生成式人工智能系统应用员

国家职业标准

（征求意见稿）

1. 职业概况

1.1 职业名称

生成式人工智能系统应用员

1.2 职业编码

4-04-05-13

1.3 职业定义

运用生成式人工智能技术及工具，从事生成式人工智能系统设计、调用、训练、优化、维护管理等工作的人员。

1.4 职业技能等级

本职业共设五个等级，分别为：五级/初级工、四级/中级工、三级/高级工、二级/技师、一级/高级技师。

1.5 职业环境条件

室内，常温。

1.6 职业能力特征

智力正常，具有一定的表达能力、计算能力、沟通能力、空间感，知觉、色觉、听觉正常，动作协调。

1.7 普通受教育程度

高中毕业（或同等学力）。

1.8 职业培训要求

1.8.1 培训参考时长

五级/初级工不少于80标准学时；四级/中级工不少于80标准学时；三级/高级工不少于64标准学时；二级/技师不少于64标准学时；一级/高级技师不少于64标准学时。

1.8.2 培训教师

培训五级/初级工、四级/中级工的教师应具有本职业三级/高级工及以上职业资格(职业技能等级)证书或相关专业中级及以上专业技术职务任职资格；

培训三级/高级工的教师应具有本职业二级/技师及以上职业资格(职业技能等级)证书或相关专业中级及以上专业技术职务任职资格；

培训二级/技师的教师应具有本职业一级/高级技师职业资格(职业技能等级)证书或相关专业高级专业技术职务任职资格；

培训一级/高级技师的教师应具有本职业一级/高级技师职业资格(职业技能等级)证书 2 年（含）以上或相关专业高级专业技术职务任职资格 2 年（含）以上。

1.8.3 培训场所设备

理论知识培训在标准教室或线上平台进行；操作技能培训根据工作要求，在具有支撑生成式人工智能系统应用的相应软、硬件的培训场所进行。

1.9 职业技能评价要求

1.9.1 申报条件

1.具备以下条件之一者，可申报五级/初级工：

(1)年满 16 周岁，拟从事本职业或相关职业[1]工作。

(2)年满 16 周岁，从事本职业或相关职业工作。

2.具备以下条件之一者，可申报四级/中级工：

(1)累计从事本职业或相关职业工作满 5 年。

(2)取得本职业或相关职业五级/初级工职业资格(职业技能等级)证书后，累计从事本职业或相关职业工作满 3 年。

(3)取得本专业或相关专业[2]的技工院校或中等及以上职业院校、专科及以上

---

1 相关职业：人工智能工程技术人员、计算机软件工程技术人员、计算机网络工程技术人员、信息系统分析工程技术人员、嵌入式系统设计工程技术人员、大数据工程技术人员、自动控制工程技术人员、计算机程序设计员、计算机软件测试员、数据库运行管理员、人工智能训练师、数字孪生应用技术员、虚拟现实产品设计师等，下同。

2 相关专业：计算机辅助设计与制造、机电一体化技术、智能制造技术应用、数字孪生技术应用、工业互联网与大数据应用、计算机网络应用、计算机程序设计、计算机应用与维修、计算机信息管理、计算机游戏制作、计算机动画制作、计算机广告制作、多媒体制作、云计算技术应用、工业互联网技术应用、虚拟现实技术应用、人工智能技术应用、数字媒体技术应用、区块链技术应用、工业设计、平面设计、电子信息技术、服务机器人装配与维护、计算机应用、计算机网络技术、软件与信息服务、数字媒体技术应用、大数据技术应用、移动应用技术与服务、网络信息安全、网站建设与管理、计算机平面设计、人工智

普通高等学校毕业证书(含在读应届毕业生)。

3.具备以下条件之一者，可申报三级/高级工：

(1)累计从事本职业或相关职业工作满10年。

(2)取得本职业或相关职业四级/中级工职业资格(职业技能等级)证书后，累计从事本职业或相关职业工作满4年。

(3)取得符合专业对应关系的初级职称(专业技术人员职业资格)后，累计从事本职业或相关职业工作满1年。

(4)取得本专业或相关专业的技工院校高级工及以上毕业证书(含在读应届毕业生)。

(5)取得本职业或相关职业四级/中级工职业资格(职业技能等级)证书，并取得高等职业学校、专科及以上普通高等学校本专业或相关专业毕业证书(含在读应届毕业生)。

(6)取得经评估论证的高等职业学校、专科及以上普通高等学校本专业或相关专业的毕业证书(含在读应届毕业生)。

4.具备以下条件之一者，可申报二级/技师：

(1)取得本职业或相关职业三级/高级工职业资格(职业技能等级)证书后，累计从事本职业或相关职业工作满5年。

能技术与应用、虚拟现实技术与应用、数字化设计与制造技术、智能制造装备技术、机电一体化技术、智能机电技术、智能控制技术、智能机器人技术、工业互联网应用、电子信息工程技术、应用电子技术、移动互联网应用技术、汽车智能技术、智能产品开发与应用、计算机应用技术、计算机网络技术、软件技术、数字媒体技术、大数据技术、云计算技术应用、信息安全技术应用、虚拟现实技术应用、人工智能技术应用、嵌入式技术应用、工业互联网技术、区块链技术应用、移动应用开发、工业软件开发技术、动漫制作技术、密码技术应用、人工智能数据工程技术、通信软件技术、智能互联网络技术、网络规划与优化技术、机械设计制造及自动化、智能制造工程技术、数控技术、装备智能化技术、机械电子工程技术、电气工程及自动化、智能控制技术、机器人技术、自动化技术与应用、现代测控工程技术、工业互联网工程、电子信息工程技术、计算机应用工程、网络工程技术、软件工程技术、数字媒体技术、大数据工程技术、云计算技术、信息安全与管理、虚拟现实技术、人工智能工程技术、嵌入式技术、工业互联网技术、区块链技术、集成电路工程技术、机械设计制造及其自动化、机械电子工程、智能制造工程、智能交互设计、电气工程及其自动化、电气工程与智能控制、信息工程、人工智能、智能测控工程、智能视听工程、智能视觉工程、自动化、机器人工程、计算机科学与技术、软件工程、网络工程、信息安全、物联网工程、数字媒体技术、智能科学与技术、空间信息与数字技术、电子与计算机工程、数据科学与大数据技术、网络空间安全、新媒体技术、电影制作、保密技术、服务科学与工程、虚拟现实技术、区块链工程、密码科学与技术、工业软件、未来机器人、交叉工程、信息管理与信息系统、大数据管理与应用、数字媒体艺术、新媒体艺术、机械工程、电气工程、电子科学与技术、信息与通信工程、控制科学与工程、计算机科学与技术、软件工程、网络空间安全、电子信息、智能科学与技术等，下同。

(2)取得符合专业对应关系的初级职称(专业技术人员职业资格)后，累计从事本职业或相关职业工作满5年，并在取得本职业或相关职业三级/高级工职业资格(职业技能等级)证书后，从事本职业或相关职业工作满1年。

(3)取得符合专业对应关系的中级职称(专业技术人员职业资格)后，累计从事本职业或相关职业工作满1年。

(4)取得本职业或相关职业三级/高级工职业资格(职业技能等级)证书的高级技工学校、技师学院毕业生，累计从事本职业或相关职业工作满2年。

(5)取得本职业或相关职业三级/高级工职业资格(职业技能等级)证书满2年的技师学院预备技师班、技师班学生。

5.具备以下条件之一者，可申报一级/高级技师：

(1)取得本职业或相关职业二级/技师职业资格(职业技能等级)证书后，累计从事本职业或相关职业工作满5年。

(2)取得符合专业对应关系的中级职称后，累计从事本职业或相关职业工作满5年，并在取得本职业或相关职业二级/技师职业资格(职业技能等级)证书后，从事本职业或相关职业工作满1年。

(3)取得符合专业对应关系的高级职称(专业技术人员职业资格)后，累计从事本职业或相关职业工作满1年。

1.9.2 评价方式

分为理论知识考试、操作技能考核以及综合评审。理论知识考试以笔试、机考等方式为主，主要考核从业人员从事本职业应掌握的基本要求和相关知识要求；操作技能考核主要采用现场操作、模拟操作等方式进行，主要考核从业人员从事本职业应具备的技能水平；综合评审主要针对二级/技师和一级/高级技师，通常采取审阅申报材料、答辩等方式进行全面评议和审查。

理论知识考试、操作技能考核和综合评审均实行百分制，成绩皆达60分(含)以上者为合格。

1.9.3 监考人员、考评人员与考生配比

理论知识考试中的监考人员与考生配比不低于1∶15，且每个考场不少于2名监考人员；操作技能考核中的考评人员与考生配比1∶10，且考评人员为3人（含）以上单数；综合评审委员为3人（含）以上单数。

1.9.4 评价时长

理论知识考试时间不少于60分钟，操作技能考核时间不少于60分钟。综合

评审时间不少于30分钟。

1.9.5 评价场所设备

理论知识考试在标准教室进行，操作技能考核根据工作要求，在具有支撑生成式人工智能系统应用的相应软、硬件的评价场所进行；综合评审在标准教室或会议室进行。

征求意见稿

第一部分

（本节内容涉及生成式人工智能系统应用员职业，不包含生成式人工智能系统测试员。）

2. 基本要求

2.1 职业道德

2.1.1 职业道德基本知识

2.1.2 职业守则

（1）诚实守信，保守秘密。

（2）遵纪守法，严守伦理。

（3）尊重原创，客观公正。

（4）爱岗敬业，服务大众。

（5）团结协作，勇于创新。

（6）持续学习，追求卓越。

2.2 基础知识

2.2.1 专业基础知识

（1）计算机操作知识。

（2）编程基础知识。

（3）人工智能基础知识。

（4）常用办公软件操作知识。

2.2.2 工程实践相关知识

（1）文档规范、代码规范、质量保障规范相关知识。

（2）项目管理、资料管理、计算机设备管理相关知识。

（3）知识产权相关知识。

2.2.3 业务实践相关知识

（1）人工智能行业及产品知识

（2）人工智能产业应用相关知识

（3）人工智能发展现状与趋势相关知识

（4）生成式人工智能技术和产品相关知识

2.2.3 人工智能伦理及安全知识

（1）人工智能安全与隐私保护相关知识。

（2）人工智能道德伦理相关原则及标准相关知识。

（3）生成式人工智能服务安全、内容标识办法相关知识。

2.2.2 相关法律、法规知识

（1）《中华人民共和国民法典》相关知识。

（2）《中华人民共和国劳动法》相关知识。

（3）《中华人民共和国劳动合同法》相关知识。

（4）《中华人民共和国网络安全法》相关知识。

（5）《中华人民共和国著作权法》相关知识。

（6）《中华人民共和国数据安全法》相关知识。

（7）《中华人民共和国个人信息保护法》相关知识。

（8）《中华人民共和国保守国家秘密法》相关知识。

（9）《互联网信息服务算法推荐管理规定》相关知识。

（10）《互联网信息服务深度合成管理规定》相关知识。

（11）《生成式人工智能服务管理暂行办法》相关知识。

（12）《人工智能生成合成内容标识办法》相关知识。

（13）《数据出境安全评估办法》相关知识。

3. 工作要求

本标准对五级/初级工、四级/中级工、三级/高级工、二级/技师、一级/高级技师的技能要求和相关知识要求依次递进，高级别涵盖低级别的要求。

3.1 五级/初级工

职业功能	工作内容	技能要求	相关知识要求
1.内容生成与模型应用	1.1 生成文本	1.1.1 能按照固定模板的格式和内容要求，生成对应的文本 1.1.2 能根据需求填充模板，生成符合要求的文本 1.1.3 能检查生成文本的准确性和完整性，修正明显错误 1.1.4 能检查生成文本的合规性，识别并修正违规信息，核验人工智能生成标识	1.1.1 文本的格式规范 1.1.2 文本模板的结构组成 1.1.3 文本内容准确性校验的方法 1.1.4 内容安全审核的基本标准、人工智能生成内容标识规范
	1.2 生成图像	1.2.1 能使用术语描述单一物体形状、颜色等视觉特征 1.2.2 能使用图像生成工具，根据描述生成对应的图像 1.2.3 能对生成的图像进行尺寸调整、裁剪、格式转换、图像旋转 1.2.4 能检查生成图像的合规性，识别并修正违规内容，核验人工智能生成标识	1.2.1 图像属性和格式知识 1.2.2 单一物体和简单场景的描述方法和要求 1.2.3 图像生成工具的操作方法 1.2.4 人工智能生成图像的合规识别标准
	1.3 生成音频	1.3.1 能将文本、语音等内容输入音频合成工具，生成文本、语音对应的音频 1.3.2 能调整语音合成作品的语速、音量等基础参数 1.3.3 能生成符合场景需求的音效	1.3.1 音频文件的属性及参数 1.3.2 语音合成中语速、音量、语调的调节范围及效果 1.3.3 音效与应用场景的匹配原则

		1.3.4 能检查生成音频的合规性，识别并修正违规内容，核验人工智能生成标识	1.3.4 生成式人工智能作品标识要求
	1.4 生成视频	1.4.1 能使用人工智能视频生成工具，选择固定画面模板，生成符合规格的视频画面 1.4.2 能为生成的短时长视频添加基础文字说明或简单音频 1.4.3 能检查生成视频的完整性和播放流畅性，修正影响完整性或流畅性的问题 1.4.4 能对生成视频进行版权合规性检查，识别并修正违规内容，核验人工智能生成标识	1.4.1 人工智能视频生成工具的操作方法 1.4.2 视频格式、时长、分辨率、帧率的基础概念及设置要求 1.4.3 固定画面视频的构图基本原则 1.4.4 视频与音频同步的基础原理及检查方法
	1.5 驱动数字人	1.5.1 能按固定流程模板搭建脚本框架，形成符合场景需求的交互脚本 1.5.2 能选择适配文本，生成符合数字人交互逻辑的脚本 1.5.3 能统计并修正脚本中的错别字、语句不通顺等显性问题 1.5.4 能检查脚本合规性，识别并修正违法、不良、偏见内容，按流程上报安全风险	1.5.1 固定流程模板结构及核心对话节点组成 1.5.2 场景模板文本选择方法及匹配度标准 1.5.3 脚本明显问题统计与修正方法 1.5.4 数字人交互脚本的合规识别标准、安全风险上报流程
2. 数据治理与模型训练	2.1 数据采集	2.1.1 能按指定范围和格式，从公开或内部数据源收集文本、图像等数据，形成数据集 2.1.2 能使用办公软件记录数据来源、格式及数量等元信息，生成数据元信息记录表	2.1.1 基础数据的类型与特征 2.1.2 数据收集的基本流程与规范 2.1.3 数据完整性基本知识 2.1.4 数据元信息相关

		2.1.3 能检查数据完整性，补充缺失基础字段，编制检查报告及完整数据集	知识
	2.2 数据标注	2.2.1 能根据标注指南，分类标注文本，形成分类标注后的文本数据集 2.2.2 能使用图像标注工具标注图片，形成标注后图像及标注信息文件 2.2.3 能核对标注结果与指南的一致性，修正误标、漏标	2.2.1 数据标注的基本概念与目的 2.2.2 文本分类标注的基础标准 2.2.3 标注工具的操作原理 2.2.4 标注结果核对方法
	2.3 数据分析	2.3.1 能将标注完成的数据按类别整理归档 2.3.2 能使用表格工具统计不同类别标注数据的数量，生成基础统计报表及数据统计分析说明 2.3.3 能检查标注结果文件的存储路径和命名格式	2.3.1 数据归档的基本分类方法 2.3.2 统计报表的基础构成要素 2.3.3 文件存储路径与命名的规范要求
3. 系统运维与优化	3.1 系统监测	3.1.1 能逐项检查系统运行指标及运维优化项，记录结果并判断异常 3.1.2 能用系统后台或监控工具监控 CPU（中央处理器）GPU（图像处理器）、内存、磁盘 I/O（输入/输出）等指标，识别异常波动并生成监控分析记录 3.1.3 能用诊断工具检测模型服务端口连接状态及 CPU（中央处理器）、GPU（图像处理器）、内存占用等指标，生成运行状态检测报告	3.1.1 系统运行检查的步骤与检查项设置方法 3.1.2 日志信息的基本类型与识别方式 3.1.3 内存占用、接口延迟等常见生成式人工智能系统运行状态指标 3.1.4 运维工具的功能与使用方法
	3.2 故障运维	3.2.1 能区分系统运行故障类型并定位故障环节 3.2.2 能使用接口调试工具	3.2.1 系统运行故障的常见表现形式与初步判断方法

		验证接口响应的正确性与稳定性 3.2.3 能使用记录工具记录故障处理流程，并形成反馈报告	3.2.2 服务重启、缓存清除等常用恢复操作的执行流程 3.2.3 故障处理记录表单填写要求与内容结构 3.2.4 故障报告的基本格式与撰写方法

征求意见稿

3.2 四级/中级工

职业功能	工作内容	技能要求	相关知识要求
1.内容生成与模型应用	1.1 生成文本	1.1.1 能根据需求确定风趣、严肃等文本风格，生成对应风格的文案 1.1.2 能按照结构化框架生成文本初稿 1.1.3 能根据反馈，调整文本内容，优化表达逻辑和语言准确性，形成符合反馈要求的优化后文本	1.1.1 不同文本风格的语言特征与表达规范 1.1.2 结构化报告的框架组成与撰写要求 1.1.3 文本内容逻辑性校验的基本方法
	1.2 生成图像	1.2.1 能描述特定风格的视觉特征和细节要求，形成可直接用于图像生成的明确描述文本 1.2.2 能使用人工智能图像生成工具，并通过提示词编辑修改图像 1.2.3 能根据产品参数和使用场景，生成符合要求的产品示意图 1.2.4 能根据需求，统一调整生成图像风格	1.2.1 各类视觉风格的核心元素与表现手法 1.2.2 产品示意图设计要点 1.2.3 图像风格统一性调整的基础技巧
	1.3 生成音视频	1.3.1 能根据角色生成多角色语音 1.3.2 能根据场景形成与场景贴合度良好的音频片段 1.3.3 能设计动画的关键帧和过渡效果，生成流畅自然且符合步骤逻辑的动画片段 1.3.4 能为视频添加字幕、标注等元素	1.3.1 语速、语调、音色等语音特征 1.3.2 不同场景氛围的配乐类型与选择标准 1.3.3 视频添加字幕、标识等元素的方法 1.3.4 动画的关键帧设计与过渡效果原理
	1.4 模型选择	1.4.1 能根据业务需求选择公共模型及服务 1.4.2 能调用公共模型接口，并应用公共模型接口返	1.4.1 公共模型接口调用方法 1.4.2 模型接口的参数含义及填写规范

		回数据或模型功能	1.4.3 公共模型接口调用结果的解析方法
	1.5 优化内容	1.5.1 能根据内容类型调整生成式人工智能工具的关键参数 1.5.2 能记录不同参数组合的效果 1.5.3 能通过调整提示词减少生成内容中的偏见	1.5.1 各类内容生成的基础参数含义与调整范围 1.5.2 参数微调对生成内容质量的影响规律 1.5.3 参数组合效果的记录与分析方法 1.5.4 生成式人工智能偏见的类型与检测方法 1.5.5 公平性约束的提示词设计方法
	1.6 驱动数字人	1.6.1 能结合场景特点选定数字人形象 1.6.2 能用预设动作模块组合生成动作序列 1.6.3 能调整动作序列时长与衔接节奏	1.6.1 场景需求与数字人形象的匹配关系 1.6.2 预设动作模块的组合方法与动作序列生成规则 1.6.3 动作序列时长与衔接节奏的调整技巧
2. 数据治理与模型训练	2.1 数据采集	2.1.1 能依据数据质量指标筛选符合需求的数据源 2.1.2 能评估数据源，编制数据源合规性评估报告 2.1.3 能选择适配业务场景的数据源	2.1.1 数据质量评估的核心指标（完整性、准确性、时效性） 2.1.2 数据源合法性与合规性的判断标准 2.1.3 不同类型数据源的适配场景特征 2.1.4 数据源优劣分析和对比方法
	2.2 数据处理	2.2.1 能判断并删除数据中的重复记录，生成去重后的数据文件 2.2.2 能运用统计方法识别并修正数据中的异常值 2.2.3 能发现含违法、不良信息的数据，识别并移除含隐	2.2.1 数据重复、错误的常见类型 2.2.2 统计方法识别异常值的基本原理 2.2.3 数据格式转换的基本方法

		私数据的记录	2.2.4 数据清洗的基本原则 2.2.5 数据合规性检查标准
	2.3 数据标注	2.3.1 能对文本、图像、音频三类型数据进行标注 2.3.2 能根据标注指南，完成多维度标注 2.3.3 能使用自动化标注工具，按要求完成数据标注任务并输出标注文件	2.3.1 文本、图像、音频数据的标注差异与要点 2.3.2 多维度标注的逻辑框架与协同规则 2.3.3 自动化标注工具的功能特点与操作方法
	2.4 数据分析	2.4.1 能制订抽样检验方案，按比例抽取标注数据并核查标注质量 2.4.2 能计算标注准确率、一致性等指标，评估整体质量，形成评估报告 2.4.3 能依检验结果指导修正不合格标注，生成修正指导书及最终标注数据集 2.4.4 能跟踪记录标注过程中模型运行安全事件	2.4.1 抽样检验的样本量确定方法与原则 2.4.2 标注准确率、一致性等评估指标的计算方式 2.4.3 不合格标注内容的修正标准与流程 2.4.4 模型安全事件跟踪记录方法
	2.5 模型训练	2.5.1 能按模型要求划分训练集、验证集与测试集 2.5.2 能对数据进行标准化处理，适配模型输入格式，形成训练数据文件 2.5.3 能检查训练数据分布均衡性，补充稀缺样本，形成均衡化数据集 2.5.4 能在数据准备过程中，进行数据加密、访问控制、数据脱敏等	2.5.1 训练集、验证集、测试集的划分比例与原则 2.5.2 数据标准化处理方法 2.5.3 训练数据分布均衡性的评估指标与调整方法 2.5.4 数据窃取、对抗性攻击等生成式人工智能数据安全风险的防范方法与技术措施（如数据加密、访问控制）
3. 系统运维	3.1 系统功能	3.1.1 能按测试计划编写测	3.1.1 功能测试的基本

与优化	测试	试用例，验证模型接口、生成逻辑及输入输出 3.1.2 能按运维规范，通过命令行或脚本完成服务重启、内存释放与缓存清除 3.1.3 能分析功能测试中发现的问题并整理成缺陷报告 3.1.4 能在测试中识别、记录并反馈生成内容中的偏见和歧视内容	流程与测试用例设计方法 3.1.2 接口调试工具的操作方法及测试参数配置技巧 3.1.3 模型输入输出结构、数据格式和返回状态码的判定标准 3.1.4 缺陷记录与反馈报告的撰写体例与方法
	3.2 故障运维	3.2.1 能分析报错堆栈或异常关键词，定位故障模块及调用链，判断错误或异常原因 3.2.2 能通过配置调整、服务重启、依赖修复等方式修复系统故障 3.2.3 能通过复测及监控对比验证问题消除情况，并编制问题处理记录 3.2.4 能应用接口访问控制、输入数据过滤等防护措施	3.2.1 日志文件分析方法与常见故障关键字 3.2.2 系统配置文件结构与常用参数调整方法 3.2.3 服务重启、端口冲突排查、权限异常处理等故障修复流程 3.2.4 接口访问控制与输入数据过滤等基础安全防护方法或步骤
	3.3 系统监测	3.3.1 能部署和配置日志采集工具记录模型服务日志 3.3.2 能使用监控工具监控系统负载、响应时间等指标 3.3.3 能设置告警参数并根据监控数据预判潜在问题	3.3.1 日志采集与传输工具的结构组成与配置语法 3.3.2 系统运行监控工具的工作原理与部署方式 3.3.3 关键性能指标的阈值设置方法 3.3.4 告警参数编写方法与告警级别分类标准
4.系统架构设计	4.1 智能体组建	4.1.1 能配置管理顺序控制、条件分支与并行推理等多智能体调用流程 4.1.2 能配置智能体间数据	4.1.1 多智能体编排与集成策略设计方法 4.1.2 智能体 MCP（模型上下文协议）接口规

		映射与接口适配规则，实现数据格式转换与参数对接 4.1.3 能用流程设计工具配置智能体调用流程，执行功能测试与路径验证	范、参数传递与数据适配机制 4.1.3 流程引擎或工作流调度工具的使用方法 4.1.4 生成式人工智能平台安全评估标准、安全协议配置流程
	4.2 系统流程设计	4.2.1 能按业务场景配置含用户输入、模型处理等节点的标准化内容生成流程 4.2.2 能设定生成内容质量校验点并集成相关检测工具 4.2.3 能编写内容生成流程规范文档 4.2.4 能对跨境数据与版权进行合规检查	4.2.1 内容生成的典型流程结构与关键节点 4.2.2 内容安全检测工具的功能与接入方式 4.2.3 业务流程规范文档的结构与撰写规范 4.2.4 数据出境安全评估办法、版权检测第三方应用程序编程接口（API）调用规范
	4.3 模型接入	4.3.1 能设计第三方应用程序编程接口（API）、本地模型服务及云端部署模型等不同模型的接入方式 4.3.2 能建立包括身份验证、请求限流、负载切换等模型服务调用逻辑 4.3.3 能配置服务逻辑中的异常处理与回退机制 4.3.4 能部署身份验证模块与审计日志系统	4.3.1 模型服务部署类型与访问控制策略 4.3.2 应用程序接口网关、服务代理与限流熔断机制 4.3.3 异常处理与容错机制设计方法 4.3.4 身份验证协议原理、日志留存要求

3.3 三级/高级工

职业功能	工作内容	技能要求	相关知识要求
1.内容生成与模型应用	1.1 生成文本	1.1.1 能结合行业知识生成专业分析报告 1.1.2 能设计多轮对话内容并制作符合角色设定的脚本	1.1.1 专业领域分析报告的结构规范与行业术语体系 1.1.2 多轮对话脚本的角色设定与语言风格一

		1.1.3 能校验优化文本，修正术语错误与逻辑问题	致性原则 1.1.3 报告文本专业性校验的行业标准与方法
	1.2 生成图像	1.2.1 能依据需求编制专属视觉创意方案 1.2.2 能创作概念图，形成逻辑清晰的视觉方案 1.2.3 能融合多种视觉元素，生成符合创意主题的图像作品	1.2.1 视觉创意方案设计的核心知识、独特性呈现技巧及图像生成的规范标准 1.2.2 概念图创作的完整流程、逻辑表达方法及创意落地的实现路径 1.2.3 多种视觉元素的筛选原则、融合技巧，以及层次感与艺术感营造的综合设计方法
	1.3 生成音视频	1.3.1 能使用生成式人工智能工具生成情感起伏且匹配语境的语音 1.3.2 能制作含多镜头切换、特效处理的叙事性短片配音	1.3.1 情感化语音的语调、语速与语境匹配规律 1.3.2 景别、运镜等叙事性短片的镜头语言与叙事结构 1.3.3 音视频同步的技术标准与时间轴校准方法
	1.4 模型选择	1.4.1 能构建多维度模型评估体系，明确各维度量化指标及权重，形成评估标准文档 1.4.2 能根据场景需求选择模型 1.4.3 能调整模型训练参数并能评估微调后模型的性能变化	1.4.1 模型性能的多维度评估框架 1.4.2 不同模型在特定任务中的优劣势对比分析方法 1.4.3 模型选择的成本效益分析与风险规避原则 1.4.4 模型微调的参数调整范围与影响规律 1.4.5 微调后模型生成效果的评估指标
	1.5 优化内容	1.5.1 能建立内容优化评估	1.5.1 复杂需求的拆解

		标准，优化迭代生成结果，形成符合评估标准的内容 1.5.2 能结合用户反馈和场景需要，通过多轮调整实现内容与需求匹配，场景适配 1.5.3 能总结优化规律，形成特定场景下内容生成最优路径	方法与评估标准设计原则 1.5.2 用户反馈的结构化分析技巧与迭代优先级判定标准 1.5.3 内容生成优化规律提炼方法、特定场景最优路径梳理逻辑及有效性验证技巧
	1.6 驱动数字人	1.6.1 能描述数字人表情、动作和语音同步偏差的具体表现，形成偏差问题清单 1.6.2 能运用数字人生成工具调整数字人表情、动作和语音的同步性 1.6.3 能根据语音情感强度与节奏，优化动态表情力度与时机	1.6.1 音频特征提取技术及语音关键信息量化方法，动态表情与语音节奏匹配度的衡量标准 1.6.2 时间对齐算法知识，语音与动态表情同步误差的范围控制 1.6.3 深度学习模型在语音情感建模中的应用方法，动态表情呈现力度和时机的优化方法
2. 数据治理与模型训练	2.1 数据采集	2.1.1 能根据业务需求确定数据采集范围、频率及格式，形成数据采集要素清单及说明文档 2.1.2 能设计多源数据采集的协同机制，编制协同机制设计方案 2.1.3 能设计数据采集过程中的质量控制节点	2.1.1 数据采集的全流程设计框架 2.1.2 多源数据协同采集的技术原理 2.1.3 数据采集质量控制的关键节点设置方法
	2.2 数据处理	2.2.1 能设计数据清洗流程 2.2.2 能设计自动化清洗脚本并形成可运行文件 2.2.3 能针对不同类型数据制订清洗规则 2.2.4 能通过对比测试验证优化后清洗流程的有效性	2.2.1 自动化清洗脚本的开发逻辑 2.2.2 不同类型数据的特性及清洗规则差异 2.2.3 清洗流程优化效果的评估指标
	2.3 数据标	2.3.1 能根据模型训练目标	2.3.1 标注维度与层级

	注	定义标注维度与层级体系，形成标注维度与层级体系定义文档 2.3.2 能编写详细的标注指南，明确边界案例的处理规则 2.3.3 能建立标注规范动态更新机制，形成机制文件及更新记录	体系的设计原则 2.3.2 边界案例的界定标准与处理逻辑 2.3.3 标注规范的动态更新机制设计要点
	2.4 数据分析	2.4.1 能运用工具分析数据的分布特征，挖掘数据中的关联关系，形成数据分析报告 2.4.2 能根据特征分析结果编制数据增强建议方案 2.4.3 能设计数据分类分级方案，明确不同级别数据的生成式人工智能系统使用限制	2.4.1 统计工具的核心功能及应用场景 2.4.2 数据分布特征的量化指标体系 2.4.3 数据隐含关联的挖掘方法 2.4.4 数据安全治理框架与实施方法
	2.5 模型训练	2.5.1 能根据场景数据规模、特征维度及任务目标，选择适配基础模型架构，配置初始参数，形成选型及训练方案 2.5.2 能监控模型训练的损失值、准确率等指标变化，调整模型训练策略 2.5.3 能根据训练结果调整迭代策略，优化模型收敛效果	2.5.1 常见基础模型架构的适用场景 2.5.2 模型训练参数的配置原理 2.5.3 模型训练指标（损失值、准确率等）的解读方法
3. 系统运维与优化	3.1 系统分析	3.1.1 能通过监控平台或日志系统采集响应时间等指标，分析趋势与阈值 3.1.2 能使用性能分析工具识别系统瓶颈点 3.1.3 能对模型推理速度、应用程序接口响应效率等指标进行量化评估	3.1.1 性能评估常用指标及其计算方法 3.1.2 模型推理流程与系统组件资源消耗关系 3.1.3 性能分析工具的使用方法与数据解释逻辑 3.1.4 性能分析报告的撰写要素与结构
	3.2 系统优化	3.2.1 能重构模型服务调用逻辑	3.2.1 模型服务架构与调用流程原理

		3.2.2 能根据不同负载场景配置 batch_size（批量大小）max_tokens（最大标记数量）等模型服务参数 3.2.3 能部署异步调用机制或任务队列系统 3.2.4 能制订模型安全检查清单并定期开展安全评估	3.2.2 模型调用配置参数的功能及优化策略 3.2.3 异步调用与消息队列系统的基本原理与部署方式 3.2.4 性能提升对模型精度、稳定性可能产生的影响因素 3.2.5 模型安全检查清单编制方法与安全评估流程
	3.3 系统部署	3.3.1 能基于系统部署需求配置操作系统环境、运行依赖及硬件资源参数 3.3.2 能使用脚本工具或容器技术部署基础运行环境 3.3.3 能安装模型运行所需依赖包并设置路径 3.3.4 能记录并维护系统环境配置文档	3.3.1 操作系统基础配置方法与命令 3.3.2 常见依赖安装工具的使用方法 3.3.3 容器化部署工具基础原理与操作流程 3.3.4 环境配置文档的标准结构与记录要点
	3.4 系统监测	3.4.1 能部署服务网关 3.4.2 能设置限流机制	3.4.1 服务网关配置参数与负载均衡算法原理 3.4.2 限流与熔断技术的作用机制及实现方法 3.4.3 并发处理下系统容量评估与压测方法
	3.5 故障运维	3.5.1 能设计日志记录结构、埋点策略与关键路径追踪方法，定位系统故障 3.5.2 能基于日志、监控、指标数据等多维数据源建立故障分析流程图 3.5.3 能通过异常模式识别和原因追溯方法定位系统运行故障	3.5.1 故障定位相关日志结构设计与采集方法 3.5.2 故障根因分析流程与决策路径构建思路 3.5.3 各类故障特征（性能下降、内存泄漏、模型崩溃等）的典型表现 3.5.4 故障溯源技术与自动化分析工具原理
4. 系统架构	4.1 系统构	4.1.1 能构建支持文本、图	4.1.1 多模态模型的调

设计	建	像、音频、视频等多模态输入、输出的大模型系统架构 4.1.2 能规划多模态数据的接入点、预处理模块与输出统一接口 4.1.3 能整合不同模态模型的部署方式	用逻辑与输入、输出要求 4.1.2 跨模态数据融合与标准化处理方法 4.1.3 多模态系统的架构设计模式
	4.2 设计模块间通信机制	4.2.1 能设计支持模型、数据库、前端界面、日志系统等模块间的数据交互流程 4.2.2 能定义模块之间数据接口协议 4.2.3 能实现数据传输中的状态控制、失败重试和流程回滚	4.2.1 系统模块间的数据流结构与通信方式 4.2.2 数据接口设计规范与接口文档管理工具 4.2.3 数据一致性、事务控制与异常恢复机制
	4.3 模型调用	4.3.1 能设计不同模型版本、模型能力范围与性能指标的管理体系 4.3.2 能建立基于任务优先级、模型负载、输出质量等规则的模型自动调用策略 4.3.3 能配置任务调度系统，实现模型请求分发、运行状态监控与错误告警	4.3.1 模型注册、版本控制与能力标签体系的设计方法 4.3.2 任务调度平台原理与配置方式 4.3.3 调度策略与模型资源分配算法
	4.4 系统流程设计	4.4.1 能评估现有生成流程中存在的性能瓶颈、调用冗余与错误链路 4.4.2 能优化生成策略，通过重构生成流程结构提升生成效率与结果质量	4.4.1 生成流程优化方法，思维链、提示工程、上下文工程缺名词 4.4.2 系统性能监控指标与性能瓶颈分析工具 4.4.3 工作流结构优化与任务节点合并原则

3.4 二级/技师

职业功能	工作内容	技能要求	相关知识要求
1.内容生成与模型应用	1.1 生成跨模态内容	1.1.1 能设计文本与动态图像/视频映射规则 1.1.2 能统一色调、语言风格	1.1.1 文本与图像、视频的特征映射机制等跨模态内容生成的技术原理

		等跨模态内容风格 1.1.3 能优化跨模态生成的时序同步性	1.1.2 不同模态内容风格统一性的评估标准与协调方法 1.1.3 跨模态生成时序同步性的技术指标与优化手段
	1.2 优化内容	1.2.1 能建立内容偏差识别标准，定位模型逻辑错误与风格偏移 1.2.2 能制订包含提示词优化、参数调整双路径等人工智能生成内容的质量修正方案 1.2.3 能记录并按场景分类整理偏差类型及解决方法，形成偏差处理知识库	1.2.1 逻辑错误、风格偏移等内容偏差类型及其具体表现形式 1.2.2 偏差识别的量化评估方法与判断标准 1.2.3 提示词优化、参数调整等偏差修正手段的适用场景与操作规范
	1.3 设计生成流程	1.3.1 能梳理内容生成全流程逻辑，绘制流程关系图，撰写说明文档 1.3.2 能搭建自动化生成链路，实现从输入需求到输出成品的流程化运转 1.3.3 能设置流程节点的校验机制	1.3.1 自动化内容生成链路的核心环节与逻辑关系设计原则 1.3.2 质量阈值、审核要点等流程节点校验机制的设置标准 1.3.3 生成流程效率与稳定性的平衡策略
	1.4 模型选择	1.4.1 能剖析编码器、解码器等模型内部模块，明确其对特定生成能力的影响 1.4.2 能通过针对性调整模块参数或结构，提升模型在专业场景的生成精度 1.4.3 能评估组件优化后的整体性能	1.4.1 编码器、解码器等模型内部核心模块的功能与作用机制 1.4.2 模块参数调整对特定生成能力的影响规律 1.4.3 生成精度、效率、兼容性等模型组件优化效果的评估维度
	1.5 工具开发	1.5.1 能基于开源框架与平台的开发能力设计行业专用生成工具的技术架构 1.5.2 能将生成功能封装成易用接口	1.5.1 主流开源框架的技术特性与适用场景 1.5.2 行业专用生成功能的封装方法与接口设计规范

		1.5.3 能测试工具的稳定性和兼容性 1.5.4 能依照业务需求调用第三方应用程序编程接口（API），开发业务工具	1.5.3 工具稳定性与兼容性的测试标准与验证方法
2. 数据治理与模型训练	2.1 建立质量标准	2.1.1 能按照行业规范与业务需求，制订覆盖数据全生命周期的质量标准体系，形成相关标准文档。 2.1.2 能定义数据质量量化指标及阈值范围 2.1.3 能根据实际应用效果动态优化质量标准指标	2.1.1 数据全生命周期各阶段的质量控制点 2.1.2 数据质量量化指标的定义方法与行业基准 2.1.3 质量标准动态校准的流程与评估方法
	2.2 数据处理	2.2.1 能使用大数据处理工具，完成分布式存储、读取与分片，依据数据特征优化分片策略 2.2.2 能对大数据进行清洗，并通过压缩优化提升存储效率 2.2.3 能监测大数据处理过程中处理速度、资源占用率等关键指标，及时发现并反馈明显异常	2.2.1 主流大数据处理工具的使用方法，以及数据分布式存储、读取和分片策略相关知识 2.2.2 大规模数据清洗（去重、处理缺失值）和数据压缩技术的相关知识 2.2.3 大规模数据处理过程中的关键指标（处理速度、资源占用率）及异常识别
	2.3 解决数据难题	2.3.1 能分析产生数据矛盾的深层原因，并设计创新解决方案 2.3.2 能总结数据难题的解决经验，形成可复用的处理方案 2.3.3 能量化评估模型运行的安全风险并形成管理报告	2.3.1 复杂数据矛盾（多源冲突、缺失值过高等）的分析框架 2.3.2 数据融合与智能补全的技术原理 2.3.3 数据难题解决方案的复用性评估标准 2.3.4 模型安全风险量

			化评估方法与安全管理报告编制方法
	2.4 模型训练	2.4.1 能设计阶梯式训练策略 2.4.2 能针对训练过程中的过拟合、收敛缓慢等问题，制订优化措施，生成问题优化方案并记录实施效果 2.4.3 能构建基于知识库的垂类模型	2.4.1 不同模型类型的训练策略适配特征 2.4.2 阶梯式训练中参数配比的设计逻辑 2.4.3 模型训练常见问题(过拟合、收敛缓慢等)的成因与解决方法 2.4.4 基于知识库的大模型应用系统构建
3. 系统运维与优化	3.1 系统优化	3.1.1 能配置线程池大小、GPU（图形处理器）分配策略、内存限制等资源、调度参数 3.1.2 能应用容器编排平台（Kubernetes）等容器编排工具，制订资源调度规则	3.1.1 服务调度策略及亲和性调度、资源配额等参数设置方法 3.1.2 容器编排平台（Kubernetes）等容器编排系统的资源调度机制与配置方法
	3.2 系统更新	3.2.1 能开发或配置自动化流程，实现模型版本检测、文件下载、完整性校验与替换部署操作 3.2.2 能配置灰度更新策略，保障模型更新过程中系统稳定运行 3.2.3 能设计模型更新日志机制，追踪模型版本与调用记录 3.2.4 能设计生成式人工智能安全事件应急响应机制	3.2.1 模型版本控制与版本标识规范 3.2.2 自动化更新流程设计思路与常用工具 3.2.3 灰度发布与回滚机制原理 3.2.4 日志记录结构设计及其在模型溯源中的作用 3.2.4 网络安全应急响应体系建设方法
	3.3 系统部署	3.3.1 能归纳不同平台部署流程差异，制订标准化模板与操作规范 3.3.2 能编写自动化部署脚本或构建多平台兼容镜像 3.3.3 能设计并部署服务主备架构与故障自动切换机制	3.3.1 跨平台部署常见差异点（文件系统、命令行工具、依赖包等） 3.3.2 脚本自动化部署语言和容器镜像构建工具 3.3.3 安全配置策略在

		3.3.4 能选型与部署分布式数据处理框架并完成数据管道配置	多平台部署中的差异与应对措施
	3.4 系统监测	3.4.1 能设计多任务并行处理流程，设置任务调度优先级和分发策略 3.4.2 能部署并配置负载均衡工具，实现任务请求合理分流与节点间均衡 3.4.3 能实时监控任务调度性能，结合指标数据优化负载均衡策略与资源分配逻辑	3.4.1 轮询、最小连接数、基于权重的分发等多任务调度原理、策略 3.4.2 常见负载均衡架构模型及其配置方式 3.4.3 高并发调度系统的性能瓶颈识别方法与调优逻辑
	3.5 故障运维	3.5.1 能制订数据定期备份、快照创建策略、恢复路径与验证测试等流程的灾备方案 3.5.2 能制订容错应急预案，进行灾备演练 3.5.3 能设计具备自动重试、故障转移与多点容灾机制的模型服务部署方案 3.5.4 能配置包括健康检查、熔断降级、请求限流与优雅关闭机制等内容的服务可用性策略	3.5.1 容灾系统分级设计理念与典型部署架构 3.5.2 容灾演练步骤、演练指标与应急预案评估方法 3.5.3 高可用架构设计原则与主动-被动切换、主从同步等故障恢复模式 3.5.4 模型服务监控与告警工具的使用方法 3.5.5 限流熔断组件与服务质量控制策略
4.系统架构设计	4.1 系统构建	4.1.1 能设计支持横向扩展、弹性伸缩的系统整体架构 4.1.2 能拆分系统功能模块，构建微服务或插件化架构 4.1.3 能制订架构扩展条件、升级路径方案 4.1.4 能选型与部署分布式数据处理框架并配置数据管道	4.1.1 分布式架构、服务解耦等可扩展系统架构设计原则 4.1.2 微服务架构模式与容器化平台（Docker）、容器编排平台（Kubernetes）等容器化技术 4.1.3 系统弹性扩展机制与负载监控策略 4.1.4 分布式数据处理框架与任务调度原理

			4.1.5 数据缓存与高并发访问优化策略
	4.2 模型调用	4.2.1 能根据不同行业或任务场景设计匹配的生成流程与模型选择规则 4.2.2 能设计生成任务路由逻辑，在不同场景间实现策略复用与个性化输出	4.2.1 多场景建模技术与语境理解方法 4.2.2 规则引擎、模板匹配、多模型选择等生成策略配置方式 4.2.3 个性化生成策略中的上下文保持与交互管理机制
	4.3 系统评估	4.3.1 能制订模型响应速度、调用成功率、资源占用等性能的评估流程 4.3.2 能构建性能基准测试环境并采集评估数据 4.3.3 能分析性能瓶颈并提出优化建议	4.3.1 系统性能评估指标体系，包括延迟、每秒事务数（TPS）、每秒查询数（QPS）等 4.3.2 性能测试方法与工具使用方法 4.3.3 性能调优与资源配比分析方法
5.技术支持与管理	5.1 制订规范	5.1.1 能制订技术支持服务流程标准和包含首次响应时间、问题解决率等的技术支持绩效指标体系 5.1.2 能评估支持流程有效性，并持续完善制度内容 5.1.3 能识别并处理数据偏见、信息泄露、虚假信息生成等复杂的生成式人工智能伦理与安全风险 5.1.4 能设计并绘制受理、处理、验证、反馈与复盘全流程流程图	5.1.1 技术支持服务流程标准，及典型问题处理方法 5.1.2 问题响应级别与服务等级协议设定方法 5.1.3 运维制度文件撰写规范与流程优化方法 5.1.4 技术支持绩效评价模型与关键绩效指标（KPI）设计、目标与关键成果法（OKR）实施等常用方法 5.1.5 文案生成、图像生成、视频生成等生成式人工智能创作工具的使用方法
	5.2 建立知识库	5.2.1 能设计知识库结构并分类整理典型案例、常见问题、操作指引等内容	5.2.1 知识管理模型与知识分类体系

		5.2.2 能制订知识审核、更新、沉淀机制 5.2.3 能构建支持分层机制	5.2.2 知识库系统功能结构与维护方式 5.2.3 支持服务分层结构（L1/L2/L3 支持）与转交机制
	5.3 项目管理	5.3.1 能建立文档分类体系，并分类管理技术文档 5.3.2 能使用 Git（分布式版本控制系统）、SVN（集中式版本控制系统）等版本管理工具规范文档迭代过程 5.3.3 能完成关键节点文档的归档与交付	5.3.1 项目文档种类、模板结构与内容要素 5.3.2 文档版本控制策略与变更日志管理方法 5.3.3 文档生命周期管理规范与审阅机制
	5.4 资源配置与管理	5.4.1 能设计资源管理报表，统一管理账号、模型、算力、应用程序接口权限等资源 5.4.2 能监督资源配置、申请、审批、使用、监控等流程 5.4.3 能分析资源使用数据，提供优化建议或调度策略	5.4.1 生成式人工智能资源管理体系设计与权限控制机制 5.4.2 不同类型资源的计量与配额模型 5.4.3 数据可视化工具与资源分析报告生成方法
6 培训和指导	6.1 培训	6.1.1 能编写培训讲义 6.1.2 能对五级/初级工、四级/中级工、三级/高级工开展培训	6.1.1 技术培训制度与流程 6.1.2 搜集和整理的方法以及 PPT 制作的方法
	6.2 指导	6.2.1 能制订数据处理人员的技能提升计划 6.2.2 能审核五级/初级工、四级/中级工、三级/高级工的数据处理结果，提出改进建议并指导优化 6.2.3 能建立数据处理团队的协作机制，提升整体工作效率	6.2.1 实践教学方法 6.2.2 技术指导方法 6.2.3 数据处理人员的技能分级与提升路径 6.2.4 低级别数据处理结果的审核要点与评价标准 6.2.5 团队协作机制设计的基本原则

3.5 一级/高级技师

职业功能	工作内容	技能要求	相关知识要求
1.内容生成与模型应用	1.1 设计生成方案	1.1.1 能调研垂直领域业务流程与内容需求；规划全链条人工智能生成内容系统架构，形成设计方案 1.1.2 能整合数据采集、模型训练、内容生成、审核分发等环节，构建闭环式生成方案 1.1.3 能评估方案可行性与落地成本，制订分阶段实施计划，编制计划书 1.1.4 能结合行业特性与合规要求，构建多维度内容质量评估指标体系 1.1.5 能制订内容生成全流程操作规范 1.1.6 能根据行业反馈动态修订与完善标准体系	1.1.1 垂直领域人工智能生成内容系统的架构设计原理与核心组件功能 1.1.2 行业业务流程与内容生成需求的映射方法及分析框架 1.1.3 与业务相关的生成式系统搭建方案及可行性评估指标 1.1.4 开源生成式人工智能生态建设与企业实践方法 1.1.5 行业内容质量评估体系的构建原则与核心指标设计方法 1.1.6 行业法规、业务需求、用户体验等内容生成规范的制定依据
	1.2 新技术应用	1.2.1 能编制前沿生成技术动态跟踪报告 1.2.2 能编制新型技术与产业场景适配的分析报告 1.2.3 能设计技术落地验证方案与试点路径	1.2.1 前沿生成技术的核心原理与技术特性 1.2.2 新型技术与产业场景的适配性评估维度与匹配方法 1.2.3 前沿模型在产业场景中落地的风险评估与规避策略
	1.3 内容生成	1.3.1 能应用低数据场景设计合成、迁移学习等数据增强策略，编制增强方案 1.3.2 能拆解需求的核心要素，通过模型融合或算法创新解决生成问题 1.3.3 能建立极端场景问题案例库，提炼复用技术方案与应对策略，编制案例手册及策	1.3.1 低数据场景下的数据增强技术原理与应用方法 1.3.2 内容生成需求的拆解逻辑与生成瓶颈的技术突破路径 1.3.3 极端场景生成难题的解决方案评估标准与效果验证方法

		略指南 1.3.4 能审核内容创作方案与模型优化策略，提供改进建议，形成审核意见报告	1.3.4 高级内容创作的行业标准与专业评估维度
2. 数据治理与模型训练	2.1 数据治理	2.1.1 能结合行业趋势和组织战略，形成覆盖数据全生命周期的数据治理框架文档 2.1.2 能制订数据治理的制度规范并组织实施，编制落地实施报告 2.1.3 能评估治理体系效能并进行流程优化 2.1.4 能设计生成式人工智能系统应用的安全评估标准和流程	2.1.1 数据治理体系的框架设计原则 2.1.2 数据全生命周期各阶段的管控要点 2.1.3 数据治理效能评估的核心指标与方法 2.1.4 生成式人工智能安全风险评估与管控方法
	2.2 数据规划	2.2.1 能基于业务目标和技术发展，制订中长期数据资源规划与布局方案 2.2.2 能分析数据治理业务实施中的风险并制订应对策略 2.2.3 能建立数据治理与业务体系的协同融合机制及实施计划	2.2.1 数据资源规划与业务目标的匹配逻辑 2.2.2 数据治理中的风险识别与管控机制 2.2.3 数据价值转化的路径与评估模型
	2.3 优化训练框架	2.3.1 能设计多场景适配、支持大规模多类型模型并行训练的分布式训练框架 2.3.2 能优化训练框架资源调度，并形成优化报告及性能测试数据 2.3.3 能结合前沿技术制订训练框架功能升级方案并升级训练框架功能，编制升级后框架的使用手册	2.3.1 分布式训练框架的架构设计原理 2.3.2 大规模模型并行训练的资源调度策略 2.3.3 前沿训练技术的适配场景与融合方法
	2.4 技术创新	2.4.1 能跟踪数据治理与模型训练前沿技术，评估应用价值	2.4.1 数据治理与模型训练领域的前沿技术发展趋势

		2.4.2 能研究和分析技术创新项目研发与实施要点，形成技术创新项目成果报告及实施案例 2.4.3 能将创新成果转化为技术标准或解决方案，形成可推广的技术标准文件及行业应用实施方案	2.4.2 技术创新项目的研发流程与成果转化路径 2.4.3 行业技术标准的制定原则与推广机制
3. 系统运维与优化	3.1 故障运维	3.1.1 能制订生成式人工智能系统运维标准流程 3.1.2 能制订系统运维标准操作规程，并通过流程建模工具实现全流程可视化管理 3.1.3 能定期评估运维流程的适用性、通用性与可扩展性，提出优化建议并持续改进 3.1.4 能根据用户访问量波动与服务压力配置自动扩缩容策略 3.1.5 能制订跨地域、多节点部署架构与容灾方案	3.1.1 IT 运维流程建模方法 3.1.2 运维标准化文件结构、编写规范与审核流程 3.1.3 流程优化评估方法与生命周期管理策略 3.1.4 分布式计算架构原理与调度机制 3.1.5 容器编排系统的高级配置策略与集群管理方法 3.1.6 多节点部署同步机制与跨地域网络延迟控制策略 3.1.7 并行部署环境下的测试、监控与版本控制方法
	3.2 系统监测	3.2.1 能设计并集成多源数据采集、指标监控、智能预警与故障诊断模块，构建智能监控体系 3.2.2 能配置基于规则与机器学习算法的异常检测模型，进行故障预测、定位与预警推送	3.2.1 系统监控平台的模块化设计原理 3.2.2 基线偏移、时序预测等异常检测算法的原理与应用场景 3.2.3 数据可视化技术与监控大屏设计规范 3.2.4 跨平台数据采集与联动控制机制
	3.3 系统优化	3.3.1 能设计并部署资源调度优化策略，动态调节资源分	3.3.1 系统自主优化策略设计方法与算法原理

		配 3.3.2 能在模型推理过程中应用加速机制 3.3.3 能基于系统运行反馈实时调整算法策略，实现调度逻辑的持续自优化	3.3.2 强化学习、进化算法等优化技术在系统调度中的应用方法 3.3.3 模型推理加速技术及其系统集成方法 3.3.4 实时反馈数据采集与闭环控制机制
	3.4 技术创新	3.4.1 能结合技术发展趋势，研究并提出智能运维（AIOps）、无服务器架构（Serverless）等前沿运维技术的系统集成与应用方案 3.4.2 能评估新技术的实施可行性、风险与投入产出比（ROI），并形成技术改进与管理建议	3.4.1 智能运维（AIOps）、无服务器架构（Serverless）等新兴技术架构原理与发展动态 3.4.2 运维技术路线图制订方法与战略评估工具 3.4.3 跨部门技术协同的组织流程与管理方法 3.4.4 运维系统升级评估指标与技术选型策略
4.系统架构设计	4.1 系统构建	4.1.1 能设定模型适用边界、优先级与路由策略 4.1.2 能设计统一支持本地部署、公有云、私有云与混合云的跨平台架构体系 4.1.3 能制订多平台环境下的模型镜像、数据一致性与服务治理方案 4.1.4 能基于AGI（通用人工智能）、边云协同等技术趋势设计系统的演进路线 4.1.5 能制订支持系统解耦、模块重构与接口扩展的演进策略 4.1.6 能制订支持技术替代、扩展性与兼容性控制的系统生命周期管理机制 4.1.7 能评估企业级生成式	4.1.1 异构模型的技术特征与接口标准 4.1.2 集成学习（Ensemble）、策略路由、提示词（Prompt）调度等模型融合与切换机制 4.1.3 多模型协同系统中的性能瓶颈识别与优化技术 4.1.4 云原生、边缘计算、K8s多集群等多平台部署架构的关键技术 4.1.5 容器管理、持续集成与持续部署（持续集成/持续交付（CI/CD））流程设计方法 4.1.6 跨平台资源协同、配置管理与安全控制技

		人工智能应用的自主可控程度，制订国产化替代路线图	术 4.1.7 生成式人工智能技术栈国产化评估方法
	4.2 系统集成	4.2.1 能设计具备任务识别、意图理解、上下文管理等能力的自适应生成系统框架 4.2.2 能集成策略优化模块，动态调整实现生成策略 4.2.3 能构建自学习机制，实现系统持续演进与个性化响应	4.2.1 自适应系统的体系结构与智能调控原理 4.2.2 用户建模、上下文跟踪与意图识别技术 4.2.3 强化学习、策略微调等反馈驱动优化方法
5.技术支持与管理	5.1 制订规范	5.1.1 能归纳不同行业特点共性需求，设计标准化的生成式人工智能应用支持方案模板 5.1.2 能分析典型行业场景与任务流，配置适配的模型、数据结构与交互流程 5.1.3 能评估模板的适用性与迁移性，并制订定制化改造策略 5.1.5 能构建服务质量监控指标体系并实施指标常态化评估 5.1.7 能制订与业务相匹配的生成式人工智能安全管理制度	5.1.1 垂直行业业务流程建模与场景分析方法 5.1.2 行业级生成式人工智能应用架构设计原则与模块化配置思路 5.1.3 模板化技术方案评估维度与适配性测评方法 5.1.4 技术服务标准设计方法与适配流程 5.1.5 服务质量管理与评估指标体系 5.1.6 标准落地实施路径与持续改进机制 5.1.7 企业级生成式人工智能安全管理体系建设方法
	5.2 资源配置与管理	5.2.1 能设计产品、研发、运维、客服等多角色协同的技术支持组织机制 5.2.2 能制订跨部门沟通接口、任务分工与信息共享机制	5.2.1 责任分工矩阵（RACI）模型等跨部门协同建模方法与组织设计理论 5.2.2 技术支持协作平台与项目管理工具的集成策略 5.2.3 非暴力沟通、利益平衡模型等沟通与冲突

			协调技术
6 培训和指导	6.1 培训	6.1.1 能根据客户类型与使用目标设计生成式人工智能技术培训内容和培训方案 6.1.2 能开发生成式人工智能技术应用的培训课件、使用手册、操作演示视频等配套培训材料，并形成标准化培训资源包 6.1.3 能实施体系化的培训服务，包括现场讲解、互动答疑、反馈收集与效果评估	6.1.1 培训需求分析方法与培训内容结构设计原则 6.1.2 培训材料编制规范与多媒体资源开发工具使用方法 6.1.3 体系化培训实施流程与效果评估方法
	6.2 指导	6.2.1 能设计培训体系，并监督指导培训体系，评估 6.2.2 能指导五级/初级工、四级/中级工、三级/高级工、二级/技师开展培训工作，监控培训活动的执行质量	6.2.1 生成式人工智能产品及技术培训需求 6.2.2 培训指导与监督方法，岗位培训辅导技巧

4. 权重表

4.1 理论知识权重表

项目 \ 技能等级		五级/初级工（%）	四级/中级工（%）	三级/高级工（%）	二级/技师（%）	一级/高级技师（%）
基本要求	职业道德	5	5	5	5	5
	基础知识	15	15	10	10	5
相关知识要求	内容生成与模型应用	50	30	10	5	5
	数据治理与模型训练	20	20	30	20	5
	系统运维与优化	10	20	25	15	10
	系统架构设计	-	10	20	30	30
	技术支持与管理	-	-	-	10	35
	培训和指导	-	-	-	5	5

4.2 技能要求权重表

项目 \ 技能等级		五级/初级工（%）	四级/中级工（%）	三级/高级工（%）	二级/技师（%）	一级/高级技师（%）
技能要求	内容生成与模型应用	70	50	10	5	5
	数据治理与模型训练	20	15	30	15	5
	系统运维与优化	10	25	30	20	15
	系统架构设计	-	10	30	40	45
	技术支持与管理	-	-	-	15	25
	培训和指导	-	-	-	5	5

第二部分

（本节内容涉及一个工种：生成式人工智能系统测试员。）

1. 职业概况

1.1 职业（工种）名称

生成式人工智能系统应用员S（生成式人工智能系统测试员）

1.2 职业编码

4-04-05-13

1.3 工种定义

运用专业测试工具和方法，从事生成式人工智能系统的功能、性能、安全、伦理、合规性等测试评估的技术人员。

1.4 职业技能等级

本职业共设四个等级，分别为：四级/中级工、三级/高级工、二级/技师、一级/高级技师。

1.5 职业环境条件

室内，常温。

1.6 职业能力特征

智力正常，具有一定的表达能力、沟通能力、空间感，知觉、色觉、听觉正常，动作协调。

1.7 普通受教育程度

高中毕业（或同等学力）。

1.8 职业培训要求

1.8.1 培训参考时长

四级/中级工不少于80标准学时；三级/高级工不少于64标准学时；二级/技师不少于64标准学时；一级/高级技师不少于64标准学时。

1.8.2 培训教师

培训四级/中级工的教师应具有本职业三级/高级工及以上职业资格（职业技能等级）证书或相关专业中级及以上专业技术职务任职资格。

培训三级/高级工的教师应具有本职业二级/技师及以上职业资格(职业技能等级)证书或相关专业中级及以上专业技术职务任职资格。

培训二级/技师的教师应具有本职业一级/高级技师职业资格（职业技能等级）证书或相关专业高级专业技术职务任职资格。

培训一级/高级技师的教师应具有本职业一级/高级技师职业资格（职业技能等级）证书2年（含）以上或相关专业高级专业技术职务任职资格2年（含）以上。

1.8.3 培训场所设备

理论知识培训在标准教室或线上平台进行；操作技能培训根据工作要求，在具有支撑生成式人工智能系统应用的相应软、硬件的培训场所进行。

1.9 职业技能评价要求

1.9.1 申报条件

1.具备以下条件之一者，可申报五级/初级工：

(1)年满16周岁，拟从事本职业或相关职业[3]工作。

(2)年满16周岁，从事本职业或相关职业工作。

2.具备以下条件之一者，可申报四级/中级工：

(1)累计从事本职业或相关职业工作满5年。

(2)取得本职业或相关职业五级/初级工职业资格(职业技能等级)证书后，累计从事本职业或相关职业工作满3年。

(3)取得本专业或相关专业[4]的技工院校或中等及以上职业院校、专科及以上

---

3 相关职业：人工智能工程技术人员、计算机软件工程技术人员、计算机网络工程技术人员、信息系统分析工程技术人员、嵌入式系统设计工程技术人员、大数据工程技术人员、自动控制工程技术人员、计算机程序设计员、计算机软件测试员、数据库运行管理员、生成式人工智能系统应用员、人工智能训练师、数字孪生应用技术员、虚拟现实产品设计师等。

4 相关专业：保密技术、大数据技术、电气工程及自动化、电气工程与智能控制、电影制作、电子科学与技术、电子信息技术、电子与计算机工程、动漫制作技术、多媒体制作、服务机器人装配与维护、服务科学与工程、工业互联网技术、工业互联网与大数据应用、工业软件、工业设计、工业智能工程技术、机电一体化技术、机器人技术、机械电子工程、机械工程、机械设计制造及自动化、集成电路工程技术、计算机程序设计、计算机动画制作、计算机辅助设计与制造、计算机广告制作、计算机科学与技术、计算机平面设计、计算机网络技术、计算机信息管理、计算机应用、计算机应用与维修、计算机游戏制作、交叉工程、开源技术应用、空间信息与数字技术、控制科学与工程、密码技术应用、密码科学与技术、平面设计、汽车智能技术、嵌入式技术、区块链技术、人工智能技术应用、人工智能数据工程技术、软件工程、软件技术、软件与信息服务、数据科学与大数据技术、数控技术、数字化设计与制造技术、数字孪生应用技术、数字媒体技术、数字媒体艺术、通信软件技术、网络工程、网络规划与优化技术、网络空间安全、网站建设与管理、未来机器人、物联网工程、现代测控工程技术、新媒体艺术、信创系统技术应用、信息安全、信息管理与信息系统、虚拟现实技术、移动互联网应用技术、应用电子技术、云计算技术、智能测

普通高等学校毕业证书(含在读应届毕业生)。

3.具备以下条件之一者，可申报三级/高级工：

（1）累计从事本职业或相关职业工作满 10 年。

（2）取得本职业或相关职业四级/中级工职业资格（职业技能等级）证书后，累计从事本职业或相关职业工作满 4 年。

（3）取得符合专业对应关系的初级职称（专业技术人员职业资格）后，累计从事本职业或相关职业工作满 1 年。

（4）取得本专业或相关专业的技工院校高级工及以上毕业证书（含在读应届毕业生）。

（5）取得本职业或相关职业四级/中级工职业资格（职业技能等级）证书，并取得高等职业学校、专科及以上普通高等学校本专业或相关专业毕业证书（含在读应届毕业生）。

（6）取得经评估论证的高等职业学校、专科及以上普通高等学校本专业或相关专业的毕业证书（含在读应届毕业生）。

4.具备以下条件之一者，可申报二级/技师：

（1）取得本职业或相关职业三级/高级工职业资格（职业技能等级）证书后，累计从事本职业或相关职业工作满 5 年。

（2）取得符合专业对应关系的初级职称（专业技术人员职业资格）后，累计从事本职业或相关职业工作满 5 年，并在取得本职业或相关职业三级/高级工职业资格（职业技能等级）证书后，从事本职业或相关职业工作满 1 年。

（3）取得符合专业对应关系的中级职称（专业技术人员职业资格）后，累计从事本职业或相关职业工作满 1 年。

（4）取得本职业或相关职业三级/高级工职业资格（职业技能等级）证书的高级技工学校、技师学院毕业生，累计从事本职业或相关职业工作满 2 年。

（5）取得本职业或相关职业三级/高级工职业资格（职业技能等级）证书满 2 年的技师学院预备技师班、技师班学生。

控工程、智能产品开发与应用、智能互联网络技术、智能机电技术、智能机器人技术、智能交互设计、智能科学与技术、智能控制技术、智能视听工程、智能体技术应用、智能制造工程、智能制造装备技术、装备智能化技术、自动化等。

5.具备以下条件之一者，可申报一级/高级技师：

（1）取得本职业或相关职业二级/技师职业资格（职业技能等级）证书后，累计从事本职业或相关职业工作满 5 年。

（2）取得符合专业对应关系的中级职称后，累计从事本职业或相关职业工作满 5 年，并在取得本职业或相关职业二级/技师职业资格（职业技能等级）证书后，从事本职业或相关职业工作满 1 年。

（3）取得符合专业对应关系的高级职称（专业技术人员职业资格）后，累计从事本职业或相关职业工作满 1 年。

1.9.2 评价方式

分为理论知识考试、操作技能考核以及综合评审。理论知识考试以笔试、机考等方式为主，主要考核从业人员从事本职业应掌握的基本要求和相关知识要求。操作技能考核主要采用现场操作、模拟操作等方式进行，主要考核从业人员从事本职业应具备的技能水平。综合评审主要针对二级/技师和一级/高级技师，通常采取审阅申报材料、答辩等方式进行全面评议和审查。

理论知识考试、操作技能考核和综合评审均实行百分制，成绩皆达 60 分（含）以上者为合格。

1.9.3 监考人员、考评人员与考生配比

理论知识考试中的监考人员与考生配比不低于 1:15，且每个考场不少于 2 名监考人员；操作技能考核中的考评人员与考生配比不低于 1:10，且考评人员为 3 人（含）以上单数；综合评审委员为 3 人（含）以上单数。

1.9.4 评价时长

理论知识考试时间不少于 60 分钟，操作技能考核时间四级/中级工、三级/高级工不少于 60 分钟，二级/技师、一级/高级技师不少于 45 分钟。综合评审时间不少于 20 分钟。

1.9.5 评价场所设备

理论知识考试在标准教室进行，操作技能考核根据工作要求，在具有支撑生成式人工智能系统应用的相应软、硬件的评价场所进行；综合评审在标准教室或会议室进行。

5. 基本要求

2.1 职业道德

2.1.1 职业道德基本知识

2.1.2 职业守则

（1）诚实守信，保守秘密。

（2）遵纪守法，严守伦理。

（3）尊重原创，客观公正。

（4）爱岗敬业，服务大众。

（5）团结协作，勇于创新。

（6）持续学习，追求卓越。

2.2 基础知识

2.2.1 专业基础知识

（1）计算机软件、硬件、网络等操作知识

（2）编程基础知识

（3）人工智能基本概念、数据处理、模型训练等基础知识

（4）常用办公软件操作知识

2.2.2 工程实践相关知识

（1）文档规范、代码规范、质量保障规范相关知识

（2）项目管理、资料管理、计算机设备管理相关知识

（3）知识产权相关知识

2.2.3 业务实践相关知识

（1）人工智能行业及产品知识

（2）人工智能产业应用相关知识

（3）人工智能发展现状与趋势相关知识

（4）生成式人工智能技术和产品相关知识

2.2.4 人工智能伦理及安全知识

（1）人工智能安全与隐私保护相关知识

（2）人工智能道德伦理相关原则及标准相关知识

（3）生成式人工智能服务安全、内容标识办法相关知识

2.2.5 相关法律、法规知识

（1）《中华人民共和国民法典》相关知识

（2）《中华人民共和国劳动法》相关知识

（3）《中华人民共和国劳动合同法》相关知识

（4）《中华人民共和国网络安全法》相关知识

（5）《中华人民共和国著作权法》相关知识

（6）《中华人民共和国数据安全法》相关知识

（7）《中华人民共和国个人信息保护法》相关知识

（8）《中华人民共和国保守国家秘密法》相关知识

（9）《互联网信息服务算法推荐管理规定》相关知识

（10）《互联网信息服务深度合成管理规定》相关知识

（11）《生成式人工智能服务管理暂行办法》相关知识

（12）《人工智能生成合成内容标识办法》相关知识

（13）《数据出境安全评估办法》相关知识

（14）《科技伦理审查办法（试行）》相关知识

6. 工作要求

本标准对四级/中级工、三级/高级工、二级/技师、一级/高级技师的技能要求和相关知识要求依次递进，高级别涵盖低级别的要求。

3.1 四级/中级工

职业功能	工作内容	技能要求	相关知识要求
1.测试环境准备	1.1 环境构建	1.1.1 能识别和安装模型推理的运行环境 1.1.2 能对照模型运行要求检查系统资源配置情况 1.1.3 能加载指定版本的预训练模型，并验证模型加载情况 1.1.4 能按规范填写测试运行环境配置记录	1.1.1 生成式人工智能系统架构 1.1.2 算力资源的参数 1.1.3 模型文件格式 1.1.4 运行环境配置规范
	1.2 配置验证	1.2.1 能按照操作说明，配置生成式人工智能系统的评测工具 1.2.2 能按照测试需求，配置模型	1.2.1 生成式人工智能系统的评测指标 1.2.2 提示词工程概念及

		接口、输入输出格式及评测规则 1.2.3 能记录工具版本、配置参数与验证结果	使用方法 1.2.3 评测数据集参数和基准
	1.3 测试数据采集	1.3.1 能依据测试用例，采集测试所需的结构化数据集 1.3.2 能使用数据处理工具完成结构化数据的预处理操作 1.3.3 能记录测试数据的格式、数量等元数据信息	1.3.1 数据集采集方法 1.3.2 结构化数据预处理方法 1.3.3 数据记录规范
2.行为测试	2.1 生成能力测试	2.1.1 能依据提示词测试用例，测试文本、图像或语音等单一类型的生成能力 2.1.2 能按照测试模板，人工核对并记录生成结果 2.1.3 能标记生成结果中未回答问题、输出为空、严重跑题等不符合指令要求的情况	2.1.1 测试提示词编写的要求、方法及评测目标 2.1.2 测试模板应用方法 2.1.3 异常结果特征
	2.2 任务执行与工具使用能力测试	2.2.1 能依据测试用例，测试检索增强生成、工具调用、多步骤任务等单一场景下的模型能力 2.2.2 能根据测试模板，核对并标注模型的工具触发情况、任务完成状态、输入输出格式等执行结果 2.2.3 能在执行过程中，识别并记录未理解指令、执行阻塞、输出与任务无关等失败情况	2.2.1 智能体概念 2.2.2 模型的工具调用规范 2.2.3 任务执行的异常类型
	2.3 上下文与记忆能力测试	2.3.1 能依据测试用例，执行跨轮对话测试，记录相同或相似查询在不同轮次中的回答一致性问题 2.3.2 能在指定时长或多轮长期对话测试中，记录模型出现的失忆现象与回答矛盾点 2.3.3 能填写上下文相关缺陷信息，记录复现步骤与对话上下文快照	2.3.1 大模型上下文窗口的概念与对话记忆机制 2.3.2 跨轮对话一致性的判断标准 2.3.3 缺陷记录的规范与上下文信息采集的要点
	2.4 语言理解与推理能力测试	2.4.1 能依据测试用例，测试事实问答、指令遵循、实体/关系识别、逻辑问题等单一类型的能力，并	2.4.1 自然语言处理术语 2.4.2 推理逻辑结构的识别方法

		记录模型的输入与输出 2.4.2 能按照测试模板中的判定规则，判断模型理解输入内容的显性语义的准确性 2.4.3 能识别并记录模型出现的理解偏差、逻辑矛盾等问题	2.4.3 事实类问答测试的流程与记录规范 2.4.4 语言理解偏差的类型
	2.5 场景化任务与行业适配测试	2.5.1 能测试单一行业场景任务目标与模型生成结果间的一致性 2.5.2 能辨识场景术语与业务之间的偏差 2.5.3 能分类场景测试结果中的不适配问题	2.5.1 行业业务场景与术语体系 2.5.2 场景测试目标与业务一致性判定方法 2.5.3 行业场景不适配问题分类规则
3.性能测试	3.1 推理性能评估	3.1.1 能依据测试规程，使用推理性能监测工具采集首词元（token）时间、总响应时间、吞吐量及资源占用等性能数据 3.1.2 能汇总推理性能测试数据，识别性能异常	3.1.1 推理性能测试工具使用方法 3.1.2 生成式人工智能模型推理性能测试指标
	3.2 模型稳定性与鲁棒性测试	3.2.1 能依据测试用例，执行固定输入条件下的重复测试，记录模型输出一致性问题 3.2.2 能执行预设的同义替换、添加空格等提示词扰动测试用例，检查存在的错误或服务崩溃现象	3.2.1 生成式模型稳定性测试方法 3.2.2 生成式模型鲁棒性测试方法
	3.3 并发性能测试	3.3.1 能依据测试用例，利用工具执行模型的并发请求测试 3.3.2 能识别并发测试中出现的大量超时、请求中断等异常现象 3.3.3 能依据并发性能的数据分析需求，记录测试结果	3.3.1 并发的概念 3.3.2 并发请求测试工具使用方法 3.3.3 并发性能测试异常现象判断方法
4.安全测试	4.1 系统供应链安全测试	4.1.1 能对模型文件、数据集及依赖组件进行完整性校验和来源验证 4.1.2 能使用扫描工具，检查安全漏洞及协议合规性 4.1.3 能维护供应链资产台账，记录组件信息与安全检测结果	4.1.1 哈希算法与数字签名校验概念 4.1.2 协议特征与合规性的风险常识 4.1.3 软件物料清单的记录规范 4.1.4 漏洞分级标准
	4.2 隐私与数据安全测试	4.2.1 能识别并标记生成内容中的身份证号、手机号、地址等个	4.2.1 个人信息保护原则 4.2.2 数据泄露的形式

		人敏感信息字段 4.2.2 能验证模型对隐私请求的拒绝响应 4.2.3 能记录提示词泄露、模型记忆泄露等数据泄露事件	4.2.3 模型记忆泄密风险的类型
	4.3 模型对抗性安全测试	4.3.1 能依据测试用例，测试指令干扰、角色伪装、历史信息干扰等形式的对抗 4.3.2 能依据安全应对方式清单，执行模型对风险内容响应的对抗性测试 4.3.3 能依据对抗性安全数据分析需求和数据记录规范，记录测试结果	4.3.1 对抗攻击类型 4.3.2 风险内容识别方法 4.3.3 安全应对机制
	4.4 智能体自主交互安全测试	4.4.1 能依据测试用例，测试单一智能体的自主交互能力 4.4.2 能依据安全策略，检查智能体在工具调用、资源访问等操作中的越权行为或异常输出 4.4.3 能在预设极端或诱导场景中，测试智能体违反安全约束的行为 4.4.4 能依据智能体自主交互安全数据分析需求和数据记录规范，记录测试结果	4.4.1 智能体自主交互测试流程和方法 4.4.2 权限控制策略 4.4.3 越权行为识别方法 4.4.4 测试结果记录规范
5.伦理评估	5.1 伦理与合规性审查	5.1.1 能依据伦理与合规性检查清单，识别并标记生成内容中包含暴力、色情、歧视等违背伦理的表述 5.1.2 能使用版权检测工具，识别并标记生成内容中所包含的受版权保护内容 5.1.3 能检查生成内容中包含的“AI 生成”等强制性标识 5.1.4 能记录伦理与合规性检测结果，填写生成内容、问题类型、标记位置及判定结论	5.1.1 生成式人工智能伦理风险类型 5.1.2 受版权保护文本的表现形式 5.1.3 生成式人工智能输出内容强制性标识规定 5.1.4 伦理与合规性检测结果记录规范
	5.2 误导性内容识别	5.2.1 能依据测试用例，核对事实准确性	5.2.1 误导性内容的类型 5.2.2 误导性内容识别方

		5.2.2 能识别并标注模型输出中存在的事实性误导、立场价值性误导等内容 5.2.3 能按照模板，记录误导性内容测试结果	法 5.2.3 测试结果模板化记录规范

3.2 三级/高级工

职业功能	工作内容	技能要求	相关知识要求
1. 测试环境准备	1.1 测试需求分析	1.1.1 能解析业务需求文档，提取测试场景及对应的功能要求，编制结构化的测试点清单 1.1.2 能使用需求跟踪矩阵，映射测试点与原始业务需求条目 1.1.3 能划分不同测试对象的测试边界与优先级 1.1.4 能按规范编制测试需求分析记录	1.1.1 需求分析方法 1.1.2 需求追溯与需求映射方法 1.1.3 测试对象的划分方法 1.1.4 测试文档规范与编制方法
	1.2 环境构建	1.2.1 能识别和配置不同类型的算力资源 1.2.2 能验证推理框架的版本兼容性和应用编程接口（API） 1.2.3 能检查和优化系统资源分配 1.2.4 能加载和验证多种格式的模型文件	1.2.1 算力资源配置方法 1.2.2 深度学习框架配置与优化的方法 1.2.3 资源分配优化规范 1.2.4 模型版本管理规范
	1.3 测试工具与评测框架配置验证	1.3.1 能配置多模态评测工具链 1.3.2 能依据测试需求，配置评测框架的评测指标、评分规则 1.3.3 能排查并修正配置错误或异常结果	1.3.1 多模态评测工具链配置方法 1.3.2 评测指标与规则配置方法 1.3.3 配置异常排查与修正方法
	1.4 测试数据采集	1.4.1 能依据测试用例，采集测试所需的多模态数据 1.4.2 能使用数据处理工具，完成多模态数据的预处理操作 1.4.3 能依据测试需求，分类标注测试数据	1.4.1 多模态数据采集方法 1.4.2 数据清洗算法与预处理操作规范 1.4.3 数据标注规范
	1.5 测试提示	1.5.1 能依据测试需求文档，构建	1.5.1 需求文档解析方法

	词集质量检查	覆盖用户使用场景的测试提示词 1.5.2 能按照模板，为每条测试提示词标注测试目标与预期输出 1.5.3 能在测试执行前，对提示词进行去重与一致性检查等预处理	1.5.2 提示词设计原则、框架及方法 1.5.3 不同类型提示词的构造方法
2.行为测试	2.1 生成能力测试	2.1.1 能根据生成能力测试要求，测试文本、图像、语音多模态生成任务 2.1.2 能按照文本相关度、图像匹配度、语音准确性等标准化质量维度，评估生成结果 2.1.3 能使用数据分析工具，统计生成内容成功率、异常输出比例等测试分析结果	2.1.1 多模态生成任务测试方法 2.1.2 生成结果质量指标 2.1.3 测试结果统计与分析工具使用方法
	2.2 任务执行与工具使用能力测试	2.2.1 能依据测试用例，测试跨模态检索增强、多工具联动、多轮任务链等场景下的模型能力 2.2.2 能使用测试分析工具，分析触发准确率、任务完成率、输入输出格式符合率等量化指标 2.2.3 能对测试中的失败情况进行分类，记录异常触发条件	2.2.1 跨模态检索增强技术 2.2.2 多工具联动方法 2.2.3 多轮任务链调用方法 2.2.4 测试工具使用方法 2.2.5 异常触发的类型
	2.3 上下文与记忆能力测试	2.3.1 能测试信息延续、问题追问、意图变更、实体修改等多场景的跨轮对话 2.3.2 能使用对话评估工具，统计模型在多轮对话中的上下文保持成功率、失忆率与回答漂移率等指标 2.3.3 能分析上下文不一致与记忆丢失等缺陷原因，定位问题发生的环节	2.3.1 跨轮次一致性评估指标计算方法 2.3.2 长期对话稳定性测试规范与失忆率统计逻辑 2.3.3 多样化追问策略设计方法及评估标准 2.3.4 提示词优化对记忆的影响
	2.4 语言理解与推理能力测试	2.4.1 能依据测试用例，在多场景下，测试模型事实回答、指令遵循、逻辑问题等多类型综合指令的语言理解与推理能力 2.4.2 能使用知识库或可信数据源，验证模型生成的事实性内容 2.4.3 能使用语义分析工具，统计	2.4.1 语义分析工具使用方法 2.4.2 可信数据源使用规范 2.4.3 逻辑谬误类型与表现形式 2.4.4 文本问题的识别方法

		语义理解准确率、实体识别正确率等指标 2.4.4 能识别指代歧义、逻辑矛盾、实体关系混淆等问题，并分类统计其结果	
	2.5 场景化任务与行业适配测试	2.5.1 能测试多行业、多场景下的模型适配性 2.5.2 能归类行业术语与业务偏差 2.5.3 能基于场景测试结果，定位模型适配问题的主要触发条件	2.5.1 行业典型应用场景 2.5.2 行业术语与业务流程偏差 2.5.3 场景任务结果统计与问题归纳的方法
3.性能测试	3.1 推理性能评估	3.1.1 能执行多步推理和条件推理等多种任务的性能测试 3.1.2 能识别模型在不同推理任务中的性能差异 3.1.3 能根据测试结果，对照预设的基线要求判断性能数据的达成度	3.1.1 模型推理任务性能测试与差异分析方法 3.1.2 模型性能测试基线标准
	3.2 模型稳定性与鲁棒性测试	3.2.1 能在预设测试条件下，对同类样本进行批量测试，分析模型输出的一致性与波动情况 3.2.2 能按照测试需求，构建语句残缺、语序调整和指令歧义等扰动测试用例 3.2.3 能通过边界和异常输入测试，评估系统的容错能力 3.2.4 能执行长时间的稳定性压力测试，监控系统的内存泄漏或性能衰减迹象	3.2.1 稳定性测试执行规范 3.2.2 自然语言扰动构造方法 3.2.3 系统容错机制分析方法 3.2.4 稳定性测试与内存监控方法
	3.3 可扩展性与并发性能测试	3.3.1 能配置测试工具，测定系统的最大并发量 3.3.2 能在预设的扩展方案条件下，分别执行扩展前与扩展后的并发测试，形成可对比数据 3.3.3 能统计不同并发与扩展条件下的平均响应时间、吞吐量和错误率等性能数据	3.3.1 并发测试策略执行流程 3.3.2 并发或负载测试实施方法 3.3.3 可扩展性与并发性能测试数据的采集、记录与结构化存储方法
4.安全测试	4.1 系统供应链安全测试	4.1.1 能分析供应链组件漏洞详情，验证漏洞有效性并排除误报	4.1.1 漏洞有效性验证方法与误报清洗规则

		4.1.2 能评估供应链及运行环境等安全，识别容器镜像的分层风险 4.1.3 能监测上游组件演进动态，识别版本更迭带来的安全回归风险	4.1.2 供应链与运行环境加固基线 4.1.3 容器镜像分层安全机制 4.1.4 动态监测与版本安全回归风险识别方法
	4.2 隐私与数据安全测试	4.2.1 能针对隐私保护需求，设计专项测试用例，评估模型对提示词隐私保护指令的执行情况 4.2.2 能模拟提示词注入、上下文诱导等攻击场景，测试模型间接隐私泄露防护能力 4.2.3 能分析隐私风险等级并编写测试报告，区分直接、间接和提示词等不同泄露类型	4.2.1 模型隐私间接泄露识别方法 4.2.2 提示词注入攻击原理 4.2.3 隐私风险等级分析方法
	4.3 模型对抗性安全测试	4.3.1 能判定模型在对抗输入下的安全策略触发情况与输出合规性 4.3.2 能统计并分析对抗攻击成功率等安全指标 4.3.3 能使用自动化脚本执行批量对抗测试	4.3.1 模型对抗输出合规性判定标准 4.3.2 模型对抗安全指标 4.3.3 自动化脚本与批量对抗测试方法
	4.4 智能体自主交互安全测试	4.4.1 能构建交互测试场景，验证智能体行为边界与鉴权机制 4.4.2 能在多轮、自主推进的交互中，识别逐步出现的策略漂移或安全边界弱化现象 4.4.3 能测试多工具调用与资源访问控制的安全性，追踪越权路径并形成分析结论	4.4.1 智能体行为边界验证方法 4.4.2 策略漂移和安全边界弱化识别方法 4.4.3 越权链路分析方法
5.伦理评估	5.1 伦理与合规性审查	5.1.1 能判断对应的行业领域生成内容中包含免责声明等必要内容 5.1.2 能构造包含不同性别、年龄、职业、地域等属性的测试输入，比较模型在相同任务条件下的输出差异 5.1.3 能对伦理与合规问题进行分类并判定严重程度	5.1.1 行业领域信息披露规范 5.1.2 公平性测试中敏感属性差异判定依据 5.1.3 伦理与合规问题的分类标准

	5.2 误导性内容识别与可解释性验证	5.2.1 能在多轮对话与不同表达方式下，识别因隐性误导、断章取义或过度简化等导致的误导内容 5.2.2 能执行多维度的可解释性验证，评估模型决策逻辑与人类认知逻辑的一致性 5.2.3 能分类归纳误导性内容	5.2.1 多轮对话中误导的形式 5.2.2 多轮对话中误导识别方法 5.2.3 多维度的可解释性验证方法

3.3 二级/技师

职业功能	工作内容	技能要求	相关知识要求
1. 测试环境准备	1.1 测试需求分析	1.1.1 能分析生成式人工智能系统的功能结构、应用模式与运行边界，编写结构化测试需求分析报告 1.1.2 能结合生成式人工智能系统的业务场景特性，设计可量化的质量指标 1.1.3 能梳理合规与安全的约束边界，将各类约束要求转化为测试判定依据	1.1.1 结构化测试需求分析方法 1.1.2 场景化测试指标构建方法 1.1.3 数据与内容安全规范
	1.2 环境构建	1.2.1 能设计并构建分布式推理环境 1.2.2 能编写模型版本识别和兼容性验证的自动化脚本 1.2.3 能监控和分析测试过程中的资源使用情况，识别性能瓶颈 1.2.4 能配置和管理容器化的模型部署环境	1.2.1 分布式系统架构与部署方法 1.2.2 模型版本兼容性验证方法 1.2.3 模型性能监控与优化方法 1.2.4 容器化技术与微服务架构
	1.3 测试工具与评测框架配置验证	1.3.1 能根据不同测试目标，选择并配置适应的测试工具或评测框架 1.3.2 能验证工具与评测框架的适配性 1.3.3 能依据测试需求，选择并集成对抗性测试与鲁棒性评测工具	1.3.1 对抗性测试方法 1.3.2 鲁棒性测试方法 1.3.3 评测框架适配能力的验证方法
	1.4 测试数据	1.4.1 能针对跨领域业务需求，	1.4.1 数据工程与数据项

	采集	设计并实施多场景融合的数据集构建方案 1.4.2 能评估数据质量，撰写数据质量报告 1.4.3 能编写数据预处理自动化脚本	目管理方法 1.4.2 数据治理规范的相关内容 1.4.3 数据质量评估方法 1.4.4 测试数据自动化工具原理与应用方法
	1.5 测试提示词集设计	1.5.1 能依据模型功能范围，设计覆盖不同能力维度的提示词 1.5.2 能针对同一测试目标，构建多种表达方式的等价提示词 1.5.3 能设计包含歧义、约束冲突或上下文依赖的测试提示词	1.5.1 模型功能需求解析方法 1.5.2 等价提示词的定义与构造方法 1.5.3 歧义、约束冲突、上下文依赖的测试提示词的设计方法
2.行为测试	2.1 生成能力测试	2.1.1 能依据测试方案中的测试提示词，进行代码生成等专业领域测试，并分析模型输出结果 2.1.2 能识别表面形式正确，但不符合需求的隐性问题 2.1.3 能依据模型功能范围，设计覆盖创作生成、指令遵循、结构化生成等能力的测试用例	2.1.1 隐性缺陷的识别方法 2.1.2 模型生成能力的测试用例设计方法
	2.2 任务执行与工具使用能力测试	2.2.1 能依据模型能力范围，设计检索增强（RAG）边界测试、多模态工具联动等多场景的测试用例 2.2.2 能分析定位模型多任务链执行过程中的问题 2.2.3 能开发多任务链、多工具联动测试的自动化脚本	2.2.1 RAG 边界测试方法 2.2.2 任务链阻塞分析方法 2.2.3 联动测试自动化脚本编写方法
	2.3 上下文与记忆能力测试	2.3.1 能依据测试需求，设计覆盖不同上下文长度与复杂度的测试用例 2.3.2 能设计长期对话稳定性评估指标，量化不同对话时长、不同业务场景下的记忆保持率与一致性准确率 2.3.3 能通过日志分析与测试工具，定位上下文不一致和记忆衰减的触发条件	2.3.1 大语言模型搜索方法及序列任务生成原理 2.3.2 长期记忆增强框架核心原理 2.3.3 上下文一致性的分析方法 2.3.4 对话测试自动化脚本开发与优化规范

		2.3.4 能设计覆盖高频重复测试场景跨轮对话的自动化测试脚本	
	2.4 语言理解与推理能力测试	2.4.1 能针对多步骤的数学问题、条件判断链、双重否定及讽刺、隐喻等特定能力维度，设计专项评测方案 2.4.2 能构建多轮推理对话场景，测试模型的逻辑链条完整性 2.4.3 能依据测试方案，量化评估模型的推理能力 2.4.4 能定位推理能力中的缺陷并分析原因	2.4.1 指令分解与任务规划方法 2.4.2 逻辑推理模型评测方案的设计方法 2.4.3 模型推理能力缺陷定位方法 2.4.4 推理能力缺陷根因分析方法
	2.5 场景化任务与行业适配测试	2.5.1 能依据行业业务流程构建场景任务测试用例 2.5.2 能识别行业适配中的专业性偏差与潜在风险 2.5.3 能基于量化指标，评价模型行业适配能力	2.5.1 行业业务流程与关键任务节点的分析方法 2.5.2 行业适配偏差类型与风险的识别规则 2.5.3 模型的行业适配能力的评估方法
3.性能测试	3.1 推理性能评估	3.1.1 能依据模型能力特征，设计覆盖推理步数变化、上下文长度变化等不同推理复杂度的性能测试用例 3.1.2 能构造包含并发请求的测试场景，评估模型在负载变化条件下的推理性能 3.1.3 能分析性能数据，定位性能瓶颈，分析性能下降的原因 3.1.4 能编写自动化脚本，定期执行性能回归测试并生成报告	3.1.1 推理复杂度测试用例设计方法 3.1.2 并发负载测试场景设计方法 3.1.3 系统性能瓶颈诊断方法 3.1.4 自动化测试脚本编写方法
	3.2 模型稳定性与鲁棒性测试	3.2.1 能依据模型能力特征，设计覆盖输入噪声、上下文变化和参数边界等多种扰动类型的测试用例 3.2.2 能构造连续运行或高频调用场景，验证模型在长时间运行条件下的稳定性 3.2.3 能分析测试结果，识别模型在不同扰动下出现的事实、逻	3.2.1 鲁棒性测试扰动类型 3.2.2 鲁棒性测试场景设计方法 3.2.3 模型压力测试与疲劳测试方法 3.2.4 模型错误类型

		辑和格式等错误问题	
	3.3 可扩展性与并发性能测试	3.3.1 能设计并发逐级递增测试方案，定位系统的性能拐点 3.3.2 能分析定位高并发场景下的性能瓶颈 3.3.3 能结合测试结果，分析系统在扩展条件下未产生预期性能提升的原因	3.3.1 并发负载测试策略与性能拐点识别方法 3.3.2 性能瓶颈定位方法 3.3.3 性能提升的方法
4.安全测试	4.1 系统供应链安全测试	4.1.1 能设计自动生成软件物料清单的工具 4.1.2 能构建依赖混淆、组件投毒攻击等测试场景，验证供应链引入渠道的安全性 4.1.3 能建立外部模型仓库监测与预警机制，识别开源生态中的投毒风险	4.1.1 供应链安全集成技术 4.1.2 软件物料的供应链清单标准 4.1.3 依赖混淆、组件投毒攻击方法
	4.2 隐私安全测试	4.2.1 能设计包含成员推断、属性推断等技术的隐私攻击测试用例 4.2.2 能量化评估模型隐私泄露风险的等级 4.2.3 能配置并使用自动化工具检测提示词隐私泄露	4.2.1 隐私攻击的类型 4.2.2 隐私泄露风险量化评估方法 4.2.3 提示词隐私安全测试方法 4.2.4 隐私泄露自动化检测工具的配置与使用方法
	4.3 模型对抗性安全测试	4.3.1 能依据模型安全机制，设计覆盖多种攻击路径的对抗性测试用例 4.3.2 能构建包含上下文诱导、条件嵌套等对抗类型的测试场景，验证模型在对抗条件下的安全性 4.3.3 能结合测试数据，定位模型在对抗防御中的失效触发条件 4.3.4 能编写批量对抗测试自动化脚本	4.3.1 攻击路径的类型 4.3.2 对抗场景构造方法 4.3.3 防御失效分析方法 4.3.4 批量对抗测试自动化脚本的编写方法
	4.4 智能体自主交互安全测试	4.4.1 能构建覆盖长期运行、多条件触发和任务嵌套等维度的智能体自主交互测试场景 4.4.2 能分析智能体在决策路径	4.4.1 智能体自主交互测试场景构建方法 4.4.2 决策路径与行为链条中的隐性安全分析方法

		与行为链条中的隐性安全失效点 4.4.3 能归纳总结智能体在自主交互中出现的风险模式	4.4.3 智能体交互风险特征
5.伦理评估	5.1 伦理与合规性审查	5.1.1 能设计弱约束提示、模糊指令和边界问题等多类型伦理与合规性测试场景 5.1.2 能结合测试结果，分析模型在长期交互中的伦理立场漂移或合规规则失效的现象 5.1.3 能总结模型伦理与合规问题的触发模式与高风险场景	5.1.1 伦理与合规性测试场景的设计方法 5.1.2 模型伦理立场稳定性与规则一致性的评估原理 5.1.3 伦理立场漂移的判断标准
	5.2 误导性内容识别与可解释性验证	5.2.1 能设计覆盖不同知识领域的误导性内容测试场景 5.2.2 能在输入条件、上下文继承与中间决策结果等构成的生成链路中，定位误导性内容产生的环节 5.2.3 能总结隐性误导的形式与触发条件 5.2.4 能基于输入条件、上下文信息与模型生成结果，定位解释缺失或逻辑断裂的具体环节	5.2.1 多领域误导性内容测试场景的设计方法 5.2.2 生成式人工智能生成链路中的错误传播机制 5.2.3 隐形误导内容的形式与触发条件特征
6.培训与指导	6.1 培训	6.1.1 能编写培训计划与讲义 6.1.2 能根据讲义制作培训课件 6.1.3 能对三级/高级工及以下级别人员开展知识和技能培训	6.1.1 技术培训制度与流程 6.1.2 培训课件制作方法 6.1.3 进阶培训教学方法
	6.2 指导	6.2.1 能制订生成式人工智能系统测试人员的技能提升计划 6.2.2 能审核三级/高级工及以下级别人员的测试结果，提出改进建议	6.2.1 实践教学方法 6.2.2 技术指导方法 6.2.3 测试结果的审核要点与评价标准

3.4 一级/高级技师

职业功能	工作内容	技能要求	相关知识要求
1. 测试环境准备	1.1 测试需求分析	1.1.1 能将测试需求转化为不同领域专属测试点 1.1.2 能从系统整体角度，评估	1.1.1 领域专属测试点设计方法 1.1.2 测试需求评估方法

		测试需求的完整性、一致性与可执行性	
	1.2 环境构建	1.2.1 能设计测试环境架构，整合多种推理框架和工具链 1.2.2 能建立模型版本管理和控制的标准化流程 1.2.3 能实现测试环境的自动化部署和运维监控 1.2.4 能设计并配置安全策略	1.2.1 推理架构设计方法 1.2.2 版本管理规范 1.2.3 自动化运维方法 1.2.4 网络安全与访问控制规范
	1.3 测试工具设计与开发	1.3.1 能设计与搭建智能评测中台 1.3.2 能开发多模态多轮交互、分布式推理等场景下的测试工具	1.3.1 智能评测中台架构设计方法 1.3.2 多源评测工具评估方法 1.3.3 测评工具适配性与有效性验证方法
	1.4 测试提示词集覆盖规划	1.4.1 能规划重点测试领域提示词集的数量、结构、类型等 1.4.2 能依据提示词覆盖率指标，评估测试提示词集质量 1.4.3 能针对模型新增能力或已知问题，动态优化测试提示词集	1.4.1 提示词集规划方法 1.4.2 提示词集质量评估率方法 1.4.3 提示词集的迭代管理与版本控制方法
2.行为测试	2.1 生成能力测试	2.1.1 能构建生成能力的自动化测试框架 2.1.2 能基于测试目标，设计生成能力测试指标，编写领域专属的生成能力测试方案 2.1.3 能设计可复用的生成能力测试方法与流程规范 2.1.4 能设计生成质量评价指标，量化评估测试结果	2.1.1 自动化测试框架的构建方法 2.1.2 生成能力测试方案构建方法 2.1.3 可复用的测试方法与流程规范设计方法 2.1.4 应用领域生成能力测试方案定制方法 2.1.5 生成质量评价指标的设计方法
	2.2 任务执行与工具使用能力测试	2.2.1 能基于系统应用目标，设计覆盖多工具协同、多模态任务链等需求的测试方案 2.2.2 能设计覆盖任务完成率、步骤效率、资源消耗等多维度的执行能力评估体系 2.2.3 能构建任务执行与工具使用的自动化测试框架	2.2.1 多工具协同、多模态任务链测试方案设计方法 2.2.2 执行能力评估体系设计方法 2.2.3 自动化测试框架集成方法

	2.3 上下文与记忆能力测试	2.3.1 能搭建分布式上下文与记忆能力测试架构，集成多模态对话测试工具 2.3.2 能设计长期对话压力测试指标与方案，评估模型在极限上下文窗口下的记忆稳定性与一致性 2.3.3 能优化上下文与记忆能力测试流程，构建测试规范	2.3.1 分布式测试环境搭建方法 2.3.2 多模态工具集成方法 2.3.3 上下文与记忆能力测试的流程优化方法 2.3.4 上下文与记忆能力测试规范构建方法
	2.4 语言理解与推理能力测试	2.4.1 能设计覆盖多领域、多语言场景的语言理解与推理测试指标及方案 2.4.2 能设计逻辑陷阱等方面的对抗性测试用例 2.4.3 能使用推理工具，分析并验证模型推理的决策路径 2.4.4 能设计语言理解准确率、推理正确率、推理链完整率等量化指标	2.4.1 跨领域语言理解测试设计原则 2.4.2 对抗性测试用例设计方法 2.4.3 推理工具的使用方法 2.4.4 语言理解与推理能力相关量化评估指标的设计方法
	2.5 场景化任务与行业适配测试	2.5.1 能构建行业场景化任务测试指标与方案 2.5.2 能基于测试结果编写模型的行业适配性测试报告 2.5.3 能解读场景化任务与行业适配测试结果，为面向场景化或行业交付提供决策建议	2.5.1 场景化任务测试方案构建方法 2.5.2 行业适配性评价指标的设计规则 2.5.3 行业适配性报告编制的方法 2.5.4 行业适配性测试结果解读方法
3.性能测试	3.1 推理性能评估	3.1.1 能基于系统应用需求，设计推理性能评估指标与方案 3.1.2 能针对量化、编译优化等不同优化技术对性能指标的影响，提出优化技术选型建议 3.1.3 能解读性能评估结果，为系统优化提供决策建议	3.1.1 推理性能评估方法 3.1.2 优化技术选型方法 3.1.3 性能评估数据解读方法
	3.2 模型稳定性与鲁棒性测试	3.2.1 能基于系统应用要求，设计包括扰动策略和判定标准等内容的稳定性与鲁棒性测试指标与方案 3.2.2 能结合业务领域需求，分	3.2.1 稳定性与鲁棒性多维度测试的设计原则 3.2.2 特定业务场景下稳定性与鲁棒性的风险评估方法

		析稳定性或鲁棒性的风险 3.2.3 能解读稳定性与鲁棒性评估结果，为部署架构优化与系统上线决策提供意见	3.2.3 稳定性与鲁棒性数据测试结果解读方法
	3.3 可扩展性与并发性能测试	3.3.1 能根据系统业务场景和使用规模，设计可扩展性与并发性能测试指标与方案 3.3.2 能设计扩展与并发能力评价方法，量化最大并发承载能力、稳定运行区间和扩展效率等指标 3.3.3 能解读可扩展性与并发性能评估结果	3.3.1 扩展与并发性联合测试框架设计方法 3.3.2 扩展与并发能力评价指标体系设计方法 3.3.3 可扩展性与并发性能数据分析方法
4.安全测试	4.1 系统供应链安全测试	4.1.1 能设计供应链安全风险的测试指标与方案 4.1.2 能分析人工智能系统软件物料清单，绘制组件依赖风险图谱 4.1.3 能建立外部交付模型与数据的安全验收办法 4.1.4 能设计供应链安全事件应急响应方案，完成攻击溯源与风险定性	4.1.1 供应链安全测试方案设计方法 4.1.2 软件物料清单依赖分析技术 4.1.3 交付模型与数据安全验收标准 4.1.4 供应链攻防机制与对抗原理
	4.2 隐私与数据安全测试	4.2.1 能构建隐私与数据安全测试指标与方案 4.2.2 能设计可复用的，覆盖数据采集、处理、存储和输出等环节的隐私与数据安全测试流程与规范 4.2.3 能评估隐私增强技术在不同场景下的效能损耗与保护强度并提供选型建议 4.2.4 能评估数据跨境传输的合规性	4.2.1 数据泄露风险监测机制设计方法 4.2.2 提示词隐私安全测试方案设计方法 4.2.3 隐私增强技术评估方法 4.2.4 数据主权与跨境传输合规要求
	4.3 模型对抗性安全测试	4.3.1 能设计模型对抗性安全测试指标与方案 4.3.2 能设计可复用的对抗性安全测试方法、攻击库与流程规范 4.3.3 能结合业务风险场景，分	4.3.1 生成式模型对抗攻击机理 4.3.2 对抗性安全测试方案的相关内容 4.3.3 对抗安全量化指标

		析对抗性安全缺陷对系统整体安全的影响 4.3.4 能对模型对抗性安全测试结果进行综合解读，为安全策略调整、模型上线审查与风险控制提供建议	体系设计方法 4.3.4 系统性安全影响分析方法 4.3.5 风险研判模型的特征 4.3.6 安全决策机制
	4.4 智能体自主交互安全测试	4.4.1 能设计智能体自主交互安全测试指标与方案 4.4.2 能制订自主交互安全测试技术规范 4.4.3 能评估系统自主交互在业务安全、运行稳定性与合规性等方面的风险 4.4.4 能解读智能体自主交互安全测试数据，为架构设计、控制策略调整和上线审核提供建议	4.4.1 智能体安全测试方案设计方法 4.4.2 安全评估指标设计方法 4.4.3 自主交互风险评估方法 4.4.4 自主交互安全测试数据分析方法
5.伦理评估	5.1 伦理与合规性审查	5.1.1 能依据法律法规、行业规范及组织内部制度，编制伦理与合规性审查清单与方案 5.1.2 能制订合规评估审查与审计的标准化流程 5.1.3 能评估系统在不同应用场景下，伦理与合规风险的发生概率与潜在影响范围 5.1.4 能解读伦理与合规性审查结果	5.1.1 伦理与合规性审查清单的设计方法 5.1.2 伦理与合规性审查方案的设计方法 5.1.3 伦理与合规性审查标准化流程的设计方法 5.1.4 伦理与合规风险概率与影响范围的评估方法 5.1.5 伦理与合规性审查结果的分析方法
	5.2 误导性内容识别与可解释性验证	5.2.1 能设计误导性内容识别与可解释性验证测试指标与方案 5.2.2 能制订覆盖数据、模型、提示、运行日志等环节的可解释性测试流程与规范 5.2.3 能解读误导性内容识别与可解释性验证的测试结果	5.2.1 误导性内容识别方案的设计方法 5.2.2 可解释性验证方案的设计方法 5.2.3 误导性内容识别指标的设计方法 5.2.4 可解释性指标的设计方法 5.2.5 误导性风险评估的方法
6.培训与指导	6.1 培训	6.1.1 能制订培训体系规划 6.1.2 能审核二级/技师制作课件内容	6.1.1 培训体系构建方法 6.1.2 管理培训方法 6.1.3 培训效果评估方法

		6.1.3 能对二级/技师及以下级别人员开展管理方法培训 6.1.4 能评估二级/技师培训效果	
	6.2 指导	6.2.1 能制订业务指导策略体系 6.2.2 能对二级/技师及以下进行业务指导	6.2.1 业务指导策略体系编制方法 6.2.2 生成式人工智能系统测试前沿理论

征求意见稿

7. 权重表

4.1 理论知识权重表

技能等级 \ 项目		四级/中级工（%）	三级/高级工（%）	二级/技师（%）	一级/高级技师（%）
基本要求	职业道德	5	5	5	5
	基础知识	15	15	10	10
相关知识要求	测试环境准备	40	30	15	10
	行为测试	20	15	15	15
	性能测试	10	15	20	20
	安全测试	5	10	15	20
	伦理评估	5	10	15	15
	培训与指导	-	-	5	5

4.2 技能要求权重表

技能等级 \ 项目		四级/中级工（%）	三级/高级工（%）	二级/技师（%）	一级/高级技师（%）
相关技能要求	测试环境准备	50	40	20	10
	行为测试	25	20	20	15
	性能测试	15	20	25	25
	安全测试	5	10	15	25
	伦理评估	5	10	15	20
	培训与指导	-	-	5	5