.2.25]

3.4

自然语言理解 natural language understanding

通过对功能单元从已传入的功能单元中的自然语言形式的文本或语音中的提取信息，并产生对给定文本或语音及其表示的描述。

[来源：GB/T 5271.28-2023，28.01.18]

3.5

自然语言处理 natural language processing

（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 41867-2022，3.3.16]

3.6

自然语言生成 natural language generation

将带有语义的数据转换为自然语言的任务。

[来源：GB/T 41867-2022，3.3.17]

4 符号和缩略语

下列符号和缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

HTTP：超文本传输协议（Hyper Text Transfer Protocol）

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）

NLG：自然语言生成（Natural Language Generation）

NLP：自然语言处理（Natural Language Processing）

NLU：自然语言理解（Natural Language Understanding）

TS：文本摘要（Text Summarization）

TTS：语音合成（Text To Speech）

5 能力概述

可信智能体应用场景能力要求包括模型接管层、核心能力层、认知交互层、应用场景层、安全服务层等方面，参考架构如图1所示。

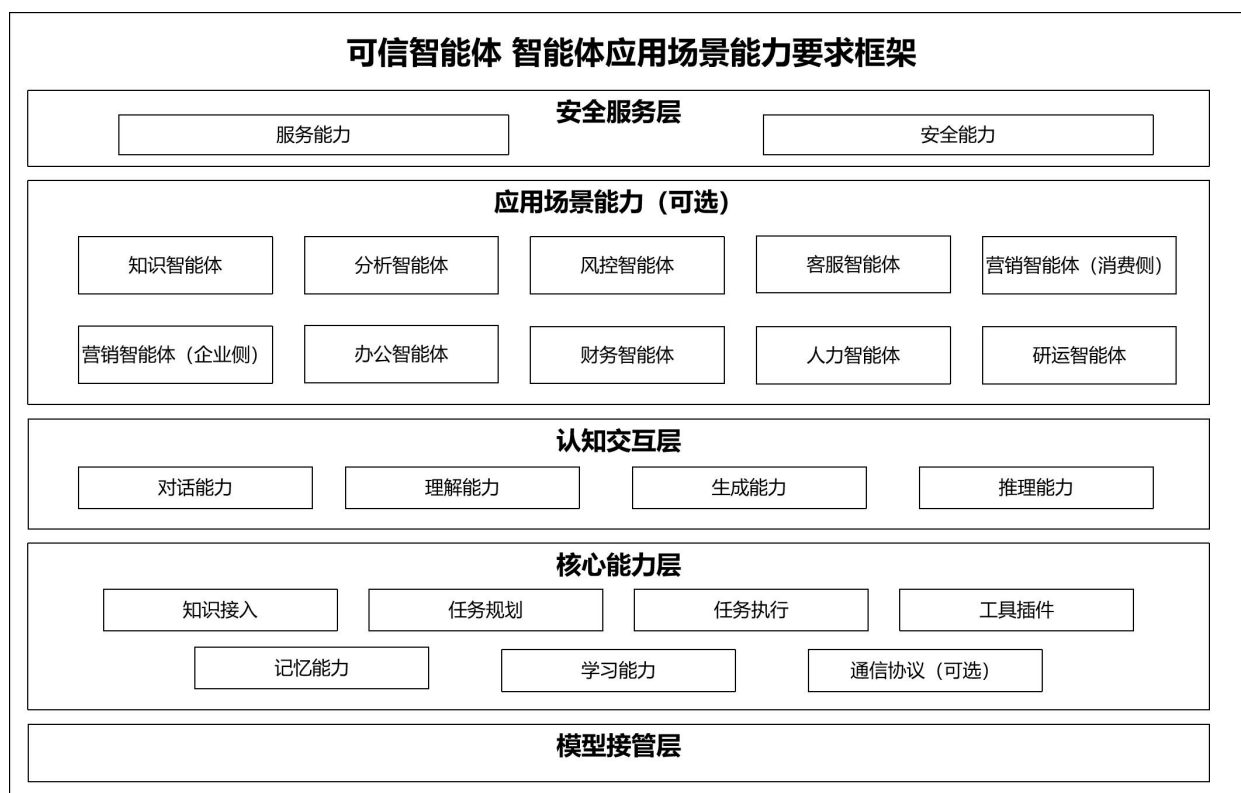


图 1 可信智能体 智能体应用场景能力要求框架

6 模型接管层

- 应支持主流大模型的接入，允许用户通过配置文件或管理界面完成模型选择、版本切换及超参数调整；
- 应支持基于应用场景的智能模型路由策略，结合环境感知数据、输入数据和模型能力等信息，动态选择最合适的模型；
- 宜支持选择模型具备Function Calling（工具调用）等能力；

7 核心能力层

7.1 知识接入

- 应支持结构化与非结构化知识源的统一接入，兼容数据库（SQL/NoSQL）、知识图谱（RDF/OWL）、文档库（WORD/PDF/HTML/Markdown/...）、API服务等多数据源；
- 宜支持知识库管理功能，包括不限于知识的自动整理、更新、搜索、删除、版本管理等；
- 宜具备知识分类标签体系，能够根据预设的标签，对接入的各类知识进行自动识别和归类识别；
- 宜支持引入知识图谱技术，将碎片化实体-关系自动抽取、融合，生成可视化知识网络，能够全面呈现知识关联图谱，帮助用户系统地掌握相关知识体系；
- 宜提供知识向量化服务，应通过嵌入模型将多模态知识映射至统一语义向量空间，并兼容主流向量数据库；
- 宜提供混合检索服务，支持语义检索、关键词检索、规则检索等服务，支持多角度、多层级的检索召回；

7.2 任务规划

- a) 应具备任务理解能力，支持对用户输入的任务目标的理解能力，包括对任务意图、关键信息的准确识别；
- b) 应具备任务分解能力，支持将复杂任务分解为多个子任务的能力，确保每个子任务具有明确的执行步骤和目标；
- c) 应具备路径规划能力，支持将复杂任务按最优路径拆解为原子操作序列，路径算法参数可配置；
- d) 宜具备动态调整能力，支持根据实时数据和业务变化动态调整任务规划的能力，确保任务执行的灵活性和适应性；
- e) 宜具备任务优先级评估能力，支持根据任务紧急程度、重要性等因素评估任务优先级的能力；

7.3 任务执行

- a) 应具备具执行能力，能够根据决策自动启动和执行任务，无需人工干预，支持多种任务类型，包括但不限于数据处理、文件操作、系统操作、网络请求等；
- b) 应具备人机协作能力，支持任务进行的人工干预，包括且不限于补充任务数据、修改任务内容、打断任务进程等；
- c) 宜具备跨系统协同能力，支持与其他系统或智能体的协同工，具备异构API接口动态适配能力，支持常规数据结构和传输协议
- d) 宜具备状态监控能力，支持可视化实时展示任务进度、任务状态、资源占用及异常告警情况等；

7.4 工具插件

- a) 应支持AI工具相关能力，支持智能体快速调用，包括不限于NLP（自然语言处理）、ASR（语音识别）、TTS（文本到语音）、图像识别、数据处理、图表生成、文生图、图片编辑、图片文字提取等主流常用工具组件等；
- b) 应支持用户对插件进行配置和定义，包括增加新插件、删除现有插件以及展示插件的详细信息，用户可以根据智能体的需求，为当前智能体添加所需的插件以增强其功能；
- c) 宜支持工具扩展，包括且不限于搜索引擎、数据库操作、自定义工具封装等；
- d) 宜具备工具测试功能，对用户添加配置的工具进行在线测试；

7.5 记忆能力

- a) 应支持对历史交互记录的存储和检索功能，能够根据用户需求快速定位并调用过往对话中的关键信息；
- b) 应支持对情景信息的理解、记忆、查找能力，情景信息指智能体可感知的信息，包括系统信息、用户画像、外部环境信息等；
- c) 应支持按短期记忆（最近10轮对话）、及长期记忆（用户画像、偏好存储）分别加密存储，且支持用户自主删除；
- d) 应支持设置记忆有效期，自动清理过期对话痕迹，避免信息冗余和过时；
- e) 宜支持记忆总结和提炼，实现对不同用户更加个性化的对话风格和内容；

7.6 学习能力

- a) 应支持能够基于积累的用户交互数据、任务执行数据等，通过机器学习算法（如监督学习、无监督学习、强化学习等）进行模型训练和优化，不断提升自然语言理解、任务执行等能力；

- b) 应支持用户反馈机制，能够根据用户对任务执行结果的评价（如满意、不满意、改进建议等），对自身行为和策略进行调整和优化；

7.7 通信协议（可选）

- a) 宜兼容MCP（Model Context Protocol）协议，能够与遵循该协议的MCP服务器进行无缝通信；
- b) 宜兼容ANP（Agent Network Protocol）协议，能够与遵循该协议的智能体进行无缝通信，确保智能体之间安全、高效且灵活地协作与交互；
- c) 宜兼容A2A协议（Agent-to-Agent）协议，能够与遵循该协议的其他智能体进行无缝通信；

8 认知交互层

8.1 对话能力

- a) 应支持多种对话类型，并支持各形态对话的无缝切换，包括不限于任务式对话、问答式对话及工具调用对话；
- b) 应支持智能问答引擎，采用先进的自然语言处理技术，并依托海量知识库，能够精准理解用户以自然语言形式提出的各类问题，涵盖专业领域技术咨询、学术研究资料查询等各类场景，且能迅速输出准确、简洁、易懂的答案；
- c) 应支持单轮对话、多轮对话能力，多轮对话场景中需能够留存过往交互内容，基于历史信息引导对话持续深入推进，避免出现逻辑断层，进而提升整体交互体验；
- d) 宜支持会话状态持久化，实现跨设备上下文同步（如保留近30天记录），并具备对话摘要自动生成能力，便于用户快速回顾关键信息；
- e) 宜上下文感知的问题推荐功能，能够基于当前问题或历史交互记录，自动生成多个候选扩展问题，引导用户深入探索；
- f) 宜支持意图澄清机制，当检测到用户意图存在歧义、信息不完整或表述模糊时，应主动启动多轮对话，通过结构化提问逐步明确用户需求；

8.2 理解能力

- a) 应支持准确理解自然语言输入的意图和内容，具备包括语义理解、语法分析、意图识别等核心能力，同时需能够适配复杂对话场景，并支持领域特定语言的解析；
- b) 应支持在多轮对话中对上下文信息的理解和利用能力，在问答交互过程中支持多轮连续交互，能够依据上下文语境智能推理，持续生成连贯且针对性强的回应，以实现类人际间深度对话效果；

8.3 生成能力

- a) 应支持文本生成能力，依据上下文主题、风格与字数约束等条件，生成输出符合场景需求的文本内容；
- b) 宜支持代码生成能力，依据代码插件工具，可根据规划任务要求自动编写、调试并执行代码，完成执行类任务；
- c) 宜支持图像生成能力，通过提示词驱动多模态模型，生成输出指定分辨率、风格与元素的合规图像；
- d) 宜支持音视频生成能力，基于提示词与脚本模板，实时合成高清音视频，支持语音克隆、字幕同步等；

8.4 推理能力

- a) 应支持基于知识推理，具备利用预定义的知识库（如事实、规则、概念）进行推理能力，结合用户的意图进行推理，以生成兼顾用户预期和知识库参考内容的回复，以降低内容幻觉风险；
- b) 应支持基于对话推理，具备根据上下文信息进行推理能力，通过对交互过程中产生的语境信息分析，更精准理解用户意图并提供适配的回应；
- c) 应支持基于数学逻辑计算推理，具备通过数学逻辑（如代数、几何、概率论）进行推理能力，以解决数学问题或验证逻辑命题；
- d) 宜支持基于因果推理，通过分析因果关系进行推理，以预测事件的结果或推断事件的原因能力；
- e) 宜支持基于深度推理，通过多步推理和复杂逻辑分析，解决复杂问题或理解复杂概念能力；

9 应用场景层（可选）

9.1 知识智能体

- a) 应具备知识语义检索能力，支持对用户输入的自然语言查询（如关键词、问句、长文本描述）进行深层语义解析，提取核心意图、实体、情感等信息，支持将查询与知识库文档转换为向量，通过计算向量相似度（如余弦相似度）实现跨句式、跨表述的语义匹配，支持知识卡片、知识结构化和知识溯源的检索结果输出；
- b) 应具备知识图谱检索能力，支持基于实体关系网络的结构化检索方式，通过挖掘实体、属性及关系间的语义关联，利用知识图谱的“实体 - 关系 - 属性”三元组结构，实现多维度、可推理的智能检索；
- c) 应具备知识问答与推荐能力，支持基于对用户输入进行深度语义解析与检索，生成内容清晰逻辑合理的知识回复，所生成内容均基于知识库中明确的知识来源生成且标明引用出处，支持面向用户的个性化知识推荐能力，能够结合用户的行为、兴趣、意图及业务上下文动态调整推荐内容，优先推荐权威来源、最新内容、用户常用领域等；
- d) 宜具备知识混合检索能力，支持根据查询特征（如实体、关系、结构化需求）自动选择或组合检索方式，融合文本语义检索、知识图谱检索和结构化数据检索，动态策略适配，实现多维度知识联动召回，支持多维度意图识别，精准判断检索目标，将查询拆解为子任务，分发至对应模块，实现智能检索路由；
- e) 宜具备多模态知识检索能力，支持自动对多模态知识库内容进行特征提取与索引，将检索到的文本、图片、音视频信息转换为模型可理解的格式，辅助生成多模态回答，支持文本、图片、音频、视频等多种模态知识协同检索的技术，将不同模态的信息转换为统一文本语义空间的向量或特征，实现“以文搜图、以图搜文、多模态联合召回”等跨模态检索能力；

9.2 分析智能体

- a) 应具备数据查询能力，支持自然语言问答交互方式提供业务数据查询、常见业务指标计算、数据异常检测等服务；
- b) 应具备数据分析能力，针对多维度数据进行统计分析，能够快速解读数据特征和分布，智能生成可视化图表（如折线图、饼图、漏斗图），支持交互式上卷下钻分析；
- c) 宜支持波动归因能力，能够对业务关键指标进行计算，获取历史变化趋势，结合知识库、外部数据等信息，关联业务事件（如促销活动、系统故障），针对指标波动原因进行拆解分析，实现业务洞察；

- d) 应具备数据决策，支持根据业务场景需求（如经营分析、运营复盘），对业务关键指标进行趋势预测，智能生成决策建议，结合报告模板，可进一步生成数据分析报告，支持多格式文档导出和链接形式分享；

9.3 风控智能体

- a) 应具备合规审查能力，构通过构建行内外合规知识库，借助大模型对营销宣传、公示公告、制度协议等内容（word、excel、pdf、图片、视频）进行智能审核，识别出潜在的不合规项，并提供法规依据及整改建议，降低合规风险；
- b) 应具备内部操作审计能力，实时解析员工操作日志、权限变更、敏感数据访问等行为，识别越权、异常批量操作等内部威胁，生成可追溯的审计报告；
- c) 应具备合规风险预测能力，基于历史处罚案例、监管动态、业务变更等数据，构建合规风险预测模型，可提前天输出潜在违规场景及概率，支持管理层前置整改；
- d) 应具备交易风险实时监测能力，实时采集交易流水、账户行为、地理位置等多维数据，利用大模型异常检测算法对欺诈、洗钱、套现等高风险交易进行毫秒级预警，并输出风险等级与处置建议；
- e) 应具备舆情分析能力，借助大模型对内外部数据进行深度分析与抓取，识别企业相关的舆情信息，有效识别正面、负面的舆论趋势，帮助企业及时掌握舆情动态；

9.4 客服智能体

- a) 应具备多渠道接入与同步能力，支持多渠道接入（包括不限于企业微信、网页聊天窗口、电话IVR等），实现对话内容的跨渠道状态同步；
- b) 应具备客服咨询响应能力，支持基于自然语言理解与自然语言生成能力，实现对用户咨询的实时解析与响应，支持答案来源标注，标注内容可包括知识库文档、外部服务接口等，支持多轮对话上下文跟踪能力，可主动引导客户补充信息，以精准理解客户需求；
- c) 应具备情感识别与交互能力，支持语音与文本双向情感分析（如语调强度、关键词频率等），能够自动识别客户情绪，基于问题分类生成结构化安抚话术库，并智能匹配解决方案（如自动退款、补发流程等）；
- d) 应具备智能工单处理能力，支持从对话中自动提取工单关键信息，包括客户ID、问题类型、紧急程度等信息，支持智能分辨处理部门并完成工单分派，同时生成全链路审计日志以供追溯；
- e) 应具备智能质检能力，支持语音/文字质检多维度指标分析（如关键词出现频率、对话完整性等），并提供可视化分析及问题归因（如关联系统监控指标等），支持语音与文本双向交互的服务评价，并生成智能化反馈；
- f) 应具备智能外呼能力，支持按预设时间、频次及规则自动发起外呼，无需人工干预，支持语音识别和语音合成能力，能够与客户进行自然流畅的语音交流，支持基于客户历史行为及数据模型预测潜在需求，动态优化外呼策略，提升接通与转化成功率；

9.5 营销智能体（消费侧）

- a) 应具备智能客户洞察能力，持整合多源数据（如CRM系统数据、社交媒体交互数据等）构建360度用户画像，具备用户群体动态聚类分析能力，可基于画像特征划分用户群体并映射关联标签；
- b) 应具备智能精准营销能力，支持通过多维度分析（如协同过滤算法、用户偏好预测模型等）生成产品或服务推荐结果，支持官网内容智能推荐及展示优先级排序，匹配用户潜在需求，支持根据产品核心亮点及用户画像自动生成营销话术，包括场景化方案介绍、产品价值说明等内容，支持按客户画像关联权重确定推送优先级并完成分发；

- c) 宜具备AI外呼与自动化触达能力，支持通过语音通话、短信等方式实现批量外呼，并自动识别客户意图（如是否接受报价、是否有意向进一步沟通等核心意图），支持外呼数据全量记录（如接通率、商机转化率、各话术使用频率等），并能生成可视化外呼效果分析报告；
- d) 宜具备营销效果追踪能力，支持营销活动全流程效果分析，可统计点击率(CTR)、转化率(CVR)、潜在客户转化漏斗等核心指标并生成数据看板，支持通过 A/B 测试对比不同营销策略（如话术版本、推荐组合、触达时机等）的实时效果差异，基于分析结果生成决策建议报告；
- e) 宜具备智能营销培训能力，支持对客户经理进行260度维度评价，评价维度应涵盖业绩数据、擅长产品领域、优势营销场景等，支持模拟真实客户行为及对话逻辑，为营销人员提供话术表达、业务流程处理等场景的演练环境，支持对客户经理的回复内容进行评估，评估维度包括但不限于合规性、信息准确性及表达流畅度等；

9.6 营销智能体（企业侧）

- a) 应具备行业趋势研判能力，支持自动化采集行业相关数据，涵盖市场动态、研报、专利及招投标信息等，构建多维度数据分析体系，支持基于大模型构建行业景气度评估模型，综合政策导向、市场份额变化、价格走势等相关指标，生成行业景气指数曲线图、周期波动预测表等，辅助客户快速判断行业所处周期阶段及未来趋势；
- b) 应具备企业侧智能客户洞察能力，支持对客户相关数据进行分析，包括但不限于客户基本信息、采购数据、账务数据、中标数据等，从而实现客户分级分类差异化运营，识别潜在拓客机会，支持监控企业客户健康度与生态结构，实现客户价值分层管理，并具备客户风险预警能力；
- c) 应具备智能营销商机推荐能力，支持通过大模型对业务场景进行深入分析，精准提供个性化和场景化的线索及商机建议，包括但不限于历史相似商机推荐、上下游关系商机推荐等；
- d) 宜具备智能营销策略生成能力，支持营销意图识别与分析，基于大模型输入需求（如背景、客户画像等）识别问题与诉求，支持智能生成逻辑清晰的营销方案，方案包含不限于公司介绍、行业分析、解决方案及案例等内容；
- e) 宜具备智能标书与合同能力，支持自动解析招投标文件，自动生成商务、技术和报价部分，并可基于招标文件要求对投标文件进行智能检查，自动检测并提示内容完整性、准确性和合规性方面的问题，支持合同内容生成与草拟，同时可对合同内容进行智能审核与风险识别；

9.7 办公智能体

- a) 应具备会议安排能力，自动协调参会者空闲时间，自动通知会议参与方，自动生成会议纪要并生成后续工作任务至第三方平台（OA系统、邮件等）；
- b) 应具备邮件处理能力，自动分类邮件（如重要、垃圾、待处理），提取关键信息（如截止日期、任务描述），智能回复建议（基于模板和上下文生成草稿），智能生成代办任务并提交到工作通知列表中；
- c) 应具备文档管理能力，提供多种文档模板，支持用户根据需求快速自动生成标准化文档，如报告、合同、会议纪要等，同时能够根据文档内容自动生成摘要，提取关键信息，帮助用户快速了解文档核心内容，并支持文档内容检索（支持关键词、语义搜索）；
- d) 应具备员工问答助手能力，通过企业级知识库，为企业员工提供公司制度、业务流程、合规要求、技术支持等方面的解答；

9.8 财务智能体

- a) 应具备智能差旅报销能力，支持端到端差旅闭环管理，包括不限于一键发起申请、智能差旅校验、自动比价订票、差旅途中OCR票据实时归集、自动生成报销单、自动入账、差旅成本可视化分析；
- b) 应具备智能发票识别能力，支持多票种、多版式OCR包括不限于增值税专/普票、电子普票、火车票、出租车票、定额发票等，自动提取票面全字段，调用税务接口完成验真、查重、价税分离，异常票实时预警；
- c) 宜具备财报分析能力，可根据总账数据一键生成资产负债表、利润表、现金流量表及附注等财务报表，并支持多维度钻取，实时扫描应收逾期、费用超标、税负异常等，输出风险等级、影响金额与处置建议；
- d) 宜具备资金预测能力，基于历史现金流、合同收付款计划、预算执行进度，滚动预测未来周资金缺口与盈余，自动生成融资或理财建议；
- e) 宜具备税务管理能力，一键算税、自动申报、税负对标、优惠政策推送及留抵退税模拟测算，确保合规与税负最优；

9.9 人力智能体

- a) 应具备智能简历筛选能力：支持多格式简历批量解析，基于NLP技术提取简历关键信息（教育背景、工作经历），简历画像与岗位画像自动匹配；
- b) 应具备智能面试安排能力：支持自动排期、跨时区协调、多面试官同步调面试官与候选人时间，利用多模态能力，自动整理面试反馈，并自动汇总面试结果（如评分表、录用建议）；
- c) 宜具备员工培训能力：支持基于岗位画像与绩效数据生成个性化学习路径，提供情景化AI训战、实时考核与效果追踪；
- d) 宜具备组织洞察能力：支持实时人才盘点、继任梯队分析、离职预测模型，输出可视化人力仪表盘；

9.10 研运智能体

- a) 应具备故障诊断能力，通过日志聚类分析，识别异常模式，依赖故障知识图谱构建故障传播路径，定位异常根因，基于故障知识库或运维大模型匹配历史解决方案，并自动化执行预设修复脚本（也可以进一步采用代码模型自动生成故障解决脚本并执行）；
- b) 应具备环境变更能力，系统变更智能预检查；自动化测试上线流程，智能兼容性验证；SQL稽核，进行静态SQL分析和动态风险评估；自动化制定巡检策略，进行覆盖基础设施、应用服务的统一巡检；
- c) 应具备代码辅助能力，根据自然语言描述生成函数级代码，支持Python、Java、SQL等语言；
- d) 宜具备代码审查能力：静态分析检测代码潜在缺陷（如空指针、资源泄漏），动态进行安全漏洞扫描（如SQL注入、XSS）；
- e) 宜具备系统性能优化能力，支持通过APM（应用性能监控）数据自动生成性能分析报告，提供智能调参建议；

10 安全服务层

10.1 服务能力

- a) 应支持将智能体能力以API、SDK等形式对外发布；

- b) 应支持将智能体以浏览器插件形式对外发布；
- c) 应支持将智能体以URL（网络链接）的方式对外发布；
- d) 宜支持发布到第三方平台，如微信、抖音、飞书等开放平台；

10.2 安全能力

- a) 应支持基于角色的访问控制（RBAC），通过定义不同的用户角色并分配相应的权限级别；
 - b) 应支持根据业务需求的变化实时调整用户的权限设置，保证权限管理的灵活性和适应性；
 - c) 应采用加密算法对存储和传输中的数据进行加密处理，保护数据免受未经授权的访问或泄露
 - d) 应支持定期执行数据备份操作，并制定完善的数据恢复计划；
 - e) 应支持确保个人信息（PII）和其他敏感数据在收集、处理、存储和共享过程中的安全性，遵守相关的法律法规要求；
 - f) 应支持定期对应用程序进行安全漏洞扫描，并及时修补发现的安全缺陷，防止潜在的安全威胁利用这些漏洞进行攻击；
 - g) 应支持安全审计追踪能力，包括不限于所有智能体调用记录、配置变更、权限调整等关键操作，应记录完整的安全操作日志（包括权限变更、数据访问记录、工具调用记录、配置变更），日志保留周期需符合GDPR等法规要求（至少6个月）；
 - h) 应支持内容安全能力，包括不限于多级内容审核机制、权威知识验证技术、全维度伦理审查体系等。
-