核能领域数据安全风险评估方法

1 范围

本文件提出了核能领域数据安全风险评估的基本要求、实施流程、评估内容、评估方法及评估结果判定准则，明确了数据安全风险评估各阶段的实施要点和工作方法。

本文件适用于指导核能领域网络运营者开展数据处理活动的安全风险评估工作，并为监管机构或第三方安全评估机构等单位开展核能领域数据安全评估工作提供参考。

注：涉及国家秘密的数据和军事数据不适用于本文件。开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

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

3 术语和定义、缩略词

3.1 术语和定义

GB/T 25069-2022 界定的以及下列术语和定义适用于本文件。

3.1.1

数据 data

任何以电子或者其他方式对信息的记录。

[来源:数据安全法，第三条]

3.1.2

网络数据 network data

通过网络收集、存储、传输、处理和产生的各种电子数据。

注：本文件中评估的数据类型限定为网络数据。

[来源:网络安全法，第七十六条]

3.1.3

网络运营者 network operator

网络的所有者、管理者和网络服务提供者

[来源:网络安全法，第七十六条]

3.1.4

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

[来源:数据安全法，第三条]

3.1.5

数据处理活动 data processing activities

数据的收集、存储、使用和加工、传输、提供、公开、交易、出境、销毁等活动。

[来源:数据安全法，第三条，有修改：增加“交易、出境、销毁”]

3.1.6

合理性 rationality

数据处理活动遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，不危害国家安全、公共利益，不得损害组织的合法权益。

[来源:数据安全法，第八条，有修改]

3.1.7

数据安全风险 data security risk

由于开展数据处理活动不合理、缺少有效的数据安全措施等，导致数据安全事件的发生及其对国家安全、公共利益或者组织合法权益造成的影响。

3.1.8

数据安全风险评估 data security risk assessment

对数据和数据处理活动的安全风险和违法违规问题进行检测评估的过程。

3.1.9

安全措施 security measure

保护数据和数据处理活动、抵御数据安全风险事件而实施的各种安全管理和技术实践、规程和机制。

3.1.10

业务 business

组织为实现某项发展战略而开展的运营活动，该活动具有明确的目标，并延续一段时间。

3.1.11

风险源 risk source

可能导致危害数据和数据处理的保密性、完整性、可用性和合理性等不希望事故的原因、条件、情形或行为。

注：风险源，既包括安全威胁利用脆弱性可能导致数据安全事件的风险源(简称为“数据安全风险源”)，也包括数据处理活动不合理操作可能造成违法违规处理事件的风险源(简称为“违法违规处理风险源”)。

3.1.12

重要数据 important data

一旦泄露可能直接影响国家安全、公共安全、经济安全和社会稳定的数据。

注：重要数据包括未公开的政府信息,数量达到一定规模的基因、地理、矿产信息等,原则上不包括个人信息、企业内部经营管理信息等。

[来源: GB/T 41479—2022 信息安全技术 网络数据处理安全要求，3.9]

3.1.13

核能领域 nuclear energy field

涉及核能、核技术科研及应用的相关领域。覆盖铀矿冶、核燃料、核电、核工程建设、装备制造、后处理、核技术科研、核技术应用、核环保等核科技工业全产业链，包含研发设计、工程建造安装、运营、退役等全周期业务流程。

3.1.14

数据处理者 data processor

在数据处理活动中自主决定处理目的和处理方式的独立法人单位。

3.1.15

数据交易 data transaction

数据供方和需方之间以数据商品作为交易对象，进行的以货币或货币等价物交换数据商品的行为。

注 1：数据商品包括用于交易的原始数据或加工处理后的数据衍生产品。

注 2：数据交易包括以大数据或其衍生品作为数据商品的数据交易，也包括以传统数据或其衍生品作为数据商品的、数据交易。

[来源:GB/T 37932-2019 信息安全技术 数据交易服务安全要求，3.1]

3.1.16

数据出境 data export

数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息。

[来源:数据出境安全评估办法，第二条，有修改]

3.2 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

SDK：软件开发工具包（Software Development Kit）

SaaS：软件服务（Software as a Service）

OA：办公自动化（Office Automation）

4 核能领域风险评估基本要求与流程

4.1 评估适用对象

4.1.1 通用评估对象

核能数据拥有方、核能数据处理方，视为核能领域数据安全评估对象。

4.1.2 重点评估对象

符合以下情形之一的，视为核能领域数据安全重点评估对象：

a) 重要数据或核心数据处理者；
b) 关键信息基础设施运营者；
c) 大型数据平台运营者；
d) 赴境外上市的数据处理者；
e) 网络安全等级保护三级及以上运营者；
f) 其他法律法规或有关部门规定的重点评估对象。

4.2 评估触发场景

4.2.1 周期性评估

通用评估对象应每三年至少开展一次核能领域数据安全风险评估工作，重点评估对象应每年至少开展一次核能领域数据安全风险评估工作。

4.2.2 触发性评估

符合以下情形之一的，需结合实际情况触发核能领域数据安全风险评估工作：

a) 核能领域的数据处理者在重要数据获取、共享、交易、委托处理或向境外提供前，应开展数据安全风险评估。
b) 核能领域的数据处理者开展高风险数据处理活动前，宜开展数据安全风险评估，高风险数据处理活动包括但不限于:
    1) 重要数据处理者合并、分立、解散、被宣告破产进行数据转移;
    2) 承载重要数据处理活动的信息系统发生架构调整、下线等重大变更;
    3) 基于不同业务目的的数据汇聚融合;
    4) 新技术应用可能带来数据安全风险的;
    5) 法律法规或有关部门规定要评估的情形;
    6) 其他可能直接危害国家安全、公共利益或者大量组织合法权益的数据处理活动。
c) 对于已经评估过数据安全风险评估的数据处理活动，当数据范围、数据处理活动、环境、相关方等发生重大变更时，需重新开展数据安全风险评估。
d) 核能领域重要系统上线前，可根据实际需要开展数据安全风险评估。
e) 国家及行业主管部门的相关要求发生变化时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大数据安全事件时，应开展数据安全风险评估。

4.3 事前报批与风险评估报送

4.3.1 事前报批

根据数据处理者开展高风险数据处理活动前做的数据安全风险评估结果，在降低风险的措施缺失、处理可能导致高风险的情况下，数据处理者在进行数据处理活动前，应当向有关主管部门进行事前报批。

4.3.2 风险评估报送

重要数据、核心数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送数据安全风险评估报告。

4.3.3 信息提供

在事前咨询（咨询模版参考附录 B.2）与风险评估报告报送（报送模版按照有关主管部门要求）时，数据处理者应提供下列信息：

a) 涉及的数据处理相关方信息与各自责任说明；
b) 拟进行或已经进行的数据处理的目的和方式；
c) 重要数据或核心数据的处理者应明确数据安全负责人，并提供其联系方式，非重要数据处理者，提供数据安全接口人联系方式；
d) 数据安全风险评估报告，其中涉及重要数据处理的安全风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等；
e) 监管机构要求的其他信息。

4.4 评估实施流程

数据安全风险评估实施流程，主要包括评估准备、数据和数据处理活动识别、风险源识别、风险分析、评估总结五个阶段，如图 1 所示：

a） 评估准备：是数据安全风险评估的初始预备阶段，在评估实施前应完成评估准备工作，输出数据安全风险评估工作方案、前期调研表单等；
b） 要素识别：识别可能影响数据安全风险的要素，包括识别数据处理者的基本情况、业务和信息系统、数据资产、数据处理活动、数据安全防护措施。掌握数据处理者、业务和信息系统基本情况，摸排涉及的数据资产和数据处理活动，厘清之间的关系，了解采取的数据安全防护措施情况。输出要素识别清单等，具备条件的，可绘制数据流图。
c） 风险识别：基于要素识别情况，通过对数据安全管理、数据处理活动、数据安全技术等方面进行评估，识别可能存在的风险源，掌握被评估对象或同行业相关数据安全事件历史发生情况，识别现有安全措施完备性并对其有效性进行验证，从而发现可能存在的数据泄露、篡改、破坏、不合理处理等数据安全风险，形成风险评估记录文档、技术评估报告等。

注：风险源，包括安全威胁利用脆弱性可能导致数据安全事件的情形，和数据处理活动不合理可能造成的风险隐患等。

d） 安全分析：主要在要素识别和风险识别的基础上，进行数据安全分析，输出数据安全风险清单；
e） 评估总结：主要用于编制数据安全风险评估报告，提出风险处置建议，分析残余风险、风险评估后评价。

风险沟通和评估过程文档管理贯穿于整个风险评估过程。风险评估工作是持续性的活动，当被评估对象的政策环境、外部威胁环境、业务目标、安全目标等发生变化时，应重新开展风险评估。

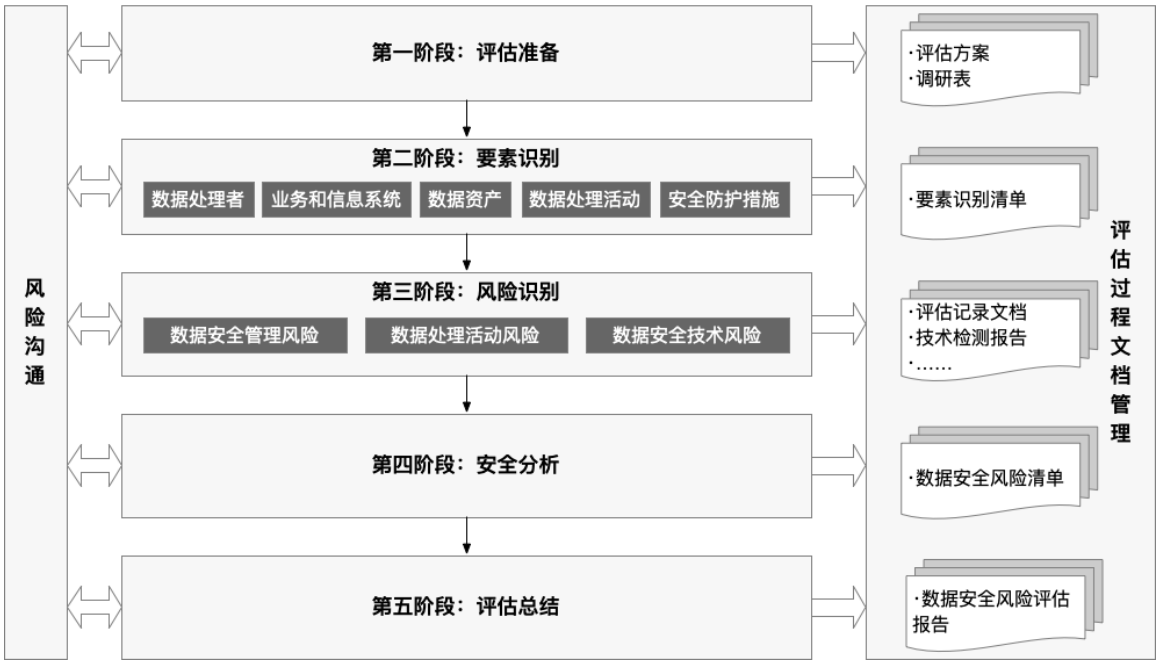

图 1 数据安全风险评估实施流程图

4.5 评估内容框架

在要素识别的基础上，数据安全风险评估主要围绕数据处理活动、数据安全管理、数据安全技术等方面开展，评估内容框架如图 2 所示。

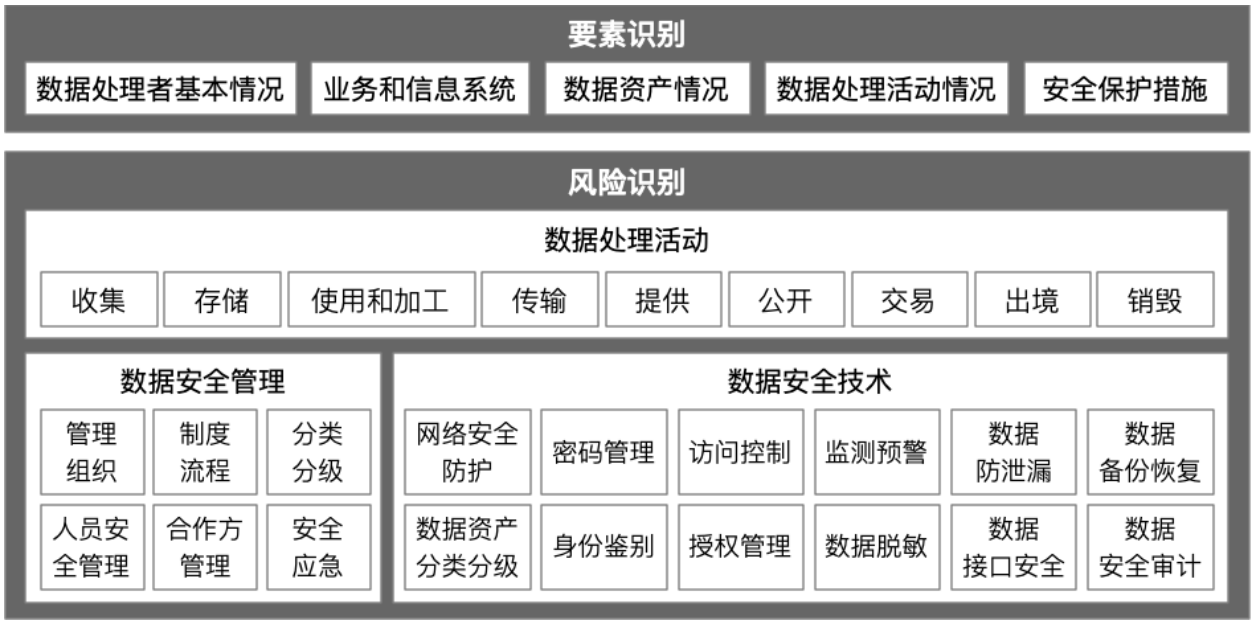

图 2 数据安全风险评估内容框架图

5 核能领域数据安全风险评估实施

5.1 评估准备

5.1.1 确定评估目标

明确数据安全风险评估的目标，常见目标包括但不限于:

a) 对核能领域数据处理者的数据和数据处理活动进行全面安全评估，了解处理的数据及开展数据处理活动的情况，发现存在的数据安全风险和违法违规问题，及时防范数据安全风险；
b) 对重要数据处理活动定期开展风险评估，了解处理的重要数据的种类、数量、分布及开展数据处理活动的情况，对面临的数据安全风险及其应对措施进行评估；
c) 对开展共享、交易、委托处理、向境外提供重要数据的活动进行数据安全风险评估，发现对外提供重要数据可能存在的数据安全风险和问题；
d) 在开展可能直接影响国家安全、公共利益或者大量组织合法权益的数据处理活动前开展数据安全风险评估，发现可能存在数据安全风险和违法违规问题；
e) 根据数据安全事件和监管需求，由国家、行业或地方主管监管部门组织开展数据安全评估检查，发现数据安全风险和问题。

5.1.2 确定评估范围

根据评估目标确定数据安全风险评估的对象、范围和边界，明确评估涉及的数据资产、数据处理活动、业务、信息系统、人员和内外部组织等。

数据安全风险评估工作主要围绕数据和数据处理活动开展，评估范围可能是组织全部的数据及数据处理活动相关的各类资产和部门，也可能是某个独立的业务、信息系统、数据资产、数据处理活动或部门等。

评估范围应至少包含评估对象开展数据处理活动所涉及的最高等级数据，以供判断该评估对象的数据安全风险等级全貌。

核能领域数据安全重点评估对象，需增强评估要求，评估范围应包括但不限于以下内容：

a) 涉及的评估对象应包括核能领域核心、重要数据处理者，及其与总包方、监理方、施工方和其他技术和服务提供单位工作中收集、产生和处理的数据；
b) 涉及的数据应包括结构化数据和非结构化数据。数据存储介质应包含但不限于磁盘、光盘、磁带等电子存储，数据存储方式包含但不限于本地存储、私有云及互联网公有云存储等；
c) 涉及的数据处理活动包括核能领域项目规划设计、调研选址、工程建设和施工、设备制造和安装、系统和设备调试、移交接产、运营期信息系统运行、安全生产及经营管理数据处理等;
d) 涉及的信息系统包括自有及使用其他单位提供的管理类信息系统、生产控制系统、网络和信息化工具软件，管理类信息系统如各类 OA 系统、ERP 系统、工程管理系统等，生产控制系统包括核电厂电力监控系统、核应急系统等。

5.1.3 组建评估团队

根据评估目标和评估范围，组建数据安全风险评估团队，由评估管理单位、评估方、被评估方等相关人员组成，必要时也可邀请有经验的数据安全专家组成专家组。

a) 被评估方通常由组织的数据安全负责人和安全、法务、合规、运维、研发、业务、数据、风险等部门相关人员组成；
b) 如需选择第三方评估机构，应按照有关规定或标准选择满足数据安全评估机构能力要求的评估机构；
c) 评估团队应做好评估前的表格、文档、评估工具等各项准备工作，并按照需求签署保密协议，评估团队在检查评估中获取的信息，只能用于评估工作和实施数据安全保护。

核能领域数据安全重点评估对象，需增强评估要求，组建评估团队应包括但不限于以下内容：

a) 根据评估目标和评估范围，数据安全风险评估团队，应由核能领域数据安全重点评估对象组织包括本单位、上级公司网络安全、数据安全团队、同行、相关协会、及其总包方、监理方、施工方和其他技术和服务提供单位有经验的数据安全专家组成，必要时也可邀请当地公安、行业主管部委及有经验的数据安全专家组参与；
b) 评估团队应包含被评估对象所在单位的数据安全管理人员和负责人员、网络安全和信息化专业人员、生产控制系统相关专业人员、安全管理人员以及相关的法务、合规、业务等部门人员，以及与上述人员工作有密切数据往来的总包方、监理方、施工方和其他技术和服务人员；
c) 如需选择第三方评估机构，应按照有关规定或标准选择满足数据安全评估机构能力要求的评估机构，评估机构应该具备能源、电力或核能领域工作相关评估经验；
d) 评估团队人员应不少于 5 人，外部成员应不少于 60%，评估组长应由外部成员担任。

5.1.4 制定评估方案

根据评估目标、评估范围和调研情况，明确数据安全风险评估的评估依据、评估内容和评价准则，制定评估方案。

a) 确定评估依据。针对评估目标和范围确定评估依据，常见评估依据包括但不限于:
   1) 数据安全法律、行政法规、司法解释，如《网络安全法》、《数据安全法》等；
   2) 国家网信部门、公安机关、安全部门等有关部门的数据安全部门规章、规范性文件；
   3) 核能领域主管部门的数据安全部门规章、规范性文件，如国家发改委《电力监控系统安全防护规定》、国家能源局《电力监控系统安全防护总体方案》、《核电厂网络安全技术政策》、《能源行业数据分类分级标准规范》、《能源领域数据安全管理办法》等；
   4) 地方区域的数据安全政策规定和监管要求，如《福建省大数据发展条例》、《广东省公共数据管理办法》、《山东省大数据发展促进条例》、《辽宁省大数据发展应用条例》等涉及的地方区域；
   5) 现行数据安全国家标准、行业标准、地方标准和团体标准等，如《信息安全技术 大数据安全管理指南》、《信息安全技术 重要数据识别指南》（征求意见稿）、《信息安全技术 网络数据分类分级要求》（征求意见稿）等；
   6) 被评估方的监管单位、上级单位或本单位的数据安全、网络安全等相关安全要求。
b) 确定评估内容。结合评估目标和评估依据，确定核能领域被评估对象适用的数据安全评估内容，明确核心数据和重要数据的范围，评估内容应包括但不限于组织与人员、制度与政策、信息系统、数据对象、数据安全相关的文化、宣传、培训等外部环境等。
c) 确定评价准则。综合考虑评估的目标、范围、依据等因素，制定适合于核能领域评估对象的的风险评价准则等。
d) 制定评估方案。编制数据安全风险评估工作方案并获得评估管理方的支持、认可，方案包括但不限于评估概述、评估内容和方法、评估人员、工作计划、调研评估准备清单等内容。调研准备清单参照附录 B，包括 B.1 项目相关方联系表、B.2 资料收集清单、B.3 评估准备事项。

5.2 要素识别

5.2.1 数据处理者识别

对被评估的数据处理者基本情况进行调研，调研内容应包括但不限于：

a) 单位名称、组织机构代码、办公地址、法人信息、人员规模、经营范围、数据安全负责人及其职务、联系方式等基本信息；
b) 单位性质，例如企业、事业单位、社会团体、互联网平台运营者、关键信息基础设施运营者等；

c） 所属核能领域和业务运营归属地，开展数据处理活动所在国家和地区等。

5.2.2 业务和信息系统识别

对被评估的业务和信息系统基本情况进行调研，调研内容应包括但不限于：

a） 网络和信息系统基本情况，包括网络规模、拓扑结构、信息系统等情况和对外连接、运营维护等情况以及是否为关键信息基础设施等情况；
b） 业务基本信息，包括业务描述、业务类型、服务对象、业务流程、用户规模等基本信息；
c） 业务是否涉及重要数据或核心数据处理；
d） 识别业务的信息系统、App 和小程序情况；
e） 数据中心和使用云平台情况；
f） 识别业务接入的外部第三方产品、服务或 SDK 的情况，包括名称、版本、提供方、使用目的、合同协议等。

核能领域数据安全重点评估对象，需增强评估要求，业务和信息系统基本情况调研内容应包括但不限于：

a） 业务范围：被评估对象在核能领域项目设计、施工、调试、监理，及运营生产核心、生产支持、生产监督、经营管理、网络和信息化工具软件等相关的信息系统，以及系统数据存储和处理情况，并判断是否涉及重要数据或核心数据处理，如涉及需要说明处理情况；
b） 上述业务范围内自有或使用第三方提供的信息系统、App 和小程序、工具软件、SaaS 应用等，如 OA、工程管理系统、财务系统、设备管理系统、移交接产系统、设计管理系统、调试系统等；
c） 上述业务范围内的系统与其他系统的接口情况。

5.2.3 数据资产识别

针对被评估的业务和信息系统，梳理结构化数据资产（如数据库表等）和非结构化数据资产（如图标文件等），摸清数据底数，输出数据资产清单。涉及范围包括但不限于生产环境、测试环境、备份存储环境、云存储环境、个人工作终端、数据采集设备终端等收集和产生的数据。识别内容包括但不限于：

a） 识别结构化和非结构化数据资产清单；
b） 识别数据分类分级情况，包括数据分类分级规则、数据类别、数据级别、重要数据和核心数据目录情况等；
c） 识别重要数据、核心数据在业务领域、组织、部门和信息系统的分布情况，如数据种类、数据量、归口管理部门、归口管理人员等、数据存储位置、外送上报等；

核能领域数据安全重点评估对象，需增强评估要求，数据范围应包括但不限于：设计数据、施工数据、设备数据、移交接产数据、调试数据，业务系统数据和信息化管理工具软件数据、生产管理和经营管理数据、核心数据、重要数据和一般数据、内部数据和外部数据、以及交易数据、主数据、指标数据、日志数据、元数据和参考与引用数据等。

5.2.4 数据处理活动识别

针对被评估的业务或数据，识别开展的数据处理活动情况，输出数据处理情况清单。识别内容包括但不限于：

a） 数据收集情况，如数据收集渠道、收集方式、数据范围、收集目的、收集频率、外部数据源、相关系统，以及在被评估方外部公共场所安装图像采集、个人身份识别设备的情况等；
b） 数据存储情况，如数据存储方式、数据中心、存储系统（如数据库、大数据平台、云存储、网盘、存储介质等）、外部存储机构、存储地点、存储期限、备份冗余策略等；

c） 数据使用和加工情况，如数据使用和加工目的、方式、范围、场景、算法规则、相关系统和部门，数据清洗、转换、标注等加工情况，核心数据、重要数据或个人信息委托处理、共同处理的情况等；
d） 数据传输情况，如数据传输途径和方式（如互联网、VPN、物理专线等在线通道情况，或采用介质等离线传输情况）、传输协议、内部数据共享、数据接口等；
e） 数据提供情况，如数据提供的目的、方式、范围、数据接收方、合同协议、对外提供的个人信息和重要数据的种类、数量、范围、敏感程度、保存期限等；
f） 数据公开情况，如数据公开目的、方式、对象范围、受众数量、组织、地域等；
g） 数据交易情况，如数据交易参与方、交易对象、数据商品、数据确权定价、数据交易服务机构和交易过程等；
h） 数据出境情况，如是否存在个人或重要数据出境，如跨境业务、跨境办公、境外上市、使用境外云服务或数据中心、国际交流合作等场景的数据出境情况；
i） 数据销毁情况，如数据销毁情形、销毁方式、数据归档、介质销毁等。

5.2.5 安全防护措施识别

识别安全防护措施情况，包括但不限于：
a） 数据安全管理组织、人员及制度情况；
b） 数据资产及分类分级管理情况；
c） 防火墙、入侵检测、入侵防御等网络安全设备及策略情况；
d） 访问控制和身份鉴别情况；
e） 网络安全漏洞管理及修复情况；
f） VPN 等远程管理软件的用户及管理情况；
g） 设备、系统及用户的账号或口令管理情况；
h） 加密、脱敏、匿名化、去标识化等安全技术应用情况。

5.3 风险识别

5.3.1 概述

数据安全风险识别，主要围绕数据安全措施、数据安全风险源和不合理处理数据风险源，通过对数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面进行评估，发现可能存在的数据安全问题和风险隐患。具体实施时可按照以下步骤开展：
a） 如果被评估方已开展过相关的评估工作，应先对已开展的评估工作结论进行分析；
b） 数据处理者均应针对数据处理活动、数据安全管理与数据安全技术三方面内容进行风险评估；
c） 梳理各评估项的评估结果和发现的风险问题，输出数据安全风险评估记录。

5.3.2 已开展评估工作结论分析

被评估方应当按照国家法律法规、强制性国家标准等文件要求，通过有关评估。在开展风险评估时，应记录被评估方应开展的评估工作及实际开展情况，主要包括：
a） 数据处理活动涉及应开展评估工作名称、要求来源等基本情况；
b） 已开展评估工作有效性（指是否由有资质机构，按照正常程序开展）；
c） 评估内容和结果，及评估工作开展情况；

已开展评估工作情况应由被评估方提供证明材料，评估人员通过访谈、检查、测试等方式验证证明材料真实性、有效性。

若评估对象未实施或通过国家法律法规、强制性国家标准等文件要求的评估工作，如网络安全等级保护测评、云计算服务安全评估、互联网信息服务算法推荐安全评估、数据出境安全评估等，则判定存在未按要求开展评估工作的安全风险。

5.4 安全分析

根据数据安全风险识别评估的评估结果，对评估对象当前数据安全现状、所面临的数据安全问题，按严重程度及主要安全风险情况等进行分析，安全风险等级划分标准见 9.1，并提出相应改进建议。数据安全评估牵头部门就以上评估结果、安全分析及安全建议等情况组织本机构内部审核和确认工作，并会同评估团队各参与方形成最终安全分析结论。

5.5 评估总结

5.5.1 编制评估报告

对评估结果进行分析总结，编制数据安全风险评估报告(报告模板参见附录 C.1)。评估报告的内容应包括但不限于以下内容：

a) 评估报送单位真实性承诺；
b) 单位评估工作组织情况、评估时间安排情况、参与人员情况；
c) 评估概述，包括评估目的及依据，评估对象和范围，评估结论概要；
d) 被评估方基本信息，业务、信息系统情况；
e) 已开展安全评估结果分析；
f) 数据处理活动安全风险识别。包括数据收集、存储、传输、使用和加工、提供、公开、删除等方面安全风险识别情况；
g) 数据安全管理风险识别，包括数据安全制度流程、组织管理、分类分级、人员安全管理、数据合作方管理、数据安全应急、数据安全投诉举报等方面风险识别情况；
h) 数据安全技术风险识别，包括身份鉴别与访问控制、数据安全监控与审计、数据脱敏、数据防泄漏、数据接口安全等技术安全风险识别情况，及相关技术手段完备性、有效性；
i) 安全分析，基于数据资产及处理活动，结合评估情况，对评估对象当前数据安全现状、所面临的数据安全问题，按严重程度及主要安全风险情况等进行分析，说明安全问题数目，填写‘核能领域数据安全问题清单”(清单模版参考附件 B.3)；
j) 风险处置情况，依据不同评估方式风险处置要求，说明风险处置情况；
k) 数据安全风险评估过程的关键记录和证据，应在附录中列出。若不方便在附录中完整列出，应在附录中列出证据关键信息和序号，在提交评估报告时作为附件一并提交。涉及重要数据的，应当详细列出处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

5.5.2 风险处置建议

评估人员结合实际情况，对发现的数据安全风险提出处置建议，酌情指导数据处理者整改。数据处理者按照组织的风险接受规则，制定相应的数据安全风险处置方案。常见数据安全风险处置措施包括不限于以下选项：

a) 停止收集某些类型的数据；
b) 预处理阶段对某些类型数据进行销毁；
c) 缩小处理范围；
d) 缩短存储期限；
e) 采取额外的技术措施；

f) 加强对应数据处理活动岗位人员培训；。
g) 匿名化、去标识化；
h) 完善管理制度；
i) 采用其他数据处理技术；
j) 补充签署协议（针对数据转移）；
k) 修订隐私条款。

5.5.3 残余风险分析

评估人员根据数据处理者决定的风险处置措施，结合风险识别和评估方法，预判措施有效性和残余风险，形成记录。

5.5.4 风险评估后评价

风险评估后评价是在被评估方完成残余风险处置后，由评估方对风险处置结果的跟踪、评价、总结经验，并反馈到数据安全风险评估相关方、促进评估方和被评估方数据安全风险评估活动效果持续提升、结束本次数据安全风险评估活动的闭环管理机制。

6 数据处理活动风险评估

依据核能领域数据分类分级规范与方法，梳理生产与管理业务数据流，并结合数据资产清单及数据分级情况，对业务必须最小数据集、生命周期各环节的数据处理活动安全合规情况进行分析和判断，对数据生命周期各环节数据安全保护措施的落地情况及其有效性进行验证。

数据处理活动风险评估内容见表 1。

表1 数据处理活动风险评估内容

序号	风险识别类别	风险识别说明	重点评估内容	结果判定
1.	数据收集安全	数据收集安全风险识别，主要从数据收集合法正当性、间接收集数据安全、自动收集数据安全、数据质量管理等方面进行评估，发现可能存在的数据收集安全风险和违法违规问题，掌握数据安全防护措施部署情况。	1. 是否存在窃取或者以其他非法方式收集数据的情况。 2. 数据收集活动是否得到合法授权。 3. 是否在法律、行政法规规定的目的和范围内收集数据。 4. 是否通过合同协议等方式，约定从外部机构收集的数据范围、收集方式、使用目的、授权同意和安全措施等内容。 5. 是否对外部数据源和外部收集数据进行鉴别和记录。 6. 是否存在从非法、假冒的外部数据源收集伪造、不真实数据风险。 7. 是否对外部数据源和外部收集数据的合法性、安全性和授权同意情况进行审核。 8. 是否制定数据质量管理制度，明确数据质量管理要求。 9. 是否明确了关于数据清洗、转换和加载等行为的安全要求。 10. 是否建立数据质量监控措施，对异常数据及时告警或更正。 11. 是否能够对收集数据真实性、准确性、安全性进行校验。 12. 使用系统批量采集数据时，是否采用摘要、消息认证码、数字签名等密码技术确保采	结果评价： 符合:满足左列第 1 至 14 项。 基本符合：满足左列第 1 至 14 项中的至少 12 项； 不符合:不满足左列超过 2 项。

			集过程数据的完整性。 13. 是否进行日志记录，并采取技术措施确保数据来源的可追溯性。 14. 采集重要核心数据时，是否结合口令密码、设备指纹、设备物理位置、网络接入方式、设备风险情况等多种因素对数据采集设备或系统的真实性进行增强验证。	
2.	数据存储安全	数据存储安全风险识别，主要从逻辑存储安全、存储介质安全等方面进行评估，发现可能存在的数据存储安全风险和违法违规问题，掌握数据安全防护措施部署情况。	1. 是否根据相应的数据类别和级别采取相应的存储方式和安全措施，如加密存储、去标识化存储等。 2. 是否对数据处理活动涉及到的系统进行安全防护，能够具备网络攻击等事件的防护能力。 3. 是否对数据存储系统配置扫描工具，定期对主要数据存储系统的安全配置进行扫描，以保证其符合安全基线要求。 4. 是否对数据存储系统进行访问权限管理，根据数据的类别和级别以及访问人员应用的角色进行权限的分配和管理。 5. 是否对存储介质的访问和使用行为进行记录和审计。 6. 是否对存储介质的性能进行监控，包括存储介质的使用历史、性能指标、或损坏情况，对超过安全阈值的存储介质进行预警。 7. 保存数据的信息系统，其网络安全建设及监督管理是否满足网络安全等级保护相应要求。 8. 是否对数据存储区域进行规划，并对不同区域之间的数据流动进行安全管控。 9. 是否对生产数据采取实时备份与异步备份、增量备份与完全备份的方式，提供本地数据备份与恢复功能。 10. 是否将我国境内产生的核能领域数据存储在我国境内（国家及行业主管部门另有规定的除外）。	结果评价： 符合:满足左列第 1 至 10 项。 基本符合：满足左列第 10 项，以及第 1 至 9 项中的至少 7 项。 不符合:不满足左列第 1 至 9 中的多项，或不满足左列第 10 项。
3.	数据传输安全	数据传输安全风险识别，主要从数据传输过程中通信双方身份识别、数据传输双方的抗抵赖性、数据的保密性、完整性及可用性保护、数据传输安全策略等方面进行评估，发现可能存在的数据传输安全风险和违法违规问题，掌握数据安全防护措施部署情况。	1. 是否在数据通信两端采取身份鉴别机制，确保数据传输到预期目标。 2. 数据传输已使用安全的密码算法，无 MD5、DES-CBC、SHA1 等不安全的算法不安全算法应用 3. 是否具备数据传输双方抗抵赖性、数据完整性校验措施 4. 是否根据国家相关法律法规中关于数据传输的相关要求设计相应的数据传输策略，保证数据传输的合理性。 5. 是否依据数据分类分级结果制定不同级别数据的传输安全策略。 6. 是否建立对传输加密算法配置、变更、管理等操作过程的审核和监管机制。 7. 是否具备数据传输安全策略有效性审计措施，当发生策略失效的情况时，能够及时向管理员提供告警或提示。 8. 是否对重要数据的传输行为进行记录和审计。 9. 是否对数据传输、接收行为的记录和审计情况进行定期检查。	结果评价： 符合:满足左列第 1 至 6 项。 基本符合：满足左列的 1 至 3 项 不符合:不满足左列第 1 至 6 项中的多项或不满足 1、2 项。
4.	数据使用和	数据使用和加工安全	1. 是否对待加工数据的来源可靠性、合规性	结果评价：

	加工安全	风险识别，主要从数据来源合法性、数据正当使用、数据导入导出安全、数据处理环境安全、数据加工安全及数据加工过程监督等方面进行评估，发现可能存在的数据使用和加工安全风险和违法违规问题，掌握数据安全防护措施部署情况	以及待加工数据的范围和等级进行确认，保证数据的来源可靠、合规、数据的范围及等级在本次处理的范围内 2. 是否在数据使用和加工过程中对敏感数据进行脱敏处理。 3. 是否对数据导入导出的终端设备、用户或服务组件执行有效的访问控制，以确保其身份的真实性和合法性，并对相关行为导入导出行为进行定期审计。 4. 是否建立数据使用和加工的安全管理制度，不限于数据使用正当性、数据资源申请、数据导出、数据分析需求等制度流程。 5. 是否建立不同级别的数据权限申请审批流程，确保数据正当使用。 6. 是否记录并保存数据使用过程中对重要数据的操作行为。 7. 是否对数据加工过程进行必要的监督和检查，确保加工过程的数据安全性	符合:满足左列第 1 至 7 项。 基本符合：满足左列的 1 至 3 项 不符合:不满足左列第 1 至 7 项中的多项或不满足 1、2 项。
5.	数据提供安全	数据提供安全风险识别，主要从数据提供合法正当必要、数据提供安全管理、数据提供安全技术、数据接收方安全等方面进行评估，发现可能存在的数据提供安全风险和违法违规问题，掌握数据安全防护措施部署情况	1. 数据提供过程中，不存在未采取保护措施或保护措施不足，造成数据的破坏、泄露或篡改的情况。 2. 数据提供过程中，不存在未根据国家或行业有关要求进行分类分级管理的情况。 3. 数据提供过程中，不存在未按要求进行审批的情况。 4. 数据提供方和接收方，在提供前已签署数据提供协议，明确相关方安全责任等情况（对于有关监管部门照行业监管要求统一执行）。 5. 在数据提供前，对接收方的数据安全能力进行调查评估。 6. 数据提供协议中明确提供的范围、使用方式、时限、用途以及相应的安全保护措施、违约责任。 7. 针对数据提供相关安全事件制定应急响应预案。 8. 不存在未经授权将数据提供给组织外或非授权场景业务的情况。 9. 不存在提供超时、超量、超数据类型向数据接收方提供合同约定外数据的情况。 10. 实施数据提供行为记录、抗抵赖等措施。 11. 如存在数据公开需求，则应建立数据公开的相关技术工具（如：数据发布系统），能够对公开数据登记、用户注册等进行验证。	结果评价： 完全符合:满足左列第 1 至 11 项。 基本符合：至少满足左列第 1、2、3、4、6、8、等 6 项 不符合:不满足左列 1、2、3、4、6、8、9 等 6 项中的 1 项或者多项。
6.	数据公开安全	数据公开安全风险识别，主要从数据公开安全管理、敏感信息公开等方面进行评估，发现可能存在的数据公开安全风险和违法违规问题，掌握数据安全防护措施部署情况	1. 对核行业监管部门明确规定需要保密的内容不得进行公开。 2. 制定数据公开管理制度和操作规范，建立数据公开管理措施和机制，降低公开数据被篡改和破坏风险。 3. 制定数据公开目录。 4. 在数据公开前，评估数据公开的影响，尤其对国家安全、公共利益产生的影响，涉及个人信息的，评估对个人信息保护产生的影响。 5. 对数据公开过程进行日志记录。 6. 公开后，定期对公开数据所面临的安全风险进行评估，涉及个人信息的，是否对个	结果评价： 完全符合:满足左列第 1 至 8 项。 基本符合：至少满足左列第 1、2、3、4、5、等 5 项 不符合:不满足左列 1、2、3、4、5、等 5 项 中的 1 项或者多项。