ICS 35.240
CCS L60

# T/ZSIA

浙 江 省 软 件 行 业 协 会 团 体 标 准

T/ZSIA 0004-202X

# 职业人员人工智能技术能力评估规范

Specification for the evaluation of artificial intelligence technical proficiency of technological practitioner

（征求意见稿）

202X - XX - XX 发布　　202X - XX - XX 实施

浙江省软件行业协会　　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。

本文件代替T/ZSIA 0004—2023《职业人员人工智能技术能力评估规范》，与T/ZSIA 0004—2023相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了“生成式人工智能基础”专业知识要求（见5.2.4、6.2.3、7.2.3）；

b) 增加了“智能体基础”专业知识要求（见5.2.5、6.2.4、7.2.4）；

c) 增加了“伦理与合规能力要求”（见5.5、6.5、7.5）；

d) 增加了“生成式人工智能应用能力”应用能力要求（见5.4.3、6.4.3、7.4.3）；

e) 增加了“智能体应用能力”应用能力要求（见5.4.4、6.4.4、7.4.4）；

f) 修改了“范围”的适用描述（见第1章，2023年版的第1章）；

g) 增加了规范性引用文件（见第2章）；

h) 修改了“评估要素”，将评估要素从3大类9小类调整为4大类15小类（见第4章，2023年版的第4章）；

i) 在各能力要求中增加了开放性表述，以适应人工智能技术的快速发展（见第5章、第6章、第7章）。

请注意本文件的某些内容可能涉及专利。本文件发布机构不承担识别专利的责任。

本文件由浙江省软件行业协会提出、归口并组织实施。

本文件起草单位：浙江省软件行业协会、浙江大学人工智能研究所、网易（杭州）网络有限公司、创业慧康科技股份有限公司、浙大网新科技股份有限公司、信雅达科技股份有限公司、浙江邦盛科技股份有限公司、杭州科技职业技术学院、浙江捷众科技股份有限公司、纳里健康科技有限公司、杭州小影创新科技股份有限公司、浙江和达科技股份有限公司、杭州永荣实业有限公司、诺基亚通信系统技术（北京）有限公司浙江分公司、杭州一蓦信息科技有限公司、浙江一山智慧医疗研究有限公司。

本文件主要起草人：……。

本文件及其所代替文件的历次版本发布情况为：

2023年首次发布为T/ZSIA 0004—2023；

本次为第一次修订。

# 职业人员人工智能技术能力评估规范

## 1 范围

本文件规定了职业人员人工智能技术能力评估要素、初级能力要求、中级能力要求、高级能力要求和评估管理要求。

本文件适用于指导从事人工智能技术开发与应用的相关人员开展人工智能技术能力的评估。

## 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 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

GB/T 45288.3—2025 人工智能 大模型 第3部分：服务能力成熟度评估

GB/T 45654—2025 网络安全技术 生成式人工智能服务安全基本要求

## 3 术语和定义

上述引用文件界定的以及下列术语和定义适用于本文件。

3.1

**能力评估 capability evaluation**

评估个人在特定领域或任务中的技能、知识和能力水平，衡量其在特定领域内的表现和能力。

3.2

**工程能力 engineering capability**

工程师或技术人员在实践中应用科学和技术知识、技能和经验的能力。包括设计、开发、测试、维护和改进工程系统或产品的能力。

3.3

**代码规范 code specification**

一组约定俗成的准则和规则，用于指导开发人员编写清晰、可读性强、易于维护的代码。

3.4

**算法 algorithms**

一组由计算机程序实现，用于能够在有限时间内解决特定问题或执行特定任务的有序步骤。

3.5

**模型 model**

一种可以从输入数据中学习规律，用于预测未知数据的输出值或进行其他任务的计算机程序或算法。

3.6

**模型部署与运维能力 model deployment and O&M capabilities**

在机器学习或深度学习项目中将训练好的模型成功部署到生产环境，并保证其稳定运行和高效维护的能力。

3.7

**计算机视觉 computer vision**

一种涉及计算机和数字图像处理的技术，通过使用数字图像和视频来模拟人类视觉系统，并进行自动化分析和理解。

3.8

**生成式人工智能 generative artificial intelligence**

能够基于学习到的数据分布生成新的内容（文本、图像、音频、视频、代码等）的人工智能技术，包括大语言模型、多模态模型等。

3.9

**提示词工程 prompt engineering**

通过设计和优化输入提示词，以引导大模型生成符合预期目标（如特定格式、风格、内容）的输出的一整套技术和方法。

3.10

**智能体 agent**

能够感知环境、自主决策并执行动作以实现特定目标的实体，包括基于大语言模型的智能体（LLM Agent）、代码智能体（Coding Agent）、自主智能体（Autonomous Agent）等。

3.11

**技能 skill**

智能体可调用的原子能力单元，包括工具调用、API接口、代码执行、数据库查询等可复用功能模块。

3.12

**子智能体 subagent**

被父智能体调度管理的从属智能体，实现任务分解、并行处理与结果聚合。

3.13

**工具使用机制 tool use; function calling**

智能体通过结构化输出调用外部工具扩展能力范围的技术机制。

3.14

**MCP协议 model context protocol**

标准化智能体与外部工具、数据源交互的开放协议。

3.15

**多智能体系统 multi-agent system**

多个智能体通过协作、竞争或通信完成复杂任务的系统架构。

3.16

**低代码智能体平台 low-code agent platform**

通过可视化界面和拖拽式操作快速构建智能体的开发平台。

3.17

**伦理与合规 ethics and compliance**

在人工智能系统的设计、开发、部署和应用过程中，遵循法律法规、社会伦理、隐私保护、公平性、透明性、可控性等原则的要求。具体包括增进人类福祉、促进公平公正、保护隐私安全、确保可信可控等内容。

## 4 评估要素

职业人员人工智能技术能力评估标准，能力级别分为初级、中级、高级三个级别。

人工智能技术能力评估要素主要包括专业知识、工程能力、应用能力和伦理与合规能力共4大类15小类（见图 1）。其中，专业知识包括编程基础、数据分析基础、机器学习基础、神经网络基础、生成式人工智能基础、智能体基础；工程能力包括代码规范能力、算法模型实现能力、模型部署与运维能力；应用能力包括行业知识能力、业务应用能力、生成式人工智能应用、智能体应用能力；伦理与合规能力为各等级必备基础能力，分为基础伦理意识、伦理风险评估、伦理治理体系三个层次。各级别对要素要求见表 1。

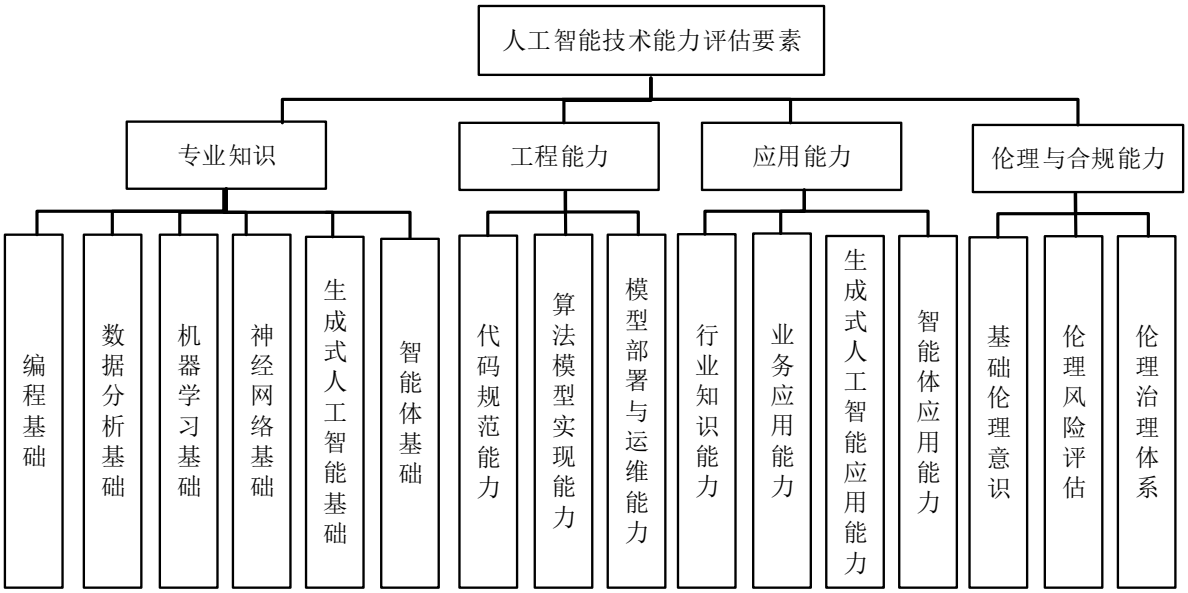


**图1　人工智能技术能力评估要素图**

**表1　人工智能技术能力评估要素要求**

| 要素 | | 等级 | | |
|---|---|---|---|---|
| | | 初级 | 中级 | 高级 |
| 专业知识 | 编程基础 | ★☆☆ | ★★☆ | ★★★ |
| | 数据分析基础 | ★☆☆ | ★★☆ | ★★★ |
| | 机器学习基础 | ★☆☆ | ★★☆ | ★★★ |
| | 神经网络基础 | ☆☆☆ | ★☆☆ | ★★★ |
| | 生成式人工智能基础 | ★☆☆ | ★★☆ | ★★★ |
| | 智能体基础 | ★☆☆ | ★★☆ | ★★★ |
| 工程能力 | 代码规范能力 | ★☆☆ | ★☆☆ | ★★★ |
| | 算法模型实现能力 | ★☆☆ | ★★☆ | ★★★ |
| | 模型部署与运维能力 | ★☆☆ | ★★☆ | ★★★ |
| 应用能力 | 行业知识能力 | ★☆☆ | ★★☆ | ★★★ |
| | 业务应用能力 | ★☆☆ | ★★☆ | ★★★ |
| | 生成式人工智能应用能力 | ★☆☆ | ★★☆ | ★★★ |
| | 智能体应用能力 | ★☆☆ | ★★☆ | ★★★ |
| 伦理与合规能力 | 基础伦理意识 | ★☆☆ | ★★☆ | ★★★ |
| | 伦理风险评估 | ★☆☆ | ★★☆ | ★★★ |
| | 伦理治理体系 | ★☆☆ | ★★☆ | ★★★ |
| 注1：覆盖的业务场景包括但不限于智能医疗、智能交通、智能家居、智能制造、智能金融、智慧零售、智能通信、智慧教育等领域。<br>注2：等级符号说明：★☆☆代表熟悉；★★☆代表掌握；★★★代表精通；☆☆☆代表不作要求。 | | | | |

## 5　初级能力要求

### 5.1　基本要求

掌握编程语言使用技巧与特性，理解机器学习基础算法、熟练使用编程语言对给定数据任务选择合适的模型设计方案，能够完成基础数据分析和机器学习建模类工作。具备使用生成式人工智能

完成基础任务及应用的能力，了解提示工程基础方法，能够识别内容安全风险。具备使用多样化智能体应用的能力，能够使用低代码平台搭建简单智能体，了解人机协作基础模式。具备基础人工智能伦理意识，能够识别常见伦理风险，了解数据隐私保护和合规基本要求。

## 5.2 专业知识要求

### 5.2.1 编程基础

应具备程序开发经验，包括但不限于以下内容：

a) 能够熟练地使用人工智能开发常用编程语言；
b) 掌握数据分析与机器学习建模等相关的第三方库；
c) 能够使用面向对象的编程语言实现给定需求。

### 5.2.2 数据分析基础

应具备数据分析和可视化能力，包括但不限于以下内容：

a) 能够对原始数据进行数据清洗、数据聚合等预处理；
b) 能够利用数据进行特征工程，构造新的数据指标；
c) 能够对数据进行可视化呈现。

### 5.2.3 机器学习基础

应具备使用机器学习模型解决问题的能力，包括但不限于以下内容：

a) 熟悉一种以上分类算法的原理；
b) 熟悉一种以上回归算法的原理；
c) 熟悉一种以上聚类算法的原理；
d) 具备机器学习模型的使用及调优经验等。

### 5.2.4 生成式人工智能基础

应具备使用生成式人工智能完成基础任务的能力，包括但不限于以下内容：

a) 了解大语言模型的基本工作原理，如：预训练、生成；
b) 能够使用主流大模型 API，完成文本生成、摘要、分类等任务；
c) 具备基础的提示词工程意识，能够编写简单的结构化提示，如：角色设定、任务描述、输出格式要求等；
d) 了解生成式人工智能的内容安全风险，如幻觉、偏见、有害内容等，能够识别并上报明显风险输出。

### 5.2.5 智能体基础

应具备智能体技术基础认知与多样化应用能力，包括但不限于以下内容：

a) 了解智能体的基本概念、架构与工作原理（感知、决策、执行）；
b) 了解技能（Skill）与工具（Tool）的区别与联系；
c) 能够使用多样化的智能体应用，例如：人工智能编程助手、办公智能体、创意智能体、生活智能体；
d) 能够使用低代码智能体平台，搭建简单的对话式智能体，了解可视化工作流编排基础；
e) 了解人机协作的基本模式，能够评估智能体输出质量并进行必要的人工干预。

## 5.3 工程能力要求

### 5.3.1 代码规范能力

应具备良好的文档习惯，有规范化意识，包括但不限于以下内容：

a) 能够组织维护技术文档或技术博客；
b) 能够根据代码规范要求，独立撰写设计文档；
c) 能够遵守代码规范进行开发，有规范化意识。

### 5.3.2 算法模型实现能力

应具备一定的开发经验和独立开发的能力，包括但不限于以下内容：

a) 能够遵循一定理论和原则，独立地进行数据策略迭代及特征工程相关工作；
b) 能够独立使用指定的机器学习平台，训练机器学习模型，进行预测计算，并对模型效果进行调优。

#### 5.3.3 模型部署与运维能力

应具备模型线上部署和维护能力，包括但不限于以下内容：

a) 能够将模型封装成服务的形式并通过网络进行调用；
b) 能够维护模型线上服务的并发使用。

### 5.4 应用能力要求

#### 5.4.1 行业知识能力

应了解一定的人工智能行业知识，包括但不限于以下内容：
能够处理现实场景下采集到的数据，对数据进行清洗等操作。

#### 5.4.2 业务应用能力

应具备一定的将人工智能与实际场景相结合的能力,包括但不限于以下内容：
能够针对不同场景的不同数据，构建不同的模型进行适配。

#### 5.4.3 生成式人工智能应用能力

应具备使用生成式人工智能工具完成业务任务的能力。包括但不限于以下内容：

a) 能够根据任务类型选择合适的生成式人工智能工具（文本生成、图像生成、代码生成等），完成日常工作任务；
b) 能够编写有效的提示词，引导生成式人工智能输出符合需求的内容，并进行多轮迭代优化；
c) 能够识别生成式人工智能输出的明显错误、偏见或不当内容，进行人工审核与修正；
d) 了解生成式人工智能工具的能力边界与使用限制，知晓何时需要转交人工处理或采用其他方案。

#### 5.4.4 智能体应用能力

应具备使用多样化智能体应用与低代码平台搭建能力，以及其他相关人工智能应用能力，包括但不限于以下内容：

a) 能够熟练使用至少两类智能体应用，如：编程类+办公类或创意类+生活类，了解其能力边界与适用场景；
b) 能够使用低代码平台，通过可视化界面配置提示词、知识库和基础工具调用，搭建面向特定场景的智能体；
c) 能够对智能体输出结果进行审查、评估和修正，建立基础的人机协作工作流；
d) 了解智能体应用的基本评估指标，如：响应质量、任务完成率、用户满意度等。

### 5.5 伦理与合规能力要求

#### 5.5.1 基础伦理意识

应了解基础的人工智能伦理认知和法律法规知识，包括但不限于以下内容：

a) 了解人工智能伦理基本原则；
b) 了解人工智能相关法律法规。

#### 5.5.2 伦理风险评估

应能够识别常见伦理风险的能力，包括但不限于以下内容：

a) 能够在开发中识别明显的算法偏见和歧视风险；
b) 能够识别模型输出的内容安全风险。

#### 5.5.3 伦理治理体系

应了解基础的合规治理认知，包括但不限于以下内容：

a) 了解数据采集与使用的合规边界；
b) 了解企业人工智能治理的基本流程与责任分工。

# 6 中级能力要求

## 6.1 基本要求

在达到第5章要求的基础上，掌握深度学习的基础知识，熟悉常见人工智能模型及其应用领域，理解人工智能任务的需求。掌握生成式人工智能的应用开发技术及应用，能够构建RAG系统，了解模型微调方法。掌握智能体技能设计与MCP协议，能够构建单智能体系统，使用低代码平台设计复杂工作流。具备人工智能伦理风险评估与合规实施能力，能够系统识别伦理风险并建立相应的安全与治理机制。在实验室或实习工作岗位中能承担一部分任务。

## 6.2 专业知识要求

### 6.2.1 编程基础

应熟练掌握算法开发，包括但不限于以下内容：
a) 充分理解面向对象编程语言的特性，并能熟练开发；
b) 熟练利用深度学习框架进行深度神经网络搭建。

### 6.2.2 神经网络基础

应能够进行神经网络模型调研与开发，包括但不限于以下内容：
a) 具备神经网络模型使用及实战经验；
b) 熟练掌握卷积神经网络和循环神经网络的工作原理，深入理解 Transformer 架构、注意力机制及其在视觉和语言模型中的应用，理解并掌握关键知识点（反向传播、卷积层、池化层、全连接层、循环神经单元、自注意力机制、位置编码、梯度传播等）；
c) 能够调用及运行深度的神经网络模型，当需要进行参数调整和适配到自身的应用问题时，对关键参数（数据策略、网络中的核心模块、参数规模、优化算法、损失函数、正则项）能提出解决方案。

### 6.2.3 生成式人工智能基础

应具备生成式人工智能应用开发能力，包括但不限于以下内容：
a) 熟练掌握提示词工程技术，如：零样本/少样本提示、思维链提示、结构化输出、提示词模板化；
b) 能够构建RAG系统，实现基于私有知识库的问答应用；
c) 了解多模态模型的基本应用；
d) 了解大模型微调和参数高效微调的基本方法，能够准备训练数据并启动微调流程。

### 6.2.4 智能体基础

应具备智能体技术设计与实现能力，包括但不限于以下内容：
a) 掌握技能设计方法，能够封装应用程序编程接口、数据库查询、代码执行等为可复用的技能模块；
b) 掌握工具使用机制，能够设计智能体与外部工具的交互接口；
c) 掌握MCP协议，能够实现标准化智能体与外部数据源的连接；
d) 了解子智能体概念，能够设计简单的父子智能体协作流程，实现任务分解与结果汇总；
e) 能够设计单智能体的状态管理、记忆机制和任务规划能力；
f) 了解低代码智能体平台的高级功能，能够设计复杂工作流、多轮对话管理和条件分支逻辑。

## 6.3 工程能力要求

### 6.3.1 代码规范能力

应能够熟练运用文档、代码和质量保障规范，包括但不限于以下内容：

a) 规范化意识已经融入工作（包括文档规范、代码规范、质量保障规范）；
b) 能够按照规范参与多人合作。

#### 6.3.2 算法模型实现能力

应具备独立的算法开发能力，并熟悉深度学习任务开发全流程，包括但不限于以下内容：
a) 能够独立地使用指定的深度学习框架，训练深度学习模型，对模型效果进行一定的调优；
b) 能够以深度学习理论为指导，分析数据、迭代数据策略、完成特征优化，并进行模型选型、模型训练、模型表现优化；
c) 熟悉深度学习应用开发的全流程；
d) 能够基于大模型应用程序编程接口或开源模型，完成业务场景的生成式人工智能应用开发；
e) 能够合理使用人工智能编程助手提升开发效率，建立人工智能生成代码的审查、测试和集成流程，确保代码质量与安全。

#### 6.3.3 模型部署与运维能力

应具备模型线上部署和维护能力，包括但不限于以下内容：
a) 能够将模型封装成服务应用；
b) 能够维护模型在异构计算场景下的服务。
c) 能够使用容器化技术（Docker）部署模型服务；
d) 了解模型版本管理与对照测试的基本方法；
e) 了解模型监控指标（延迟、吞吐量、漂移检测）概念。

### 6.4 应用能力要求

#### 6.4.1 行业知识能力

应具备独立的将神经网络模型与不同领域场景结合的能力，包括但不限于以下内容：
a) 能够不断地优化神经网络模型，使其在实际应用场景下平衡精度与推理速度；
b) 能够对神经网络进行剪枝和量化处理，使其在不同计算能力的设备上进行推理。

#### 6.4.2 业务应用能力

应具备评估生成式人工智能应用价值与设计人机协作的能力，包括但不限于以下内容：
a) 能够评估生成式人工智能应用的业务价值与潜在风险；
b) 能够设计人机协作流程，合理分配人工智能与人工的边界。

#### 6.4.3 生成式人工智能应用能力

应具备生成式人工智能应用开发与业务集成的能力，包括但不限于以下内容：
a) 能够基于大模型应用程序编程接口或开源模型，开发面向特定业务场景的生成式人工智能应用（如智能客服、营销文案生成、数据报告自动生成等）；
b) 能够设计人机协作流程，明确生成式人工智能与人工的职责边界，建立输出审核与质量控制机制；
c) 能够评估生成式人工智能应用的业务效果（效率提升、成本降低、用户满意度），并进行持续优化；
d) 能够推动生成式人工智能应用在团队/部门内的落地推广，开展基础的用户培训与支持。

#### 6.4.4 智能体应用能力

应具备智能体应用开发与业务集成能力，包括但不限于以下内容：
a) 能够使用人工智能编程助手进行代码分析、重构、调试和自动化开发任务；
b) 能够开发基于技能调用的智能体应用，集成外部应用程序编程接口和数据库；
c) 能够基于低代码开发平台或代码框架，构建面向业务场景的智能体应用（如智能客服、数据分析助手、内容运营助手），实现与现有业务系统的集成；
d) 能够设计复杂的多轮对话工作流，实现条件分支、循环和异常处理；
e) 能够评估智能体应用的效果，优化人机协作流程。

### 6.5 伦理与合规能力要求

#### 6.5.1 基础伦理意识

应深入理解伦理原则并能在项目中应用，包括但不限于以下内容：

a) 深入理解人工智能伦理原则，能够在项目决策中权衡伦理冲突；
b) 掌握行业特定的人工智能合规要求（医疗人工智能的医疗器械监管、金融人工智能的算法备案要求、推荐算法的透明度义务等）。

#### 6.5.2 伦理风险评估

应能够系统评估和缓解伦理风险，包括但不限于以下内容：

a) 能够进行人工智能系统的伦理影响评估，系统识别应用场景中的伦理风险（隐私泄露、算法歧视、虚假信息生成、深度伪造滥用）；
b) 能够实施算法公平性检测与偏见缓解措施（数据重平衡、公平性约束优化）；
c) 能够实施模型可解释性方案，满足业务透明性需求（特征重要性分析、注意力可视化、决策路径追踪）。

#### 6.5.3 伦理治理体系

应能够建立和实施合规治理流程，包括但不限于以下内容：

a) 能够建立数据治理流程，确保训练数据合规（数据来源合法性审查、个人信息脱敏、数据最小化原则等）；
b) 能够建立人工审核机制与人工智能输出内容安全过滤机制；
c) 能够建立模型全生命周期的合规管理流程。

## 7 高级能力要求

### 7.1 基本要求

在达到第6章要求的基础上，有系统的人工智能知识体系，在某个领域有着坚实的基础，具备理解和复现前沿算法的能力。精通生成式人工智能技术栈，具备模型微调、对齐、推理优化及系统级架构设计能力。精通智能体技术，具备子智能体设计、多智能体系统架构、自主智能体开发能力，能够评估低代码平台与代码级开发的适用边界。精通人工智能伦理治理体系，能够制定治理框架、建立安全对齐机制、处理伦理危机，确保技术应用的负责任创新。在资深专家的领导下能够独立承担产品模型开发调优任务。

### 7.2 专业知识要求

#### 7.2.1 编程基础

应能够提出业务技术方案，解决特定技术问题，包括但不限于以下内容：

a) 能够对深度学习应用开发过程中遇到的技术难题提供技术解决方案；
b) 能够对矩阵计算和计算程序的开发技术选型有一定的判断和见解；
c) 有深度学习应用开发经验。

#### 7.2.2 神经网络基础

应能够自主进行神经网络算法开发，包括但不限于以下内容：

a) 能够充分理解各种新型模型和相关技术资料；
b) 能够根据实际业务需求，使用工具或平台搭建神经网络模型；
c) 能够针对自然语言处理、计算机视觉、语音处理三大领域中的至少一类任务，对该任务上的模型进行调优并达到特定的需求指标；
d) 能够合理组合、改造并创新深度学习模型来解决更加复杂的应用问题，有成功开发经验。

#### 7.2.3 生成式人工智能基础

应具备大语言模型系统级开发能力，包括但不限于以下内容：

a) 精通大模型预训练、监督微调、基于人类反馈的强化学习等模型对齐技术；
b) 能够进行多模态大模型的应用开发与调优（视觉-语言模型、语音-语言模型）；
c) 掌握模型压缩与推理优化技术；
d) 能够设计大模型应用架构，如：RAG 系统深度优化、智能体系统设计、多模型编排、混合专家系统；
e) 了解大模型安全与对齐的前沿研究。

#### 7.2.4 智能体基础

应具备智能体系统架构设计与前沿研究能力，包括但不限于以下内容：
a) 能够设计多智能体协作系统，实现智能体间的任务分配、协作与冲突解决；
b) 能够设计子智能体架构，实现复杂任务的层次化分解、并行执行与结果聚合；
c) 能够设计自主任务执行智能体，具备长期记忆管理、环境感知与自主规划能力；
d) 精通 MCP 协议的高级应用，能够设计跨平台、跨厂商的智能体技能生态与标准化接口；
e) 了解智能体安全与对齐的前沿研究；
f) 能够评估低代码平台与代码级开发的适用边界，为企业选择合适的智能体建设路径。

### 7.3 工程能力要求

#### 7.3.1 代码规范能力

应能够熟练运用文档、代码和质量保障规范，包括但不限于以下内容：
a) 具备对文档、代码和质量保障的规范化意识；
b) 能够组织制定文档规范及技术规范；
c) 能够按照规范参与多人合作。

#### 7.3.2 算法模型实现能力

应具备独立的算法开发能力，包括但不限于以下内容：
a) 熟悉深度学习任务开发全流程；
b) 有良好的机器学习基础知识；
c) 能够理解业务需求，并准确地转化为技术语言；
d) 能够根据业务需求快速选择合适模型，制定技术方案，提出学习性能优化方案；
e) 能够将业务需求转化为算法策略，提出见解和方案；
f) 能够设计生成式人工智能应用的技术架构，包括模型选型、推理优化方案、成本控制策略；
g) 能够设计人工智能编程智能体系统，实现从需求分析、架构设计、代码实现到测试部署的全流程自动化开发。

#### 7.3.3 模型部署与运维能力

应具备模型线上部署和维护能力，包括但不限于以下内容：
a) 能够对模型进行修改和裁剪，满足边缘端部署；
b) 能够维护模型在云边端（云端、边缘端、终端设备）的稳定运行；
c) 能够设计高可用、可扩展的模型服务架构；
d) 精通异构计算优化；
e) 能够实现大模型的高效服务化部署；
f) 能够建立模型治理体系；
g) 能够设计智能体服务的部署架构，支持技能动态加载、状态管理、长期记忆存储、子智能体调度和异步任务执行；
h) 能够设计多智能体系统的通信机制、容错策略与负载均衡方案。

### 7.4 应用能力要求

应具备开发适用工业界或科研界前沿领域的人工智能模型能力，包括但不限于以下内容：
a) 在基础科学领域如生物、材料、物理、数学等领域，能够开发具有开拓性的人工智能模型；

b) 在应用科学领域如芯片制造、医疗健康、公共安全等领域，能够开发和应用具有广泛适用性的人工智能模型。

#### 7.4.1 行业知识能力

应具备开发适用工业界或科研界前沿领域的人工智能模型能力，包括但不限于以下内容：

a) 在基础科学领域如生物、材料、物理、数学等领域，能够开发具有开拓性的人工智能模型；
b) 在应用科学领域如芯片制造、医疗健康、公共安全等领域，能够开发和应用具有广泛适用性的人工智能模型；
c) 能够评估人工智能技术对行业伦理和社会影响的长期趋势（就业影响、数字鸿沟、技术依赖）。

#### 7.4.2 业务应用能力

应能够推动深度学习在自身业务和产品上的应用，包括但不限于以下内容：

a) 深入分析业务需求，了解产品特性和研发关键点；
b) 在技术设计时能针对产品、架构的未来发展进行预留性及可扩展性的设计；
c) 能够熟练使用深度学习建模方法解决实际需求问题；
d) 能够设计负责任的人工智能产品方案，平衡技术创新与伦理约束；
e) 能够建立人工智能应用的治理框架，包括内容审核、用户反馈、应急响应机制。

#### 7.4.3 生成式人工智能应用能力

应具备生成式人工智能系统级应用架构设计与战略治理能力，包括但不限于以下内容：

a) 能够设计企业级生成式人工智能应用架构，包括模型选型策略、多模型编排、与现有业务系统的深度集成方案；
b) 能够制定生成式人工智能应用的治理框架，包括内容安全策略、数据隐私保护、合规审查流程、应急响应机制；
c) 能够评估新兴生成式人工智能技术（如多模态大模型、推理模型、智能体生成系统）的业务价值，制定技术引入路线图；
d) 能够建立生成式人工智能应用的全生命周期管理体系，包括需求评估、效果度量、持续监控、迭代优化和退役机制；
e) 能够统筹管理企业内多个生成式人工智能应用项目，协调跨部门资源，推动形成标准化的应用开发最佳实践。

#### 7.4.4 智能体应用能力

应具备智能体系统落地与复杂场景应用能力，包括但不限于以下内容：

a) 能够推动人工智能编程智能体在软件工程领域的应用，评估人机协作开发模式对团队效率、代码质量和知识传承的影响；
b) 能够设计多智能体系统在企业业务场景中的架构，实现跨部门、跨系统的智能协作；
c) 能够设计自主智能体的应用场景，评估自主决策边界与人工监督机制；
d) 能够评估智能体组织的 KPI 与协作激励机制，优化人机协作流程；
e) 能够进行企业级低代码平台的选型、私有化部署和生态建设，或基于开源框架构建定制化智能体平台。

### 7.5 伦理与合规能力要求

#### 7.5.1 基础伦理意识

应深入理解伦理原则并能在复杂场景下指导决策，包括但不限于以下内容：

a) 深入理解人工智能伦理原则内涵，能够在复杂项目决策中权衡多方伦理冲突；
b) 熟悉国际人工智能伦理准则与行业最佳实践，能够指导团队伦理决策；
c) 能够进行人工智能伦理培训与宣导，提升组织整体伦理意识。

#### 7.5.2 伦理风险评估

应能够设计安全机制并处理复杂伦理危机，包括但不限于以下内容：

a) 能够设计人工智能系统的安全对齐方案，建立安全测试机制，防范滥用与攻击风险；
b) 能够进行人工智能系统的社会影响评估，确保技术符合社会公共利益；
c) 能够处理人工智能伦理危机事件，建立应急响应与问责机制；
d) 能够建立持续的风险监测与预警机制。

#### 7.5.3 伦理治理体系

应能够设计企业级治理框架并指导国际合规实践，包括但不限于以下内容：

a) 能够制定企业级人工智能伦理治理框架、政策与审查流程；
b) 能够建立跨部门的人工智能伦理审查委员会，制定伦理决策标准；
c) 能够掌握国际人工智能治理框架（欧盟人工智能法案、美国人工智能风险管理框架、中国生成式人工智能服务管理暂行办法）并指导合规实践；
d) 能够建立人工智能系统的全生命周期治理体系，从需求分析到退役的全流程伦理管理。

## 8 评估管理要求

### 8.1 评估机构要求

评估机构应为省级软件行业协会并符合以下要求：

a) 建立了规范化的评估流程；
b) 建立了评估专家库；
c) 具有专门的办事部门和人员。

### 8.2 评估流程

职业人员人工智能技术能力评估流程如下：

a) 参评人员提供能力佐证材料、身份证明材料等信息；
b) 审核通过后参评人员登录线上评估平台参与线上评测；
c) 评测后经过专家综合评审，根据附录 A 评估结果说明的要求，对不同等级进行评估结果确定，并颁发能力证明。

### 8.3 评估方式

评估方式如下：

a) 由评估机构组织行业专家共同组成评审专家组；
b) 按照第 4 章、第 5 章、第 6 章、第 7 章的要求，逐项据实评审；
c) 若对所评材料真实性产生疑问，可要求参评人员补充说明或暂缓评估；
d) 评估工作定期组织。

### 8.4 评估监管

a) 职业人员人工智能技术能力评估工作应接受行业主管部门的监督和指导；
b) 职业人员人工智能技术能力评估过程中，如发生费用应接受监督和指导；
c) 建立评估结果的申诉与复核机制；
d) 对违反人工智能伦理规范造成严重后果的持证人员，应建立能力证明的暂停或撤销机制；
e) 建立伦理投诉渠道，接受社会对持证人员人工智能伦理行为的监督。

# 附 录 A
（资料性）
评估结果说明

职业人员人工智能技术能力线上评测分数由4部分构成，分别是客观题分数、代码题分数、案例题分数和报告及能力证明材料分数，总分为100分。其中报告内容为根据题目要求，撰写某一新型人工智能技术在参评人员所在领域的具体应用报告，包括且不限于应用场景、应用形式、应用过程中可能遇到的问题及伦理风险防控措施等。不同等级的分数占比不同，分数占比见表A.1。

表A.1 人工智能技术能力题目评分占比

| 等级 | 客观题占比 | 代码题占比 | 案例题占比 | 报告及能力证明材料占比 |
|---|---|---|---|---|
| 初级 | 20% | 20% | 40% | 20% |
| 中级 | 10% | 20% | 40% | 30% |
| 高级 | 10% | 20% | 30% | 40% |

其中前三类题目总分在60%及以上（即初级不低于48分，中级不低于42分，高级不低于36分）的参评人员，进入复审；复审阶段由专家对报告及能力证明材料进行评估打分，单项分值60%及以上（即初级不低于12分，中级不低于18分，高级不低于24分），以上四类题目总分在60分及以上的准予颁发能力证明。

# 参 考 文 献

[1]T/CASME 508—2023 人工智能应用软件开发技术规范
[2]T/AIIA 004—2023 人工智能企业等级评定规范
[3]T/QDAIIA 002—2023 人工智能企业评价规范
[4]GB/T 45225—2025 人工智能 深度学习算法评估
[5]GB/T 45674—2025 网络安全技术 生成式人工智能数据标注安全规范
[6]GB/T 45081—2024 人工智能 管理体系
[7]GB/T 42888—2023 信息安全技术 机器学习算法安全评估规范