ICS 35.030
CCS M 10

YD

中华人民共和国通信行业标准

YD/T 6415—2025

工业领域数据安全风险评估规范

Specification for data security risk assessment in the industrial field

2025-05-09 发布　　2025-08-01 实施

中华人民共和国工业和信息化部 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。

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。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：国家工业信息安全发展研究中心、福建省工业信息产业发展研究中心、哈尔滨工程大学、深信服科技股份有限公司、福建师范大学、联想（北京）有限公司、烟台中科网络技术研究所、北京睿航至臻科技有限公司、北京数安行科技有限公司、阳光电源股份有限公司、上海观安信息技术股份有限公司、郑州信大捷安信息技术股份有限公司、北京天融信网络安全技术有限公司、亚信科技（成都）有限公司、北京万里红科技有限公司、华为技术有限公司、宝马中国投资有限公司、长扬科技（北京）股份有限公司、杭州安恒信息技术股份有限公司、北京恒安嘉新安全技术有限公司、烽台科技（北京）有限公司。

本文件主要起草人：柳彩云、李俊、李耀兵、孙岩、王海洋、王墨、黄鹏、郑丽娜、刘奕彤、刘泽超、宋博韬、翁颖、曲海阔、许力、刘俊、姜守义、刘玉红、李睿、王颖、谢江、刘为华、张静、廖双晓、姜国通、邵萌、孙斌、张亚京、王晓翔、尚程、王启蒙。

工业领域数据安全风险评估规范

1 范围

本文件规定了工业领域数据安全风险评估的基本原则、要素、流程及方法等内容。

本文件适用于工业领域重要数据和核心数据处理者在中华人民共和国境内开展数据处理活动的数据安全风险评估。工业领域一般数据处理者对其数据处理活动的数据安全风险评估，也可参照本文件。

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—2022 信息安全技术 术语

YD/T 4981—2024 工业领域重要数据识别指南

YD/T 4982—2024 工业企业数据安全防护要求

3 术语和定义

GB/T 25069—2022、YD/T 4981—2024、YD/T 4982—2024 界定的以及下列术语和定义适用于本文件。

3.1

数据 data

任何以电子或者其他方式对信息的记录。

3.2

工业数据 industrial data

工业数据是指工业各行业各领域在研发设计、生产制造、经营管理、运行维护、平台运营等过程中产生和收集的数据。

3.3

风险评估 risk assessment

风险识别、风险分析和风险评价的全过程。

[来源：GB/T 29246—2017，2.71]

注：本文件专指工业领域数据安全风险评估。

3.4

合规性评估 compliance assessment

判定数据处理者对数据处理活动是否符合法律法规、政策文件、标准规范相关要求的行为。

3.5

数据载体 data carrier

数据处理活动中使用的系统、平台、设备、媒介等。

3.6

评估报告 evaluation report

根据评估方法的要求，在履行必要的评估程序后，对被评估对象出具的书面工作报告，是评估机构履行评估任务或数据处理者进行自评估的成果。

4 缩略语

下列缩略语适用于本文件。

CVSS：通用漏洞评分系统（Common Vulnerability Scoring System）

5 评估内容

工业领域数据安全风险评估包括合规性评估和安全风险分析两部分内容，其中合规性评估由正当必要性评估、基础性安全评估、数据全生命周期安全评估三部分组成，重点分析数据处理活动及所对应的数据种类、数量、目的、方式、范围以及保障能力是否符合法律、行政法规、标准规范要求；安全风险分析由风险源识别、安全影响分析、综合风险研判三部分组成，通过综合分析数据处理活动面临的威胁、所采用的保障措施情况以及发生数据泄漏、损毁、丢失等安全事件后产生的影响范围、程度等因素，综合研判数据处理活动安全风险等级。工业领域数据安全风险评估可由数据处理者自行组织，也可委托第三方评估机构开展。

6 评估原则

工业领域数据安全风险评估工作遵循以下原则：

a） 规范性原则：遵循工业领域行业相关要求开展数据安全风险评估工作；

b） 客观公正原则：评估人员在评估活动中应充分收集证据，对评估对象实施的安全措施的有效性和可靠性做出客观公平的判断；

c） 可复现原则：在相同的环境下，对同一评估对象，不同的评估人员依照相同的要求，使用相同的方法，对每个评估实施过程的重复执行都应得到相同的评估结果；

d） 可控性原则：在评估过程中，应保障参与评估的人员、使用的技术和工具、评估过程都是可控的；

e） 完备性原则：严格按照被评估对象所涉及的评估范围进行全面的评估；

f） 最小影响原则：从相关管理层和工具技术层面，将评估工作对数据和承载数据的应用、系统、网络正常运行的可能影响降低到最低限度，不会对评估对象涉及的应用、系统、网络运行产生明显影响；

g） 保密性原则：在实施评估过程中，应保护数据处理者的商业秘密不被泄露。

7 评估方法

7.1 人员访谈

评估人员通过与被评估数据处理者相关人员进行交流、讨论、询问等活动，对数据的处理、保障措施设计和实施情况进行了解、分析和取证，以评估数据安全保障措施有效性。通常在评估过程中深入数据处理者实地核查时使用，数据处理者需要安排熟悉数据流转过程及数据载体的人员参加访谈。

7.2 资料查验

评估人员查阅数据安全相关文件资料，如数据安全管理制度、安全策略和机制、合同协议、安全配置和设计文档、系统运行记录等相关文件，用以评估数据安全管理相关制度文件是否符合标准要求。通常在评估准备阶段以及开展数据安全现场评估时使用该方法，数据处理者需要事先完整准备上述文档以供评估人员查阅。

7.3 人工核验

数据处理者安排相关人员进行现场演示，评估人员根据信息系统等载体演示情况进行查验，以评估数据安全保障措施有效性。通常在评估过程中深入数据处理者实地核查时使用，如系统存在高度保密性、可用性的要求，评估可通过事后提供日志列表或测试环境等方式进行。

7.4 工具测试

评估人员通过使用适当的数据安全评估评测工具或通过技术手段实际测试数据载体，查看、分析被测试响应输出结果，以评估数据安全保障措施有效性。通常是评估人员针对数据全生命周期涉及的相关技术指标进行验证时使用，评估人员需要事先进行业务注册、准备验证工具等以完成相关评估指标。工具测试前充分评估检测过程对数据载体等造成的影响，对于业务不可中断的系统、应用等，可考虑采用模拟系统验证、离线环境验证等方式。

8 评估流程

8.1 总体流程

工业领域数据安全风险评估的实施过程一般包括组建评估团队、确定评估范围、制定评估方案、实施风险评估、形成评估报告等内容，具体流程如图1所示。

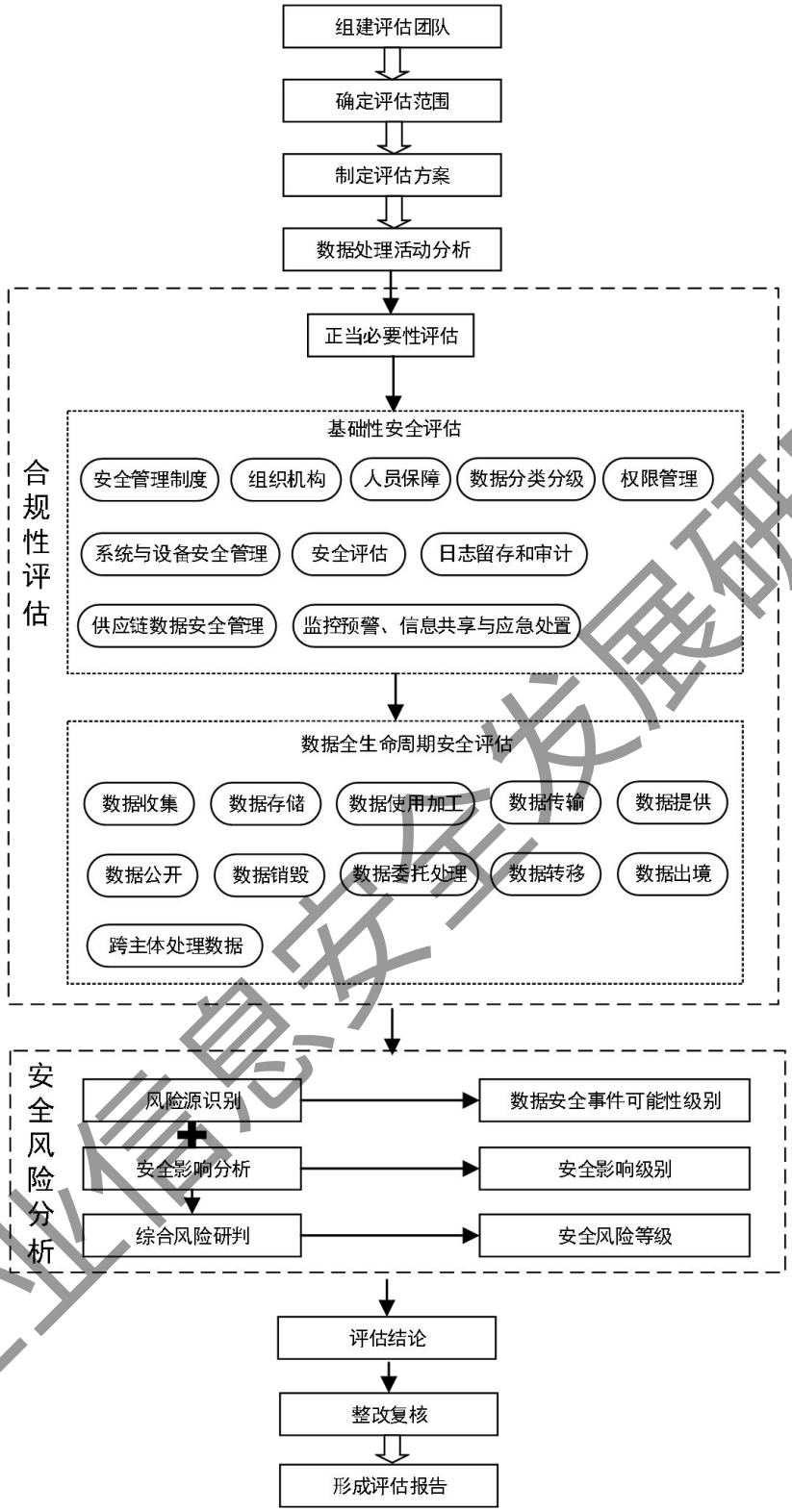

图1 工业领域数据安全风险评估流程

8.2 组建评估团队

风险评估工作开展前，应综合考虑组织规模、业务种类、数据数量、种类、涉及数据载体的复杂程度等因素，组建至少包括组织管理、业务运营、技术保障、安全合规等人员组成的评估团队，必要时可聘请相关专业的技术专家和技术负责人组成专家小组。评估团队原则

上应具备不少于5名专业评估人员，包括1名评估团队组长、4名评估团队成员，其中至少4人应熟悉数据安全风险评估的方法和流程，掌握依据数据安全风险评估相关标准规范开展风险评估的能力，并取得工业和信息化领域数据安全风险评估相关技能评价证书。评估团队组长负责统筹安排评估工作并推进评估工作开展，组织完成评估结论、编写评估报告等。

委托第三方评估机构开展评估工作时，数据处理者应与被委托机构共同组建评估团队，确定评估团队组长和团队成员。同时，数据处理者还应指定本单位至少1名数据安全专业人员为评估工作对接人，负责协调本单位相应资源、对第三方评估机构相应工作进行管理和监督。此外，在评估工作开展前，数据处理者还应及时与被委托机构沟通，签订书面评估委托协议或评估合同，规范开展评估工作，保障数据处理者的安全生产运行和数据安全。

8.3 确定评估范围

评估团队应首先制定《数据安全风险评估调研表》并提供给数据处理者，通过发放调查表格、电话沟通等远程指导方式，或现场调研、会议等线下方式指导数据处理者完整、准确填写，实现对数据处理者全部数据处理活动的充分调研，了解掌握数据种类、范围、处理方式以及相关数据载体的基本情况，进而确定评估范围。数据安全风险评估范围应覆盖数据处理者全部重要数据和核心数据，以及一定比例的一般数据。一般数据以抽样方式选取，应尽量保证评估数据范围覆盖全部数据类别（二级子类）（可参考附录A），且数据载体避免重复。调研了解的信息内容包括：

a） 数据的种类、数量；
b） 处理数据的目的、方式、范围以及业务场景；
c） 数据载体情况，包括功能、架构、数据库、表格、字段清单结构、可对外传输数据的接口清单、按组件和接口划分的数据流示意图、数据处理涉及的数据流示意图；
d） 数据安全保障措施情况，包括管理制度建设及落实情况、技术手段建设及应用情况、数据安全管理机构人员设置及履职情况等；
e） 数据处理实施情况，包括数据操作方式（现场运行、外部托管、云外包等）、可接触到数据的人员范围及权限分配情况、数据存储位置、备份与恢复、留存时限等；
f） 如涉及委托接收方处理或与接收方共享、转让数据的，应包括共享、转让的目的、方式、范围以及接收方身份、接收方数据安全保障情况、接收方接入信息系统描述、安全责任划分情况等。

8.4 制定评估方案

评估团队可根据实际需要制定风险评估工作方案。工作方案制定过程中，需与涉及数据处理活动的业务部门积极沟通，保障评估的可行性。评估方案包括评估范围、评估依据、评估团队基本信息、工作计划、使用的评估工具情况、保障条件等。

8.5 实施风险评估

评估团队首先进行数据处理活动分析，明确评估范围内数据处理活动及所对应的数据名称、类别、级别、规模，处理数据的目的和方式、使用范围、涉及的接收方及数据载体情况等。然后开展合规性评估，包括正当必要性评估、基础性安全评估和数据全生命周期安全评估，研判合规性评估结果。最后，进一步开展安全风险分析，通过风险源识别判断安全事件发生的可能性级别，结合安全影响分析结果，研判数据处理活动安全风险等级（分为极高、高、中、低四个等级）。合规性评估不通过的，可以直接判定安全风险分析中的风险源识别环节结果（可能性级别）为高。在形成评估结论后，数据处理者应依据评估结论开展风险整改与复核。

注：若合规性评估中正当必要性未满足，则合规性评估不通过。合规性评估的基础性安全评估和数据全生命周期安全评估每项评估结果可分为符合、不符合、部分符合，分别对应1分、0分和0.5分，以及不计算得分，针对基础性安全评估和数据全生命周期安全评估指标项，若X为符合项数量，Y为部分符合项数量、Z为不符合项数量，则平均归一化算数分值= (X+0.5Y) /(X+Y+Z)。平均归一化算数分值小于0.7，则判定合规性评估不通过，平均归一化算数分值大于等于0.7，则判定合规性评估通过。

8.6 形成评估报告

评估团队在完成实施风险评估后，经与数据处理者协商一致，根据评估结论形成评估报告，评估报告应包含数据处理者基本情况、评估团队基本情况、数据处理活动分析、合规性评估、安全风险分析、评估结论及应对措施等（评估报告模板详见附录B）。

9 实施风险评估

9.1 数据处理活动分析

不同业务、活动、场景下数据处理目的、方式、范围以及数据种类、数量等均不相同。为全面、科学地评估数据处理活动的综合安全风险，评估团队在正式开展风险评估前，应进行数据处理活动分析。数据处理活动分析主要包括，识别数据处理者所有一般数据、重要数据和核心数据处理活动及各处理活动所对应的数据名称、类别、级别、规模，处理目的和方式、使用范围、涉及的接收方及数据载体情况等，形成一般数据处理活动分析表（详见附录表B.1）与重要数据、核心数据处理活动分析表（详见附录表B.2）。

9.2 合规性评估

9.2.1 正当必要性评估

评估团队应查验数据处理活动所涉及的业务说明、需求分析、合同协议、监管文件等能反映数据处理目的的相关文件，评估分析数据处理目的是否合理、正当，所涉及的数据数量、类型、频率是否为实现该目的下的最小范围。其中合理、正当的目的包括：

a） 合法开展业务所必需的；
b） 配合政府机构工作所必需的；
c） 开展合法科学研究所必需的；
d） 开展合法新闻报道所必需的；
e） 履行合同义务所必需的；
f） 保障公民合法权益、生命健康、财产安全等所必需的；
g） 履行法律法规所规定的义务所必需的。

9.2.2 基础性安全评估

9.2.2.1 一般数据基础性安全评估

评估团队应重点评估的内容包括：

a） 安全管理制度
   1） 查阅数据处理者数据全生命周期安全管理制度及其更新修订记录等相关材料，评估其是否结合所属行业领域的数据特征、数据处理场景等，建立数据安全管理制度，明确组织机构、责任落实、安全防护、风险评估、应急处置、培训教育等管理要求，并按照需求进行修订；
   2） 访谈数据处理者相关人员，评估其是否知悉相关制度规范。

b） 组织机构

查阅数据处理者数据安全岗位职责等相关文档，评估数据处理者是否明确数据安全管理的责任部门，统筹负责数据处理活动的安全监督管理。

c） 人员保障

1） 查阅数据安全管理部门组织架构、数据安全管理人员配备情况等相关材料，评估其是否根据企业和岗位性质，配备数据安全管理人员，统筹负责数据处理活动的安全监督管理；

2） 访谈数据处理者数据安全管理人员，评估其是否清楚自身职责；

3） 查阅培训记录，评估其是否定期开展数据安全教育与技能培训，强化从业人员数据安全意识和专业技能；

4） 访谈数据处理者相关人员，评估其是否定期参加数据安全教育培训，是否具备数据安全意识和专业技能。

d） 数据分类分级

查阅数据处理者数据安全相关制度文件、数据资产清单，评估是否明确数据资产的梳理手段、梳理方式、梳理周期等，定期梳理本企业数据，形成数据资产清单并定期更新。

e） 权限管理

1） 查阅数据处理者权限管理制度等相关材料，评估其是否合理确定数据处理活动的操作权限，严格实施人员权限管理；

2） 访谈相关人员，评估其是否知悉数据处理平台或系统账号管理机制；

3） 查阅数据处理者权限管理制度等相关材料或核查相关系统平台，评估其是否按照最小授权原则分配账号权限。

f） 系统与设备安全管理

1） 核查数据处理者数据载体安全配置清单审计记录（如配置核对表），评估是否对数据库、研发终端、生产设备、开发代码库等数据载体及数据采集系统进行安全配置，建立安全配置清单，定期进行配置审计；

2） 核查数据处理者安全漏洞补丁升级记录及加固措施，评估其是否及时采取升级措施，短期内无法升级的，是否开展针对性安全加固；

3） 查阅数据处理者身份认证相关管理制度，核查数据处理者数据载体登录账户及口令设定情况，账户口令管理制度，评估其强度及管理制度是否满足需求；

4） 以人工核验、工具测试等方式，核查数据处理者数据载体是否使用默认口令或弱口令，是否定期更新口令；

5） 核查服务器、工程师站等主机，评估其是否部署防病毒软件或采用应用软件白名单技术，防范勒索病毒等造成的数据破坏攻击行为。

g） 供应链数据安全管理

1） 查阅数据处理者供应链相关合同、协议，评估其是否明确供应链数据安全风险控制措施，以合同、协议等方式明确供应商、生产商、服务商等供应链主体的数据安全防护要求和责任落实要求；

2） 通过人工核验或工具测试等方式，核查其是否对供应链管理系统的接入接口做好授权认证等保护措施。

h） 日志留存和审计

1） 通过人工核验或工具测试等方式，检查数据处理者的日志留存管理情况，评估其是否对数据处理日志及系统运行日志进行记录；

2） 通过人工核验等方式，评估其日志记录保存时间是否不低于 6 个月；

3） 通过人工核验或工具测试等方式，评估数据处理者是否对其数据处理活动进行定期审计。

i） 监控预警、信息共享与应急处置

1） 通过人工核验或工具测试等方式，评估其是否根据实际情况建设数据安全风险监测能力，及时排查安全隐患，采取必要的措施防范数据安全风险；

2） 访谈相关人员，评估其是否在接到数据安全风险通报信息后，及时处置风险并按要求反馈处置情况；

3） 查阅数据处理者数据安全事件风险报告等相关材料，评估其是否及时向本地区行业监管部门上报可能造成较大及以上安全事件；

4） 查阅数据处理者数据安全事件应急预案及应急措施、应急演练计划、演练记录等相关材料，评估数据处理者是否根据业务场景制定数据安全事件应急预案，并与行业监管部门数据安全事件应急预案进行衔接；

5） 访谈相关人员，评估其是否知悉数据安全事件应急预案、应急演练等相关内容，评估数据处理者是否在发生数据安全事件时能够及时采取应急措施、上报事件及处置情况，是否及时提醒用户；

6） 查阅数据处理者数据安全事件应急处置记录、报送记录等相关材料，评估其是否在发生数据安全事件时，能及时按照应急管理制度和预案实施应急措施；

7） 查阅数据处理者数据安全事件应急处置记录、报送记录、总结报告等相关材料，评估其是否在事件处置完成后及时形成总结报告，并将数据安全事件处置情况等报告本地区行业监管部门。

9.2.2.2 重要数据和核心数据基础性安全评估

在覆盖一般数据基础性安全评估基础上，针对重要数据和核心数据还应进一步开展以下评估工作：

a） 组织机构

1） 查阅数据处理者数据安全管理组织架构体系，访谈数据安全相关人员，评估数据处理者是否建立覆盖本单位相关部门的数据安全工作体系，包括数据安全管理责任部门，采购、法务、审计、人力、财务等职能管理部门，以及研发设计、生产制造、运营维护、销售营销等业务部门，是否建立常态化沟通与协作机制；

2） 查阅数据处理者数据安全管理组织架构体系、责任部门职责、管理办法、年度工作计划等相关材料，评估其是否明确数据安全管理部门，是否明确了数据安全管理部门的职责并有序开展工业数据安全管理相关工作；

3） 访谈数据处理者数据安全负责人及数据安全责任部门人员，评估其是否明确工业数据安全管理责任部门的职责，是否能够按照相应要求进行数据安全管理；

4） 查阅数据处理者数据安全岗位职责等相关文档，评估其是否明确数据安全授权审批事项、审批部门和审批人等；

5） 访谈数据处理者数据安全授权审批相关人员，评估其是否知悉授权审批事项及流程；

6） 查阅数据处理者数据安全授权审批相关记录表，评估相关审批机制是否有效实施落地。

b） 人员保障

1） 查阅数据处理者岗位设置等相关材料，评估是否明确数据处理者数据安全负责人，其岗位职责是否可以指导数据安全管理责任部门、协调各相关部门开展数据安全工作，牵头制定数据安全管理制度规范和防护措施，监督制度规范和措

施的执行落实等；

2） 访谈数据处理者数据安全负责人，评估其是否明晰自身岗位职责；

3） 查阅数据处理者岗位设置等相关材料，评估是否将能获知重要数据和核心数据内容的人员确定为关键岗位人员，并签署数据安全责任书，责任书内容包括数据安全岗位职责、义务、处罚措施、注意事项等；

4） 访谈数据安全关键岗位人员，评估其是否明晰自身职责，包括数据安全管理制度执行落实、权限管理、安全审计、应急响应、数据安全事件处置和信息报送等。

c） 数据分类分级

1） 查验数据处理者是否按照相关法律法规、标准规范要求形成重要数据和核心数据目录，并向本地区行业监管部门备案；

2） 查验数据处理者重要数据和核心数据目录备案登记记录，是否按照有关规定开展目录备案和备案变更工作。

d） 权限管理

1） 查阅数据处理者权限管理制度或核查登记审批记录等相关材料，评估其是否根据实际建立内部登记、审批等工作机制和流程；

2） 查阅数据处理者权限管理制度及日志记录等相关材料，评估其是否在涉及处理重要数据和核心数据、授权特定人员超权限处理数据、实施重大操作（如数据批量复制、公开、销毁等）时进行审批；

3） 查阅数据处理者权限管理制度等相关材料，评估其是否定期对权限分配情况进行复核；

4） 查阅数据处理者权限管理制度等相关材料，评估其是否在人员变更、调离或终止劳动合同时，及时变更或终止其数据处理权限。

e） 系统与设备安全管理

1） 以人工核验、工具测试等方式，评估其是否对涉及重要数据和核心数据处理活动的数据载体的访问行为进行双因子身份鉴别；

2） 以人工核验、工具测试等方式，评估其是否通过工业防火墙、网闸等防护设备，对工业控制网络安全区域边界进行逻辑隔离安全防护；

3） 以人工核验、工具测试等方式，评估其是否对工业控制系统、工业互联网平台等的开发、测试和生产环境进行逻辑或物理隔离；

4） 以人工核验、工具测试等方式，评估其是否对处理重要数据和核心数据的系统提供不低于 GB/T 22239-2019 第三级要求的防护。

f） 安全评估

1） 查阅数据处理者数据安全风险安全评估报告、报送记录、整改方案、整改实施记录等相关材料，评估其是否每年至少开展一次安全风险评估，及时整改风险问题，并向本地区行业监管部门报送评估报告；

2） 访谈相关人员，评估其是否知悉重要数据和核心数据安全风险评估开展情况，存在自行评估的情况，评估相关人员是否知悉评估流程及内容；

3） 查阅数据处理者数据安全动态评估报告等相关材料，评估其是否在跨不同法人主体提供、转移、委托处理核心数据时开展数据安全风险评估。

g） 日志留存和审计

1） 通过人工核验或工具测试等方式，检查数据处理者是否对高风险操作（如批量复制、批量传输、批量销毁等操作）日志进行备份；

2） 查阅数据处理者维护数据安全所需的日志，评估数据处理者涉及安全事件处置

溯源的相关日志留存时间是否不少于 1 年，涉及向他人提供、委托处理、共同处理重要数据的，相关日志留存时间是否不少于 3 年；

3） 通过人工核验或工具测试等方式，评估数据处理者涉及核心数据安全、事件处置、溯源相关的日志留存时间是否不少于 3 年；

4） 通过人工核验或工具测试等方式，评估数据处理者是否配备数据安全审计相关技术能力，定期开展审计活动，将重要数据和核心数据收集、传输、使用、提供等处理活动纳入审计范围。

h） 监控预警、信息共享与应急处置

1） 查阅数据处理者数据安全事件风险报告等相关材料，评估其是否及时向本地区行业监管部门上报涉及重要数据和核心数据的安全风险情况；

2） 查阅数据处理者数据安全事件应急处置记录、报送记录等相关材料，评估其在发生涉及重要数据和核心数据的安全事件时，是否能够及时向本地区行业监管部门报告，在可能损害用户合法权益时及时告知用户，并提供减轻危害的措施。

9.2.3 数据全生命周期安全评估

9.2.3.1 一般数据全生命周期安全评估

评估团队应重点评估的内容包括：

a） 数据收集

1） 通过查阅文档、人工核验等方式，核实数据操作规程、数据收集记录、安全协议文件等相关材料，评估其数据收集过程是否符合合法、正当的原则，并且不以窃取或其他非法方式收集数据；

2） 访谈数据处理者数据收集相关人员，评估其是否按照合法、正当的原则开展数据收集工作，是否知悉数据处理者数据收集的规则和要求。

b） 数据存储

1） 访谈相关人员，评估其是否按照法律、行政法规规定和用户约定的方式、期限进行数据存储；

2） 查阅数据处理者数据备份及恢复记录等相关材料，评估其是否根据实际情况开展数据备份；

3） 访谈数据备份相关人员，评估其是否知悉数据处理者数据备份要求；

4） 通过人工核验或工具测试等方式，评估数据处理者在数据存储过程中是否采用身份鉴别和访问控制机制；

5） 通过人工核验或工具测试等方式，评估其对于非联网独立控制单元，如传感、控制或执行单元等，是否采用物理安全措施保障生产环境的设备数据访问或调试接口不暴露，是否采用机密性和完整性防护措施，保障现场存储数据不被泄露、篡改或破坏。

c） 数据使用加工

1） 通过查阅文档、人工核验等方式，评估数据处理者是否在利用数据进行自动化决策时，保证决策的透明度和结果的公平合理；

2） 通过查阅文档、人工核验等方式，评估数据处理者是否对必要开通的网络服务采取安全接入代理等技术，是否进行用户身份认证和应用鉴权。

d） 数据传输

1） 查阅数据处理者数据操作规程等相关材料，评估其是否明确了数据传输安全相关要求；

2） 通过人工核验等方式，评估数据处理者是否根据传输的数据类型、级别和应用场景，制定安全策略；

3） 访谈相关人员，评估其在工业设备间通信、设备与平台通信时，是否对通信端身份、安全策略、安全状态进行双向鉴别，是否建立数据安全传输信道；

4） 通过人工核验或工具测试等方式，检查数据处理者部署的数据安全防护措施，评估其是否对通信端身份、安全策略、安全状态进行双向鉴别，是否建立数据安全传输信道。

e） 数据提供

查阅数据处理者数据提供记录等相关材料，评估其是否数据提供的范围、数量、条件、程序、时间等，是否建立跨网、跨安全域的数据提供安全操作规范，保障数据提供安全。

f） 数据公开

1） 查阅数据处理者数据公开等相关材料，评估其是否明确数据公开范围、类别、条件、流程等数据公开安全策略；

2） 查阅数据处理者数据公开记录、风险评估报告等相关材料，评估其是否在数据公开披露前，对数据公开可能对国家安全、公共利益产生的影响进行分析研判，是否将可能造成重大影响的数据公开。

g） 数据销毁

1） 查阅数据销毁制度、操作规程及数据销毁表单记录等相关材料，评估其是否明确数据销毁对象、规则、流程和技术等要求，是否对销毁活动进行记录和留存；

2） 访谈数据销毁相关人员，评估其是否明晰数据销毁流程。

h） 数据委托处理

查阅合同协议等相关材料，评估其是否明确委托方与受托方的数据安全责任和义务。

i） 数据出境

1） 访谈相关人员，评估其明确出境数据的名称、类型、数据接收方、安全保护措施等；

2） 访谈相关人员，评估其在开展个人信息出境时，是否结合实际按要求订立个人信息出境标准合同备案等。

j） 数据转移

查阅数据转移方案、通知记录等相关材料，评估其是否在数据转移前明确数据转移方案，是否明确通知数据转移后受影响用户。

9.2.3.2 重要数据全生命周期安全评估

在一般数据处理活动全生命周期安全评估基础上，进一步开展以下评估：

a） 数据收集

1） 查阅数据处理者数据操作规程、数据收集记录等相关材料，评估其是否对数据收集的来源、时间、类型、数量、频度、流向等信息进行记录，避免出现超范围数据收集活动；

2） 查阅数据处理者数据操作规程、数据收集记录、数据收集审批流程等相关材料，评估其在数据收集前，是否对所涉及的软硬件工具、设备、系统、平台、接口以及收集技术等，采取必要的测试、认证、鉴权等措施，并进行内部审批；

3） 访谈数据处理者数据收集相关人员，评估其是否知悉数据收集要求及内部审批流程；

4） 通过人工核验或工具测试等方式，检查数据处理者是否对数据收集环境、软硬件工具设备、系统、平台、接口以及收集技术等，采取了必要的测试、认证、鉴权等措施；

5） 通过人工核验或工具测试等方式，检查数据处理者是否对数据收集行为进行监测，确保数据收集的合规性和执行上的一致性，评估其是否能够发现数据收集异常行为并及时告警；

6） 查阅数据处理者间接获取数据记录、第三方承诺协议等相关材料，评估其在数据获取过程中是否要求数据提供方做出数据源合法性的书面承诺，明确双方法律责任。

b） 数据存储

1） 通过人工核验或工具测试等方式，评估数据处理者在数据存储过程中是否采用校验技术、加密技术、数字签名等措施；

2） 通过人工核验或工具测试等方式，评估数据处理者对重要数据和核心数据的存储介质是否进行安全管理；

3） 通过人工核验或工具测试等方式，评估相应存储系统是否可直接通过公共信息网络访问；

4） 通过人工核验或工具测试等方式，检查数据处理者采取的数据存储安全检测与恢复措施、风险告警信息记录等，评估其是否能够检测到数据在存储过程中保密性、完整性、可用性受到破坏，并进行告警，同时采取必要的措施恢复数据；

5） 通过人工核验或工具测试等方式，检查数据处理者重要数据和核心数据的备份日志文件、备份数据访问与安全存储等情况，评估其是否对重要数据和核心数据进行了定期备份；

6） 通过人工核验或工具测试等方式，检查重要数据和核心数据的相关恢复测试情况，评估是否定期开展恢复测试，并判断恢复测试的有效性。

c） 数据使用加工

1） 访谈数据使用加工相关人员，评估其是否熟练掌握数据使用加工过程中的授权和验证措施；

2） 通过人工核验或工具测试等方式，评估数据处理者是否在数据使用加工过程中采用了授权和验证方式；

3） 查阅数据处理者数据加工过程记录等相关材料，评估其是否明确数据获取方式、访问接口、授权机制、处理结果安全等内容并周期性的检查用户操作数据的情况，统一管理数据使用权限；

4） 通过人工核验或工具测试等方式，检查数据处理者数据使用加工的环境安全情况，评估其是否能够采用恶意代码检测、身份鉴别、访问控制等技术手段保障环境安全；

5） 通过人工核验或工具测试等方式，检查数据处理者的数据脱敏方法和技术手段，评估其是否在不影响数据加工与分析的情况下，对数据脱敏后再进行处理。

d） 数据传输

1） 通过人工核验或工具测试等方式，检查数据处理者在数据传输过程中时采取数据加密、数据校验、安全传输通道、安全传输协议等措施，必要时是否采用单向隔离传输等技术手段；

2） 查阅数据处理者数据传输机制等相关材料，评估其是否在数据传输过程配备安全技术手段，是否具备数据传输异常检测技术能力；

3） 通过人工核验或工具测试等方式，检查数据处理者是否具备数据传输异常检测技术能力，是否可以对陌生IP地址、数据库异常连接等异常情况进行监测并实时告警，在检测到数据遭破坏时及时采取恢复措施；

4） 查阅数据处理者数据传输机制、传输登记审批记录等相关材料，评估其是否在涉及跨组织机构或者使用公共信息网络进行数据传输时，建立内部登记、审批机制；

5） 通过人工核验或工具测试等方式，检查数据处理者是否采取了流量限速、阻断、违规外联监测等必要措施，对工控协议数据包进行深度解析，仅允许符合安全策略的数据通过安全域边界。

e） 数据提供

1） 查阅数据处理者数据提供记录、数据安全协议、数据提供协议等相关材料，评估是否与数据获取方签订数据安全协议或在相关协议中明确数据安全内容；

2） 查阅数据处理者数据安全能力评估或核实记录等相关材料，评估其是否对数据获取方的数据安全保护能力进行评估或核实；

3） 查阅数据处理者数据安全监控记录、日志等相关材料，评估其是否对数据提供过程采取了数据安全监控措施，确保数据合理规范提供；

4） 通过人工核验或工具测试等方式，评估是否在数据接入互联网等过程中开展了数据安全监测，是否对安全风险高的网络出口和资产进行网络边界的身份认证和访问控制；

5） 通过人工核验或工具测试等方式，评估数据处理者在数据提供过程中是否采取必要的保护措施，如数据脱敏、数据标注、数据水印等技术手段；

6） 通过人工核验或工具测试等方式，评估数据处理者是否采用数据标注、水印等溯源技术，对数据流经节点及流转过程中的篡改、泄露、滥用等行为进行溯源。

f） 数据公开

1） 查阅数据处理者数据公开记录相关材料，评估可公开数据是否根据数据特点、应用场景等采取必要的数据脱敏、数据水印等技术，确保数据公开安全；

2） 通过人工核验或工具测试等方式，评估数据处理者数据公开披露时是否根据数据特点、应用场景等采取必要的数据脱敏、数据水印等安全防护措施。

g） 数据销毁

1） 通过人工核验或工具测试等方式，评估数据处理者的数据销毁技术手段，并判断数据销毁后是否可逆恢复；

2） 查阅数据操作规程及数据销毁表单记录、备案记录等相关材料，评估其是否在销毁重要数据后及时向本地区行业监管部门更新重要数据目录备案。

h） 数据委托处理

查阅数据保护能力评估机制、评估记录等相关材料，评估其是否对受托方的数据安全保护能力、资质进行评估或核实，是否与数据接收方通过合同、协议等形式明确双方的数据安全防护责任和义务。

i） 数据出境

1） 访谈相关人员，评估是否对需申报数据出境安全评估的情形按要求开展数据出境风险评估，是否向国家网信部门申报数据出境安全评估并获得批准；

2） 查阅数据出境安全评估报告、数据出境安全管理制度等相关材料，评估其是否开展数据出境安全评估，并按需采取了数据出境安全保护措施。

j） 数据转移

查阅数据转移机制、备案记录等相关材料，评估其是否在重要数据转移后，涉及重要数据目录备案内容发生变化的，能及时向本地区行业监管部门更新备案。

9.2.3.3 核心数据全生命周期安全评估

在重要数据处理活动全生命周期安全评估基础上，进一步开展以下评估：

a） 数据收集

通过人工核验或工具测试等方式，评估数据处理者是否具备数据收集行为实时监控能力，在发现异常时及时终止数据收集行为，并采用技术手段确保所有收集行为可溯源。

b） 数据存储

1） 查阅数据处理者核心数据存储等相关材料，评估其是否对核心数据存储设备进行硬件冗余；

2） 通过人工核验或工具测试等方式，评估是否对历史数据库、时序数据库、实时数据库等核心数据存储设备进行硬件冗余，启用实时数据备份功能，实施异地容灾备份，保证主设备出现故障时冗余设备可以及时切换并恢复数据；

3） 通过人工核验或工具测试等方式，评估数据处理者是否建立数据存储行为实时监控能力，在发现异常时及时终止数据访问、删除、修改等操作行为，并采用技术手段确保所有存储操作行为可溯源。

c） 数据使用加工

通过人工核验或工具测试等方式，评估数据处理者是否具备数据使用加工行为实时监控能力，在发现异常时及时终止数据使用加工行为，并采用技术手段确保所有数据挖掘、使用、加工、分析等行为可溯源。

d） 数据传输

1） 通过人工核验或工具测试等方式，评估数据处理者是否建立数据传输实时监控能力，保证能够及时告警并阻断违规传输；

2） 通过人工核验或工具测试等方式，评估数据处理者是否具备数据溯源能力，确保所有数据传输路径可恢复，数据传输行为可溯源；

3） 通过人工核验或工具测试等方式，评估数据处理者是否采用技术手段实现数据传输的真实性、不可抵赖性和可控性。

e） 数据提供

1） 跨不同法人主体提供核心数据的，应查阅数据处理者数据提供记录等相关材料，评估其是否评估数据安全风险，是否采取必要的安全防护措施，是否事先向本地区行业监管部门提出申请；

2） 跨不同法人主体提供核心数据的，且自本年度1月1日起可能累计达到总量30%及以上的，应查阅数据处理者数据提供记录等相关材料，评估其是否经行业主管部门报协调机制办公室组织开展了风险评估。

f） 数据委托处理

查阅跨主体委托处理核心数据申请报告等相关材料，评估其是否事先向本地区行业监管部门提出申请。

g） 数据转移

1） 查阅跨主体转移核心数据申请报告等相关材料，评估其是否采取必要的安全防护措施，是否事先向本地区行业监管部门提出申请；

2） 通过人工核验或工具测试等方式，评估数据处理者是否采用数据溯源系统、审计系统等技术工具对数据跨主体委托处理行为进行全流程监控、审计、存证；

3） 跨不同法人主体转移、共享核心数据的，且自本年度1月1日起可能累计达到总量30%及以上的，应查阅数据处理者跨主体转移核心数据申请报告等相关材料，评估其是否经行业主管部门报协调机制办公室组织风险评估。

9.3 安全风险分析

重要数据和核心数据处理者在完成合规性评估后，应进一步对数据处理活动的安全风险进行分析研判，并及时开展风险处置，确保安全风险可控。安全风险分析主要包括风险源识别、安全影响分析以及综合风险研判三部分，具体实施流程参见图2。

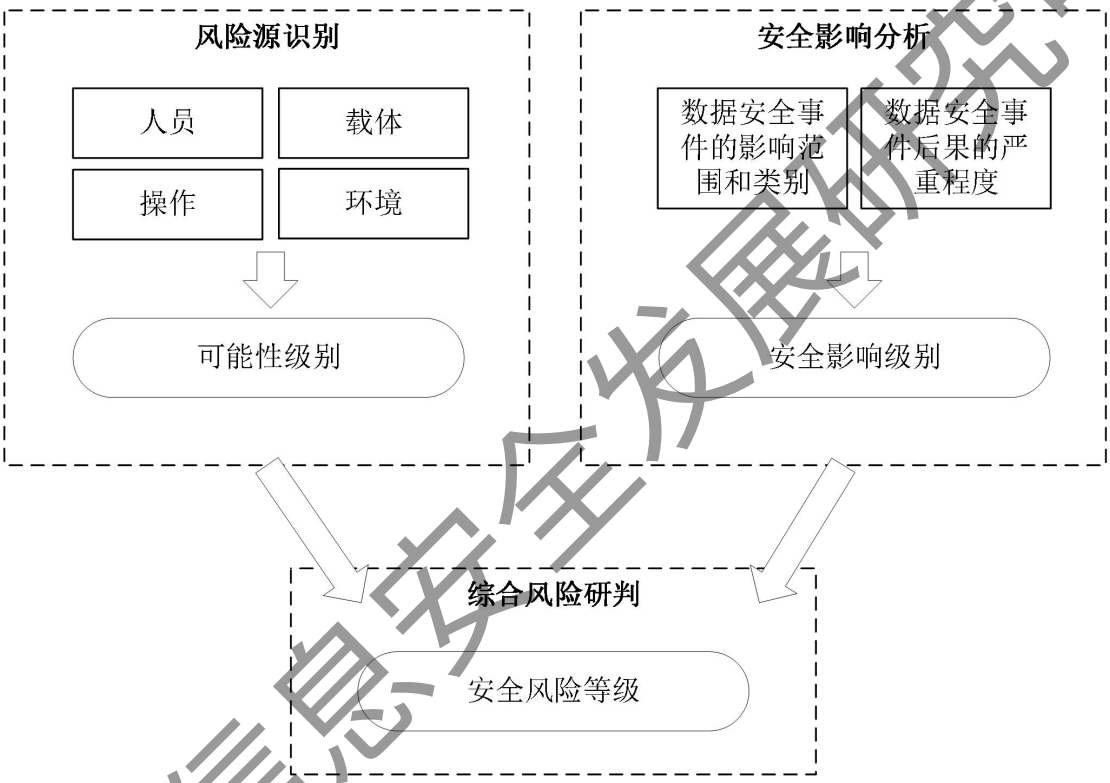

图 2 工业领域数据安全风险分析实施流程

9.3.1 风险源识别

9.3.1.1 识别范围概述

风险源识别是根据数据处理活动面临的威胁、系统的脆弱性、采取的安全措施等因素，研判数据安全事件发生的可能性级别。与数据安全事件发生可能性相关的要素可归纳为人员、载体、操作、环境等四个方面。人员包括人员管理漏洞、人员能力漏洞等情况；载体包括安全漏洞、运维漏洞、安全保护措施配备等情况；操作包括数据处理过程安全技术手段、身份鉴别、内部审批等情况；环境包括数据所处的接口环境、数据所处的网络环境等情况。

9.3.1.2 人员

评估团队可参考以下因素开展评估：

a） 数据是否存在人员管理漏洞，可参考以下因素：

1） 是否配备数据安全管理人员，统筹负责数据处理活动的安全监督管理；
2） 是否合理确定数据处理活动的操作权限，是否通过有效手段严格实施人员权限管理；
3） 从事重要数据和核心数据处理关键岗位人员是否进行背景审查，是否签订数据安全责任书；
4） 是否通过有效手段约束重要数据和核心数据岗位相关人员的非法数据处理活动，如非法盗取、非法转移，非法出境。

b） 是否存在人员能力漏洞，可参考以下因素：
1) 从事重要数据和核心数据处理关键岗位人员对数据安全政策法规有关要求是否清楚，是否理解到位；
2) 从事重要数据和核心数据处理关键岗位人员是否具备重要数据和核心数据安全防护技术能力，如是否能合理正确使用、配置组织配备的重要数据和核心数据安全防护技术工具。

9.3.1.3 载体

评估团队可参考以下因素开展评估：

a） 数据载体是否存在安全漏洞，可参考以下因素：
1） 数据载体是否存在已知且并未修复的漏洞；
2） 数据载体是否存在弱口令、默认口令；
3） 数据载体是否开放了非必要端口；
4） 数据载体是否存在未公开漏洞、后门。

b） 数据载体是否存在运维漏洞，可参考以下因素：
1） 工业现场、产线重要数据和核心数据载体是否存在远程运维，是否采取访问权限控制等安全措施；
2） 工业高端装备、重要工业控制系统及其他重要数据和核心数据载体是否存在运维外包。

c） 数据载体是否配备安全保护措施，可参考以下因素：
1） 是否对数据载体采取入侵检测、木马病毒查杀、防火墙、网闸、备份机等传统网络安全措施防范恶意攻击；
2） 是否进行移动数据载体登记，对载体带入带出是否有审批流程。

9.3.1.4 操作

评估团队可参考以下因素开展评估：

1） 数据处理过程是否根据数据级别使用数据处理相关安全技术手段，如分类分级标识、加密、脱敏、水印、防泄漏等；
2） 数据访问、使用、删除等操作是否进行身份鉴别；
3） 重要数据和核心数据批量导入导出、拷贝、交换共享、交易、上云、出境等行为是否进行内部审批；
4） 重要数据和核心数据处理过程中，是否围绕数据收集、传输、使用、提供等处理行为进行了记录、标记，是否实时开展审计，发现违规操作、异常流量等行为。

9.3.1.5 环境

评估团队可参考以下因素开展评估：

a） 数据所处的接口环境是否存在漏洞，可参考以下因素：

1） 数据所在信息系统是否存在未鉴权、未认证接口；

2） 重要数据和核心数据对应接口是否进行实时监测。

b） 数据所处的网络环境是否安全，可参考以下因素：

1） 网络环境是否根据数据类型、级别、业务模式等进行合理划分，并进行隔离；

2） 核心网络设备是否存在漏洞。

评估团队对以上因素进行充分了解后，通过人员访谈、文档查阅、工具核查等方式，识别已采取的措施与当前的状态，综合评价重要数据、核心数据安全事件发生的可能性级别。具体识别标准可参见表 1，其中可能性级别的识别应采取就高原则，根据人员、载体、操作、环境 4 个方面识别出最高可能性级别，作为数据处理活动可能引发数据安全事件的可能性级别。

表 1 可能性级别判定表

判断因素	可能性描述（对照可能性级别对应的可能性描述，从高至低进行梳理，满足一条即可判定）	可能性级别
人员	1、未配备数据安全管理人员，统筹负责数据处理活动的安全监督管理； 2、数据处理活动的操作权限未进行区分，没有有效手段限制不同身份数据处理者权限； 3、没有有效手段约束重要数据和核心数据岗位相关人员不进行非法数据处理活动，如非法盗取、非法转移，非法出境； 4、从事重要数据和核心数据处理关键岗位人员不具备重要数据安全防护技术能力，如不能合理正确使用、配置组织配备的重要数据安全防护技术工具； 5、从事重要数据和核心数据处理关键岗位人员未进行背景审查，未签订数据安全责任书。	高
	1、配备数据安全管理人员，但存在数据安全管理人员数量不充足、职责不合理清晰、能力不匹配等问题，无法全面统筹负责数据处理活动的安全监督管理； 2、数据处理活动的操作权限进行适当区分，有一定手段限制不同身份数据处理者权限，但是不能避免人员之间身份借用等问题； 3、配备一定手段约束重要数据和核心数据岗位相关人员不进行非法数据处理活动，如非法盗取、非法转移，非法出境； 4、从事重要数据和核心数据处理关键岗位人员对数据安全政策法规有关要求不清楚，不理解； 5、从事重要数据和核心数据处理关键岗位人员具备一定重要数据安全防护技术能力，但是不能快速应对、处置突发事件； 6、从事重要数据和核心数据处理关键岗位人员进行了一定背景审查，签订了数据安全责任书，但背景审查不充分。	中
	1、配备数据安全管理人员，数据安全管理人员数量充足、职责清晰合理，且相关人员能力与岗位职责互相匹配，可以全面统筹负责数据处理活动的安全监督管理； 2、数据处理活动的操作权限进行合理区分，采取有效手段限制不同身份数据处理者权限，能够避免人员之间身份借用等问题； 3、配备有效手段约束重要数据和核心数据岗位相关人员不进行非法数据	低

判断因素	可能性描述（对照可能性级别对应的可能性描述，从高至低进行梳理，满足一条即可判定）	可能性级别
	处理活动，如非法盗取、非法转移，非法出境； 4、从事重要数据和核心数据处理关键岗位人员对数据安全政策法规有关要求有深入了解，理解充分； 5、从事重要数据和核心数据处理关键岗位人员具备重要数据安全防护技术能力，能够合理进行系统、设备配置、使用，能够快速应对、处置突发事件； 6、从事重要数据和核心数据处理关键岗位人员进行了背景审查，签订了数据安全责任书，且背景审查充分。	
载体	1、数据载体存在高危及以上漏洞； 2、数据载体存在弱口令、默认口令； 3、数据载体开放了非必要端口； 4、数据载体存在未公开漏洞、后门，参考 CVSS 等漏洞等级判定规则，判定为高危及以上漏洞或漏洞影响范围较大、利用难度低； 5、工业现场、产线重要数据和核心数据载体存在远程运维，且未采取访问权限控制等安全措施； 6、工业高端装备、重要工业控制系统及其他重要数据和核心数据载体存在运维外包； 7、未对数据载体采取入侵检测、木马病毒查杀、防火墙、网闸、备份机等传统网络安全措施防范恶意攻击。	高
	1、数据载体存在低危及以上漏洞； 2、数据载体存在弱口令、默认口令，但存在弱口令的载体会定期更换口令； 3、数据载体开放了非必要端口，但开放的端口被利用可能性低； 4、数据载体存在未公开漏洞、后门，但参考 CVSS 等漏洞等级判定规则，判定为低危及以上漏洞或漏洞影响范围较小、利用难度高； 5、工业现场、产线重要数据和核心数据载体存在远程运维，但对远程运维相关人员数据访问权限进行了管理，且采取了一定安全措施保护远程运维数据； 6、工业高端装备、重要工业控制系统及其他重要数据和核心数据载体存在运维外包，但对外包人员进行了管理，并且采取措施限制人员窃取数据； 7、仅对数据载体采取木马病毒查杀、防火墙等传统网络安全措施防范恶意攻击，没有采用入侵检测、网闸、备份机备份等手段； 8、未进行移动数据载体登记，携带外出无审批流程。	中
	1、数据载体不存在漏洞、后门； 2、数据载体不存在弱口令、默认口令； 3、数据载体未开放非必要端口； 4、工业现场、产线重要数据和核心数据载体不存在远程运维； 5、工业高端装备、重要工业控制系统及其他重要数据和核心数据载体不存在运维外包； 6、对数据载体采取木马病毒查杀、防火墙、入侵检测、网闸、备份机备份等传统网络安全措施防范恶意攻击；	低

判断因素	可能性描述（对照可能性级别对应的可能性描述，从高至低进行梳理，满足一条即可判定）	可能性级别
	7、进行了移动数据载体登记，携带外出需审批。	
操作	1、数据处理过程未根据数据级别使用数据处理相关安全技术手段，如分类分级标识、加密、脱敏、水印、防泄漏等； 2、重要数据和核心数据处理过程中，未围绕数据收集、传输、使用、提供等处理行为进行记录、标记，未实时开展审计，发现违规操作、异常流量等行为； 3、数据访问、使用、删除等操作未进行身份鉴别； 4、重要数据和核心数据批量导入导出、拷贝、交换共享、交易、上云、出境等行为未进行内部审批。	高
	1、数据处理过程仅使用传输加密、脱敏、防泄漏等部分技术能力，未根据数据级别，采用技术手段对数据级别进行标识，未采用数据内容加密、硬件加密、数据水印溯源、数据安全监测等更有效手段保障数据安全； 2、重要数据和核心数据处理过程开展了一定行为记录、标记，但是未对数据全生命周期的处理活动都进行标记，开展了一定审计，但并非实施审计； 3、数据访问、使用、删除等操作进行了部分环节的身份鉴别； 4、重要数据和核心数据批量导入导出、拷贝、交换共享、交易、上云、出境等环节中，针对部分环节进行内部审批。	中
	1、数据处理过程根据数据级别使用分类分级标识、加密、脱敏、水印、防泄漏等全部数据处理相关安全技术手段，且使用手段安全有效； 2、重要数据和核心数据处理过程中，围绕数据收集、传输、使用、提供等处理行为进行了记录、标记，实时开展审计和监测，发现违规操作、异常流量等行为； 3、数据访问、使用、删除等操作全部进行了身份鉴别； 4、重要数据和核心数据批量导入导出、拷贝、交换共享、交易、上云、出境等行为全部进行了内部审批。	低
环境	1、重要数据和核心数据所在信息系统存在未鉴权、未认证接口； 2、重要数据和核心数据对应接口未进行实时监测； 3、核心网络设备存在漏洞； 4、网络环境未根据数据类型、级别、业务模式等进行合理划分，并进行隔离。	高
	1、一般数据所在信息系统存在未鉴权、未认证接口； 2、重要数据和核心数据所在信息系统接口未鉴权、未认证，但进行了实时监测； 3、网络设备存在漏洞，但不是核心网络设备，漏洞利用难度高； 4、网络环境进行了适当划分和隔离，但划分合理性差，只根据业务场景进行了划分，没有根据数据特点和级别进行划分。	中
	1、数据所在信息系统不存在未鉴权、未认证接口； 2、对重要数据和核心数据对应接口进行实时监测； 3、核心网络设备不存在漏洞； 4、网络环境能够根据数据类型、级别、业务模式等进行合理划分，并进	低

判断因素	可能性描述（对照可能性级别对应的可能性描述，从高至低进行梳理，满足一条即可判定）	可能性级别
	行隔离。	

9.3.2 安全影响分析

评估团队应综合分析数据处理活动存在安全风险时，数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对国家安全、公共利益产生何种影响及影响程度，包括以下维度：

a） 影响国土安全，是否会导致其他国家掌握我国国防建设、军事部署、关键设施等情况，进而影响我领土安全和主权完整；

b） 影响经济安全，是否会导致我国重要经济数据外泄，致使我国经济利益遭受巨大损失，引发经济风险；

c） 影响网络安全，是否会导致我国工业互联网等公共服务中断运行或主要功能故障、重要数据和核心数据泄露，对我国网络稳定运行造成巨大危害和损失；

d） 影响社会安全，是否会导致人民群众公共利益遭受危害、引发公共安全事件、影响人民群众日常生活秩序，对我国社会稳定产生重大影响；

e） 影响科技安全，是否会导致我国先进技术数据外泄，影响我国在该领域的国际领先地位。

评估团队在进行安全影响分析时候，可按照以下两方面开展：

a） 综合考虑重要数据和核心数据的种类、数量、级别等基本属性，初步分析发生数据安全事件后可能影响的范围和类别；

b） 根据数据安全事件发生后可能导致的后果严重程度，研判安全影响级别，具体判定标准可参见表2所示。

注 1：如涉及多个安全影响类别的，选取各安全影响类别下程度最高的，作为重要数据、核心数据处理活动安全影响级别。

注 2：一般数据因其数据敏感程度较低，在发生泄露、损毁、丢失等安全事件后不会对国家安全、公共利益产生较大影响，因此针对一般数据处理活动，可直接判定其安全影响级别为一般。

表 2 安全影响级别判定表

安全影响类别	安全影响严重程度描述	安全影响级别
国土安全	可能导致我国重要设施暴露在高度威胁中或严重影响我国领土、主权完整。	特别严重
	导致我国重要设施受到较高威胁或影响我国领土、主权完整。	严重
	例如导致我国重要设施受到一般威胁或可能间接影响我国领土、主权完整。	一般
经济安全	可能直接导致我国重大经济决策泄露，造成货币汇率、银行利率、物价水平、劳动就业总水平、失业率、进出口贸易总规模等发生巨大波动、GDP 显著下降等重大金融风险。	特别严重
	直接影响宏观经济运行，造成社会总供给和总需求、国民生产总值、货币汇率、银行利率、物价水平、劳动就业总水平、失业率、进出口贸易总规模等发生较大变动。	严重

安全影响类别	安全影响严重程度描述	安全影响级别
	可能严重影响市场经济运行秩序，如市场行为、市场结构、商品销售、交换关系、生产经营秩序、涉外经济关系等。	一般
网络安全	可能导致我国发生全国范围内工业互联网大面积瘫痪、顶级域名系统解析功能故障、大型互联网平台访问严重异常、大规模重要数据泄露、核心数据泄露、应急通信中断等安全事件。	特别严重
	可能导致我国发生多个省份工业互联网大面积瘫痪、大型域名系统解析功能故障、大型互联网平台访问异常、重要数据泄露、应急通信中断等安全事件。	严重
	可能导致我国一个省份工业互联网大面积瘫痪、省内具有影响力的网站和平台访问异常、重要数据泄露、应急通信中断等安全事件。	一般
社会安全	可能直接影响人民群众重要民生保障的事项、物资、工程和项目等。可能导致发生特别重大突发事件、特别重大群体性事件、暴力恐怖活动等。可能引发社会性恐慌，对社会稳定、公共利益造成特别严重危害。	特别严重
	可能导致发生重大突发事件、重大群体性事件等。可能严重影响人民群众的日常生活秩序。可能严重影响各级党政机关履行公共管理和服务职能。可能严重影响法制和社会伦理道德。	严重
	可能对人民群众的日常生活秩序造成一定影响；可能影响一定范围的企事业单位、社会团体的生产秩序、经营秩序、教学科研秩序、医疗卫生秩序等；可能影响公共场所的活动秩序、公共交通秩序。	一般
科技安全	可能导致我国工业领域尖端技术数据外泄；对我国先进科学技术研发进程等产生严重影响。	特别严重
	可能导致我国工业领域先进技术数据外泄；对我国先进科学技术研发进程等产生较大影响。	严重
	可能影响我国工业领域重要科学技术的研发进程，影响我国重要技术的相关性能指标。	一般

9.3.3 综合风险研判

评估团队应综合分析数据安全事件发生的可能性级别以及安全影响级别两方面因素，研判数据处理活动安全风险等级，安全风险等级可分为极高、高、中、低四个级别。安全风险等级判定方法可参考表3。

表 3 安全风险等级判定表

		可能性级别		
		低	中	高
安全影响级别	特别严重	中	高	极高
	严重	低	中	极高
	一般	低	低	高

评估团队在完成所有针对特定数据处理活动的安全风险评估之后，应依据风险就高原则，

以风险等级最高的结果作为数据处理活动安全风险等级。

9.3.4 评估结果与风险控制

重要数据和核心数据处理者应根据风险评估情况计算风险评估综合得分，编制形成《工业领域数据安全风险评估报告》（可参考附录B），并对风险评估结果负责，确保评估结果真实、准确，对于评估中发现的安全风险隐患，应结合重要数据和核心数据处理活动，及时采取有效的应对措施消除风险隐患。

10 评估工具

10.1 评估工具的安全要求

评估团队应使用来源可靠、安全稳定的评估工具，要求相关人员严格遵守操作流程，防止引入新的风险，并采取签订保密承诺书等方式对评估过程和结果性数据进行保护。评估工具应确保来源安全可靠，并经国家相关质检机构严格测试和校验，确保不对数据处理者生产运营造成影响。未通过检测和校验的评估工具不得应用于评估工作。

10.2 评估工具的使用要求

评估机构应确保评估人员可熟练使用相关数据安全检测评估工具，并在现场评估过程中安全、规范、合理的使用评估工具。使用防护评估工具对承载工业数据的系统、设备等进行测试时应慎重实施，尽量避免在业务高峰期进行技术测试。

10.3 数据安全风险评估工具

常用数据安全风险评估工具包括：工业数据安全防护能力评估工具、工业数据资产扫描工具、工业数据流量审计工具、工业数据安全检测评估工具、工业控制系统信息安全防护指南评估工具、工业控制系统脆弱性扫描工具、工业控制系统主机安全检查工具、工业控制系统配置核查工具等。

附 录 A

（资料性）

工业领域数据分类参考

数据一级类别	数据二级类别
研发域数据	研发设计数据
	开发测试数据
生产域数据	控制信息
	工况状态
	工艺参数
	系统日志
运维域数据	物流数据
	产品售后服务数据
外部域数据	与其他主体共享的数据
管理域数据	系统设备资产信息
	客户与产品信息
	产品供应链数据
	业务统计数据
	人事财务数据
平台运营域数据	物联收集数据
	知识库模型库数据
	平台运行与服务数据
标识运营域数据	标识数据
	标识解析数据
	标识运营数据

附 录 B

（资料性）

工业领域数据安全风险评估报告模板

一、数据处理者基本情况

简要描述数据处理者名称、性质、主营业务情况、工业业务运营情况等。

二、评估团队基本情况

简要描述评估团队组织架构、主要成员、责任义务等。

三、风险评估范围

简要描述评估数据的种类、数量、处理数据的业务场景、数据所处信息系统情况、主要数据安全保障措施整体情况、数据处理实施情况等。

（示例：本次评估主要针对XX业务场景下的XXX数据（数据量约XGB）进行评估，数据主要存储于XX信息系统XX数据库，托管于XX云。该数据涉及组织信息化管理人员XXX，业务部门XXX，数据保障措施XXX。）

四、数据处理活动分析

简要描述涉及处理数据活动的名称，数据的类型、名称、数量，处理重要数据的目的、方式、频率、涉及的接收方及信息系统情况。表B.1一般数据处理活动分析表提供了一般数据的分析样例，表B.2重要数据处理活动表提供了重要数据和核心数据处理活动分析样例，可供数据处理者参考。

表 B.1 一般数据处理活动分析表

序号	处理场景	数据类型[1]	数据项名称	数据数量[2]	处理目的	处理活动[3]	处理频率[4]	是否涉及接收方[5]	涉及信息系统名称
示例	XX 系统/XX 业务/XX 场景数据分析	研发设计数据域—开发测试代码	X 开发测试代码	2GB	XX 产品开发	数据收集、存储、使用	每小时	XX 企业（国企）	XX 系统
1	处理场景 A								

1. 按照《工业领域重要数据和核心数据识别指南（试行）》具体分类填写，包含大类及子类。
2. 按数据项填写（单位：条/GB）。
3. 处理方式包括收集、存储、使用、加工、传输、提供、公开、销毁等。
4. 实时/每小时/每天/每周/每月/每季度/每年。
5. 如有，需填写合作方名称及类型，合作方类型包括国企、民企、外企、事业单位、高校、政府机构、非盈利组织等；如没有，填写不涉及。

2	处理场景B								
	……								

表 B.2 重要数据、核心数据处理活动分析表

序号	处理场景	数据类型[6]	数据级别	数据项名称	数据数量[7]	处理目的	处理活动[8]	处理频率[9]	是否涉及数据出境[10]	涉及信息系统名称
示例	XX 系统/XX 业务/XX 场景数据分析	研发设计数据域—开发测试代码	重要数据/核心数据	X 开发测试代码	2GB	XX 产品开发	数据收集、存储、使用	每小时	XX 国家/地区-XX 企业(企业/政府机构/非盈利组织等)	XX 系统
1	处理场景A									
2	处理场景B									
	……									

五、风险评估

（一）处理活动 A 风险评估（如：XX 数据使用分析风险评估）

1、合规性评估

（1）正当必要性评估

详细描述开展数据处理活动 A 的目的、方式，以及该目的、方式下所处理的数据类型、数量、范围、频率等；简要分析该数据处理目的、方式是否合法、正当，所涉及的数据数量、类型、频率是否为实现该目的下的最小范围，同时提供相关证明材料。

（2）基础性安全评估

按照标准正文 7.2.2 的评估要点，分别详细介绍数据处理活动 A 所涉及的数据安全基础性管理措施情况，分析研判数据处理活动 A 所涉及的基础性数据安全管理制度或措施是否满足相关要求，并提供相关证明材料。

（3）数据全生命周期安全评估

1. 按照《工业领域重要数据和核心数据识别指南（试行）》具体分类填写，包含大类及子类。
2. 按数据项填写（单位：条/GB）。
3. 处理方式包括收集、存储、使用、加工、传输、提供、公开、销毁等。
4. 每小时/每天/每周/每月/每季度/每年。
5. 如有，需填写合作方名称及类型，合作方类型包括国企、民企、外企、事业单位、高校、政府机构、非盈利组织等；如没有，填写不涉及。

按照标准正文 7.2.3 的评估要点，分别详细介绍数据处理活动 A 所涉及的数据全生命周期环节安全保护情况，分析研判数据处理活动 A 所涉及的数据全生命周期安全管理措施是否满足相关要求，并提供相关证明材料。

2、安全风险分析

（1）风险源识别

按照标准正文 7.3.1 所提供 4 个评估维度以及评估方法，分别详细描述数据处理活动 A 所面临的威胁、系统的脆弱性及采取的安全措施，并分析研判数据安全事件发生的可能性级别。

（2）安全影响分析

按照标准正文 7.3.2 所提供 5 个评估维度以及评估方法，结合数据处理活动 A 所涉及的重要数据、核心数据的数量、种类、级别，以及处理目的、方式、范围等要素，分别详细描述数据处理活动 A 所涉及的数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，有可能对国家安全、公共利益产生的影响及影响程度。

（3）综合风险研判

按照标准正文 7.3.3 所提供的方法，结合数据安全事件发生的可能性级别以及安全影响级别，详细描述数据处理活动 A 综合风险等级的分析过程与结果。

（二）处理活动 B 风险评估（如 XX 数据提供风险评估）

1、合规性评估

（1）正当必要性评估

详细描述开展数据处理活动 B 的目的、方式，以及该目的、方式下所处理的数据类型、数量、范围、频率等；简要分析该数据处理目的、方式是否合法、正当，所涉及的数据数量、类型、频率是否为实现该目的下的最小范围，同时提供相关证明材料。

（2）基础性安全评估

按照标准正文 7.2.2 的评估要点，分别详细介绍数据处理活动 B 所涉及的数据安全基础性管理措施情况，分析研判数据处理活动 B 所涉及的基础性数据安全管理制度或措施是否满足相关要求，并提供相关证明材料。

（3）数据全生命周期安全评估

按照标准正文 7.2.3 的评估要点，分别详细介绍数据处理活动 B 所涉及的数据全生命周期各环节安全保护情况，分析研判数据处理活动 B 所涉及的数据全生命周期安全管理制度或措施是否满足相关要求，并提供相关证明材料。

2、安全风险分析

（1）风险源识别

按照标准正文 7.3.1 所提供 4 个评估维度以及评估方法，分别详细描述数据处理活动 B 所面临的威胁、系统的脆弱性及采取的安全措施，并分析研判数据安全事件发生的可能性级别。

（2）安全影响分析

按照标准正文 7.3.2 所提供 5 个评估维度以及评估方法，结合数据处理活动 B 所涉及的重要数据、核心数据的数量、种类、级别，以及处理目的、方式、范围等要素，分别详细描述数据处理活动 A 所涉及的数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，有可能对国家安全、公共利益产生的影响及影响程度。

（3）综合风险研判

按照标准正文 7.3.3 所提供的方法，结合数据安全事件发生的可能性级别以及安全影响级别，详细描述数据处理活动 B 综合风险等级的分析过程与结果。

（三）……

六、评估结论

（一）合规性评估结论

结合合规性评估情况，判断符合项共计X项，部分符合项共计X项，不符合项共计X项，不适用项共计X项。

（二）风险评估结论

结合各项重要数据处理活动风险等级，综合判定总体重要数据风险等级。

七、应对措施

针对各项重要数据处理活动风险评估结果，说明需采取的应对措施情况。例如，提升重要数据技术保障能力、减少重要数据承载系统与外部的交互接口、加强对重要数据接收方的管理等。

参考文献

[1]《中华人民共和国数据安全法》
[2]《中华人民共和国网络安全法》
[3]《工业和信息化领域数据安全管理办法（试行）》
[4]《GB/T 20984-2022 信息安全技术 信息安全风险评估方法》
[5]《GB/T 36466-2018 信息安全技术 工业控制系统风险评估实施指南》