

公共数据共享开放安全风险评估规范

Security risk assessment specification for open sharing of public data

2024 - 04 - 15 发布

2024 - 06 - 01 实施

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 评估原则 4

 4.1 合法性原则 4

 4.2 科学性原则 4

 4.3 扩展性原则 5

 4.4 实用性原则 5

5 共享开放属性分类 5

 5.1 共享属性分类 5

 5.2 开放属性分类 5

6 评估对象和方式 5

 6.1 评估对象 5

 6.2 评估方式 5

7 评估指标 6

8 评估流程 6

 8.1 评估流程图 6

 8.2 评估准备 6

 8.3 评估实施 7

 8.4 风险分析与评价 9

 8.5 编制报告 9

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。

本文件由滨州市大数据局提出、归口并组织实施。

本文件起草单位：滨州市智慧城市指挥运营中心。

本文件主要起草人：王耀磊、刘芊麟、肖俊辉、吴宗月、吴世柱、张汉英、林静。

引 言

为深入贯彻落实数字山东发展规划，扎实推进数字山东标准提升工程，充分发挥标准规范在数字山东建设中的支撑作用，制定本文件。

本文将规范公共数据共享开放安全风险评估工作，促进公共数据共享开放的规范化、标准化，为数据安全增加保障。

公共数据共享开放安全风险评估规范

1 范围

本文件规定了公共数据共享开放安全风险评估的评估原则、开放属性分类、评估对象和方式、评估指标、评估流程。

本文件适用于公共数据共享开放安全风险的评估。

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 4754 国民经济行业分类
GB/T 10113 分类与编码通用术语
GB/T 25069 信息安全技术 术语
GB/T 352957 信息技术 大数据 术语
GB/T 38667 信息技术 大数据 数据分类指南
GB/T 35273 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 4754、GB/T 10113、GB/T 25069、GB/T 35295和GB/T 38667、GB/T 35273界定的以及下列术语和定义适用于本文件。

3.1

公共数据 public data

国家机关、法律法规授权的具有管理公共事务职能的组织（以下统称公共管理和服务机构）在依法履行职责和提供公共服务过程中获取的数据资源以及法律法规规定纳入公共数据管理范围的其他数据资源。

3.2

共享开放行为 Sharing open behavior

公共管理和服务机构面向社会提供具备原始性、可机器读取、可供社会化利用的数据集的公共服务。

4 评估原则

4.1 合法性原则

公共数据共享开放风险评估应遵循有关法律法规及部门规定要求，优先对国家或行业有专门管理要求的数据进行识别和管理，满足相应的数据安全要求。

4.2 科学性原则

应按照公共数据的多维特征和相互间客观存在的逻辑关联，进行系统化科学化的风险评估。

4.3 扩展性原则

公共数据共享开放风险评估在总体上应具有兼容性、可扩展性，以满足未来阶段可能出现的类目增减和数据类型变化需求。

4.4 实用性原则

不设置无意义的评估项目，避免过于复杂的评估规则，设定的评估规则符合普遍认知且综合实用。

5 共享开放属性分类

5.1 共享属性分类

数据共享分为无条件共享、有条件共享和不予共享三类：

- 无附加条件共享的数据称为无条件共享类；
- 符合设定条件并通过授权共享的数据称为有条件共享类；
- 依照法律、行政法规、部门规章规定不得共享的数据称为不予共享类。

5.2 开放属性分类

公共数据按照开放属性分为无条件开放类、有条件开放类和不予开放类三种类型：

- 对涉及国家安全、商业秘密、保密商务信息、个人隐私、个人信息，或者法律、法规、规章规定不得开放的公共数据，列入不予开放类；
- 对数据安全和处理能力要求较高、时效性较强或者需要持续获取的公共数据，列入有条件开放类；其他公共数据列入无条件开放类。

不予开放类公共数据依法经过脱密、脱敏处理或者相关权利人同意开放的，可以列入无条件开放类或者有条件开放类。

6 评估对象和方式

6.1 评估对象

公共管理和服务机构之间因履行职责和提供公共服务，需要通过政务数据统一共享交换平台使用的公共数据。

6.2 评估方式

6.2.1 自评评估

数据管理机构应对本机构所管理的公共数据进行风险自评评估，确定公共数据的共享开放属性和共享开放范围，并制定风险应对措施。

6.2.2 专项评估

存在以下情形的，数据管理机构可向同级大数据行政主管部门或专业第三方机构提请风险专项评估：

- 对造成或者可能造成数据安全风险不明确或无法确定的；
- 公共数据提供方以数据安全和风险为理由不共享、不开放数据，公共数据需求方有异议的；
- 在公共数据管理过程中其他可能造成数据安全和风险的情形。

7 评估指标

安全评估项目包括制度规范、技术防护和运行管理，具体指标见附录A。

8 评估流程

8.1 评估流程图

评估流程图见图1。

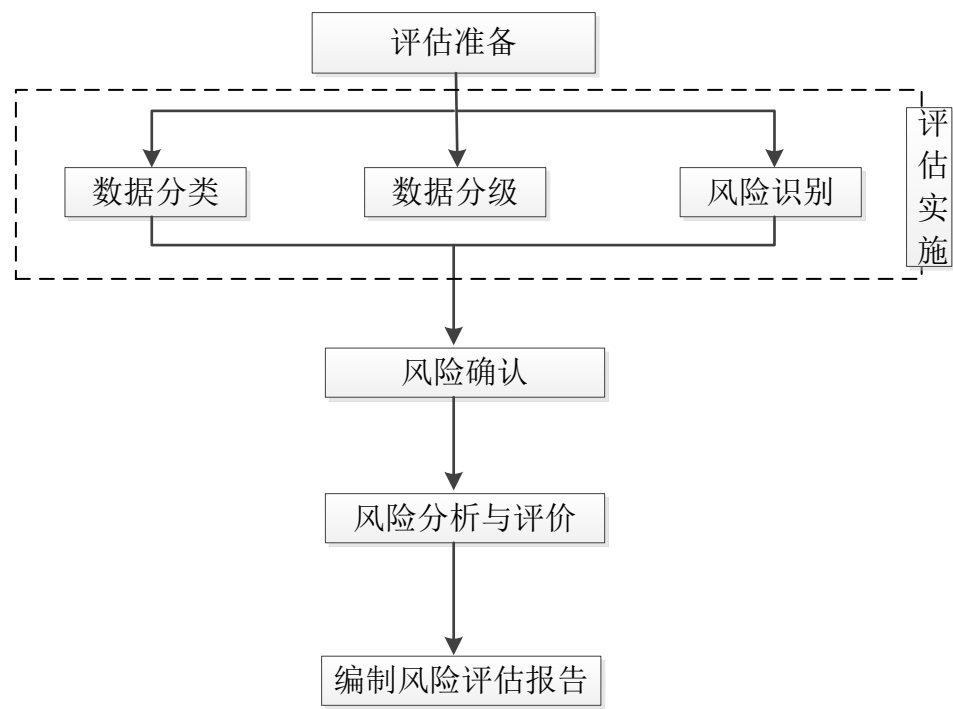


图1 公共数据共享开放安全评估流程图

8.2 评估准备

工作内容包括：

- 在考虑风险评估的工作形式、在生命周期中所处阶段和被评估单位的安全评估需求的基础上，确定风险评估目标；
- 确定风险评估的对象、范围和边界；
- 组建评估团队；
- 开展前期调研；
- 确定评估依据和指标；
- 建立风险评价准则；
- 制定评估方案。

8.3 评估实施

8.3.1 数据分类

可根据实际情况，从数据对象、数据管理、业务应用等不同维度进行分类：

- 数据对象维度：根据数据对象内容对数据进行分类；
- 数据管理维度：根据数据产生频率、产生方式、结构化特征、存储方式、质量要求等对数据进行分类；
- 业务应用维度：根据数据产生来源、所属行业、应用领域、使用频率、共享属性、开放属性等对数据进行分类。

8.3.2 数据分级

8.3.2.1 从公共数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、经济运行、社会稳定、公共利益、组织权益、个人权益可能造成的危害程度，将公共数据划分为：核心数据、重要数据和一般数据。具体分级参见表 1。

表1 数据分级

影响对象	级别		
	核心数据	重要数据	一般数据
国家安全	极其严重、严重	中等、轻微	无
经济运行	极其严重	严重、中等、轻微	无
影响对象	级别		
	核心数据	重要数据	一般数据
社会稳定	极其严重	严重	中等、轻微、无
公共利益	极其严重	严重	中等、轻微、无
个人权益	——	——	极其严重、严重、中等、轻微、无
组织权益	——	——	极其严重、严重、中等、轻微、无

8.3.2.2 由于一般数据涵盖范围较广，采用同一安全级别保护可能无法满足不同数据的安全需求，将一般数据从高到低分为：敏感数据（4 级）、较敏感数据（3 级）、低敏感数据（2 级）、不敏感数据（1 级）。具体分级见表 2。

表2 一般数据分级

数据级别	敏感级别	影响对象	影响程度	判断标准
4 级	敏感	国家安全	无	1. 数据一般不可被共享和开放，或可通过申请向特定单位或人员公开。 2. 数据遭泄露、篡改、破坏或者非法获取、非法利用、非法共享后，对国家安全、经济运行无危害；
		经济运行	无	
		社会稳定	中等、轻微	
		公共利益	中等、轻微	

		组织权益	极其严重	对社会稳定、公共利益造成中等或轻微危害；对个人权益、组织权益造成极其严重危害。
		个人权益	极其严重	
3 级	较敏感	国家安全	无	1. 数据可进行受限共享和开放。可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用；可提供给部分或部分提供给个人和组织开放使用。 2. 数据遭泄露、篡改、破坏或者非法获取、非法利用、非法共享后，对组织权益、个人权益造成严重危害；对国家安全、经济运行、社会稳定及公共利益不造成危害。
		经济运行	无	
		社会稳定	无	
		公共利益	无	
		组织权益	严重	
		个人权益	严重	
2 级	低敏感	国家安全	无	1. 数据可进行受限共享和开放。可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用；可提供给部分或部分提供给个人和组织使用。 2. 数据遭泄露、篡改、破坏或者非法获取、非法利用、非法共享后，对组织权益、个人权益造成中等危害或轻微危害；对国家安全、经济运行、社会稳定及公共利益不造成危害。
		经济运行	无	
		社会稳定	无	
		公共利益	无	
		组织权益	中等、轻微	
		个人权益	中等、轻微	
1 级	不敏感	国家安全	无	1. 原则可提供给所有政务部门共享使用并面向社会完全开放或脱敏后开放。 2. 数据遭泄露、篡改、破坏或者非法获取、非法利用、非法共享后，对组织权益、个人权益不造成危害或危害微弱可以忽略；对国家安全、经济运行、社会稳定、公共利益以及个人权益不造成危害。
		经济运行	无	
		社会稳定	无	
		公共利益	无	
		组织权益	无	
		个人权益	无	

8.3.3 风险识别

针对数据安全风险源和不合理处理数据风险源，通过对制度规范性、技术防护性和运行管理等方面进行评估，发现可能存在的数据安全问题和风险隐患。

8.4 风险分析与评价

应根据安全威胁利用数据的脆弱性造成的破坏对数据安全风险进行评价。可将公共数据共享开放安全风险等级分为高、中、低和无风险四级，具体如下：

- 高风险：数据共享开放后，会对个人、企业、其他组织或国家造成严重损害，且无法采取风险防范措施予以化解；
- 中风险：数据共享开放后，会对个人、企业、其他组织或国家机关运作造成损害，但可以采取风险防范措施降为低风险或无风险；
- 低风险：数据共享开放后，对公共秩序、公共利益影响较小，可以采取风险防范措施予以化解；
- 无风险：数据共享开放后对公共秩序、公共利益无影响。

8.5 编制报告

应将评估工作过程、评估结果形成评估报告，评估报告应包括：

- a) 评估对象；
- b) 评估范围；
- c) 评估团队；
- d) 评估场地；
- e) 评估时间；
- f) 评估方式；
- g) 评估指标及分值；
- h) 评估过程记录及关键证明材料；
- i) 安全风险；
- j) 评估结论；
- k) 整改建议、计划及已整改情况等。

附录 A
(资料性)

公共数据安全体系评估指标定义示例

- A.1 评估指标由评估子项内容、评估权重及赋分构成。
- A.2 根据评估子项在该组织数据安全体系中的重要性设置该评估子项的权重值，权重值一般为1-10的整数。
- A.3 所有高风险项应全部满足，出现一个及以上未满足高风险项且不进行整改的，公共数据安全体系评估结果暂缓出具。
- A.4 公共数据安全体系评估指标定义示例见表A.1。

表A.1 公共数据安全体系评估指标定义示例

序号	评估项(AIT)	评估子项(AS)	评估权重	赋分规则
1	制度规范	数据分类分级管理制度	6	全面性：查验制度文件是否包括分类分级原则、要求、维度、方法、操作指南、工作流程以及类别和级别变更场景、变更申请审批流程及工作要求等。(全部满足得5分)
2				可执行性：判断文件规定内容是否可在该组织落地实施。(全部满足得3分)
3				动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等。(全部满足得2分)
4		数据访问权限管理制度	7	全面性：查验制度文件是否包括对公共数据载体和公共数据权限管理系统的账号权限安全管理职责分工和工作要求等。(全部满足得5分)
5				可执行性：判断文件规定内容是否可在该组织落地实施。(全部满足得3分)
6				动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等。(全部满足得2分)
7		数据脱敏管理制度	7	全面性：查验制度文件是否充分根据公共数据分类分级结果，是否包括公共数据脱敏规则、管理要求等。(全部满足得5分)
8				可执行性：判断文件规定内容是否可在该组织落地实施。(全部满足得3分)
9				动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等。(全部满足得2分)
10				全面性：查验制度文件是否充分根据公共数据分类分级结果，进行差异化的公共数据共享和开放安全管理、技术要求、应用场景、工作流程和申请审批环节等。(全部满足得5分)

表A.1 公共数据安全体系评估指标定义示例（续）

序号	评估项(AIT)	评估子项(AS)	评估权重	赋分规则
11	制度规范	数据共享和开放 安全管理制度	7	可执行性：判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
12				动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
13		数据安全销毁管理制度	5	全面性：查验制度文件是否充分根据公共数据分类分级结果，进行公共数据销毁对象、销毁场景、销毁方式、销毁流程、销毁工作要求等。（全部满足得5分）
14				可执行性：判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
15				动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
16		供应方安全管理制度	8	全面性：查验制度文件是否包括供应方及其人员的安全管理要求、供应方及其人员的岗位安全职责、安全考核要求和处罚措施、明确了对供应方及其人员的数据保密范围、保密责任与义务、保密期限等。（全部满足得5分）
17				可执行性：判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
18				动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
19		安全监督检查制度	5	全面性：查验制度文件是否包括对公共数据安全现状的监督检查内容、方式、工作周期、工作流程等。（全部满足得5分）
20				可执行性：判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
21				动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
22		安全日志审计制度	7	全面性：查验制度文件是否包括安全审计日志的采集内容、采集方式、标准化要求、日志存储要求、审计策略和规则、异常预警及处置工作流程等。（全部满足得5分）
23				可执行性：判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
24				动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
25		安全事件管理与应急响应制度	8	全面性：查验制度文件是否包括数据安全事件分类分级方法、公共数据安全事件发现、上报、处置、溯源、总结等工作流程、数据安全应急预案编制及应急演练工作要求等。（全部满足得5分）

表 A.1 公共数据安全体系评估指标定义示例（续）

序号	评估项(AIT)	评估子项(AS)	评估权重	赋分规则
26	制度规范	安全事件管理与应急响应制度	8	可执行性：判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
27				动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
28	技术防护子体系 (AIT ₂)	数据源统一鉴别技术	4	功能性：检查该技术产品是否具备数据源身份统一鉴别、记录的功能，以及对数据真实性、有效性、规范性进行检验的功能。（全部满足得4分）
29				适用性：1. 核查该技术产品是否有效。（全部满足得2分） 2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
30				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
31		敏感数据识别技术	8	功能性：检查该技术产品是否具备敏感数据识别功能。（全部满足得4分）
32				适用性：1. 核查该技术产品是否具备有效识别出敏感数据的功能。（全部满足得2分） 2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
33				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
34		数据分类分级标识技术	8	功能性：检查该技术产品是否具备数据分类分级标识功能，以及具备对外同步接口等。（全部满足得4分）
35				适用性：1. 核查该技术产品是否具备有效标识数据类别和级别的功能。（全部满足得2分） 2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
36				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
37		数据脱敏技术	8	功能性：检查该技术产品是否具备实现敏感数据脱敏功能，是否可实现数据存储或使用脱敏功能（包含静态和动态脱敏）。（全部满足得4分）
38				适用性：1. 核查是否具备有效对存储或使用的数据进行静态或动态脱敏保护的功能。（全部满足得2分） 2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
39				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）

表A.1 公共数据安全体系评估指标定义示例（续）

序号	评估项 (AIT)	评估子项 (AS)	评估权重	赋分规则
40	技术防护子体系	数据加密技术	5	功能性：检查该技术产品是否具备实现敏感数据存储加密、传输加密等功能。（全部满足得 4 分）
41				适用性：1. 核查是否已有效对存储和传输的敏感数据实施加密保护。（全部满足得 2 分）2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得 1 分）
42				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得 3 分）
43		传输通道加密技术	6	功能性：检查该技术产品是否可实现数据传输通道加密。（全部满足得 4 分）
44				适用性：1. 核查是否已有效对数据传输通道实施加密保护；（全部满足得 2 分）2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得 1 分）
45				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得 3 分）
46		数据血缘关系技术	3	功能性：检查该技术产品是否具有追踪记录数据间的血缘关系、建立数据资产全景视图等功能。（全部满足得 4 分）
47				适用性：1. 核查是否已有效追踪记录数据间血缘关系，并准确地进行视图展示。（全部满足得 2 分）2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得 1 分）
48				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得 3 分）
49		数据备份和恢复技术	6	功能性：检查该技术产品是否具备自动化数据备份、检测备份数据完整性、数据恢复等功能。（全部满足得 4 分）
50				适用性：1. 核查该技术产品在数据遭受破坏时，数据备份和恢复机制是否有效恢复。（全部满足得 2 分）2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得 1 分）
51				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得 3 分）
52		数据防泄漏技术	7	功能性：检查该技术产品是否具备数据防泄漏功能。（全部满足得 4 分）
53				适用性：1. 核查该技术产品是否有效实现了数据流转过程的防泄漏。（全部满足得 2 分）2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得 1 分）

表 A.1 公共数据安全体系评估指标定义示例（续）

序号	评估项(AIT)	评估子项(AS)	评估权重	赋分规则
54	技术防护	数据防泄漏技术	7	安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
55		销毁数据识别技术	6	功能性：检查该技术产品是否具备符合多种销毁场景的数据的识别等功能。（全部满足得4分）
56				适用性：1. 核查该技术产品是否可有效识别并销毁符合数据销毁场景的数据。（全部满足得2分）2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
57				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
58		数据销毁技术	6	功能性：检查该技术产品是否具备符合多种销毁场景的数据的识别等功能。（全部满足得4分）
59				适用性：1. 核查该技术产品是否可有效识别并销毁符合数据销毁场景的数据。（全部满足得2分）2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
60				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
61		访问权限管理技术	8	功能性：检查该技术产品是否具备公共数据访问权限集中认证、统一访问入口、细粒度的访问控制等功能，与数据脱敏相关技术产品联动。（全部满足得4分）
62				适用性：1. 核查该技术产品是否有效支撑该组织和角色职能需求，实现公共数据访问用户的统一身份认证和访问控制。（全部满足得2分）2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
63				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
64		数据共享和开放安全技术	7	功能性：检查该技术产品是否具备访问控制、数据脱敏、接口实时数据安全监测与异常告警、据追踪溯源等功能。（全部满足得4分）
65				适用性：1. 核查该技术产品是否可有效支撑数据共享和开放安全。（全部满足得2分）2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
66				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）

表 A.1 公共数据安全体系评估指标定义示例（续）

序号	评估项(AIT)	评估子项(AS)	评估权重	赋分规则
67	技术防护子体系 (AIT ₂)	安全监测与预警技术	7	功能性：检查该技术产品是否具备可配置的量化指标，是否全量接入重要系统日志，并具备支撑威胁发现、识别、理解分析、风险预警和提供处置建议等功能。（全部满足得4分）
68				适用性：1. 核查该技术产品是否有效发现该组织数据安全风险，支撑数据安全体系建设规划。（全部满足得2分）2. 核查该技术产品性能是否满足该组织高峰期业务需求等。（全部满足得1分）
69				安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
70	运行管理	数据安全团队	6	完备性：检查是否设置了公共数据安全团队，并明确团队的各方的职责分工。检查是否设置了机构主要负责人为公共数据安全第一责任人、公共数据安全负责人及其工作职责。（全部满足得4分）
71				专业性：查验公共数据安全负责人是否具备数据安全专业知识和履职能力、是否接受安全技能培训和考核、是否具有必备的人力支持和技术支持；查验该团队成员专业安全技术能力及安全专业证书覆盖程度，接受数据安全防护技能及法规培训记录等，确保可胜任职责范围的工作。（全部满足得3分）
72				可靠性：查验安全管理负责人的个人自述、履历等情况；查验该团队成员的个人自述、履历等情况，确保有良好职业操守，无不良记录。（全部满足得3分）
73		数据分类分级管理机制	6	完整性：查验该工作机制是否与数据资源目录机制协同、是否建立维护了数据资产全景视图、是否实现分类分级闭环工作机制。（全部满足得3分）
74				符合性：查验分类分级工作实施、数据资源目录同步、分级结果反馈、分类分级机制优化等工作过程文件和记录。（全部满足得3分）
75				有效性：检查分类分级工作结果文件和记录。（全部满足得4分）
76		数据访问权限管理机制	8	完整性：查验该工作机制是否包括公共数据访问权限的分配、开通、使用、变更、重置、注销等的申请审批、实施、定期核查、清单维护等。（全部满足得3分）
77				符合性：查验公共数据访问账号权限管理工作过程文件和记录。（全部满足得3分）
78				有效性：检查公共数据访问账号权限管理工作结果文件和记录。（全部满足得4分）

表 A.1 公共数据安全体系评估指标定义示例（续）

序号	评估项(AIT)	评估子项(AS)	评估权重	赋分规则
79	运行管理	数据共享和开放安全管理	7	完整性：查验该工作机制是否包括公共数据共享和开放的 申请审批，接口上线前和上线后的安全检查、敏感数据实 时监测告警处置等。（全部满足得 3 分）
80				符合性：查验公共数据共享和开放安全管理工作过程文件 和记录。（全部满足得 3 分）
81				有效性：检查公共数据共享和开放安全管理工作结果文件 和记录。（全部满足得 4 分）
82		安全日志审计机制	7	完整性：查验该工作机制是否包括违规行为告警的核实、分析、处置和整改等环节。（全部满足得 3 分， 一项不足扣 1 分）
83				符合性：查验安全日志审计工作过程文件和记录。（全部 满足得 3 分）
84				有效性：检查安全日志审计工作的结果文件。（全部满足 得 4 分）
85		安全监督检查机制	7	完整性：查验该工作机制是否包括安全监督检查工作实施、 工作总结，问题整改、整改效果验证等环节。（全部满足 得 3 分）。
86				符合性：查验安全监督检查工作过程文件和记录。（全部 满足得 3 分）
87				有效性：检查安全监督检查工作结果文件和记录。（全部 满足得 4 分）
88		安全事件应急响应机制	8	完整性：查验该工作机制是否包括应急演练规划、实施、总结以及应急演练报告编制、应急预案优化等环节。
89				符合性：查验应急演练规划、实施、总结以及应急演练报告编制、应急预案优化等工作过程文件和记录。
90				有效性：检查应急演练规划、实施、总结以及应急演练报 告编制、应急预案优化等工作结果文件和记录；检查安全事件发生时，应急响应工作记录和结果文件。
91		安全培训机制	5	完整性：查验该工作机制是否包括培训计划制定、工作实施、效果考核、计划优化调整等环节。（全部满足得 4 分）
92				符合性：查验培训计划制定、工作实施、效果考核、计划优化调整等工作过程文件和记录。（全部满足得 3 分）
93				有效性：检查培训计划制定、工作实施、效果考核、计划优化调整等工作结果文件和记录。（全部满足得 3 分）
