“NSTL 元数据规范体系建设”专项任务成果　　2025 年 11 月　总第 11 期

信息资源管理标准规范动态报告

NSTL 数据研究管理中心

全面调研和梳理国内外信息资源管理领域标准规范的发展动态，涵盖数据管理、数据组织、知识技术相关的新标准、新规范、新模型等。

本期看点

- ISO/IEC 25642:2025 Information technology — Data governance — Data collaboration framework
- ISO/IEC 12792:2025 Information technology — Artificial intelligence (AI) — Transparency taxonomy of AI systems
- Generative Artificial Intelligence and Web-Scale Discovery
- GB/T 46411-2025 科学数据收割规范

目　录

数据管理 1

✧ ISO/IEC 25642:2025 Information technology — Data governance — Data collaboration framework 1

✧ GB/T 46411-2025 科学数据收割规范 1

✧ GB/T 46406-2025 科研项目数据管理指南 3

数据组织 5

✧ GB/T 25100.1-2025 信息与文献 都柏林核心元数据元素集 第 1 部分：核心元素 5

✧ GB/T 41207-2025 信息与文献 文件（档案）管理体系 实施指南 6

✧ GB/T 34110-2025 信息与文献 文件（档案）管理 核心概念与术语 7

知识技术 8

✧ ISO/IEC TS 42119-2:2025 Artificial intelligence — Testing of AI Part 2: Overview of testing AI systems 8

✧ ISO/IEC 12792:2025 Information technology — Artificial intelligence (AI) — Transparency taxonomy of AI systems 10

✧ Generative Artificial Intelligence and Web-Scale Discovery 11

✧ GB/T 45628-2025 人工智能 知识图谱 知识交换协议 13

✧ GB/T 46284-2025 人工智能 联邦学习技术规范 14

科技评价 16

✧ GB/T 46347-2025 人工智能 风险管理能力评估 16

✧ GB/T 46346-2025 人工智能 计算中心 计算能力评估 17

✧ GB/T 45225-2025 人工智能 深度学习算法评估 19

数据管理

✧ ISO/IEC 25642:2025 Information technology — Data governance — Data collaboration framework

【看点】国际标准化组织于 2025 年 10 月发布了《ISO 25642:2025 信息技术 数据治理 数据协调框架（Information technology — Data governance — Data collaboration framework）》，为依赖组织数据完整性履行职责的信息技术和其他领导者提供了一份蓝图，以帮助构建具备细粒度、可普遍执行的数据控制的新型数字化解决方案。

【摘要】该标准规定了零拷贝（zero-copy）数据集成的最低建议，并提供了一个数据协作框架，可在受控数据管理环境中构建模块化解决方案，这些解决方案既可独立使用，也可组合成高级数字化方案。

该框架围绕数据协作基础展开，包括：将数据与应用程序解耦、基于访问的协作优于基于复制的集成、将数据作为产品进行治理与管理、在元数据层实施控制措施、打造元数据驱动的体验、设计企业级可组合性等方面的内容。

该标准与现行国际标准 ISO/IEC 38500 IT 治理（IT governance）和 ISO/IEC 38505-1 数据治理（data governance）互为补充，旨在为组织（包括治理机构和管理层）提供实践指南，使其能够：

- 构建并管控支持通用数据访问控制的新数字能力；
- 从 IT 交付流程中根除点对点、基于复制的数据集成；
- 支持运营数据在人与人、人与系统、系统与系统之间协同，包括多 AI 系统协同。

该标准适用于包括上市公司、私营企业、政府机构和非营利组织在内的所有行业，但不面向非数据密集型运营角色，也未规定与其他系统或组件的接口。

来源：

国际标准化组织（International Organization for Standardization）：

https://www.iso.org/standard/90990.html

https://www.iso.org/obp/ui/en/#iso:std:iso-iec:25642:ed-1:v1:en

✧ GB/T 46411-2025 科学数据收割规范

【看点】国家标准化管理委员会于 10 月 5 日发布并实施了 GB/T 46411-2025《科学数据收割规范》，规定了科学数据的收割内容、收割流程、实现要求，由全国科技平台标准化技术委员会归口，主管部门为科技部。

【摘要】科学数据作为科技创新要素，其共享交换的规模和频次急剧增长，对高效及时的科学数据交换的需求日趋迫切。科学数据收割作为一种系统之间进行科学数据互操作的方式，由获取科学数据的一方主动发起，通过应用程序接口的方式获取另一个科学数据平台的科学数据信息或科学数据。收割操作可自动化、多频次地按需进行，减少人工操作工作量的同时，提升了数据交换的效率。

科学数据管理机构既可作为收割数据的一方，也可作为被收割数据的一方，进而实现科学数据管理机构间科学数据按需交换的目的，可有效提升科学数据管理机构之间科学数据汇聚和交换的规范性和效率。该标准规定了科学数据的收割内容、收割流程、实现要求，适用于科学数据管理机构开展科学数据收割，生物种质与实验材料资源库等实物科技资源平台开展科学数据收割参照使用。

科学数据收割内容包括科学数据元数据和科学数据实体（如图 1），两者的收割应分别基于科学数据清单和科学数据实体访问地址等科学数据收割辅助信息开展。科学数据收割主要包括建立连接、获取清单、元数据收割、数据实体收割等流程（如图 2），其中元数据收割和数据实体收割可同步进行。科学数据收割现实要求包括传输协议、收割操作和其他方面等的要求。

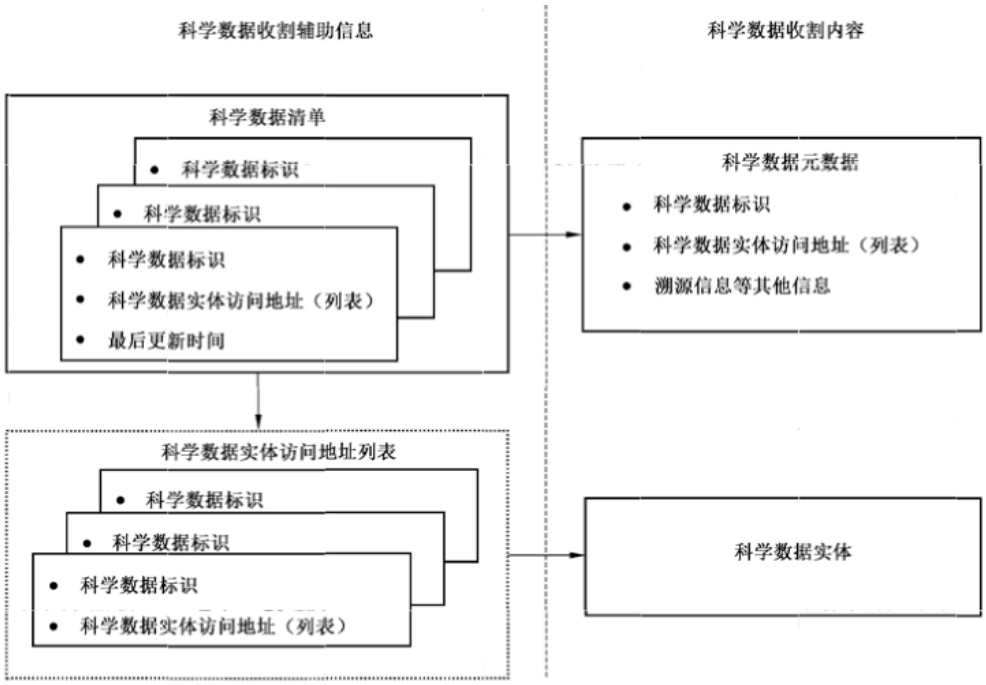

图 1 科学数据收割内容组成

图 2 科学数据收割流程

来源：

全国标准信息公共服务平台：

https://std.samr.gov.cn/gb/search/gbDetailed?id=40B74A27FD21BD79E06397BE0A0AB048

国家标准全文公开系统：

https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=6590EDF7221A60D7B15DC5E3B6FB4211

✧ GB/T 46406-2025 科研项目数据管理指南

【看点】国家标准化管理委员会于 10 月 5 日发布并实施了 GB/T 46406-2025《科研项目数据管理指南》，给出了科研项目科学数据管理活动和流程，由全国科技平台标准化技术委员会归口，主管部门为科技部。

【摘要】科学数据是国家科技创新和经济社会发展的重要基础性战略资源，其质量直接关系到科学数据的开放、共享和利用。为加强科研项目产出的科学数据的质量管理，确保科研项目汇交的科学数据的规范性、完整性、准确性、一致

性和时效性，有必要在立项启动、项目执行、项目验收或综合性评价等阶段规范科研项目科学数据管理活动。

该标准给出了科研项目科学数据管理活动和流程，提供了管理活动的任务目标、工作要点、产出要点和相关方责任的指导，适用于自然科学与技术领域基础研究、应用研究和开发研究等类型科研项目产出的科学数据管理活动，可配合GB/T 39912—2021 使用，以确保科研项目的科学数据质量。

科研项目科学数据管理活动包括科学数据产出规划、科学数据管理计划编制、科学数据产品设计、科学数据产品研制、科学数据新产品质量评价、科学数据汇交、科学数据开放共享，科学数据管理活动流程如图 3：

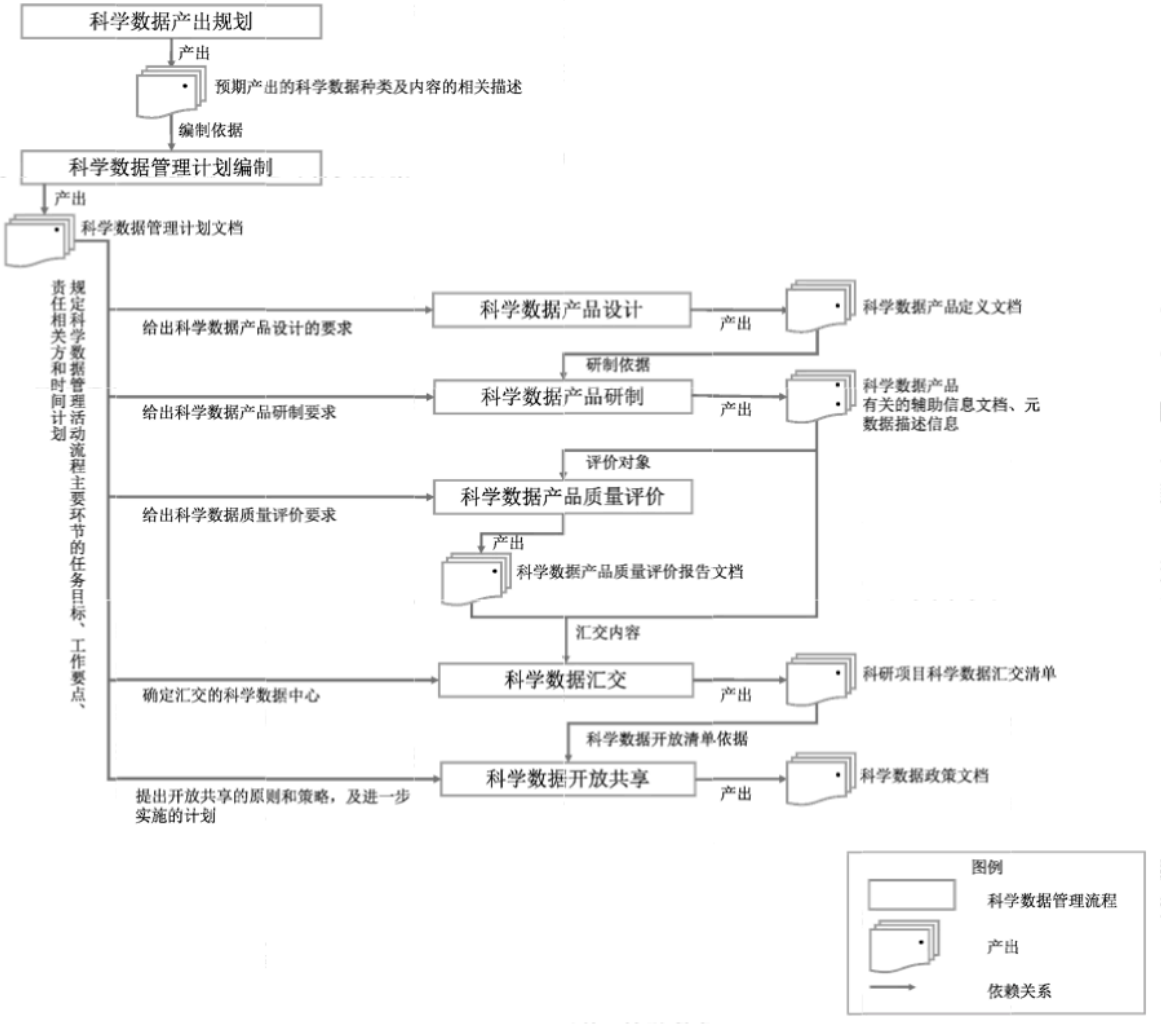

图 3 科研项目科学数据管理活动流程

依据科研项目阶段的特点，科学数据管理活动要素包括任务目标及产出、工作要点和相关方责任（如表 1）。

表 1 科研项目科学数据管理活动要素

管理活动	科学数据产出规划	科学数据管理计划编制	科学数据产品设计	科学数据产品研制	科学数据新产品质量评价	科学数据汇交	科学数据开放共享
任务目标	分析、评估和识别支持科学研究目标实现的科学数据需求和产出	结合科研项目实施计划，编制科研项目科学数据管理计划文档	依据科学数据产出规划，开展科学数据产品定义，并形成文档	按照科学数据产品定义要求，研制科学数据产品	开展科学数据质量评价活动，并形成质量评价报告	制定科学数据汇交计划，开展科学数据汇交，并获取汇交凭证	明确科研项目科学数据开放共享的政策或策略，实施科学数据开放共享，确保科学数据的可访问、可获取
责任相关方	科研项目实施机构	科研项目实施机构	科研项目实施机构	科研项目实施机构	科研项目实施机构	科研项目实施机构	科研项目实施机构
		科研项目管理机构	科研项目管理机构		科研项目管理机构	科研项目管理机构	科研项目管理机构
		科研项目管理机构		科研项目管理机构		科研项目管理机构	
科研项目阶段	立项启动阶段		执行阶段		验收阶段或综合性评价阶段		验收后或综合性评价后

来源：

全国标准信息公共服务平台：

https://std.samr.gov.cn/gb/search/gbDetailed?id=40B74A27FD9CBD79E06397BE0A0AB048

国家标准全文公开系统：

https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=C8FD9E6B52ADCBEC58136A4DC5E27A22

数据组织

✧ GB/T 25100.1-2025 信息与文献 都柏林核心元数据元素集 第1部分：核心元素

【看点】国家标准化管理委员会于 10 月 31 日发布了 GB/T 25100.1-2025《信息与文献 都柏林核心元数据元素集 第 1 部分：核心元素》，为跨领域的资源描述建立了 15 个核心元数据元素，由全国信息与文献标准化技术委员会归口，将于 2026 年 5 月 1 日实施。

【摘要】该标准是 GB/T 25100《信息与文献 都柏林核心元数据元素集》系列标准的第 1 部分，将替代 2010 年的 GB/T 25100 标准，其主要变化包括：修改了引言、调整了结构、增加了命名要素、更新了部分定义。

都柏林核心元数据元素集包含 15 个用于资源描述的核心元素，其中“核心”指它的元素比较宽泛和通用，可用于描述各种资源。该标准为跨领域的资源描述建立了 15 个核心元数据元素，这些是由都柏林核心元数据计划（DCMI）负责维护的一系列元数据词表和技术规范的一部分，完整的 DCMI 元数据术语［DCMI-TERMS］在同系列标准的第 2 部分中呈现。

该标准的主要内容包括：

一是定义标准中出现的重要术语。

二是定义核心元素的命名要素。为每个元素设置一个描述性的标签（“label”），供人类识别；为每个元素设置一个唯一的标记（“name”），用于机器处理；构造一个统一的资源标识符，作为该元素的全局唯一标识符。

三是按照命名要素对 15 个核心元素进行定义，并通过注释及示例进行详细说明。

该标准是在 GB/T 25100 标准已实施十余年之际，为适应技术飞速发展背景下，元数据的功能从对数字资源进行简单描述发展为基于语义网的数字资源整合与消费的变化，依据采用的国际标准的修订情况及国内各行业的应用情况等新要求，修订发布实施的新版国家标准。

来源：

全国标准信息公共服务平台：

https://std.samr.gov.cn/gb/search/gbDetailed?id=42BA7D06A429E936E06397BE0A0ACDC9

✧ GB/T 41207-2025 信息与文献 文件（档案）管理体系 实施指南

【看点】国家标准化管理委员会于 8 月 1 日发布了 GB/T 41207-2025《信息与文献 文件（档案）管理体系 实施指南》，为组织内实施文件管理系统（MSR）提供了实践指南，由全国信息与文献标准化技术委员会归口，将于 2026 年 2 月 1 日实施。

【摘要】当组织为了履行法律义务需要证明其在开展业务的过程中的能力，在创建和控制信息创建、控制、接收所创建的信息和维护作为证据和资产时候，GB/T 34112《信息与文献 文件管理体系 要求》明确了文件管理系统（MSR）的要求。该标准是对 2021 年首发 GB/T 41207-2021 标准的第一次修订，旨在帮助用户应用 GB/T 34112 的文件管理系统要求，描述了为满足 GB/T 34112 要求而采

取的措施以及如何记录这些措施的活动，其中所称“文件”等同于中文语境下的机关单位或组织的文件和档案。

该标准的主要内容包括：

- 解决了如何分析 MSR 需求的问题，通过分析明确了 MSR 的范围，定义了实施 MSR 与其他管理体系的关系（第 4 章）；
- 解释了领导作用以及如何获得最高管理者的承诺（第 5 章）；
- 规划了 MSR 实施和文件管理目标（第 6 章）；
- 列出了 MSR 所需的支持，如：资源、能力、意识、沟通和证明性信息（第 7 章）；
- 涉及界定、评审以及计划运营层面的内容（第 8 章）；
- 涉及对照 GB/T 34112 中定义的计划、目标和要求的绩效评价和改进（第 9、10 章）。

该标准适用于不同规模的各类型组织（例如：企业、政府机关、非营利组织等），但需要依据组织的规模、性质、复杂度以及已经实施的 MSR 的成熟级别灵活使用。小型组织能对该标准中所描述的措施进行相应的简化，而大型或复杂的组织则可能需要一个多层的管理体系，以有效实施和管理各类活动。

来源：

全国标准信息公共服务平台：

https://std.samr.gov.cn/gb/search/gbDetailed?id=3B46A026CC4D469CE06397BE0A0AEEB8

国家标准全文公开系统：

https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=FF56C04B13A09E9394E3B732D818F358

✧ GB/T 34110-2025 信息与文献 文件（档案）管理 核心概念与术语

【看点】国家标准化管理委员会于 11 月 1 日实施了 GB/T 34110-2025《信息与文献 文件（档案）管理 核心概念与术语》，首次统一了文件管理领域的核心概念和术语及定义，由全国信息与文献标准化技术委员会归口。

【摘要】该标准旨在对特定领域或学科中所使用概念的指称与定义加以规范，使用概念关系图表达了与组织、文件、鉴定、文件管理及文件过程、文件控制、体系及文件系统相关的术语概念关系，为标准制定提供了术语一致性检查和维护的工作基准。

该标准作为 GB/T 34110—2017《信息与文献 文件管理体系 基础与术语》的代替标准，删去了“文件管理体系的基础”这一章节，突出术语和定义及其概念关系，更新为纯粹的术语标准；术语总数量从 29 个扩展到 70 个，其更新内容包括新增“鉴定”“组织”“文件控制”3 大核心概念相关的 48 个术语及定义，修订与“文件”“文件管理”“文件过程”“文件系统”“文件管理体系”5 大核心概念相关的 12 个术语定义，同时删去了 7 个术语（如图 4，修改自 GB/T 34110—2025）。这一更新为整个文件管理领域明确了其核心概念及概念关系。

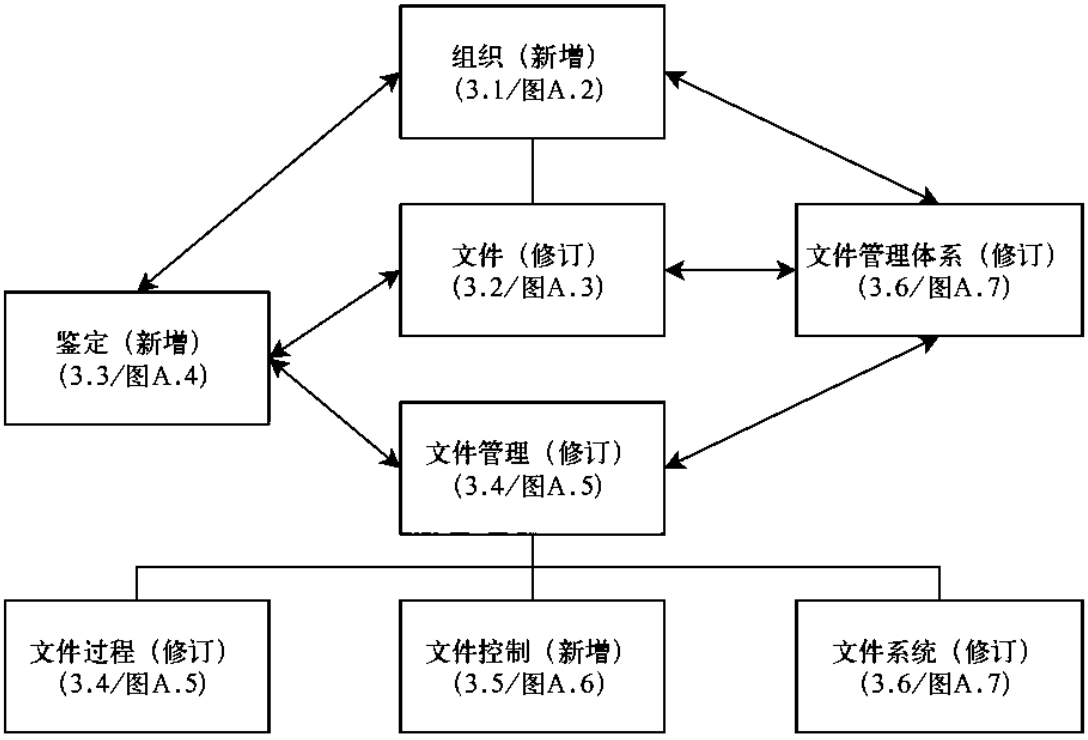

图 4 文件管理核心概念及其关系图

来源：

全国标准信息公共服务平台：

https://std.samr.gov.cn/gb/search/gbDetailed?id=33D40F11612D5D92E06397BE0A0A5B93

国家标准全文公开系统：

https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=CF38AE0855D70D6A5A455294ACE688E3

知识技术

- ✧ **ISO/IEC TS 42119-2:2025 Artificial intelligence — Testing of AI Part 2: Overview of testing AI systems**

【看点】国际标准化组织于 2025 年 11 月发布了《ISO 42119-2:2025 人工智能 AI 测试第 2 部分：AI 系统测试概述（Artificial intelligence — Testing of AI Part 2: Overview of testing AI systems）》，为 ISO/IEC/IEEE 29119 系列文件中的测试实践、方法和技术补充了细节，并描述了其在 AI 系统中的应用。

【摘要】ISO/IEC/IEEE 29119 系列旨在定义一套国际公认的软件测试标准，适用于任何组织开展各类软件测试活动。本文件规定了将 ISO/IEC/IEEE 29119 系列标准应用于 AI 系统测试的要求和指南，遵循基于风险的方法，利用与 AI 系统及其开发维护相关的风险，确定适用于 AI 系统及其组件的合适测试实践、方法和技术。

包含规定的特定测试流程的 AI 系统生命周期模型示例如下图 5：

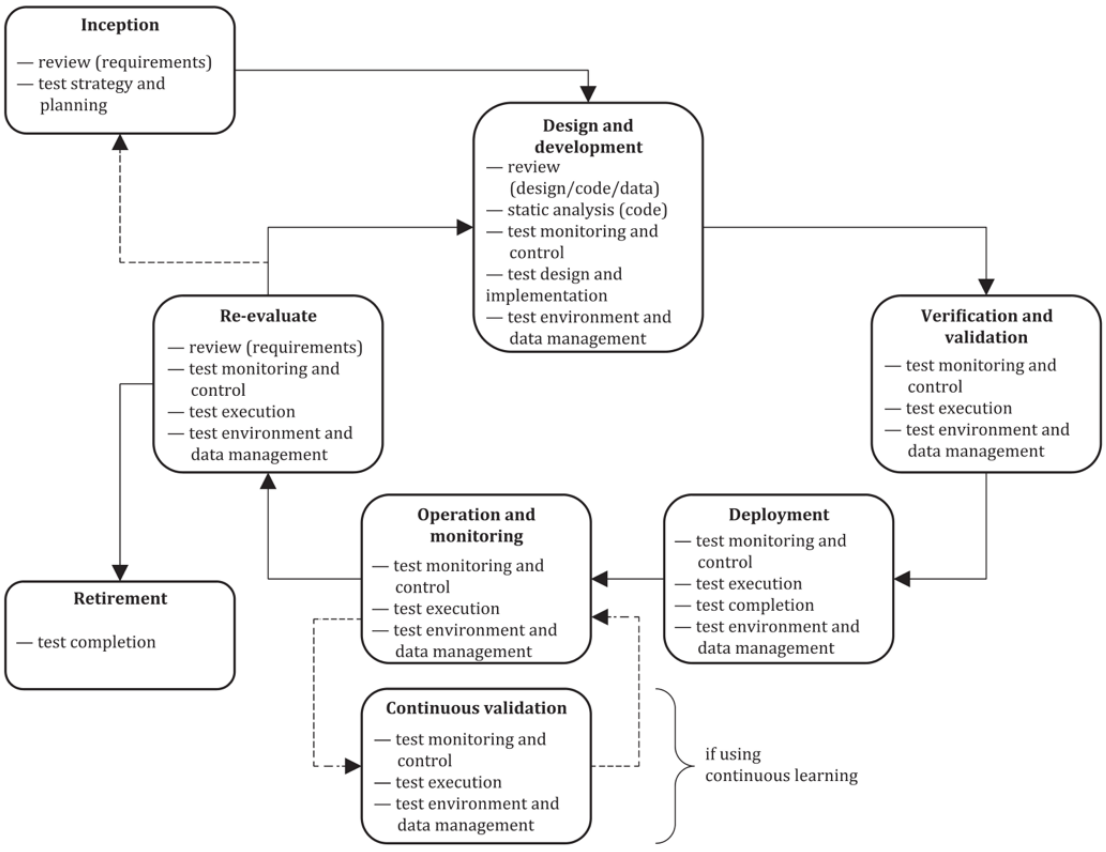

图 5 人工智能系统生命周期模型及测试专用流程示例

作为执行测试过程产物的测试文档概述如下图 6：

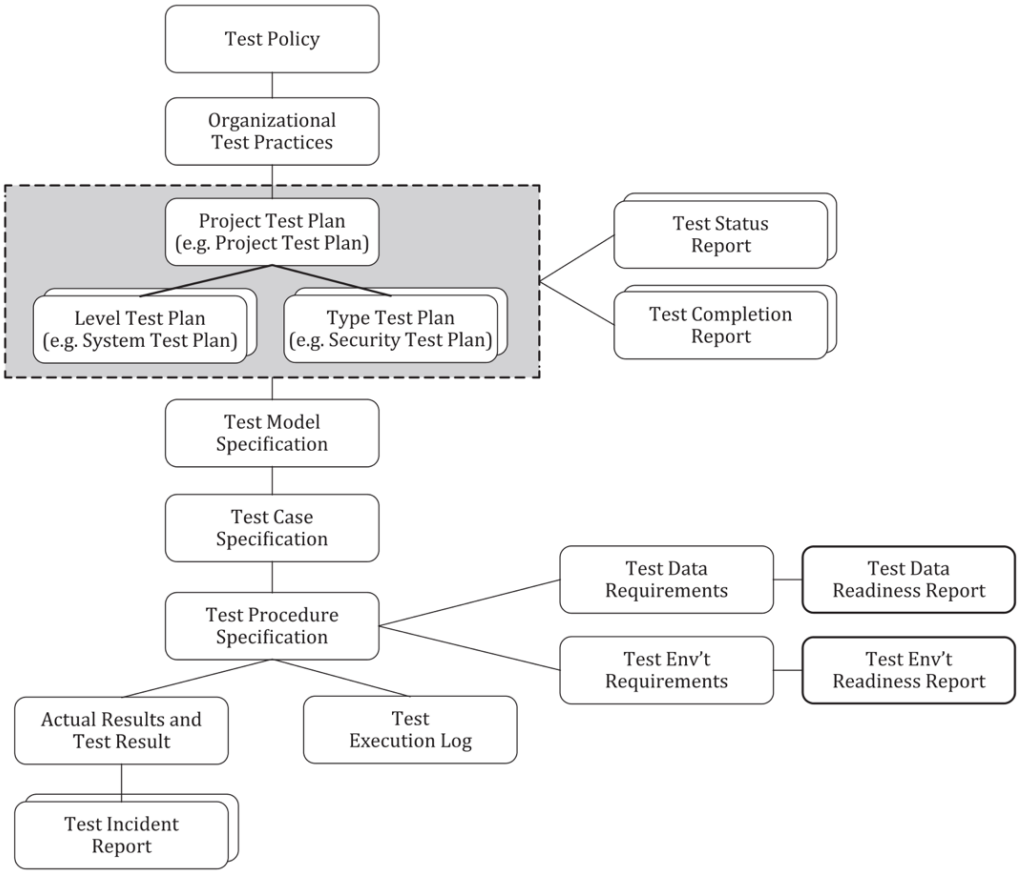

图 6 测试文档的概述

来源：

国际标准化组织（International Organization for Standardization）：

https://www.iso.org/standard/84127.html

https://www.iso.org/obp/ui/en/#iso:std:iso-iec:ts:42119:-2:ed-1:v1:en

✧ ISO/IEC 12792:2025 Information technology — Artificial intelligence (AI) — Transparency taxonomy of AI systems

【看点】国际标准化组织于 2025 年 11 月发布了《ISO 12792:2025 信息技术 人工智能（AI） AI 系统的透明度分类法（Information technology — Artificial intelligence (AI) — Transparency taxonomy of AI systems）》，阐述了信息要素的语义及其对不同利益相关方各项目标的相关性。

【摘要】AI 系统的透明度是指系统使利益相关方能够获取相关信息的特性，可能包括系统功能、局限性、数据、系统设计及设计选择等方面的信息。透明度使利益相关方能够获取信息，从而更好地理解 AI 系统的开发、部署及使用方式。

该标准规定了一套信息要素分类法，旨在帮助 AI 利益相关方识别并满足 AI 系统透明度的需求，适用于涉及 AI 系统的任何类型的组织和应用。具体包括：

- 概述内容，阐述 AI 系统透明度的概念（第 5 条）；
- 讨论了透明度需求如何因 AI 系统情境及所涉利益相关方而异（第 6 条）；
- 阐述描述 AI 系统环境的透明度要素（第 7 条）；
- 说明在 AI 系统层面应披露的透明度信息（第 8 条）；
- 聚焦系统内部运作的文档化要求（第 9 条）；
- 就数据集作为独立项目进行文档记录提供指导（第 10 条）。

该标准的目标是：（1）通过建立关于 AI 系统透明度的一致术语，提升供应链伙伴、客户、用户、社会和监管机构等不同 AI 利益相关方之间的可信度、问责制和沟通效率；（2）为 AI 利益相关方提供关于透明度不同要素的信息，阐明其相关性及在不同应用场景和目标受众中的潜在局限性；（3）为制定技术特定、行业特定或区域特定的 AI 系统透明度标准奠定基础。

来源：

国际标准化组织（International Organization for Standardization）：

https://www.iso.org/standard/84111.html

https://www.iso.org/obp/ui/en/#iso:std:iso-iec:12792:ed-1:v1:en

✧ Generative Artificial Intelligence and Web-Scale Discovery

【看点】美国国家信息标准组织于 2025 年 8 月 5 日发布了《生成式人工智能与网络级发现服务（Generative Artificial Intelligence and Web-Scale Discovery）》，呈现了开放发现计划（ODI，Open Discovery Initiative）常设委员会开展的“AI 在图书馆网络级发现服务中的应用”调研成果。

【摘要】2020 年，ODI 更新了其推荐的实践标准 NISO RP-19-2020 开放发现计划：促进发现服务透明度（Open Discovery Initiative: Promoting Transparency in Discovery）。时隔五年，生成式人工智能（GAI，Generative Artificial Intelligence）工具的崛起与爆发式增长，为网络级发现服务及学术资源传递机制带来全新命题。

ODI 希望深入了解图书馆、内容提供商和发现服务提供商对 GAI 这一新兴技术所关切的问题，于 2024 年 9 月下旬启动专项调研，以探析网络级发现服务生态系统中各参与方的期待与担忧，并将调查结果以报告形式进行展现。

该报告指出，调研创建了针对三方受访群的在线问卷调查：图书馆、内容提供商以及发现服务提供商，所有受访者都能看到相同的初始问题和结束问题。针对各群体的具体问题包括：

- 所在机构是否已开始研究将 GAI 工具应用于自身提供或授权的发现服务中；
- 对 AI 驱动的发现服务可能带来的一系列益处进行优先级排序；
- 对 AI 驱动的发现服务可能产生的一系列负面影响进行危害等级评估；
- 对三项 AI 驱动的发现服务功能对其机构员工和用户的价值评估问题；
- 其所在机构是否已就 GAI 工具的使用，对内（员工）和对外（用户）提供了指导规范；
- ODI 在确保 GAI 用于发现服务中的透明度与效力方面应发挥何种作用；
- 对 GAI 驱动的发现服务的最大期望和最深担忧（开放式问题）。

调研共发放 236 份问卷，绝大多数（72%）受访者来源于图书馆机构，内容提供商约占受访者的五分之一（18.2%），仅有 23 名（9.8%）受访者选择了“其他”或“发现服务提供商”选项。通过分析，得出以下关键结论：

1、图书馆和内容提供商的受访者对 GAI 在内容发现中的应用持有共同期望，三大共同期望包括：提高内容的可见性、更精准的内容推荐以及节省员工时间。

2、不同群体对风险的担忧呈现显著差异，其关注点往往与自身利益密切相关。图书馆受访者最担忧的三大问题为：（1）内容被篡改或捏造；（2）输入数据缺乏透明度；（3）AI 生成摘要的质量问题。内容提供商受访者最担忧的三大问题为：（1）版权侵权问题；（2）内容被篡改或捏造；（3）输入数据缺乏透明度。

3、图书馆受访者普遍认为，GAI 工具将提升网络级发现服务对用户和馆员的价值，尽管展现这一积极态度的并非压倒性多数。

4、内容提供商受访者对 GAI 的影响持审慎乐观态度：多数情况下期待其能提升自身内容的可见度，但对改善内容可及性的效果则持相对保留态度。

5、图书馆受访者尤其担心，GAI 模型的开发和查询处理需要大量数据中心支持，这可能带来环境问题。

来源：

美国国家信息标准组织（National Information Standards Organization）：

https://www.niso.org/publications/odi-ai-survey-report

https://www.dropbox.com/scl/fi/m0fs2pqtaqp2mkbdd35o3/NISO-ODI-Survey-Report-GenAI-and-Discovery_August2025.pdf?rlkey=4qlcvtj3ji55umugugk9flmjv&e=1&st=po8zkmrk&dl=0

✧ GB/T 45628-2025 人工智能 知识图谱 知识交换协议

【看点】国家标准化管理委员会于 4 月 25 日发布并实施了 GB/T 45628-2025《人工智能 知识图谱 知识交换协议》，适用于知识图谱相关系统的设计、开发、测试和部署等，由全国信息技术标准化技术委员会归口。

【摘要】该标准规定了知识交换协议总体框架、知识描述规则、基于文件的知识交换、基于消息的知识交换等。该标准描述知识交换协议，属于开放式系统互联参考模型的应用层，不包括进行知识交换时使用的通信协议。

知识图谱范畴的知识交换协议的构成如图 7，协议主要包括用于规范知识描述、知识交换以及相关的数据字典的一组规则。

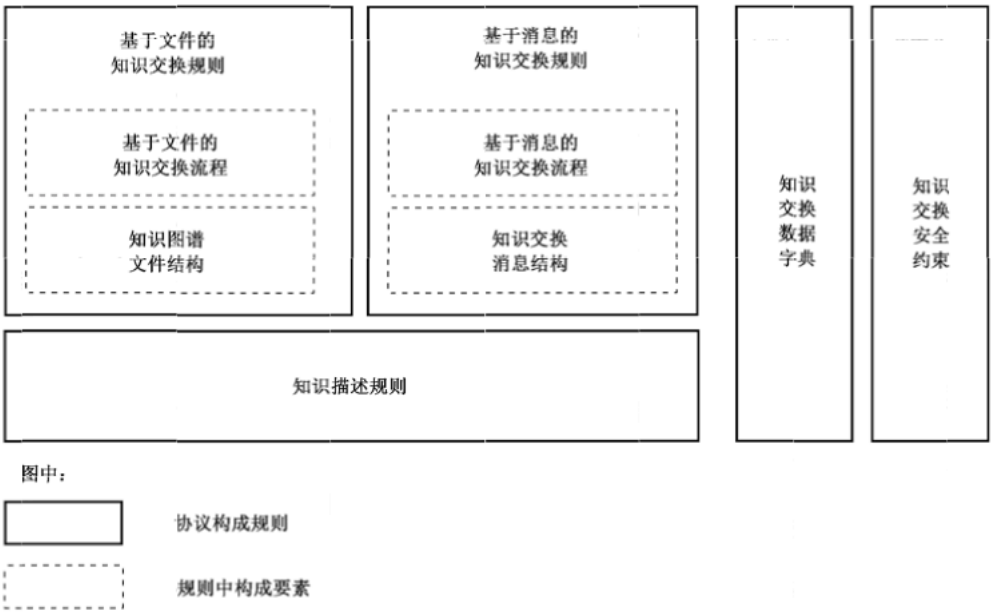

图 7 知识交换协议模型

知识交换活动涉及了知识提供方、知识消费方、知识中间方和服务管理方等四类逻辑角色，各个角色具有特定的功能职责、活动类型和数量（如图 8）。在实际的知识交换过程中，同一参与者可根据需要担任多个逻辑角色，但各角色间应保持解耦和权责独立，各方应满足数据安全要求。

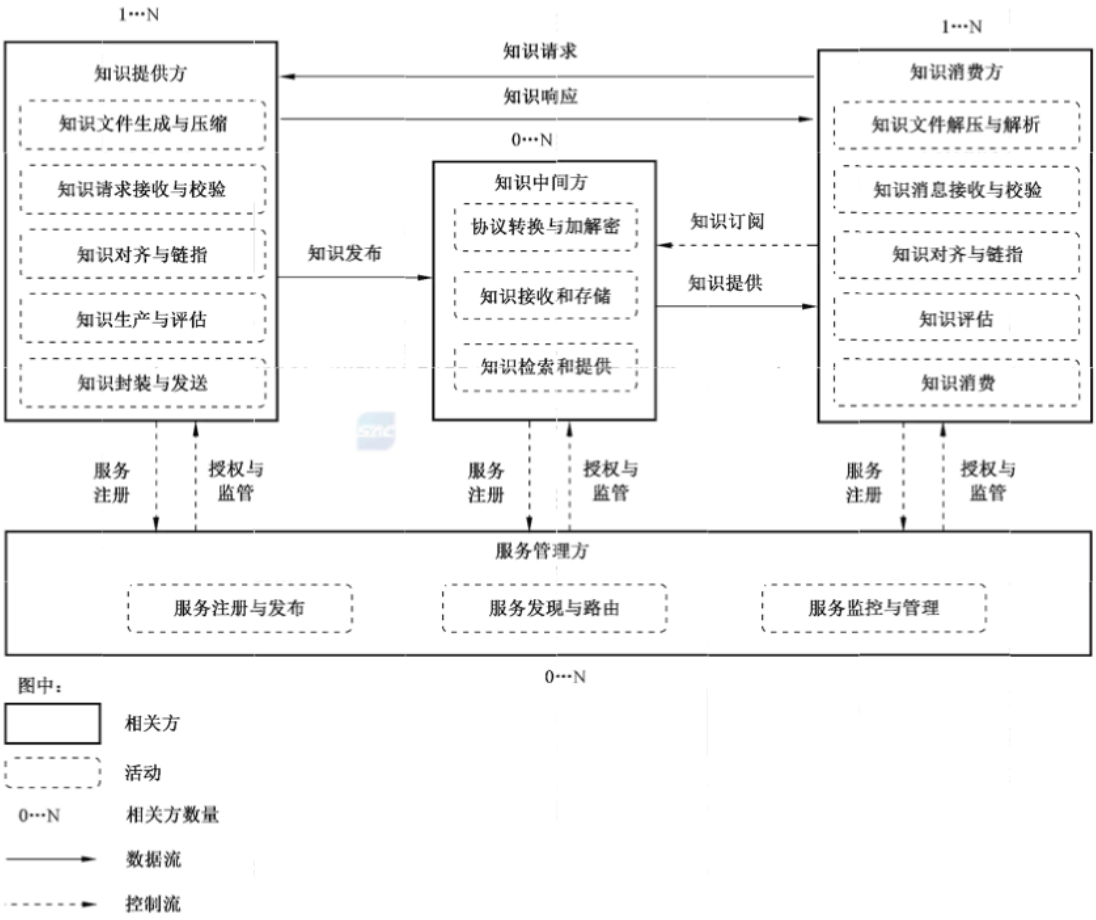

图 8 知识交换活动构成

来源：

全国标准信息公共服务平台：

https://std.samr.gov.cn/gb/search/gbDetailed?id=33D40F1161A85D92E06397BE0A0A5B93

国家标准全文公开系统：

https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=B8C141AB9E8D922A3D8285BEF067DC50

✧ GB/T 46284-2025 人工智能 联邦学习技术规范

【看点】国家标准化管理委员会于 10 月 5 日发布并实施了 GB/T 46284-2025《人工智能 联邦学习技术规范》，适用于联邦学习系统的设计、开发、测试、使用及运维，开展联邦学习应用系统的横向比较并选型，由全国信息技术标准化技术委员会归口。

【摘要】联邦学习（federated learning）指多个参与方在保证各自原始数据不出数据方定义的可信域前提下，以保护隐私数据的方式交互中间数据，从而协

作完成人工智能、机器学习任务的方法。联邦学习系统（federated learning system）是综合的计算机与通信系统，用于实现联邦学习方法。

该标准确立了联邦学习系统架构、任务参与方和任务流程，规定了联邦学习系统的功能要求和性能要求，描述了相应的测试方法。

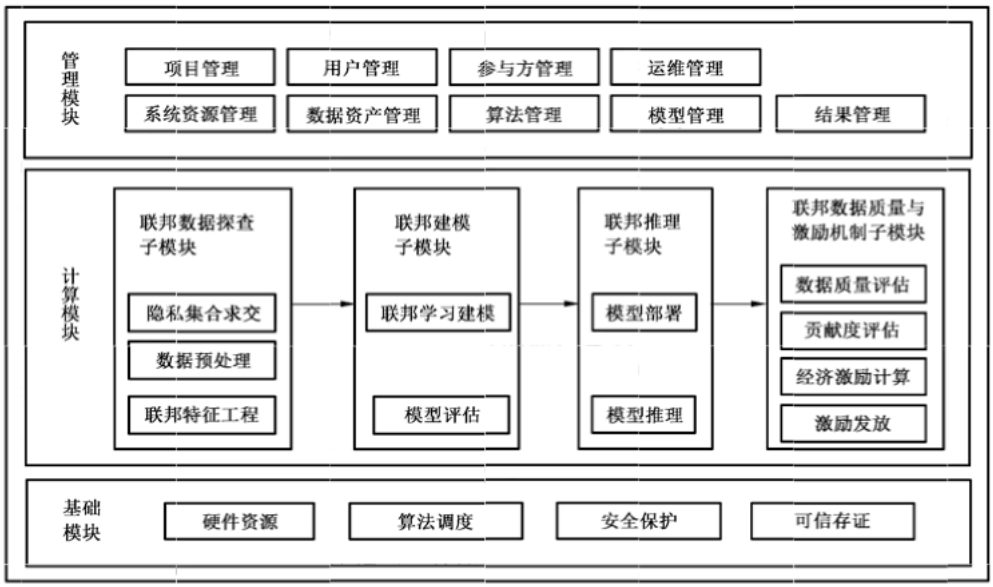

图 9 联邦学习系统架构

联邦学习系统架构如图 9，联邦学习系统各模块功能如下：

- 基础模块：支撑整个系统运行的底层核心模块，提供了基础的技术服务、公共能力以及工具支持，包含硬件资源、算法调度、安全保护和可信存证等；
- 计算模块：完成数据处理、数学计算、逻辑推理或与业务相关的特定计算任务，包含联邦数据探查子模块、联邦建模子模块、联邦推理子模块、联邦数据质量与激励机制子模块；
- 管理模块：围绕资源、数据、流程、权限以及配置等方面进行组织、控制和优化，以确保系统的高效运转、易维护性和安全性，包含系统资源管理、数据资产管理、算法管理、模型管理、结果管理、用户管理、参与方管理、项目管理、运维管理等。

来源：

全国标准信息公共服务平台：

https://std.samr.gov.cn/gb/search/gbDetailed?id=40B74A27FC92BD79E06397BE0A0AB048

国家标准全文公开系统：

https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=7E89571303D528CB14B84E9D85482F89

科技评价

✧ GB/T 46347-2025 人工智能 风险管理能力评估

【看点】国家标准化管理委员会于 10 月 5 日发布并实施了 GB/T 46347-2025《人工智能 风险管理能力评估》，以指导评估人员对组织的人工智能风险管理能力进行评估，由全国信息技术标准化技术委员会归口。

【摘要】该标准规定了组织的人工智能风险管理能力的级别与要求，描述了组织的人工智能风险管理能力的评估方法。人工智能风险管理能力框架包括风险管理策划、风险沟通、风险评估、风险处理、风险监控以及风险回顾 6 个能力域，各能力域由若干能力子域与能力项按照衡量相关能力所需维度规定（如表 2）。

表 2 人工智能风险管理能力框架

能力域	能力子域	能力项
风险管理策划	确定领导作用	确定组织方针
		确定人工智能风险管理目标
		进行资源协调
		指派职责
	制定风险政策	定义人工智能风险管理活动范围
		定义风险参数
		定义风险准则
		确定风险管理策略
		确定风险储备
风险沟通	沟通与咨询	风险沟通
		风险咨询
风险评估	风险识别	选择风险识别工具/技术/方法
		识别人工智能风险源
		识别风险后果
	风险分析	进行人工智能风险分分类
		进行风险概率分析
		进行风险影响分析
	风险评价	建立风险概率影响矩阵
		确定风险优先级
风险处理	风险应对	选择风险应对方案
		制定和实施风险处理计划
风险监控	监督与检查	风险监督
		风险检查
风险回顾	记录与报告	风险记录
		风险报告

人工智能风险管理包括风险管理策划、风险沟通、风险评估、风险处理、风险监控、风险回顾 6 个过程域（如图 10），人工智能风险管理能力等级由低到高依次分为初始级、受管理级、稳健级、量化管理级和优化级。

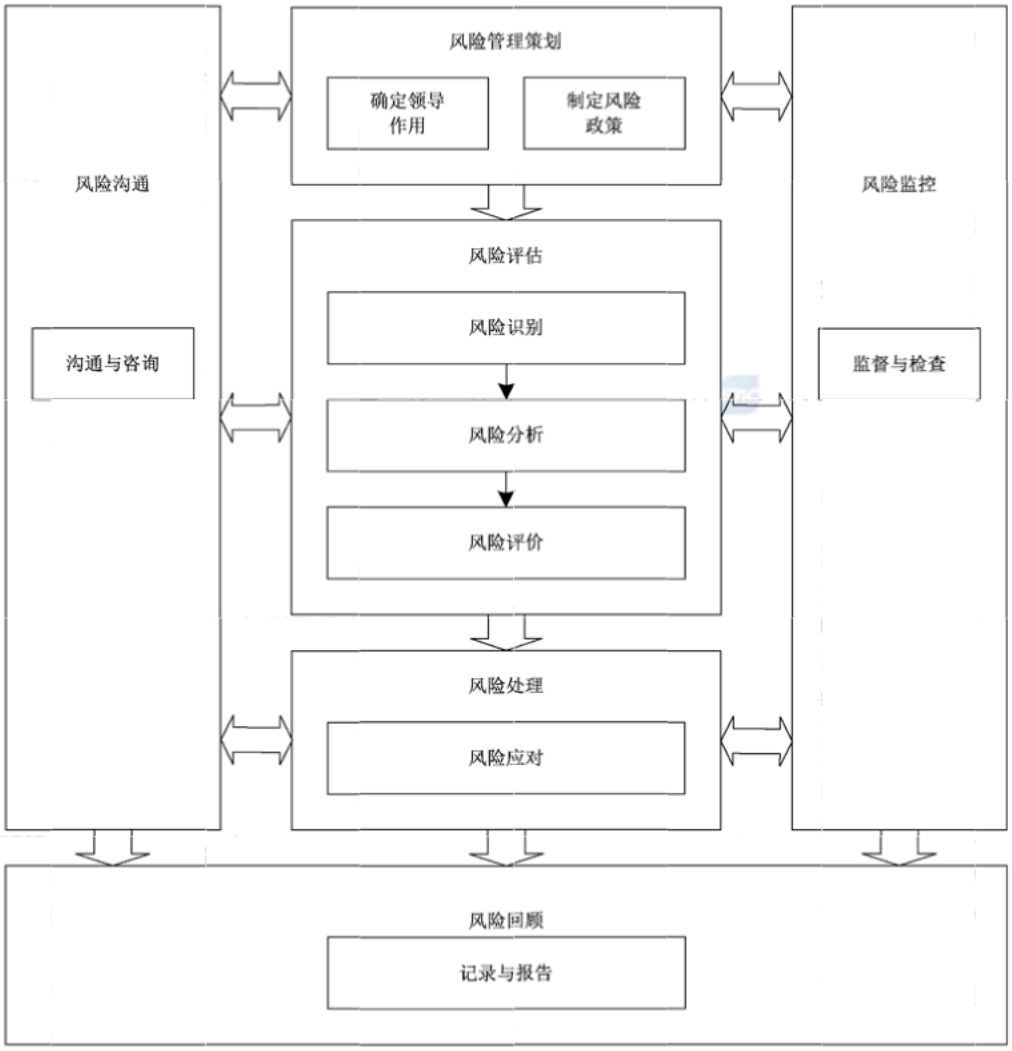

图 10 人工智能风险管理过程

来源：

全国标准信息公共服务平台：

https://std.samr.gov.cn/gb/search/gbDetailed?id=40B74A27FD32BD79E06397BE0A0AB048

国家标准全文公开系统：

https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=120779016BBA61E4408DCECE3EAD92ED

✧ GB/T 46346-2025 人工智能 计算中心 计算能力评估

【看点】国家标准化管理委员会于 10 月 5 日发布并实施了 GB/T 46346-2025《人工智能 计算中心 计算能力评估》，规定了人工智能计算中心计算能力的评估标准，描述了相应的评估方法，由全国信息技术标准化技术委员会归口。

【摘要】该标准规定了人工智能计算中心计算能力的评估标准，描述了相应的评估方法，适用于人工智能计算中心计算能力的评估，也为人工智能计算中心规划、设计、建设、服务和运维提供参考依据。

智算中心满足高性能、高稳定、高可靠、高可用等人工智能计算需求，为多个用户提供数据读写、模型训练、弹性推理等人工智能计算服务。智算中心技术架构（如图 11）由其中包含的 AI 加速器、网络互联部件、数据存储设备及相关配套软件（如：加速器驱动、加速器使能库、深度学习框架等）共同决定。

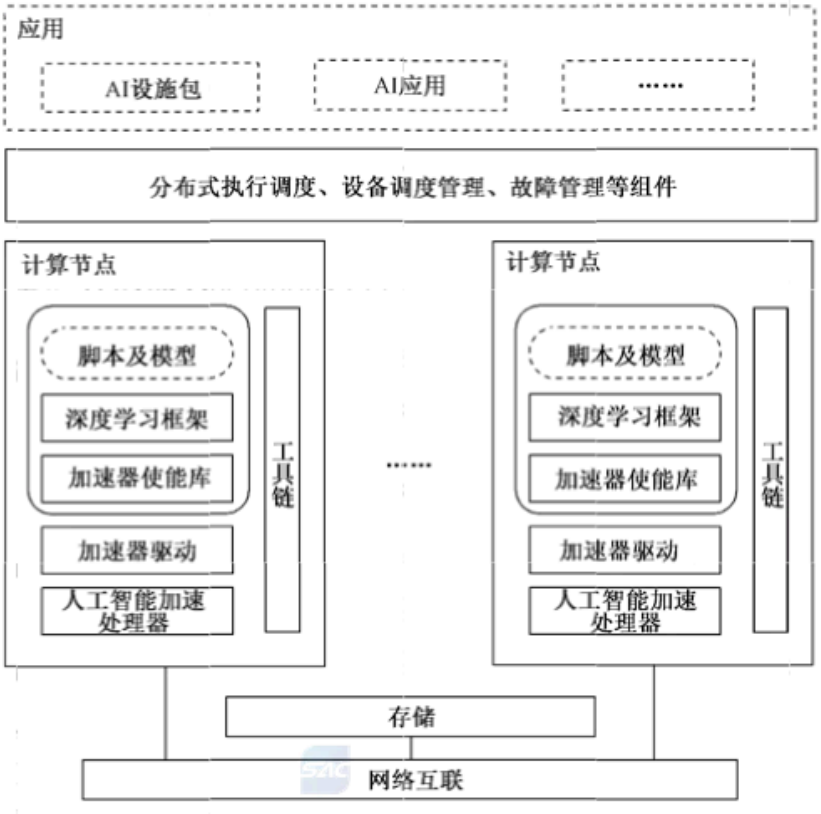

图 11 智算中心技术架构示意图

智算中心计算能力评估涉及多方面的考量，除了硬件设备本身能提供的物理人工智能计算能力（简称为“智能算力”）规模外，还包括通过任务调度、策略优化等技术有效整合计算、存储、网络设备的物理资源，以及为了支持人工智能业务，将计算资源转化为执行人工智能任务的计算能力。智算中心能力评估框架（如图 12）主要包括硬件规格能力、基础设施性能、业务处理能力三个层级，其中每个层级下划分了评估域，每一个评估域下包含一个或一组评估指标。

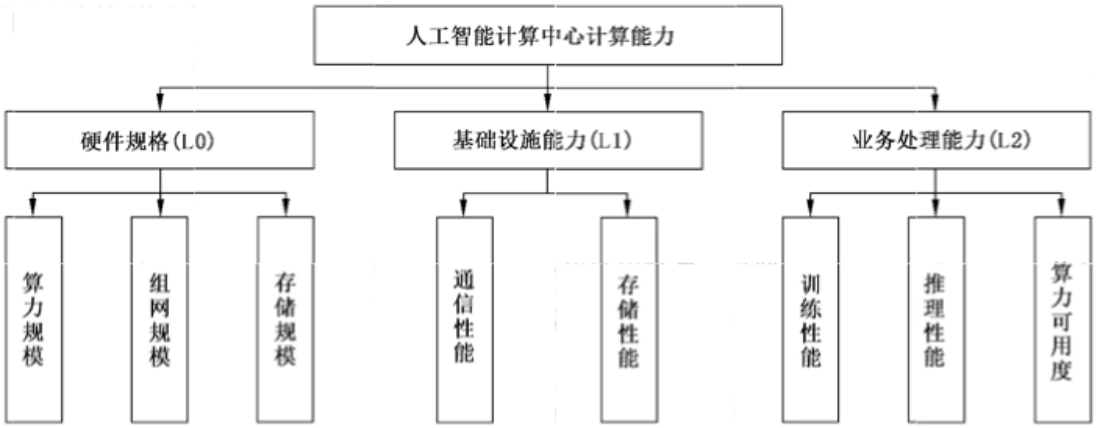

图 12 智算中心计算能力评估框架

来源：

全国标准信息公共服务平台：

https://std.samr.gov.cn/gb/search/gbDetailed?id=40B74A27FD30BD79E06397BE0A0AB048

国家标准全文公开系统：

https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=EAA759F5053C6B1EE75171F16267446F

✧ GB/T 45225-2025 人工智能 深度学习算法评估

【看点】国家标准化管理委员会于 1 月 24 日发布并实施了 GB/T 45225-2025《人工智能 深度学习算法评估》，适用于指导深度学习算法开发方、用户方以及第三方等相关组织对深度学习算法及其训练得到的深度学习模型开展评估工作，由全国信息技术标准化技术委员会归口。

【摘要】该标准确立了人工智能深度学习算法的评估指标体系，描述了评估方法等内容。深度学习算法的评估指标体系包括基础性能、效率、正确性、兼容性、可解释性、鲁棒性、安全性、公平性 8 个质量特性（如图 13）。

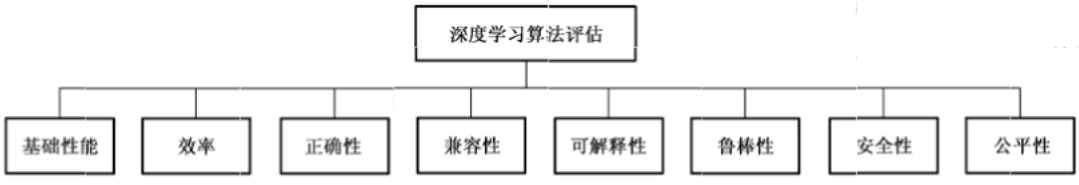

图 13 深度学习算法评估指标体系

基础性能指深度学习算法执行过程中的性能特征，不同算法可能涉及不同性能指标；效率指深度学习算法在达到给定性能目标时所消耗的资源与时间的多少；正确性指深度学习算法代码、功能等方面开发设计的正确性；兼容性指在相同软

硬件环境下，深度学习算法能够与其他产品、系统或组件交换信息和/或执行其所需的功能的程度；可解释性指深度学习算法对于结果的解释和理解能力；鲁棒性指面对非对抗增广的样本时，深度学习算法保持与实验环境中测试性能相当的能力；公平性指深度学习算法面向不同群体，保持相同输出质量的能力。

在实施评估过程中，应根据不同类型的深度学习算法，在不同质量特性下设置具体评估指标。根据算法失效的危险严重性等级，建立深度学习算法的等级目标（如表 3），从高到低依次分为优越级、进阶级、条件级、受限级四个级别。

表 3 深度学习算法的等级目标

等级目标	等级目标说明
优越级	外部环境发生扰动或面对不友好的输入，不依赖利益相关方的管理和配置，能采取有效措施，按照预期完成工作，不影响算法结果
进阶级	外部环境发生扰动或面对不友好的输入，通过利益相关方的配置及管理，待评估算法能按照预期完成工作，不影响算法结果
条件级	在友好的外部环境及输入下，待评估算法可以按照预期完成工作； 外部环境发生扰动或面对不友好的输入，通过利益相关方的配置与管理，待评估算法能按预期完成工作，不对算法结果造成重大影响
受限级	在友好的外部环境及输入下，待评估算法能按照预期完成工作； 当外部环境发生扰动或面对不友好的输入，待评估算法不能按照预期完成工作，可能对算法结果造成重大影响

深度学习算法的评估流程分为黑盒评估和白盒评估（如图 14），包括评估准备、评估执行、分析评估、评估结论等四大步骤。其中，评估准备包括输入测试数据集及算法参数、测试数据集质量审查、深度学习框架/模型的漏洞检查、选择质量特性、选择评估指标、构建评估模型等子步骤；评估执行包括推理阶段的执行、获取训练/推理阶段的数据、计算测试指标等子步骤；分析评估包括算法质量评估（多次评估）、分值计算、等级评估等子步骤；评估结论包括编制评估报告等。

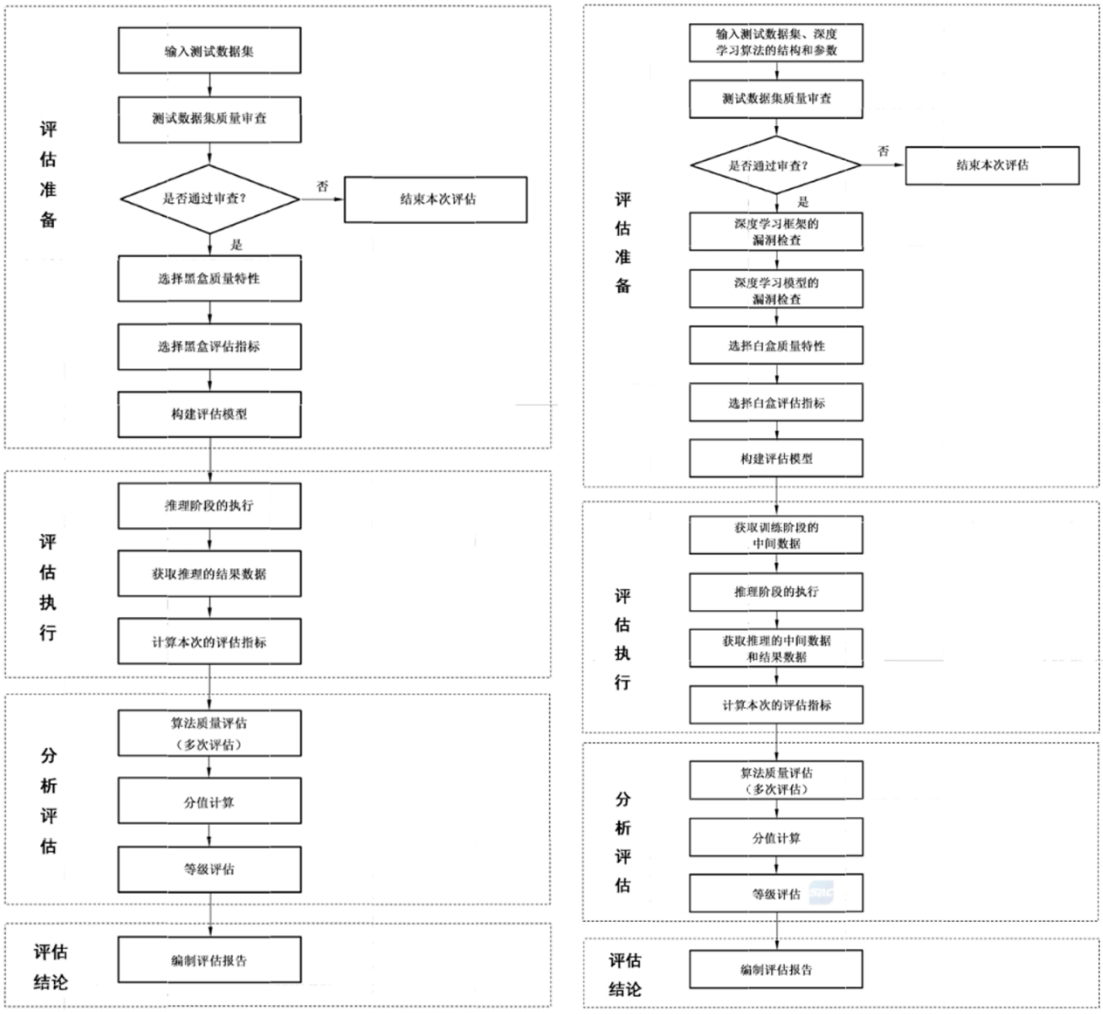

图 14 深度学习算法的黑盒评估流程（图左）和白盒评估流程（图右）

来源：

全国标准信息公共服务平台：

https://std.samr.gov.cn/gb/search/gbDetailed?id=2D5D2D0FF71A31E0E06397BE0A0A126F

国家标准全文公开系统：

https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=A53A9ED19FC16A692D1B200E5AB0F407