

ICS 点击此处添加 ICS 号

CCS 点击此处添加 CCS 号

团 体 标 准

T/CIIA XXXX—XXXX

科学数据安全能力成熟度评估规范

Maturity assessment specification of scientific data security capability

（征求意见稿）

（本草案完成时间：）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。



版权所有归属于该标准的发布机构，除非有其他规定，否则未经许可，此发行物及其章节不得以其他形式或任何手段进行复制、再版或使用，包括电子版，影印件，或发布在互联网及内部网络等。使用许可可于发布机构获取。

XXXX-XX-XX 发布

XXXX-XX-XX 实施

中国信息协会 发 布

目 次

前言 II

引 言 III

1 范围 4

2 规范性引用文件 4

3 术语和定义 4

4 评估内容 5

5 评估过程和要求 5

 5.1 概述 5

 5.2 评估过程 5

 5.3 评估准备阶段（P） 6

 5.4 评估实施阶段（D） 6

 5.5 评估评议阶段（C） 8

 5.6 改进提升阶段（A） 8

 5.7 评估要求 9

6 成熟度等级判定方法 9

 6.1 评分方法 9

 6.2 评估域权重 10

 6.3 计算方法 10

附录 A（资料性） 访谈大纲及评估证据检查打分示例 13

参考文献 15

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。

本文件由中国信息协会提出并归口。

本文件起草单位：

本文件主要起草人：

CIIA

引 言

科学数据是国家科技创新和经济社会发展的基础性战略资源，越来越深刻地影响着国家安全、经济发展和科技进步，科学数据的安全问题也面临着前所未有的挑战。科学数据中心是科学数据的载体，发挥了科学数据汇聚管理、开放共享和应用服务的重要作用，承担科学数据安全的重要使命。

科学数据安全能力成熟度，是指科学数据中心具备的科学、安全、有序管理科学数据的能力等级，从科学数据全生命周期中提炼出19个安全过程域，分别从组织建设、制度流程、技术工具和人员能力四个方面逐一阐述不同等级下应具备的安全能力。科学数据安全能力成熟度模型，可用于指导科学数据中心开展安全能力自评估，为国家和行业主管部门组织开展科学数据安全评估提供规范指引，为全面提升科学数据安全提供支撑和保障。

本文件提出的科学数据安全能力成熟度评估规范，是T/CIIA 019—2022《科学数据 安全能力成熟度模型》配套的实践方法，为科学数据安全能力成熟度模型贯彻实施提供指导，为科学数据安全能力提升提供指引。

科学数据安全能力成熟度评估规范

1 范围

本文件规定了科学数据安全能力成熟度模型的评估内容、评估过程、评估要求和成熟度等级判定方法。

本文件适用于使用科学数据安全能力成熟度模型开展评估工作。

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。

T/CIIA 019—2022 科学数据 安全能力成熟度模型

3 术语和定义

T/CIIA 019—2022 界定的以及下列术语和定义适用于本文件。

3.1

评估域 assessment domain

用于开展科学数据安全能力成熟度评估的核心条款的集合。

3.2

科学数据 scientific data

人类社会科技活动积累的或通过其他方式获取的反映客观世界的本质、特征、变化规律等原始性、基础性数据，以及根据不同科技活动需要进行系统加工整理的各类数据的集合。

[来源：GB/T 31075—2014，2.2.7]

3.3

科学数据安全 scientific data security

通过管理和技术措施，确保科学数据持续得到有效保护和合规利用的状态。

[来源：GB/T 37988—2019，3.1，有修改]

3.4

科学数据中心 scientific data center

利用信息、网络等现代技术，对科学数据进行整合汇交、分级分类、加工整理和分析挖掘，保障科学数据安全，推动科学数据开放共享，加强国内外科学数据交流与合作的专业化机构。

3.5

能力成熟度 capability maturity

对一个组织有条理的持续改进能力以及实现特定过程的连续性、可持续性、有效性和可信度水平。

3.6

科学数据安全能力成熟度模型 scientific data security capability maturity model

用于对科学数据中心等组织机构的科学数据安全保障能力成熟度进行评估的模型。

3.7

评估单位 assessed organization

接受数据安全能力成熟度评估的单位。

3.8

评估机构 assessing institution

依据科学数据安全能力成熟度模型，对评估单位进行贯标、取证、评估和出具报告的机构。

3.9

评估管理机构 assessment management institution

对科学数据安全能力成熟度证书的颁发、换发、补发、变更、注销等工作进行管理的机构。

4 评估内容

依据科学数据在采集、汇交、保存、共享、利用等生命周期的五个阶段对科学数据安全能力要求进行评估，并确定其评估域。

评估域应包含评估单位建设、制度流程、技术工具、人员能力等要素。其中，科学数据采集、科学数据汇交、科学数据保存下的能力域和能力子项为必选内容。科学数据共享和科学数据利用下的能力域和能力子项为可选项。

科学数据安全能力成熟度评估内容见表1。

表1 科学数据安全能力成熟度评估内容

能力域	科学数据采集	科学数据汇交	科学数据保存	科学数据共享	科学数据利用
能力项	数据分类分级	数据形式审查	存储媒介安全	数据发布安全	数据分析安全
	数据采集获取	数据质量审查	数据逻辑存储	数据出境安全	增值服务安全
	清洗转换加载	传输安全管理	数据备份恢复	数据接口安全	数据出版安全
	数据溯源安全		数据导入导出		数据引用安全
评估域	不可裁剪	不可裁剪	不可裁剪	可裁剪	可裁剪

注：灰底部分为可选项。

5 评估过程和要求

5.1 概述

评估过程主要涉及评估单位、评估机构、评估管理机构等相关方，本章节将明确在评估过程各阶段中涉及的相关方承担的责任、分工和要求等内容。评估具体指标见T/CIIA 019—2022。

5.2 评估过程

科学数据安全能力成熟度评估流程包括评估准备、评估实施、评估评议和改进提升四个阶段。见图1。

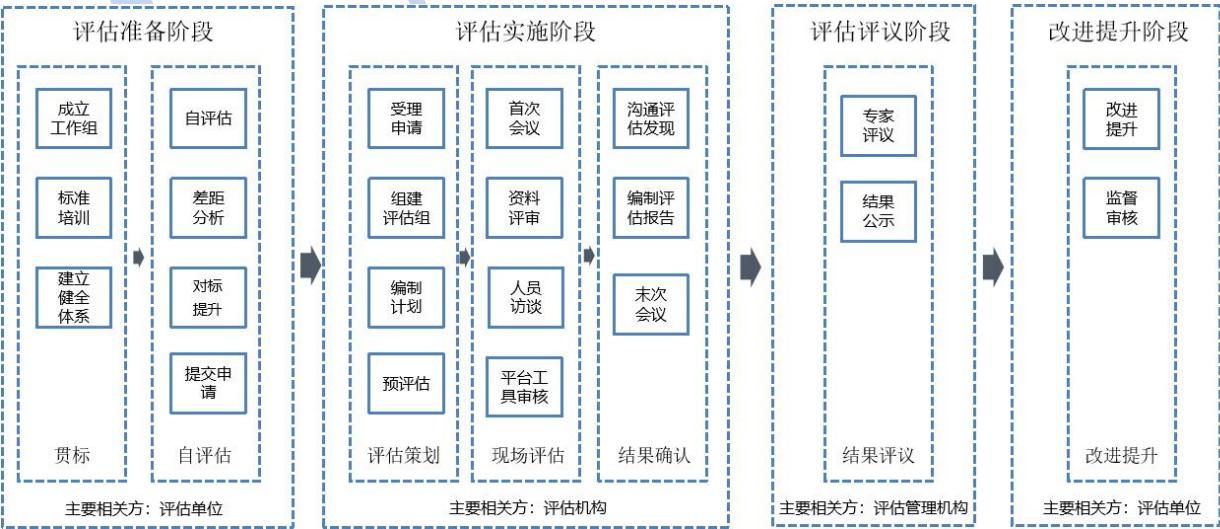


图 1 科学数据安全能力成熟度评估流程

5.3 评估准备阶段（P）

5.3.1 贯标

5.3.1.1 成立工作组

评估单位应成立工作组，协调相关人员并明确分工职责，制定初步工作计划。

5.3.1.2 标准培训

评估单位因应参加宣贯会或培训课程了解标准相关要求及评估要点。

5.3.1.3 建立健全体系

评估单位应梳理内部相关制度文件，初步对标建立健全管理体系。

5.3.2 自评

5.3.2.1 对标评估

评估单位应通过在线平台或评估报告的形式完成对标评估。

5.3.2.2 差距分析

贯标工作启动后，评估单位可申请评估机构协助进行差距分析。

5.3.2.3 对标提升

评估单位应建立数据管理评估单位，完善制度，内部运行并提升。

5.3.2.4 提交申请

评估单位应向评估机构提交有效的申请材料。

5.4 评估实施阶段（D）

5.4.1 评估策划

5.4.1.1 受理申请

评估机构受理评估单位的申请材料，并明确下列信息：

- a) 评估单位评估的范围；
- b) 评估单位的基本情况，包括名称、场地、评估单位架构、规模、人员、技术、平台、工具等以及任何与评估相关的法律义务；
- c) 评估单位申请评估体系有关的咨询，若有，提供咨询方的相关信息；
- d) 评估单位的其他要求等。

5.4.1.2 组建评估工作组

评估机构应根据实现评估目的所需要的能力以及公正性的要求来选择和任命评估工作组（包括评估工作组组长、组员以及必要的技术专家）。评估工作组应具备相关的评估能力。在评估工作组成立时，应明确下列信息：

- a) 评估目的、范围、准则和预计的评估时间；
- b) 实现评估目的所需要的评估工作组整体能力。

5.4.1.3 编写计划

评估工作组应确保编制评估方案中确定的每次评估计划，以便有关各方对评估活动的计划安排和实施时间达成一致提供依据。编写计划主要包括下列内容：

- a) 编制评估计划；
- b) 评估任务及计划的沟通。

5.4.1.4 预评估

评估工作组在预评估过程中，应明确下列内容：

- a) 审查评估单位已有的文件化管理体系信息；
- b) 评价评估单位现场的具体情况，并与评估单位的人员进行讨论，以确定下阶段工作的准备情况；
- c) 审查评估单位理解和实施标准要求的情况，特别是对管理体系的关键绩效或重要能力项、过程、目标识别的情况；
- d) 收集关于评估单位相关范围的必要信息，包括场地、工具、系统、平台、数据量、数据分布等情况，以及适用的法律法规要求；
- e) 审查所需资源的配置情况，并与评估单位商定细节；
- f) 结合标准或其他规范性文件充分了解评估单位相关现场的情况，以便提供关注点；
- g) 评价评估单位是否策划和实施了内部评估和管理评审，以及相关能力域实施程度是否证明评估单位已经为现场评估做好准备。

5.4.2 现场评估

5.4.2.1 首次会议

评估工作组应与评估单位的管理层、评估职能域或过程的负责人员及相关人员召开正式的首次会议，并记录参加人员。首次会议通常由评估工作组长主持，会议的目的是简要解释将如何进行评估活动，介绍参会人员（包括简要介绍角色和评估分工）后并应确认下列内容：

- a) 评估范围；
- b) 评估计划（包括评估的内容、范围、目的、准则）及其任何变化，以及与评估单位的其他相关安排，如末次会议的日期和时间，评估期间评估工作组与评估单位管理层沟通的时间等；
- c) 评估工作组与评估单位之间正式沟通的渠道；
- d) 评估工作组可获得所需的资源和设备；
- e) 与保密有关的事宜，如需要签订保密协议等；
- f) 适用于评估工作组的相关的工作安全、应急和安保程序；
- g) 可得到向导和观察员的角色和身份以及所需的权限；
- h) 评估单位补充说明等。

5.4.2.2 资料评审

评估工作组应对评估单位的资料进行评审，包括评估单位层面及部门层面的规章、制度、规范和管理规定等，以及评估单位在管理过程中的过程文档（如会议纪要、会签记录等）。

5.4.2.3 人员访谈

评估工作组应对评估单位的规章制度执行以及数据管理平台使用情况进行人员访谈，确认其实施过程与客观证据是否保持一致。

注：访谈方式及流程见附录A。

5.4.2.4 平台工具评估

评估工作组应对评估单位的数据管理平台使用情况进行核验，通过演示及查阅日志报告等形式，确认其实施过程与客观证据是否保持一致。

5.4.3 结果确认

5.4.3.1 沟通评估发现

评估工作组应确定评估发现，概述其符合性并详细描述情况，并予以分类和报告，为评估决定或保持认定提供充分的信息。

关于不符合项的审查发现，评估工作组应对照具体要求予以记录，包含对不符合项的清晰描述，详细标识并记录不符合项的客观证据。并与评估单位讨论不符合项，以确保证据准确且不满足项得到理解。

5.4.3.2 编制评估报告

评估工作组应向评估单位提供评估书面报告。评估工作组可识别改进机会，但不应提出具体解决办法的建议。评估机构享受有对评估报告的所有权，并在评估报告中明确下列内容：

- a) 注明评估机构；
- a) 评估单位的名称和地址及评估单位的代表；
- b) 评估的类型（如初次、监督、再评估或特殊评估）；
- c) 评估准则；
- d) 评估目的；
- e) 评估范围，特别是标识出所评估单位或部门的评估过程及评估时间；
- f) 任何偏离评估计划的情况及理由；
- g) 任何影响评估方案的重要事项；
- h) 注明评估工作组组长、评估工作组员及任何与评估工作组同行的人员；
- i) 评估活动（现场或非现场，永久或临时场所）的实施日期和地点；
- j) 与评估类型的要求一致的评估发现、对评估证据的引用及评估结论。

5.4.3.3 末次会议

评估工作组应与评估单位的管理层、评估职能域或过程的负责人员及相关人员召开正式的末次会议，并记录参加人员。末次会议通常由评估工作组组长主持，会议目的是提出评估结论，包括关于评估的推荐性意见。不符合项应以使其被理解的方式提出，并应就回应的时间达成一致。

末次会议的内容应包括以下内容，详略程度可根据评估单位对评估过程的熟悉程度确定：

- a) 向评估单位说明所获取的评估证据是基于对信息的抽样，因而会有一定的不确定性；
- b) 进行报告的方法和时间表，包括评估发现的任何分级；
- c) 评估机构处理不符合项（包括与评估单位评估状态有关的任何结果）的过程；
- d) 评估单位为评估中发现的任何不符合项的纠正措施提出计划表；
- e) 评估机构在评估后的活动；
- f) 说明投诉和申诉处理过程。

5.5 评估评议阶段（C）

5.5.1 专家评议

评估管理机构负责组织评估专家，对评估机构报送的评估结果进行合规性审查。对合规性审查中发现的存在较大问题的评估结果，评估管理机构有权驳回。对于评估机构推荐的高级别评估结论，评估管理机构应组织评估专家对评估单位进行现场答辩及线下抽查等活动。

5.5.2 结果公示

评估管理机构对通过审查、复核或评议的评估单位进行为期一周的公示（例如网站等）。无异议的，由评估机构颁发评估证书。

5.6 改进提升阶段（A）

5.6.1 改进提升

评估单位评估周期内持续改进提升措施应包括下列方面：

- a) 内部评估和管理评审；
- b) 对评估中确定的不符合采取的措施；

- c) 在实现获证评估单位目标和预期结果方面的有效性；
- d) 为持续改进而策划活动的进展；
- e) 持续的运作控制；
- f) 变更的情况。

5.6.2 监督评估

评估机构应对监督活动进行设计，以便定期对范围内有代表性的区域和职能进行监视，并应考虑获证评估单位及其体系变更的情况。

监督活动除包括对获证评估单位标准规定要求情况的现场评估，还可包括：

- a) 就评估的有关方面询问获证评估单位；
- b) 审查获证评估单位对其运作的说明（如宣传材料、网页）；
- c) 要求获证评估单位提供文件化信息（纸质或电子介质）；
- d) 其他监视获证评估单位绩效的方法。

5.7 评估要求

5.7.1 评估单位要求

评估单位应为在中华人民共和国境内依法注册、根据中华人民共和国有关法律合法成立的独立法人或其他组织。

5.7.2 评估机构要求

评估机构应符合下列要求：

- a) 应为在中华人民共和国境内依法注册、根据中华人民共和国有关法律合法成立的独立法人或其他组织；
- b) 应具备由评估管理机构正式颁发的评估机构证明；
- c) 应建立评估工作管理体系，明确责任分工，完善监督考核，对评估师的评估行为负责；
- d) 应对评估师进行考核。

5.7.3 评估师要求

评估师应符合下列要求：

- a) 应持有评估管理机构颁发的评估师资格证书；
- b) 须遵守法律法规、行业准则、自律规则，对评估结论的真实性、准确性负责。

5.7.4 评估管理机构要求

评估管理机构应符合下列要求：

- a) 应制定评估工作相关制度；
- b) 应监督管理评估流程、评估行为、评估质量；
- c) 应对评估机构进行遴选和考核；
- d) 应进行评估师培训、评估师证书管理；
- e) 应对评估证书的颁发、换发、补发、变更、注销、到期等工作进行管理；
- f) 应提供评估工作管理系统，用于评估流程管理，具备评估申请、自评估、信息发布、信息查询、投诉建议等功能；
- g) 应保留原始评估材料以备查验；
- h) 应协宣传、推广等相关工作。

6 成熟度等级判定方法

6.1 评分方法

成熟度等级判定方法是根据符合度分值划定成熟度要求满足程度，成熟度要求满足程度与得分对应表见表2。

表 2 成熟度要求满足程度与得分对应表

成熟度要求满足程度	符合度分值
满足要求	100%
大部分满足要求	70%
部分满足	50%
不满足	0

6.2 评估域权重

科学数据安全能力成熟度等级采取加权方式计算。具体能力域权重系数根据试行验证情况优化并动态调整。评估域权重应符合表3。

表 3 四大能力域与能力项对应能力域权重表

要素	能力域	能力域权重
科学数据采集	数据分类分级	0.05
	数据采集获取	0.05
	清洗转换加载	0.05
	数据溯源安全	0.05
科学数据汇交	数据形式审查	0.07
	数据质量审查	0.07
	传输安全管理	0.06
科学数据保存	存储媒介安全	0.05
	数据逻辑存储	0.05
	数据备份恢复	0.05
	数据导入导出	0.05
科学数据共享	数据发布安全	0.07
	数据出境安全	0.07
	数据接口安全	0.06
科学数据利用	数据分析安全	0.05
	增值服务安全	0.05
	数据出版安全	0.05
	数据引用安全	0.05

6.3 计算方法

综合评估流程及计算方法如下：

第一步：组织或机构根据能力域的具体要求，对满足要求的符合性进行评价打分，得到具体分值。

第二步：通过算术平均方法计算综合得分，并由各能力域的综合分值加权计算出相应要素的分值，计算方法见公式（1）。

$$S_i = s_k \times w_k, i = 1, 2, 3; k = 1, 2, \dots, j \dots\dots\dots (1)$$

式中：

s_k ——第 i 个能力域第 k 个要求的综合分值；

w_k ——第 i 个能力域第 k 个要求的权重值。

第三步：根据各个要素的属性，对各个要素进行加权求和，得到综合性能力分值，计算方法见公式（2）。

$$S = s_i \times w_i, i = 1, 2, 3 \dots\dots\dots (2)$$

式中：

s_i ——第 i 个要素的加权分值；
 w_i ——第 i 个要素的权重值。

CIIA

CIIA

附录 A

(资料性)

访谈大纲及评估证据检查打分示例

A.1 高层访谈大纲

高层访谈大纲主要包括下列内容：

- a) 为什么实施科学数据安全管理工作？
- b) 实施科学数据安全管理工作领导做了哪些工作（评估单位启动、投入资源、建设流程及机制）？
- c) 在实施科学数据安全管理工作过程中领导参与了哪些活动（亲自参与、督促检查）？
- d) 你是如何了解过程改进（项目实施）过程中存在的问题？
- e) 实施科学数据安全管理工作有何效果？（取得的、期望的）
- f) 对科学数据安全管理工作评价有何想法、意见、建议？

A.2 管理者代表访谈大纲

管理者代表访谈大纲主要包括下列内容：

- a) 如何分配项目资源（技术资源、人力资源、设备资源）？
- b) 如何掌控项目进展情况？
- c) 如何考核项目实施效果？
- d) 如何监控和处理项目的风险？
- e) 如何解决项目中遇到的问题？
- f) 对科学数据安全管理工作评价有何想法、意见、建议？

A.3 数据安全工作组访谈大纲

数据安全工作组访谈大纲主要包括下列内容：

- a) 如何策划实施科学数据安全管理工作？
- b) 科学数据安全管理工作实际情况如何与标准相结合的？
- c) 在体系文件建立过程中是如何策划和考虑的？
- d) 标准、体系文件培训是如何开展的，如何监控和考核的？
- e) 项目实施过程中是否如何指导项目组按照体系执行的、如何监控项目实施情况的？
- f) 在整个科学数据安全管理工作实施过程中是如何改进数据安全相关软件研制过程的？
- g) 科学数据安全管理工作实施过程的数据是通过什么手段分析的，如何向高层汇报的？

A.4 能力域相关人员访谈大纲

能力域相关人员访谈大纲主要包括下列内容：

- a) 项目中的管理情况；
- b) 项目中的一些技术问题的处理；
- c) 根据项目具体情况，临时性问题。

A.5 访谈提问单及打分表

访谈提问能力项基本信息见表 A.1，能力项打分表见表 A.2。

表 A.1 能力项基本信息

能力项基本信息	
能力域	
能力项	
访谈角色	
访谈时间	

访谈地点	
能力项得分	

表 A. 2 能力项打分表

能力项	能力标准	文档证据	访谈问题	访谈回答	存在问题	符合程度	备注	得分情况

CIIA

参 考 文 献

- [1] GB/T 30271—2013 信息安全技术 信息安全服务能力评估准则
- [2] GB/T 31075—2014 科技平台 通用术语
- [3] GB/T 32923—2016 信息技术 安全技术 信息安全治理
- [4] GB/T 33136—2016 信息技术服务 数据中心服务能力成熟度模型
- [5] GB/T 35069—2022 信息安全技术 术语
- [6] GB/T 35274—2017 信息安全技术 大数据服务安全能力要求
- [7] GB/T 36073—2018 数据管理能力成熟度评估模型
- [8] GB/T 36344—2018 信息技术 数据质量评价指标
- [9] GB/T 37973—2019 信息安全技术 大数据安全管理指南
- [10] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型