ICS 35.240.01
I6440

团　　体　　标　　准

T/WHCSA 006—2024

数据要素场内流通安全评估规范

Specification for security assessment of data element circulation

2024-11-26 发布　　2025-1-1 实施

武汉市网络安全协会　发布

目　　次

前　　言 III
1 范围 4
2 规范性引用文件 4
3 术语和定义 4
4 安全评估概述 4
4.1 安全评估体系框架 4
4.2 安全评估规范要求 5
5 安全评估工作流程规范 5
5.1 前期准备阶段 5
5.1.1 确定安全评估目标 5
5.1.2 确定安全评估范围 5
5.1.3 组建安全评估团队 5
5.1.4 安全评估初步调研 5
5.1.5 确定评估依据和方法 6
5.1.6 制定安全评估方案 6
5.2 安全评估阶段 6
5.2.1 按照评估方案实施评估 6
5.2.2 输出各指标评估结果 6
5.3 报告编制阶段 6
6 流通主体安全评估规范 7
6.1 流通主体安全评估 7
6.1.1 数据提供方安全能力评估 7
6.1.2 数据使用方安全能力评估 7
6.1.3 数据流通机构安全能力评估 7
6.2 第三方服务机构安全评估 7
6.2.1 数据经纪商安全能力评估 7
6.2.2 技术服务商安全能力评估 7
6.2.3 合规服务商安全能力评估 7
7 流通数据安全评估规范 7
7.1 禁止流通交易数据评估 8
7.2 流通交易数据合规性评估 8
7.2.1 一般性数据合规性评估 8
7.2.2 流通交易个人信息合规性评估 8
8 流通过程安全评估规范 8
8.1 流通前安全评估 8
8.2 流通中安全评估 8
8.3 流通后安全评估 9
8.3.1 数据使用合规性评估 9
8.3.2 合同履约与纠纷评估 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。

本文件由武汉安恒信息科技有限公司提出。

本文件由武汉市网络安全协会归口。

本文件起草单位（排名不分先后）：武汉安恒信息科技有限公司、武汉市网络安全协会、汉阳区大数据中心、长江水利委员会水文局、武汉大学国家网络安全学院、中国长江电力股份有限公司、湖北数据集团有限公司、武汉数据集团有限公司、武汉市房产和工程建设智能发展中心、武汉网络安全技术有限公司、武汉趣链数字科技有限公司、武当云谷大数据科技有限公司、国网湖北省电力有限公司信息通信公司、湖北华中电力科技开发有限责任公司等；

本文件主要起草人（排名不分先后）：彭建军、邓浩、任子骁、贾高彦、郭珍珍、刘悦恒、乔奇、张玉萍、严媛、黄颖倩、杨健平、邹冰玉、张辉、张立强、古伟、徐斌、刘剑锋、孙进、谢逸俊、徐波、张勇、郭峰、邱爽、冯浩、焦翰琳、徐挺、陈剑、牛犁青、李娜、沈沉等

数据要素场内流通安全评估规范

1 范围

本文件规定了场内流通过程中，针对流通主体、流通数据和流通行为进行安全评估的基本要求。

本文件可供场内流通各方确保场内流通活动安全进行自评估或者委托第三方专业机构进行数据交易安全评估使用，亦可为相关监管部门、行业主管部门用于评价数据流通交易活动的安全保障义务履行情况提供参考。

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 25069 信息安全技术 术语

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 37932-2019 信息安全技术 数据交易服务安全要求

GB/T 40685-2021 信息技术服务 数据资产 管理要求

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

GB/T 43697-2024 数据安全技术 数据分类分级规则

3 术语和定义

下列术语和定义适用于本文件。

数据流通安全

在数据要素流通交易过程中的安全，包括主体安全、数据安全、过程安全。

数据流通主体

从事数据流通的主要参与方，包括数据提供方、数据流通机构、数据使用方等。

第三方服务机构

以第三方的角色为数据流通交易主体独立提供专业性服务的机构，包括数据经纪商、技术服务商、合规服务商等。其中：

数据经纪商：匹配数据要素供应方和需求方的企业，如促进数据流通交易的经纪商和中介。

技术服务商：为数据流通服务提供基于技术方面的服务机构，包括数据集成、隐私计算、数据托管、数据保险、风险评估等

合规服务商：为数据流通服务提供基于合规方面的服务机构，包括合规认证、安全审计、数据公证、争议仲裁等。

4 安全评估概述

4.1 安全评估体系框架

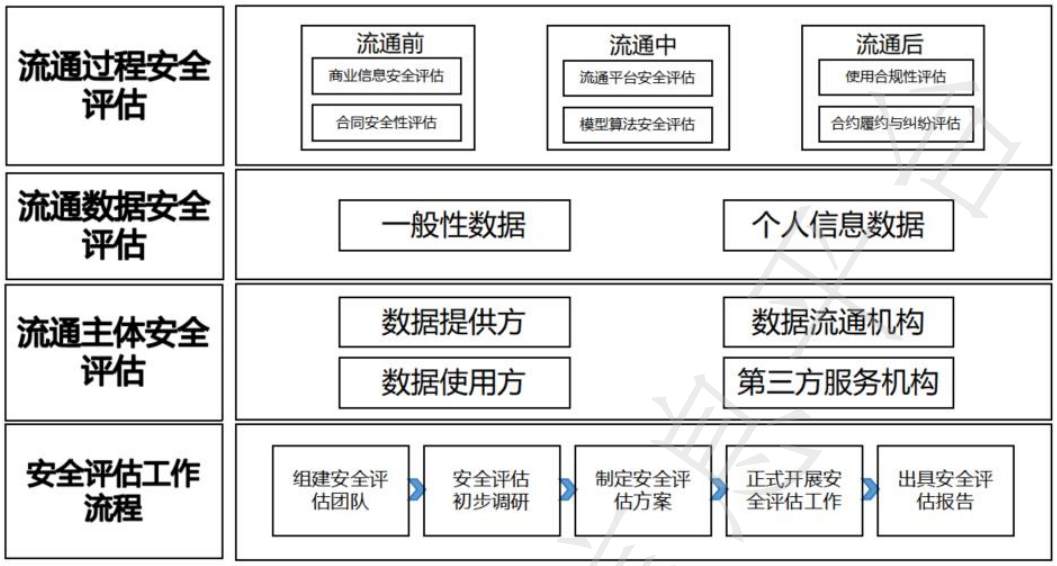

图 1　数据要素场内流通安全评估体系框架

4.2　安全评估规范要求

数据要素场内流通安全评估规范要求包括：

a)　安全评估工作流程：包括组建安全评估团队、安全评估初步调研、确定安全评估范围并制定评估方案、正式开展安全评估工作、出具安全评估报告等。

b)　流通主体安全评估：为确保参与交易的主体要求，包括对数据提供方、数据使用方、数据流通机构和第三方服务机构的技术能力等进行评估；

c)　流通数据安全评估：为确保参与流通的数据符合法律法规规定，包括对一般性数据和个人信息数据等进行评估；

d)　流通过程安全评估：为确保数据流通的行为过程是安全的，包括对流通前、流通中、流通后等进行评估。

5　安全评估工作流程规范

5.1　前期准备阶段

5.1.1　确定安全评估目标

基于被评估方所在行业标准以及其在数据流通服务中所处阶段，评估方根据不同阶段的安全性要求明确安全评估目标。

5.1.2　确定安全评估范围

根据安全评估目标，评估方确定安全评估的范围，其包括被评估方在数据流通过程中所涉及的数据、流程、系统、环境、具体业务、部门以及人员等。

5.1.3　组建安全评估团队

安全评估团队由评估方、被评估方、评估领导小组以及专家组共同组建。评估方由安全技术评估人员和安全管理评估人员组成；被评估方由安全管理人员、业务人员、数据产品开发人员、运维人员组成；评估领导小组由评估方和被评估方领导及双方有关部门负责人组成；专家组由相关专业的优秀专家和技术骨干组成。

5.1.4　安全评估初步调研

评估方对被评估方进行系统调研，调研内容应包括：

a) 主体安全评估调研：被评估方所涉及的数据流通制度规范和技术防护情况、数据服务商安全管理能力、数据流通机构征信和运营情况、数据流通主体的合规性等；
b) 数据安全评估调研：被评估方所涉及的数据产品合法合规性、数据流动和存储情况、数据开发共享情况、个人信息的匿名化处理情况、跨境数据的合法合规性等；
c) 行为安全评估调研：包含在数据流通预备阶段时数据采集情况以及物理环境和通信网络的安全性；在流通磋商阶段时敏感数据的安全性和流通环境的安全性；在流通实施阶段时体保护情况和数据保护情况；在流通结束阶段时数据使用安全、备份安全以及销毁安全的情况等。

5.1.5 确定评估依据和方法

5.1.5.1 确定评估依据

评估依据应包括：
a) 适用的法律法规以及数据流通交易服务合同；
b) 现有国际标准、国家标准、行业标准以及地方标准；
c) 数据流通制度以及安全管理制度；
d) 数据流通或交易系统自身的实时性或性能要求等。

5.1.5.2 确定评估方法

评估方法应包括：
a) 专家访谈；
b) 问卷调查；
c) 技术检测。

5.1.6 制定安全评估方案

根据被评估方的实际情况和调研结果，评估方制定安全评估方案，方案内容应包括：
a) 评估目标和范围；
b) 评估团队；
c) 评估场地；
d) 评估工作计划；
e) 评估时间进度；
f) 评估指标及分值；
g) 评估内容及方法。

5.2 安全评估阶段

5.2.1 按照评估方案实施评估

根据制定的安全评估方案检查实施阶段的相关材料并实施评估，分析评估目标和内容相对应的评估指标。

5.2.2 输出各指标评估结果

评估团队参照相应的评估标准，对每个安全评估指标进行测评，针对评估结果中可能存在的疑问或不同意见，评估方需要向被评估方提供解释和说明。

5.3 报告编制阶段

评估方以报告的形式呈现被评估方的安全评估结果，报告内容应包括：
a) 报告摘要：主要介绍评估的背景、目的、范围、方法和结论等；
b) 数据流通服务概述：对数据流通主体、流程特征、安全隐患等进行概括和描述；
c) 安全评估指标和权重：具体列出评估指标和相应的权重，并解释各项指标的意义；
d) 评估结果和分析：针对每个评估指标，给出相应的得分和分析，归纳潜在的安全问题；
e) 结论和建议：总结评估结果，提出相应的改进建议，便于相关单位开展整改工作。

6 流通主体安全评估规范

6.1 流通主体安全评估

6.1.1 数据提供方安全能力评估

评估数据提供方是否具备向数据使用方安全交付数据的能力。

a) 数据提供方提供其数据的合规性证明。

b) 数据提供方具有将数据、数据产品安全传输到流通平台的能力。

6.1.2 数据使用方安全能力评估

数据使用方安全能力评估包括基础资格要求、网络安全保护能力、数据安全保护能力以及其他能力：

a) 评估数据使用方对数据使用，是否已建立有效的内部控制机制，确保其仅按照供需双方约定的使用目的、范围、方式和期限使用数据；如涉及个人信息去标识化处理的，是否采取有效措施以防止对个人信息进行重新溯源或再识别；

b) 评估数据使用方对数据销毁，是否已建立有效的内部控制机制，确保其在按照数据流通约定完成数据处理后可以及时、有效和彻底地销毁流通数据。

6.1.3 数据流通机构安全能力评估

数据流通机构安全能力评估指标包括：

a) 评估数据商用于数据流通服务的信息系统安全保护机制是否有效运行。

b) 评估用于数据流通交易的接口，其端口与传输过程中是否已采取可有效运行的安全保护机制和必要安全措施；

c) 评估是否已建立与数据流通流通业务相关的业务规则、内部控制、风险隔离及合规检查等制度。

6.2 第三方服务机构安全评估

6.2.1 数据经纪商安全能力评估

数据经纪商安全能力评估包括：

a) 评估数据经纪商是否具有满足数据流通交易业务需求的数据流通技术、硬件设备和软件系统；

b) 评估数据商是否已建立与数据流通交易流通业务相关的业务规则、内部控制、风险隔离及合规检查等制度；

c) 评估数据经纪商在收集原始数据时，是否获得就后续数据处理与交易取得数据权利主体的同意，并提供撤回同意的方式；

d) 评估数据经纪商在处理原始数据时，是否按照数据权利主体同意的范围进行处理，不进行欺骗性、歧视性或其他恶意处理；

e) 评估数据经纪商在存储原始数据与数据产品时，是否建立了符合要求的数据分级分类管理体系，并基于此采取相应安全保障机制。

6.2.2 技术服务商安全能力评估

评估技术服务商是否具有能力提供支持业务需求的数据流通技术、硬件设备和软件系统或相关服务。

6.2.3 合规服务商安全能力评估

合规服务商安全能力评估包括：

a) 评估合规服务商就数据获取，是否仅限于提供合规服务所必需的最小范围访问数据，并建立了数据访问范围与权限的控制机制；

b) 评估合规服务商就数据保密是否采取了有效的组织措施与必要的技术措施，避免不必要的对外披露交易数据。

7 流通数据安全评估规范

7.1 禁止流通交易数据评估

数据流通交易前应当评估是否不属于以下禁止交易类型的数据：

a) 涉及国家秘密等受法律保护的数据；

b) 涉及个人信息的数据，除非获得了全部个人数据主体或未成年人的监护人的明示同意，或者进行了必要的去标识化处理以达到无法识别出个体的程度；

c) 涉及他人知识产权和商业秘密等权利的数据，除非取得权利人明确许可；

d) 从非法或违规渠道获取的数据；

e) 与原提供方所签订的合约要求禁止转售或公开的数据；

f) 其它法律法规明确禁止交易的数据。

7.2 流通交易数据合规性评估

7.2.1 一般性数据合规性评估

一般性数据合规性评估包括：

a) 评估数据提供方是否具备流通数据获取渠道合法，权利清晰无争议的承诺或证明材料；

b) 评估数据提供方是否已向数据流通机构提供拥有交易数据完整相关权益的明确声明；

c) 评估数据提供方是否已向数据流通机构提供数据真实性的明确声明；

d) 评估数据提供方是否已对流通交易数据进行分类，并对数据进行安全风险评估，出具安全风险评估报告，确保其安全风险不构成对可交易性的阻碍；

e) 评估数据提供方是否已明确流通交易数据的限定用途、使用范围、流通交易方式和使用期限。

7.2.2 流通交易个人信息合规性评估

流通交易个人信息合规性评包括：

a) 评估是否满足GB/T 35273-2020中第8章关于个人信息的委托处理、共享、转让、公开披露安全要求；

b) 评估数据提供方是否已对交易数据进行个人信息安全风险评估，提供个人信息安全风险评估报告，确保个人信息安全风险不构成对可交易性的阻碍。

8 流通过程安全评估规范

8.1 流通前安全评估

流通前期安全评估包括：

a) 在合同签订前，对于数据流通主体，评估是否已对交易数据的用途、使用范围、交易方式、使用期限和交易价格等进行协商和约定，形成有效的交易订单。

b) 在合同签订前，对于数据流通机构，评估是否已对审核通过的订单进行登记备案，并已对数据流通双方发出交易确认通知。

c) 在合同签订时，评估数据流通机构与数据流通双方是否已签订三方合同，明确数据内容、数据用途、交付质量、交付方式、交易金额、交易参与方安全责任、保密条款等内容。

d) 商业信息安全评估：交易定价、商业模式等保密

对于非公开的数据流通商业信息，如特定交易的交易定价、商业模式、或数据交易主体特殊约定不得公开的其他商业信息等信息，评估是否已建立了相关的保密机制或是否签订相关保密协议。

8.2 流通中安全评估

流通中期安全评估包括：

a) 是否已审核数据使用方的数据安全能力，确保不低于数据提供方的数据安全能力。

b) 是否已对交付数据内容进行监测和核验，并能够在发现违法违规事件时，及时中断数据流通交易行为，依法依规进行处理。

c) 是否对交易过程中的违法违规数据具有追溯能力。

d) 对于在线数据交付模式，评估数据流通机构是否已在数据流通主体间的数据传输链路上部署数据监控工具，具有完备的数据保护机制和数据泄露检测能力。

e) 对于托管数据交付模式，评估数据流通机构是否已为数据使用方建立安全的数据使用环境，并分配相应的权限；在数据使用完成后，评估数据流通机构是否在核准数据使用方的提取结果数据请求后，再向数据使用方提供结果数据。

8.3 流通后安全评估

8.3.1 数据使用合规性评估

数据使用合规性评估包括：

a) 对于数据提供方，评估是否建立了要求数据使用方反馈按照合同约定及法律法规规定相关要求，在必要范围内合法、正当、合理使用数据情况的机制。

b) 对于数据使用方，评估是否建立了自行检查是否按照合同约定及法律法规规定相关要求，在必要范围内合法、正当、合理使用数据情况的机制。

c) 对于数据流通机构，评估其是否与实际使用数据的数据使用方建立了数据使用情况反馈机制，要求数据使用方反馈按照合同约定及法律法规规定相关要求，在必要范围内合法、正当、合理使用数据情况的机制。

8.3.2 合同履约与纠纷评估

合同履约与纠纷评估包括：

a) 数据交付完成后，对于数据提供方，评估是否已及时关闭数据访问接口，发出数据交付完成确认；

b) 数据交付完成后，对于数据使用方，评估是否已及时发出数据接收完成确认；；

c) 评估数据流通机构是否为交易过程记录形成完整的交易日志并进行安全保存。