ICS 35030
CCS L80

团　　体　　标　　准

T/××× ××××—××××

能源企业数据安全风险评估方法

Data security risk assessment method for energy enterprises

××××－××－××发布　　××××－××－××实施

中国能源研究会　发布

目　次

目　次 I
前　言 III
引　言 IV
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 2
5 数据安全风险评估概述 2
5.1 工作要求 2
5.2 评估思路 3
5.3 评估内容 3
5.4 评估实施流程 3
5.5 评估手段 4
5.6 评估适用情形 5
6 数据安全风险评估准备 5
6.1 确定评估目标 5
6.2 确定评估范围 5
6.3 组建评估团队 5
6.4 开展前期准备 6
6.5 制定评估方案 6
7 数据安全风险评估调研 7
7.1 企业基本情况调研 7
7.2 信息系统调研 7
7.3 数据资产调研 7
7.4 数据处理活动调研 8
7.5 安全防护措施识别 8
8 数据安全风险识别 8
8.1 数据安全管理 8
8.2 数据安全技术 13
8.3 数据处理活动 17
8.4 个人信息保护 20
8.5 数据出境安全 21
9 数据安全风险分析与评估 21
9.1 梳理问题清单 21
9.2 数据安全风险分析 21
9.3 数据安全风险评估 24

9.4 数据安全风险清单 25
10 数据安全风险评估总结 25
10.1 编制评估报告 25
10.2 风险处置建议 25
10.3 残余风险分析 26
附 录 A （资料性） 能源大数据数据分类和分级结果示例 27
附 录 B （规范性） 典型数据安全风险类别 33
附 录 C （规范性） 数据安全风险量化分析与评估方法 35
C.1 数据安全风险危害程度量化分析方法 35
C.2 数据安全风险发生可能性量化分析方法 35
C.3 数据安全风险量化评估方法 35
附 录 D （资料性） 能源企业数据安全风险评估调研表示例 36
D.1 系统基本情况调研表 36
D.2 系统网络拓扑图 37
D.3 系统备份恢复信息调研表 37
D.4 数据安全设备情况调研表 37
D.5 数据安全管理文档调研表 37
D.6 评估工具环境调研表 38
D.7 系统相关联系人 39
附 录 E （资料性） 能源企业数据安全风险评估报告示例 40
参 考 文 献 43

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XX提出。

本文件由XX协会归口。

本文件起草单位：广东电网有限责任公司、广东电网有限责任公司信息中心、南方电网科学研究院有限责任公司、南方电网超高压输电公司、云南电网有限责任公司信息中心、中国能源建设集团广东省电力设计研究院、广东电网有限责任公司河源供电局、广东电网有限责任公司湛江供电局、上海观安信息技术股份有限公司和南瑞集团有限公司。

本文件主要起草人：。

引　言

随着能源企业数字化转型的加快，能源企业的基础业务、核心流程以及行业间的互动日益依赖于信息化平台，在此过程中生成的数据，正逐渐转化为数字资产，在能源企业信息系统内以多种形式流动和存储。与此同时，云计算、大数据、物联网和人工智能等新技术的深入应用，促进了能源企业数据从传统信息化资产向关键生产要素的转变，其价值和重要性与日俱增，然而数据泄露、滥用和篡改等安全威胁也愈发严重，其影响范畴可能从单个企业蔓延至整个行业，甚至对国家安全、社会秩序和公共利益造成冲击。

面对这一数据安全挑战，能源企业如何在保障基本业务安全需求的同时，加强数据保护，防范安全风险，确保数据价值的最大化，成为了一个迫切需要解决的问题。目前能源企业数据安全风险管控能力尚处于参差不齐的状态，开展数据安全风险评估，有助于及时全面掌握企业数据安全风险管控水平，明确企业所面临的数据安全威胁和风险，为制定防范措施及应对安全事件提供科学依据和指引，可有效防控数据安全事件风险和危害，为企业数据应用和流动提供有力保障。

为能源企业合理的制定和执行数据安全风险评估策略，提升数据安全保护和应用能力，编制本文件。

本文件凡涉及密码技术的相关内容，按国家密码管理部门及行业主管部门有关规定实施；凡涉及采用密码技术解决保密性、完整性、真实性、不可否认性需求的，遵循相关国家标准和行业标准。

能源企业数据安全风险评估方法

1 范围

本文件给出了面向能源企业数据安全风险评估的评估思路、评估内容、评估实施流程、评估手段等，明确了能源企业数据安全风险评估各阶段的实施要点和工作方法。

本文件适用于能源领域相关企业开展数据安全风险评估，并为第三方安全评估机构及相关单位开展能源领域数据安全检查与风险评估工作提供参考。

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 20984—2022 信息安全技术 信息安全风险评估方法

GB/T 25069—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 43697-2024 数据安全技术 数据分类分级规则

TC260-PG-20231A 网络安全标准实践指南——网络数据安全风险评估实施指引

3 术语和定义

GB/T 25069—2022 信息安全技术 术语界定的以及下列术语和定义适用于本文件。

3.1

能源企业 energy enterprises

从事电力、石油石化、煤炭、燃气、新能源、核能等主营业务的企业，或支撑以上主营业务开展的咨询、相关设备制造等服务的企业。

3.2

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。

3.3

数据处理活动 data processing activities

数据收集、存储、使用、加工、传输、共享、销毁等活动。

3.4

数据安全风险评估 data security risk assessment

对数据和数据处理活动安全进行信息调研、风险识别、风险分析和风险评价的整个过程。

3.5

业务 business

组织为实现某项发展规划而开展的运营活动。

注：该活动具有明确的目标，并延续一段时间。

[来源：GB/T 20984-2022,3.1.4]

3.6

风险源 risk source

可能导致危害数据的保密性、完整性、可用性和数据处理合理性等事件的威胁、脆弱性、问题、隐患等，也称“风险隐患”。

注：风险隐患，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隐患，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隐患。

3.7

安全威胁 security Threat

可能对系统或组织的数据处理活动造成危害的因素，其形式可以是对数据直接或间接的攻击，在数据机密性、完整性和可用性等方面造成损害，也可能是偶发的或蓄意的事件。

3.8

自评估 self-assessment

由数据处理者自身发起，组成机构内部评估小组或委托第三方评估机构，依据有关政策法规与标准，对评估对象的数据安全风险进行评估的活动。

[来源：GB/T 20984-2022,3.1.8,有修改]

3.9

检查评估 inspection and assessment

由数据处理者的上级主管部门、业务主管部门或国家有关主管（监管）部门发起的，依据有关政策法规与标准，对评估对象的数据安全风险进行的评估活动。

[来源：GB/T 20984-2022,3.1.9,有修改]

4 缩略语

下列缩略语适用于本文件。

App：移动互联网应用程序（Mobile Internet Application）

SDK：软件开发工具包（Software Development Kit）

5 数据安全风险评估概述

5.1 工作要求

能源企业在开展数据安全风险评估过程中，应严格遵守国家与能源行业相关法规政策，落实数据安全相关工作要求，具体如下：

a）宜委托具有信息安全服务资质（信息安全风险评估、数据安全类、信息系统审计类）的第三方安全服务机构开展评估工作；

b）企业不得委托在近3年内被行业部门通报有不良行为或被相关部门通报整改的第三方安全服务机构开展评估工作；

c）结合网络安全三同步要求，能源企业宜将数据安全风险评估贯穿于信息系统规划设计、建设验收和运行维护各阶段中，在规划设计阶段，通过风险评估以确定评估对象的安全目标；在建设验收阶段，通过风险评估以确定评估对象的安全目标达成与否；在运行维护阶段，要持续的实施风险评估以识别评估对象面临的不断变化的风险和脆弱性，从而确定安全措施的有效性，确保安全目标得以实现；

注：能源企业评估对象规划设计、建设验收和运行维护各阶段的数据安全风险评估侧重点相关内容，参照GB/T 20984—2022《信息安全风险评估方法》执行。

d）成立数据安全风险评估项目实施团队，并实行项目组长负责制，达到项目过程的可控；

e）评估人员所使用的评估工具应事先告知被评估方，并在评估实施前获得被评估方许可；

f）各相关方应严格遵守保密纪律，在项目实施过程中，做好评估材料的保密工作；

g）在国家数据安全法律法规出现更改、国家及能源行业相关标准制度发生变更、上级部委相关要求发生变化、能源企业相关标准制度发生变更、系统业务架构发生重大变化、数据资产发生重大变化、系统发生重大数据安全事件等情况时，应重新组织开展相应信息系统的局部或整体数据安全风险评估工作。

5.2 评估思路

坚持预防为主、主动发现、积极防范、对能源企业数据安全保护和处理活动进行风险评估，旨在掌握数据安全总体状况，发现数据安全隐患，提出数据安全管理和技术防护措施建议，提升能源企业数据安全防攻击、防破坏、防窃取、防泄漏、防滥用能力。能源企业数据安全风险评估主要围绕企业数据安全管理、数据安全技术和数据处理活动，聚焦可能影响数据的保密性、完整性、可用性和数据处理合理性的安全风险。首先通过信息调研识别企业基本情况、业务和信息系统、数据资产、数据处理活动、安全措施等相关要素，然后从数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面识别风险隐患，最后梳理问题清单，分析数据安全风险并给出整改建议。

5.3 评估内容

能源企业数据安全风险评估，在信息调研基础上，围绕数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面开展评估。

a）数据安全管理包括企业相关制度流程、组织机构、分类分级、人员管理、合作外包管理、安全威胁和应急管理、开发运维、云数据安全等；

b）数据处理活动包括企业相关数据收集、数据存储、数据传输、数据使用和加工、数据共享、数据销毁等；

c）数据安全技术包括企业相关网络安全防护、身份鉴别与访问控制、监测预警、数据脱敏、数据防泄漏、接口安全、备份恢复、安全审计等；

d）个人信息保护包括基本原则、告知同意、保护义务、主体权利、投诉举报、个人信息处理、敏感个人信息保护等。

5.4 评估实施流程

能源企业数据安全风险评估实施流程主要包括自评估实施流程和检查评估实施流程。

a）能源企业开展数据安全风险自评估，具体实施步骤如图1所示：

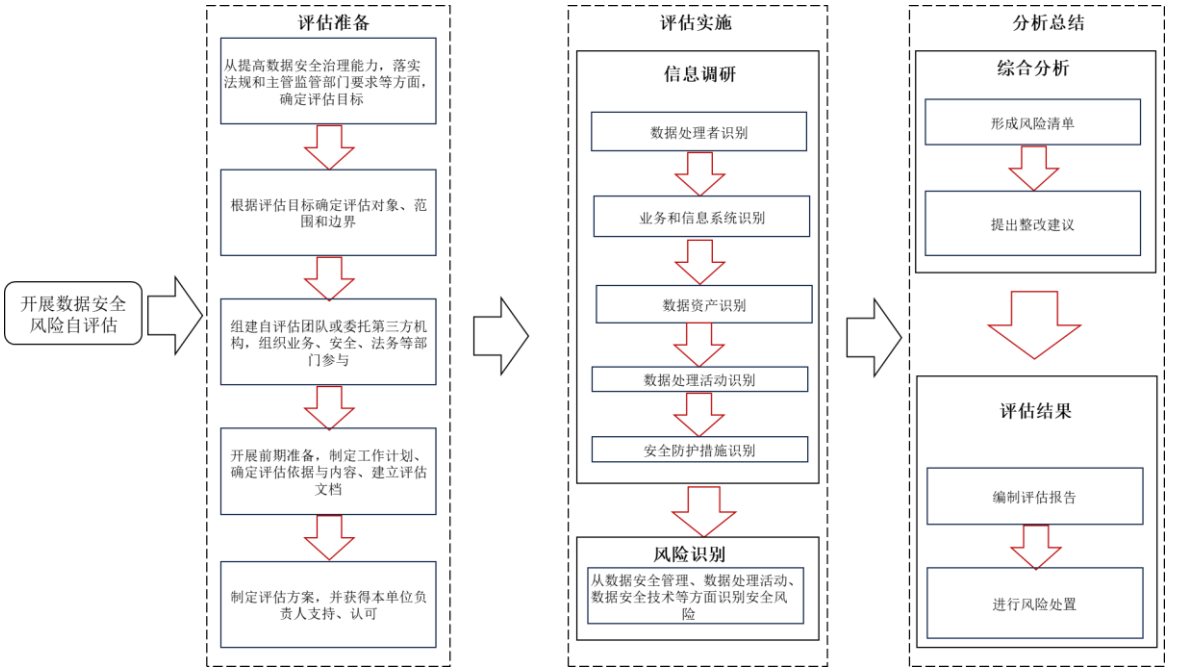

图1 能源企业数据安全自评估实施流程

b）针对能源企业数据安全情况，相关部门开展数据安全风险检查评估，具体实施步骤如图2所示：

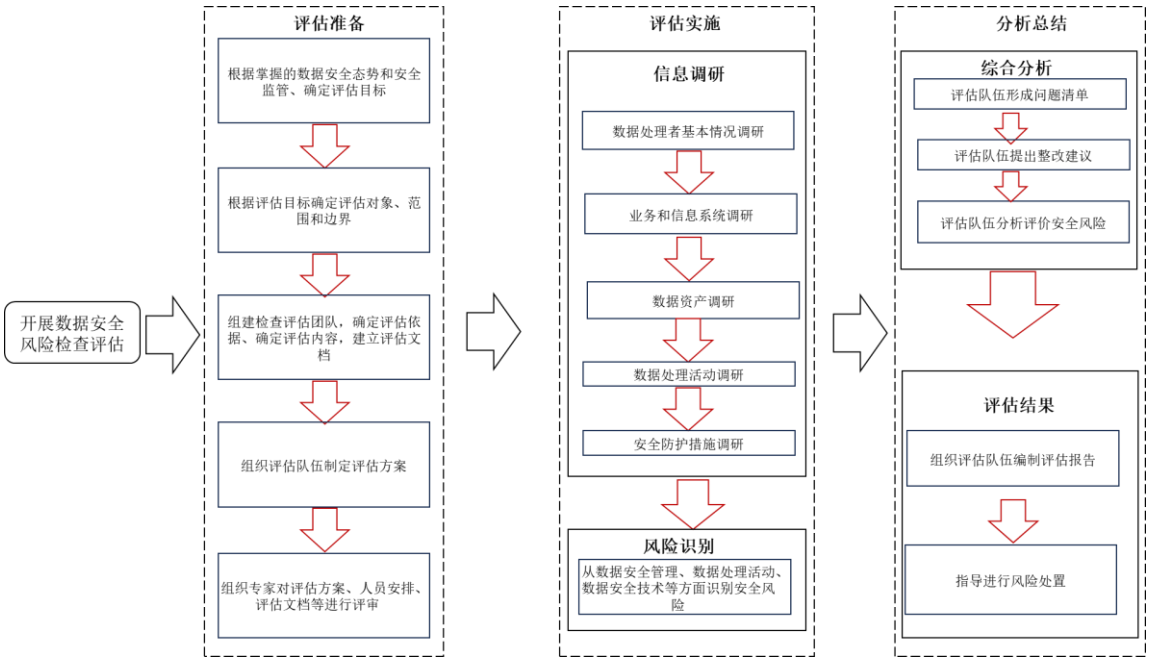

图2 能源企业数据安全检查评估实施流程

5.5 评估手段

开展能源企业数据安全风险评估时，综合采取下列评估手段进行评估：

a）人员访谈：对相关人员进行访谈，核查制度规章、防护措施、安全责任落实情况；

b）文档查验：查验安全管理制度、风险评估报告、等保测评报告等有关材料及制度落实情况的证明材料；

c）安全核查：核查网络环境、数据库和大数据平台等相关系统和设备安全策略、配置、防护措施情况；

d）技术测试：应用技术工具、渗透测试等手段查看数据资产情况、检测防护措施有效性。

5.6 评估适用情形

结合行业主管部门及关键信息基础设施安全保护要求，建议能源企业重要数据和核心数据每年至少进行一次数据安全风险评估（注：可参考附录A能源大数据数据分类分级结果示例，能源企业自行梳理重要数据和核心数据），适用于以下情形之一的，可结合实际情况开展数据安全风险评估：

a）在重要数据共享、交易、委托处理或向境外提供前，宜开展数据安全风险评估；

b）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）重要数据和个人信息处理者合并、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）数据处理者利用生物特征进行个人身份认证；

4）基于不同业务目的的数据汇聚融合；

5）委托处理、向他人提供未成年人、老年人数据；

6）新技术应用可能带来数据安全风险的；

7）法律法规或有关部门规定要评估的情形。

c）其他可能直接危害国家安全、公共利益或者大量个人、组织合法权益的数据处理活动；

d）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；

e）重要系统上线前，可根据实际需要开展数据安全风险评估；

f）当被评估对象的政策环境、外部威胁环境、业务目标、安全目标等发生重大变化时，应重新开展风险评估。

6 数据安全风险评估准备

6.1 确定评估目标

为落实《数据安全法》《个人信息保护法》等法律法规要求及安全监管需要，对能源企业数据安全管理、数据处理活动、数据安全技术和个人信息保护情况等进行安全风险评估，发现存在的安全问题和风险隐患，健全安全制度、改进安全措施、堵塞安全漏洞，进一步提升数据安全和个人信息保护能力。

企业数据安全风险评估的目标包括但不限于：

a）摸清企业数据种类、规模、分布等基本情况；

b）摸清企业数据处理活动情况；

c）发现可能影响国家安全、公共利益或者个人、组织合法权益的数据安全问题和风险；

d）发现共享、交易、委托处理、向境外提供重要数据等处理活动的数据安全问题和风险；

e）促进完善数据安全保护措施，提升数据安全保护能力。

6.2 确定评估范围

根据工作需要和评估目标，以能源企业信息系统为评估对象，明确评估范围，包括信息系统相关数据安全管理制度、数据安全建设，数据全生命周期各阶段的技术保障措施等。

6.3 组建评估团队

应组建数据安全风险评估团队，由评估机构的评估人员以及企业信息系统相关责任人组成。评估人员需具备数据安全风险评估相关能力，负责整体评估工作的开展；企业信息系统相关责任人负责配合现场评估工作的访谈，配置核查等，主要有业务负责人、系统负责人、应用系统管理员、数据库管理员、网络管理员等。评估机构在评估中获取的信息只能用于评估目的，未经授权不应泄露、出售或者非法向他人提供。

6.4 开展前期准备

6.4.1 制定工作计划

评估工作计划内容一般包括工作目的、工作要求、工作内容、工作流程、调研安排、评估总体进度安排等，开展检查评估时，主管监管部门指导评估团队按照工作要求制定评估工作计划。

6.4.2 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：

a）《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《电力行业网络安全管理办法》等法律，有关行政法规、司法解释；

b）网信部门及主（监）管部门相关数据安全规章、规范性文件；

c）地方数据安全政策规定和监管要求；

d）数据安全相关国家标准、行业标准等；

e）开展自评估时，企业已有数据安全制度规范可作为评估依据之一。

6.4.3 确定评估内容

结合评估目标、范围、依据，针对企业的实际情况，确定企业每个评估对象适用的评估内容：

a）应针对数据处理活动、数据安全管理、数据安全技术等方面进行风险评估，涉及处理个人信息的，对个人信息保护开展风险评估；

b）开展评估工作过程中，可根据任务要求、评估重点、监管需要、评估依据等，进一步完善评估内容；

c）建立评估文档。针对评估目标、范围、依据和内容，准备风险评估调研表、技术测试工具等；在评估工作开展过程中，应对评估工作相关文件进行统一编号，并规范管理。

6.5 制定评估方案

组织评估团队编制数据安全风险评估工作方案，方案内容包括但不限于：

a）评估概述：包括评估目标、评估依据等内容；

b）评估范围：包括评估对象选择方法、评估对象描述、评估范围等；

c）评估内容和方法：包括评估内容、评估准则、评估方法等内容；

d）评估人员：包括评估团队的组织结构、负责人、成员、职责分工等内容；

e）实施计划：包括时间进度安排、人员安排等内容；

f）工作要求：包括评估工作要求，安全保障条件等内容，工作要求如严格依照评估内容及标准规范，规范评估行为，按照尽量不影响企业正常工作的原则，制定评估工作应急保障和风险规避措施，明确告知企业评估可能产生的风险，严守工作纪律和保密要求等；

g）测试方案：开展技术测试前应明确测试方案，包括采用的技术工具、测试内容、测试环境、应急措施等，测试方应向企业明示测试可能涉及的安全风险，双方就测试方案达成共识，检查评估时应提前向有关部门报备。

评估团队可邀请能源领域相关数据安全、网络安全专家对评估方案进行评议，重点审核方案内容、风险管控、保护措施、可操作性、技术可行性等，进一步修改完善评估方案后，组织实施风险评估工作。

7 数据安全风险评估调研

7.1 企业基本情况调研

能源企业基本情况包括但不限于：

a) 单位名称、组织机构代码、办公地址、法定代表人信息、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) 业务运营地区，开展数据处理活动所在国家和地区等；

c) 主要业务范围、业务规模等；

d) 是否境外上市或计划赴境外上市及境外资本参与情况，或以协议控制（VIE）架构等方式实质性境外上市。

7.2 信息系统调研

信息系统情况包括但不限于：

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、覆盖地域、相关部门等基本信息；

c) 业务涉及个人信息、重要数据或核心数据处理情况；

d) 业务为政务部门或境外用户提供服务情况；

e) 信息系统、App和小程序情况，包括系统功能、网络安全等级保护备案和测评结论、入口地址、系统连接关系、数据接口、App及小程序名称和版本等；

f) 数据中心和使用云平台情况；

g) 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。

7.3 数据资产调研

梳理结构化数据资产（如数据库表等）和非结构化数据资产（如图表文件等），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。调研内容包括但不限于：

a) 数据资产情况，包括数据资产类型、数据范围、数据规模、数据形态、数据存储分布、元数据等；

b) 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(数据分类分级情况调研，可参考附录能源大数据数据分类分级结果示例)；

c) 个人信息情况，包括个人信息种类、规模、敏感程度、数据来源、业务流转及与信息系统的对应关系等；

d) 重要数据情况，包括重要数据种类、规模、行业领域、敏感程度、数据来源、业务流转及与信息系统的对应关系等；

e) 核心数据情况，包括核心数据种类、规模、行业领域、敏感程度、数据来源、业务流转及与信息系统的对应关系等；

f）其他一般数据情况。

7.4 数据处理活动调研

针对评估对象和范围，梳理数据处理活动清单，验证或绘制数据流图。数据流图应描述数据流转各环节经过的相关方、信息系统，以及每个流动环节涉及的数据类型等。调研内容包括但不限于：

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、合同协议、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，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；

d）数据使用和加工情况，如数据使用目的、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，应用算法推荐技术提供互联网信息服务的情况，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。

e）数据提供情况，如数据提供（数据共享、数据交易，因合并、分立、解散、被宣告破产等原因需要转移数据等）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，如数据公开的目的、方式、对象范围、受众数量、行业、组织、地域等。

g）数据删除情况，如数据删除情形、删除方式、数据归档、介质销毁等。

7.5 安全防护措施识别

调研能源企业已有安全措施情况，包括但不限于：

a）已开展的等级保护测评、商用密码应用安全性评估、安全检测、风险评估、安全认证、合规审计情况，及发现问题的整改情况；

b）数据安全管理组织、人员及制度情况；

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）身份鉴别与访问控制情况；

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、系统及用户的账号口令管理情况；

h）加密、脱敏、去标识化等安全技术应用情况；

i）3 年内发生的网络和数据安全事件、攻击威胁情况，如安全事件名称、数据类型和数量、发生原因、级别、处置措施、整改措施等，重大事件需提供事件调查评估报告；近 3 年发生的数据安全事件处置、记录、整改和上报情况；实际环境中通过检测工具、监测系统、日志审计等发现的威胁；近期公开发布的社会或特定行业威胁事件、威胁预警；其他可能面临的数据泄露、窃取、篡改、破坏/损毁、丢失、滥用、非法获取、非法利用、非法提供等安全威胁。

8 数据安全风险识别

8.1 数据安全管理

8.1.1 数据安全管理制度

a) 数据安全制度体系，主要包括：

1) 数据安全总体策略、方针、目标和原则制定情况；

2) 数据安全管理工作规划或工作方案制定情况；

3) 数据分类分级、数据安全评估、数据访问权限管理、数据全生命周期管理、数据安全应急响应、数据合作方管理、数据脱敏、数据加密、数据安全审计、数据资产管理、大数据平台安全等制度或要求建设情况；

4) 关键岗位的数据安全管理操作规程建设情况；

5) 制度内容与国家和行业数据安全法律法规和监管要求的符合情况；

6) 个人信息保护制度制定情况。

b) 数据安全管理制度落实，主要包括：

1) 网络安全责任制、数据安全责任制落实情况，网络安全和数据安全事件责任查处情况；

2) 数据安全制度的制定、评审、发布流程建设情况；

3) 数据安全制度的定期审核和更新情况；

4) 制度发布范围是否覆盖全面，发布方式是否正规、有效；

5) 数据安全制度落实情况，是否具备操作规程、记录表单等制度落实证明材料；

6) 制度落实监督检查机制；

7) 针对重要数据处理者，还应评估对数据处理活动定期开展数据安全风险评估的情况；向有关部门报送评估报告情况，风险评估报告至少应包含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；

8) 应检查是否结合自身数据安全要求，制定数据安全风险评估方法，明确风险评估目的、范围、依据、评估流程、评估频率、实施评估、综合评估分析等内容；

9) 在出现法律法规重大更改或增删、业务活动发生重大变化、数据资产发生重大变化、发生重大数据安全事件、数据安全管理方针发生变化等重大情况变化时，应检查是否进行局部或全面数据安全风险评估，形成数据安全风险评估报告。

8.1.2 安全组织机构

a) 数据安全组织架构，主要包括：

1) 数据安全管理机构和职能设置情况；

2) 数据安全负责人和职能设置情况；

3) 数据安全责任人履行职责包括但不限于： 组织制定数据保护计划并落实、组织开展数据安全评估，整改安全隐患，组织按要求向有关部门或网信部门报告数据安全保护和事件处置情况，组织受理并处理用户投诉和举报事项等；

4) 单位高层人员参与数据安全决策情况；

5) 对组织内部的数据安全管理执行情况、数据操作行为等进行安全监督的情况；

6) 数据安全人员和资源投入情况与组织数据安全保护需求适应性。

b)数据安全岗位设置，主要包括：

1) 数据库管理员、操作员及安全审计人员、安全运维人员、数据备份管理人员、数据恢复管理人员等；

2) 数据安全关键岗位设置情况，及职责分离、专人专岗等原则落实情况；

3) 业务部门、信息系统建设部门、信息系统运维部门数据安全人员设置情况，数据安全管理要求执行情况；

4) 特权账户所有者、关键数据处理岗位等数据安全关键岗位设立双人双岗情况。

8.1.3 分类分级管理

a) 数据资产管理，主要包括：

1) 数据资产梳理是否全面，是否能够覆盖数据库、大数据存储组件、云上对象存储或网盘等存储工具及办公计算机、U盘、光盘等存储介质中的数据；

2)是否明确数据资产管理流程等相关管控要求，按照数据资产安全管理要求进行管控。

b)数据分类分级制度，主要包括：

1) 数据分类分级保护制度建设情况，是否符合国家、行业和地方的数据分类分级规范要求；

2) 数据分类分级管理情况，及核心数据和重要数据目录建立及维护情况；

3) 是否在相关制度中明确了数据分类管理、分级保护策略，数据分类分级保护措施是否落实在数据访问权限申请、保护措施部署等方面；

4) 数据分类分级变更和审核流程情况；

5) 个人信息分类分级管理情况。

6) 是否明确数据分类标准，依据数据资源属性特征，将数据合理划分类别，形成数据资源分类目录；

7) 是否明确数据安全级别，依据数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用时，对国家安全、社会秩序和公共利益或者个人信息主体、公共管理和服务机构合法权益造成的侵害程度确定安全级别。

c) 数据分类分级保护，主要包括：

1) 是否对处理的个人信息和重要数据进行明确标识；

2) 按照数据级别建设覆盖全流程数据处理活动的安全措施情况；

3) 按照相关重要数据目录或规定，评估重要数据并进行重点保护的情况。

8.1.4 人员安全管理

a) 人员录用，主要包括：

1) 重要岗位员工录用前背景调查情况；

2) 数据处理关键岗位人员录用，对其数据安全意识或专业能力进行考核的情况；

3) 检查数据岗位人员是否具备相关资质证书，持证上岗。

b) 保密协议，主要包括：

1) 员工工作纪律和工作要求中是否明确规定员工禁止的数据安全相关行为；

2) 是否与所有涉及数据服务的人员签订安全责任承诺或保密协议，与数据安全关键岗位人员签订数据安全岗位责任协议；

3) 在重要岗位人员调离或终止劳动合同前，是否明确并告知其继续履行有关信息的保密义务要求，并签订保密承诺书。

c) 转岗离岗，主要包括：

1) 在人员转岗或离岗时，是否及时终止或变更完成相关人员数据操作权限，并明确有关人员后续的数据保护管理权限和保密责任；

2) 对终止劳动合同的人员，是否及时终止并收回其系统权限及数据权限，明确告知其继续履行有关信息的保密义务要求。

d) 数据安全培训，主要包括：

1) 数据安全培训计划制定、更新情况；

2) 开展数据安全意识教育培训，并保留相关记录情况；

3) 是否对数据安全岗位人员每年至少进行1次数据安全专项培训,对关键岗位人员进行定期数据安全技能考核情况。

8.1.5 合作外包管理

a) 合作外包管理，主要包括:

1) 数据合作方安全管理机制建设情况，如对合作方或外包服务机构的选择、评价、管理、监督机制；

2) 是否对数据合作方或外包服务机构的安全能力进行评估；

3) 对外包服务机构、人员履行安全责任义务的监督检查情况；

4) 外包人员现场服务安全管理情况。

b) 合作协议约束，主要包括:

1) 服务合同、承诺及安全保密协议情况，是否通过合同协议等方式对接收、使用本单位数据的合作方的数据使用行为进行约束；

2) 是否在合作协议中明确了数据处理目的、方式、范围，安全保护责任、数据返还或销毁要求、保密约定及违约责任和处罚条款等；

3) 合同、协议中，数据处理者与合作方、外包服务商间的数据安全责任界定情况。

c) 外包人员访问权限,主要包括：

1) 外包人员对数据与系统的访问、修改权限是否限于最小必要范围；

2) 能够在测试环境下或使用测试数据完成的,是否向外包人员开放了生产环境权限或真实数据；

3) 外包人员对敏感数据的访问及操作能否被实时监督或监测；

4) 数据外包服务账号及访问权限管理情况；

5) 外包人员远程访问操作系统或数据的情况。

d) 第三方接入与数据回收，主要包括：

1) 是否对合作方接入的系统、使用的技术工具进行了技术检测，或合作方提供专业第三方机构评估的数据安全报告，避免引入木马、后门等；

2) 为完成技术或服务目的向合作方提供的数据，在合作结束后是否进行了回收，是否要求合作方对数据进行删除；

3) 外包服务到期后，账号注销、数据回收、数据删除销毁等管理情况；

4) 为完成技术或服务目的向合作方提供的系统权限和接口，在合作结束后是否进行了停用或下线；

5)是否明确数据供应商不得私自存储公司敏感数据，并对数据供应商进行定期检查，并留存相关检查记录,合同或协议的另有规定的除外；

6)是否定期排查第三方人员个人终端电脑是否存储公司敏感数据。

8.1.6 安全威胁和应急管理

a) 安全威胁和事件，主要包括：

1) 近3年发生的网络安全或数据安全事件信息及其处置、记录、整改和上报情况，如事件名称、影响对象、发生时间和频次、发生原因、外部威胁、事件级别、处置措施、整改措施等，重大事件需提供事件调查评估报告；

2) 近1年通过安全工具、日志审计、安全测评、合规自查等发现的违规行为及处置情况；

3) 实际环境中通过监测系统、检测工具等发现的攻击威胁及处置情况；

b) 安全应急管理，主要包括：

1) 数据安全事件应急预案制定和修订情况，是否定义数据安全事件类型，明确不同类别级别事件的处置流程和方法；

2) 数据安全应急响应及处置机制建设情况，发生数据安全事件时是否立即采取处置措施，是否按照规定及时告知用户并向有关主管部门报告；

3) 数据安全事件应急演练情况；

4) 数据处理活动安全风险监测情况，发现数据安全缺陷、漏洞等风险时，是否立即采取补救措施；

5) 安全事件对个人、其他组织造成危害的，是否将安全事件和风险情况、危害后果、已经采取的补救措施等通知利害关系人，无法通知的是否采取公告等其他方式告知；

6) 面向社会提供服务的数据处理者是否建立便捷的数据安全相关投诉举报渠道，以及近3年的数据安全投诉举报处置、记录和整改情况，是否存在侵害用户个人信息合法权益的情况；

7) 检查数据安全应急处置后是否有分析事件发生原因，总结应急处置经验，调整数据安全策略，形成事件调查记录和总结报告，避免再次发生类似情况；

8) 检查是否采取技术手段对数据安全事件进行溯源，造成严重事件的应依法追究事件主体责任；

9) 检查是否根据应急预案明确的数据安全事件场景定期开展应急演练，每年至少一次，事件场景包括但不限于数据泄露、丢失、滥用、篡改、毁损、违规使用等；

10) 检查是否针对系统数据备份开展数据恢复演练，确保数据备份的可用性、有效性、完整性。

8.1.7 开发运维管理

a) 开发运维管理，主要包括：

1) 新应用开发审核流程建设情况，进行数据处理需求安全合规审核情况；

2) 开发程序的修改、更新、发布的批准授权和版本控制流程；

3) 工程实施、验收、交付的安全管理情况；

4) 对开发代码、测试数据的安全管理情况；

5) 产品或业务上线前进行安全评估的情况；

6) 开发测试环境和实际运行环境的隔离情况、测试数据和测试结果的控制情况；

7) 开发测试中使用真实个人信息、核心数据、重要数据情况，开发测试前对相关数据进行去标识化、脱敏处理（测试确需信息除外）情况；

8) 对开发和运维人员行为的监督和审计情况；

9) 远程运维的审批、管理和安全防护措施；

10) 第三方SDK或开源软件的运行维护、二次开发等技术资料完备性;

11) 检查敏感数据是否经过数据脱敏，去除与开发测试无关的数据、屏蔽原始数据信息后方可用于开发测试中使用。

8.1.8 云数据安全

a) 被评估对象使用云计算服务时，主要包括：

1) 云服务提供者、第三方厂商、云租户的安全责任划分和落实情况；

2) 上云数据的安全审核和管理情况；

3) 云安全产品服务的使用和配置情况；

4) 对云上操作行为的安全审计情况；

5) 云用户账号和权限管理情况；

6) 私有云远程运维安全管理情况；

7) 云上承载用户个人信息、重要数据、核心数据情况，是否对核心数据、重要数据、敏感个人信息实施增强的安全防护。

b) 被评估对象是云计算服务提供者时：

1) 公有云、社区云等不同类型云平台间边界防护情况；

2) 租户与云平台、数据中心间数据传输安全防护情况；

3) 针对不同服务模式、部署模式、产品和服务，云平台对相关方的数据安全责任界面划定情况及合法合规性；

4) 是否通过合同协议等方式，与租户划清云数据安全责任边界，并履行相应数据安全责任；

5) 发生数据安全风险或事件时，为租户提供事件报告、应急处置等协同保障措施情况；

6) 收集租户数据情况，是否识别重要数据、个人信息，收集方式是否安全合理，是否存在超范围收集；

7) 计算、存储、网络、数据库、安全等产品安全配置情况；

8) 第三方组件安全核查、漏洞修复情况；

9) 云产品漏洞更新和推送情况，是否会及时提供补丁推送、跟进用户漏洞更新等情况；

10) 云平台提供的基础安全防护能力情况；

11) 云产品对用户高风险操作的提示情况；

12) 对云租户的身份管理和访问控制情况；

13) 云平台保障租户数据安全的相关制度和安全措施；

14) 约定服务到期、欠费、提前终止等情形下，云数据删除和个人信息权益保障等情况；

15) 云数据备份和恢复机制是否完善，数据备份策略、备份周期、备份存储、数据恢复策略，恢复验证等是否符合安全需要；

16) 云平台开展数据安全风险评估、云计算服务安全评估等情况；

17) 云平台基础设施部署和运维情况；

18) 云安全管理中心管控情况；

19) 云数据迁移安全保障情况；

8.2 数据安全技术

8.2.1 网络安全防护

a) 网络安全防护，主要包括：

1) 网络拓扑结构、网络区域划分、IP地址分配、网络带宽设置等网络资源管理情况；

2) 网络隔离、边界防护等措施的有效性；

3) 安全策略和配置核查情况；

4) 网络访问控制、安全审计情况；

5) 安全漏洞发现及常见漏洞修复、处置情况；

6) 异常流量、恶意代码和钓鱼邮件发现及处置情况；

7) 外部攻击、内部攻击、新型攻击的发现和处置情况；

8) 未授权连接内网、外网、无线网等情况；

9) 通信链路、网络设备、计算设备等关键设备的冗余情况；

10) 对第三方组件进行安全核查、修复、更新的情况；

11) 服务器、数据库、端口、数据资源在互联网的暴露及管理情况；

12) 处理重要数据、核心数据的信息系统，应按照有关规定满足相应网络安全等级保护要求，属于关键信息基础设施的，还应符合关键信息基础设施安全保护要求。

8.2.2 身份鉴别与访问控制

a) 身份鉴别，主要包括：

1) 建立用户、设备、应用系统的身份鉴别机制情况，身份标识是否具有唯一性；

2) 身份鉴别信息是否具有复杂度要求并定期更换；

3) 是否存在可绕过鉴别机制的访问方式；

4）登录失败时采取结束会话、限制非法登录次数、设置抑制时间和网络登录连接超时自动退出等措施的情况；

5）当远程管理时，是否采取必要措施防止鉴别信息在网络传输中被窃听；

6）处理重要数据的信息系统，采用口令技术、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行鉴别的情况；

7）应检查是否对账号进行操作行为记录；

8）应检查是否对系统之间的数据访问采取身份鉴别、访问控制、安全审计、资源控制等技术措施。

b）访问控制，主要包括：

1）建立与数据类别级别相适应的访问控制机制情况，是否限定用户可访问数据范围；

2）是否在数据访问前设置身份认证等措施，防止数据的非授权访问；

3）数据访问权限与访问者的身份关联情况；

4）数据访问权限申请、审批机制的建设落实情况；

5）是否以满足业务实际需要的最小化权限原则进行授权；

6）是否对数据跨网络区域传输采取安全管控措施，包括但不限于网络及应用层的访问控制策略，控制粒度为端口级。

c）授权管理，主要包括：

1）数据权限授权审批流程建设落实情况，是否明确用户账号分配、开通、使用、变更、注销等安全保障要求，是否对数据权限申请和变更进行审核，是否严格控制管理员权限账号数量；

2）系统管理员、安全管理员、安全审计员等人员角色分离设置和权限管理情况；

3）系统权限分配表更新情况，用户账号实际权限是否满足最少够用、职权分离原则；

4）是否存在与权限申请审批结果不一致的情况；

5）是否存在多余、重复、过期的账户和角色；

6）是否存在共享账户和角色权限冲突的情况；

7）是否存在离职人员账号未及时回收、沉默账号、权限违规变更等安全问题；

8）数据批量复制、下载、导出、修改、删除等数据敏感操作是否采取多人审批授权或操作监督，并进行日志审计。

8.2.3 监测预警

监测预警，主要包括：

a）安全监测预警和信息报告机制的建设落实情况，是否明确对组织内部各类数据访问操作的日志记录要求、安全监控要求；

b）异常行为监测指标建设情况，包括IP地址、账号、数据、使用场景等，对异常行为事件进行识别、发现、跟踪和监控等；

c）对批量传输、下载、导出等敏感数据操作的安全监控和分析的情况，是否实现对数据异常访问和操作进行告警；

d）对数据交换网络流量进行安全监控和分析的情况，是否具备对异常流量和行为进行告警的能力；

e）风险信息的获取、分析、研判、通报、处置工作开展情况；

f）数据安全缺陷、漏洞等风险的监测预警能力建设情况；

g）是否具备常态化数据安全风险监测能力，持续监测数据安全风险，风险类型包括但不限于账号风险、权限风险、异常操作行为、数据出境风险、数据暴露面风险等；

h）是否配备专人负责数据安全风险监测工作，定期出具风险监测报告；

i）是否加强数据安全风险闭环管理，持续提升数据安全风险处置能力；

j）是否定期对数据安全风险监测工作的有效性、全面性进行审核验证。

8.2.4 数据脱敏

数据脱敏，主要包括：

a）数据脱敏规则、脱敏方法和脱敏数据的使用限制情况；

b）需要进行数据脱敏处理的应用场景、处理流程及操作记录情况；

c）静态数据脱敏和动态数据脱敏技术能力建设情况；

d）开发测试、人员信息公示等应用场景的数据脱敏效果验证情况；

e）对匿名化或去标识化处理的个人信息重新识别出个人信息主体的风险分析情况，是否采取相应的保护措施。

8.2.5 数据防泄漏

数据防泄漏，主要包括：

a）数据防泄漏技术手段部署情况，能否对网络、邮件、终端等关键环节进行监控并报告敏感信息的外发行为；

b）市场上售卖组织业务数据的情况，查看是否能通过公开渠道、开源网站查询到组织业务信息，如代码、数据库信息等；

c）数据防泄漏技术措施有效性；

d）检查涉及存储、处理个人敏感信息和重要数据平台系统是否配备数据防泄露能力，优先从网络侧和终端侧等进行部署，逐步扩大能力覆盖范围；

e）是否具备对网络方式（包括但不限于文件上传下载、即时通讯软件传输、邮件传输、FTP文件传输）和物理方式（包括但不限于U盘传输）等多种数据导入导出渠道进行实时监控的能力，及时对异常数据操作行为进行预警拦截，防范数据泄露风险；

f）是否采用应用泄露监控措施，配合数据安全监管中心对各类应用接口及访问过程进行监控，实现数据下载监控、文件泄漏阻断、文件泄漏脱敏、泄漏审计等能力。

8.2.6 数据接口安全

a）对外接口安全，主要包括：

1）面向互联网及合作方数据接口的接口认证鉴权与安全监控能力建设情况，是否能够限制违规接入，是否能对接口调用进行必要的自动监控和处理；

2）API密钥及密钥安全存储措施设置情况，能否避免密钥被恶意搜索或枚举；

3）不同安全等级系统间、不同区域间跨系统、跨区域数据流动的安全控制措施情况。

b）接口安全控制，主要包括：

1）接口安全控制策略设置情况，是否规定使用数据接口的安全限制和安全控制措施，明确包括接口名称、接口参数等内容的数据接口安全要求；

2）是否对涉及个人信息和重要数据的传输接口实施调用审批；

3）是否定期对接口（特别是对外数据接口）进行清查，清查不符合要求的接口是否立即关停；

4）涉及敏感数据的接口调用是否具备安全通道、加密传输、时间戳等安全措施；

5）数据接口部署身份鉴别、访问控制、授权策略、接口签名、安全传输协议等防护措施情况；

6）对接口类型、名称、参数等安全要求规范情况；

7）与接口调用方是否明确数据的使用目的、供应方式、保密约定及数据安全责任等情况；

8）是否对接口访问做日志记录，同时对接口异常事件进行告警通知的情况；

9）是否对数据接口实施调用审批流程，定期开展接口日志审计；

10) 评估是否对异常数据接口调用行为实现自动预警、拦截功能；

11) 是否对开放数据接口的平台相关接口数据交互行为进行监测，对接口访问行为进行审计；

注：开放数据接口的平台包括但不限于数据开放平台、数据共享交换平台、数据交易平台、大数据平台、能力开放平台。

12) 是否建立数据接口全生命周期管理机制，形成接口清单，动态更新接口活动状态。

8.2.7 数据备份恢复

数据备份恢复，主要包括：

a) 数据备份恢复策略和操作规程的建设落实情况；

b) 数据备份的方式、频次、保存期限、存储介质等情况；

c) 提供本地或异地数据灾备功能情况；

d) 定期开展数据备份恢复工作情况；

e) 备份和归档数据访问控制措施的有效性；

f) 定期采取必要的技术措施查验备份和归档数据完整性和可用性情况；

g) 定期开展灾难恢复演练情况。

8.2.8 安全审计

a) 审计执行，主要包括：

1) 审计的实施情况；

2) 审计策略和要求的合理性、有效性；

3) 对数据的访问权限和实际访问控制情况进行定期审计的情况，审核用户实际使用权限与审批时的目的是否保持一致，并及时清理已过期的账号和授权；

4) 特权用户安全审计情况；

5) 应检查是否配备数据安全审计员，加强数据安全审计管理，数据安全审计的覆盖面包括数据收集、数据存储、数据传输、数据使用、数据加工、数据开放共享、数据销毁与删除等数据处理活动各环节，书面明确审计策略、审计对象、审计内容、审计周期、审计结果、审计问题跟踪等要求。

b) 日志留存记录，主要包括：

1) 对数据授权访问、收集、批量复制、提供、公开、销毁、数据接口调用、下载、导出等重点环节进行日志留存管理情况；

2) 日志记录内容，是否包括执行时间、操作账号、处理方式、授权情况、IP地址、登录信息等；

3) 日志记录是否能够对识别和追溯数据操作和访问行为提供支撑；

4) 是否定期对日志进行备份，防止数据安全事件导致日志被删除；

5) 日志保存期限是否符合法律法规要求，如网络日志是否保存六个月以上。

c) 行为审计，主要包括：

1) 对网络运维管理活动、用户行为、网络异常行为、网络安全事件等审计情况；

2) 对数据库、数据接口的访问和操作行为审计情况；

3) 对数据批量复制、下载、导出、修改、删除等高风险行为的审计情况；

4) 对个人信息处理活动的合规审计情况；

5) 是否定期对数据处理活动各环节、数据账号操作、接口调用及数据安全制度落实情况进行数据安全审计，每年至少一次，形成数据安全审计报告；

6) 宜通过数据安全检查工具，从敏感数据泄露、数据明文传输、敏感文件传输，数据未授权访问、账号异常行为等方面发现数据安全隐患。

d) 终端安全管理，主要包括：

1)是否采取安全管控措施限制重要终端(如：运营、运维、开发、测试终端)导入、导出功能；

2) 是否通过网络限制终端数据发送互联网；

3) 是否采取终端加密措施，采用终端文档加密、操作系统自带的卷加密等措施，对终端内存储及处理的敏感数据进行全程加密，防范敏感数据非法复制及传播，避免敏感数据泄露；

4) 是否采用统一认证管理平台，对重要终端系统进行管控；

5) 宜检查重要终端电脑是否有避免多人共享使用。

8.3 数据处理活动

8.3.1 数据收集

a) 数据收集合法正当性，主要包括：

1) 数据收集的合法性、正当性，是否存在窃取、超范围收集、未经合法授权收集或者以其他非法方式获取数据的情况，数据收集目的和范围是否合法；

2) 违反法律、行政法规关于收集使用数据目的、范围相关要求，收集数据的情况；

3) 是否建立统一的数据采集管理机制，对采集的元数据进行管理，并在采集前及采集过程中对数据的敏感性进行初步判定，并明确合理的技术措施实施数据安全防护。

b) 数据质量控制，主要包括：

1) 数据质量管理制度建设情况，对收集数据质量和管理措施是否进行明确要求；

2) 数据质量管理和监控的情况，对异常数据及时告警或更正采取的手段措施；

3) 收集数据监控、过程记录等情况，以及安全措施应用情况；

4) 采用人工检查、自动检查或其他技术手段对数据的真实性、准确性、完整性校验情况。

c) 数据收集设备及环境安全，主要包括：

1) 检测数据收集终端或设备的安全漏洞，是否存在数据泄露风险。

8.3.2 数据存储

a)数据存储适当性，主要包括：

1) 数据存储安全策略和操作规程的建设落实情况；

2) 存储位置、期限、方式的适当性；

3) 永久存储数据类型的必要性；

4) 检查个人信息存储期限是否为实现个人信息主体授权使用目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外，超出个人信息存储期限后，应对个人信息进行删除或匿名化处理。

b)逻辑存储安全，主要包括：

1) 数据库的账号权限管理、访问控制、日志管理、加密管理、版本升级等方面要求的落实情况；

2) 检测逻辑存储系统安全漏洞，查看安全漏洞修复、处置情况；

3) 实施限制数据库管理、运维等人员操作行为的安全管理措施情况；

4) 脱敏后的数据与可用于恢复数据的信息分开存储的情况；

5) 对敏感个人信息、重要数据进行加密存储情况及加密措施有效性；

6) 重要数据和核心数据存储的防勒索应对机制情况；

7)是否明确本地数据备份与恢复安全策略，建立数据备份恢复操作规程，说明数据备份周期、备份方式、备份地点；建立数据恢复性验证机制，保障数据的可用性与完整性；

8)是否提供异地数据备份功能，是否利用通信网络将重要数据定时批量传送至备用场地；

9)是否采用校验技术或密码技术保证数据在存储过程中的完整性；

10)存储三级数据的系统是否具备并实施实时备份、异地容灾策略；

11)是否具备三级数据对应存储管理系统的热冗余，保证数据的高可用性；

12)是否对敏感数据存储环境采取严格的内容级、操作级访问控制措施，采用数据库安全网关、大数据防护系统等措施，对数据访问过程中的操作行为进行严格管控，且应达到最小授权水平。

8.3.3 数据传输

a)传输链路安全性，主要包括：

1) 数据传输安全策略和操作规程的建设落实情况；

2) 敏感个人信息和重要数据传输加密情况及加密措施有效性，是否选用安全的密码算法；

3) 个人信息和重要数据传输进行完整性保护情况；

4) 数据传输通道部署身份鉴别、安全配置、密码算法配置、密钥管理等防护措施情况；

5) 数据传输、接收的记录和安全审计情况；

6) 采取安全传输协议等安全措施情况；

7) 数据异常传输检测发现及处置情况；

8) 是否对敏感个人信息、重要数据、核心数据采用通道加密或内容加密的方式进行传输。

b) 传输链路可靠性，主要包括：

1) 网络传输链路的可用情况，包括对关键网络传输链路、网络设备节点实行冗余建设，建立容灾方案和宕机替代方案等情况。

8.3.4 数据使用和加工

a)传输链路安全

c) 数据使用和加工合法性，主要包括：

1)是否制作、发布、复制、传播违法信息。

d) 数据正当使用，主要包括：

1) 数据使用是否获得数据提供方、数据主体等相关方授权；

2) 数据使用行为与承诺或用户协议的一致性；

3)是否存在个人信息和重要数据滥用情况。

e) 数据导入导出，主要包括：

1) 数据导出安全评估和授权审批流程建设情况；

2) 导入导出审计策略和日志管理机制建设情况；

3) 导出权限管理、导出操作记录情况；

4) 定期对个人信息和重要数据导出行为进行安全审计情况；

5) 对导入数据的格式、安全性和完整性校验情况。

f) 数据处理环境，主要包括：

1) 数据处理环境设置身份鉴别、访问控制、隔离存储、加密、脱敏等安全措施情况；

2) 处理环境中的安全漏洞情况，已发现漏洞的处置情况。

g) 数据使用和加工安全措施，主要包括：

1) 数据防泄漏措施建设情况；

2) 数据使用加工过程中采取的数据脱敏、水印溯源等安全保护措施情况；

3) 数据访问与操作行为的最小化授权、访问控制、审批等管理情况；

4) 数据使用权限管理情况，如是否存在未授权访问、超范围授权、权限未及时收回、特权账号设置不合理等情况；

5) 高风险行为审计及回溯工作开展情况；

6) 是否根据不同数据使用场景采用处理措施（如去标识化、匿名化等），降低数据敏感度及暴露风险。

8.3.5 数据提供

a)数据提供合法正当必要性，主要包括：

1) 数据对外提供的目的、方式、范围的合法性、正当性、必要性；

2) 数据提供的依据和目的是否合理、明确；

3) 数据提供是否遵守法律法规和监管政策要求，是否存在非法买卖、提供他人个人信息或重要数据行为；

4) 对外提供的个人信息和重要数据范围，是否限于实现处理目的的最小范围。

b) 数据提供管理，主要包括：

1) 数据提供安全策略和操作规程的建设落实情况；

2) 签订合同协议情况，是否在合同协议中明确了处理数据的目的、方式、范围、数据安全保护措施、安全责任义务及罚则；

3) 应检查是否对数据共享过程执行统一管理，是否采用统一的数据共享管理平台，实现共享过程管理、共享数据登记管理、用户管理及组件管理等能力。

4) 应检查是否违规设置敏感数据共享区域（公司数据中心除外），如：共享数据库或共享文件服务器等。

c) 数据提供技术措施，主要包括：

1) 对所提供数据及数据提供过程的监控审计情况；

2) 跟踪记录数据流量、接收者信息及处理操作信息情况，记录日志是否完备、是否能够支撑数据安全事件溯源。

d) 数据接收方，主要包括：

1) 数据接收方的诚信状况、违法违规等情况；

2) 数据接收方处理数据的目的、方式、范围等的合法性、正当性、必要性；

3) 接收方是否承诺具备保障数据安全的管理、技术措施和能力并履行责任义务；

4)是否考核接收方的数据保护能力，掌握其发生的历史网络安全、数据安全事件处置情况；

5)应对数据接收方进行定期人工审核，确认共享后数据的防护及操作过程符合要求。

e) 数据转移安全，主要包括：

1) 是否向有关主管部门报告；

2) 是否制定数据转移方案；

3) 接收方数据安全保障能力，是否满足数据转移后不降低现有数据安全保护水平风险；

4) 没有接收方的，对相关数据删除处理情况。

8.3.6 数据公开

a) 数据公开适当性，主要包括：

1) 数据公开目的、方式、范围的适当性；

2) 数据公开目的、方式、范围与行政许可、合同授权的一致性；

3) 公开的数据内容与法律法规要求的符合程度；

4) 对公开的数据进行必要的脱敏处理、数据水印、防爬取、权限控制情况；

5) 数据公开是否会带来聚合性风险。基于被评估对象的已公开数据，结合社会经验、自然知识或其他公开信息，尝试是否可以推断出涉密信息、被评估对象其他未曾公开的关联信息，或其他对国家安全、社会公共利益有影响的信息。

b) 数据公开管理，主要包括：

1) 数据公开的安全制度、策略、操作规程和审核流程的建设落实情况；

2) 数据公开的条件、批准程序，涉及重大基础设施的信息公开是否经过主管部门批准，涉及个人信息公开是否取得个人单独同意；

3) 数据公开前的安全评估情况，是否事前评估数据公开条件、环境、权限、内容等风险；

4) 因法律法规、监管政策的更新，对不宜公开的已公开数据的处置情况；

5) 对公开数据的脱敏处理、防爬取、数字水印等控制措施。

8.3.7 数据删除

a) 数据删除管理，主要包括：

1) 数据删除流程和审批机制的建设落实情况；

2) 数据删除安全策略和操作规程，是否明确数据销毁对象、原因、销毁方式和销毁要求及对应操作规程；

3) 是否按照法律法规、合同约定、隐私政策等及时删除数据；

4) 委托第三方进行数据处理的，是否在委托结束后监督第三方删除或返还数据；

5) 数据删除有效性、彻底性验证情况，以及可能存在的多副本同步删除情况；

6) 是否明确数据存储期限，并于存储期限到期后按期删除数据，明确不可删除数据的类型及原因；

7) 缓存数据、到期备份数据的删除情况；

8)是否建立数据销毁与删除审批机制，设置相关监督角色记录数据销毁与删除操作过程；

9)是否建立常态化销毁记录审计机制，定期对数据销毁记录进行人工审核；

10)如因业务终止或组织解散，无数据承接方的，应检查是否及时有效销毁其控制的数据，法律、法规另有规定的除外；

11)是否在中国境内对介质存储的数据进行删除或销毁；

12)是否对超出存储时效的数据及时采取迁移、归档或删除等操作，数据归档及原始数据清除过程应在多人监督下完成，且保留过程记录。记录至少应包括销毁内容、销毁方式与时间、销毁人签字、监督人签字等内容。

b) 存储介质销毁，主要包括：

1) 存储介质销毁管理制度和审批机制的建设落实情况；

2) 介质销毁策略和操作规程，是否明确各类介质的销毁流程、方式和要求，是否妥善处置销毁的存储介质；

3) 存储介质销毁过程的监控、记录情况；

4) 软硬件资产维护、报废、销毁管理情况等；

5) 介质销毁措施有效性，是否对被销毁的存储介质进行数据恢复验证；

6) 是否按照数据分类分级，明确不同级别数据适当的删除措施，核心数据删除是否采用存储介质销毁方式；

7) 是否对存储数据的介质或物理设备采取难恢复的技术手段，如物理粉碎、消磁、多次擦写等。

8.4 个人信息保护

如能源企业涉及个人信息处理，还应针对个人信息处理基本原则、个人信息告知、个人信息同意、个人信息处理、敏感个人信息处理、个人信息主体权利、个人信息安全义务、个人信息投诉举报、大型网络平台个人信息保护等方面识别个人信息保护风险。可视情采纳个人信息保护影响评估工作结论，也可依据 GB/T39335 识别个人信息保护风险。

8.5 数据出境安全

如能源企业涉及将在境内运营中收集和产生的个人信息和重要数据，提供给位于境外的机构、组织、个人的数据出境，还应开展数据出境安全风险识别，主要包括：

a）是否明确数据出境业务场景，严格遵守国家法律、行政法规数据出境安全管理办法，严禁未授权数据出境行为；

b）向境外提供个人信息或者国家规定的重要数据前，应检查是否按照有关规定申请数据出境安全评估，进行国家安全审查，法律、行政法规另有规定的，从其规定；

c）是否建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。

9 数据安全风险分析与评估

9.1 梳理问题清单

结合能源企业数据资产和数据处理活动清单，针对每个评估对象的各个评估项评估情况，梳理存在的风险隐患，形成数据安全问题清单。

9.2 数据安全风险分析

9.2.1 风险分析

数据安全风险分析，主要从影响数据保密性、完整性、可用性和数据处理合理性角度分析各项风险源可能引发的数据安全风险，及风险危害程度和发生的可能性。

根据数据安全问题清单，分析数据安全风险源可能引发的安全风险（常见风险可参考附录B），如多项数据安全问题可能造成同样数据安全风险，可以将其与其他问题合并进行风险分析。

9.2.2 风险危害程度分析

风险危害程度分析，主要分析数据的价值、重要性、规模、种类，以及数据处理目的、方式、范围等要素，综合评估数据安全风险一旦发生，对国家安全、经济运行、社会秩序、公共利益或者个人、组织合法权益造成的危害程度。风险危害程度划分为5个不同的等级，等级1-5级，从低到高分别对应很低、低、中、高、很高。风险危害程度分析遵循就高从严、整体分析原则，如果该风险涉及多个数据资产，应进行累加判断，将涉及数据的风险按照最高危害等级判断。风险危害程度评价，主要考虑数据价值、数据重要性、风险源严重程度三个因素，分析方法如下：

a）数据价值主要从数据资产的经济效益、业务效益、投入成本计量等方面分析；

b）数据重要性主要从数据分级角度衡量，数据级别越高代表数据重要性越高，数据安全级别可参考《GB/T 43697-2024 数据安全技术 数据分类分级规则》确定。个人信息规模和数据敏感程度可以作为数据重要性判断的衡量因素；

c）风险源严重程度，主要考虑风险源对企业带来的危害程度。数据安全风险危害程度的判断标准如表1 所示。

表 1 数据安全风险危害程度等级参考

影响对象	危害程度	参考说明

影响对象	危害程度	参考说明
国家安全	很高	直接危害国家安全重点领域，如政治安全。
	高	关系国家安全重点领域，或者对国土、军事、经济、文化、社会、科技、电磁空间、网络、生态、资源、核、海外利益、太空、极地、深海、生物、人工智能等任一领域国家安全造成严重威胁。
	中	对国土、军事、经济、文化、社会、科技、电磁空间、网络、生态、资源、核、海外利益、太空、极地、深海、生物、人工智能等任一领域国家安全造成威胁。
经济运行	很高	1.直接影响涉及国家安全的行业、支柱产业和高新技术产业中的重要骨干企业、提供重要公共产品的行业、重大基础设施和重要矿产资源行业等关系国民经济命脉行业的运行和发展。 2.关系国民经济命脉，严重危害对社会经济发展具有重大影响的行业领域、部门、企业、资源、区域等的生产运营和经济利益。 3.对一个或多个行业领域的发展态势、业务经营、技术进步、产业生态造成特别严重危害，如对核心业务造成重大损害，导致大面积业务中断、大量业务处理能力丧失等。 4.对一个或多个省（自治区、直辖市）的经济运行造成特别严重影响，例如导致大范围停工停产、大规模基础设施长时间中断运行等。
	高	1.直接影响宏观经济运行状况和发展趋势，如社会总供给和总需求、国民经济总值和增长速度、国民经济主要比例关系、物价总水平、劳动就业总水平与失业率、货币发行总规模与增长速度、进出口贸易总规模与变动等。 2.直接影响一个或多个地级市、行业内多个企业或大规模用户，对行业发展态势、技术进步和产业生态等造成严重影响，或者直接影响行业领域核心竞争力、核心业务运行、关键产业链、核心供应链等。
	中	1.对单个行业领域发展、业务经营、技术进步、产业生态等造成一般危害，如受影响的用户和企业数量较小、生产生活区域范围较小、持续时间较短、社会负面影响较小。 2.对单个行业领域的经济运行秩序造成一般危害，如市场准入、市场行为、市场结构、商品销售、交换关系、生产经营秩序等。
社会秩序	很高	1.关系重要民生，直接影响人民群众重要民生保障的事项、物资、工程或项目等。 2.直接导致特别重大突发事件、特别重大群体性事件、暴力恐怖活动等，引起一个或多个省（自治区、直辖市）大部分地区的社会恐慌，严重影响社会正常运行。
	高	1.直接导致重大突发事件、重大群体性事件等，影响一个或多个地市大部分地区的社会稳定。 2.严重影响人民群众的日常生活秩序。 3.严重影响各级政务部门履行公共管理和服务职能。 4.严重影响法治和社会伦理道德规范。
	中	1.对人民群众的日常生活秩序造成一般影响。 2.直接影响企事业单位、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。 3.直接影响公共场所的活动秩序、公共交通秩序。

影响对象	危害程度	参考说明
公共利益	很高	1.关系重大公共利益，导致一个或多个省（自治区、直辖市）大部分地区的社会公共资源供应长期、大面积瘫痪，大范围社会成员（如1000万人以上）无法使用公共设施、获取公开数据资源、接受公共服务。 2.可能导致特别重大网络安全和数据安全事件，或者导致特别重大事故级别的安全生产事故，对公共利益造成特别严重影响，社会负面影响大。 3.可能导致特别重大突发公共卫生事件（Ⅰ级），造成社会公众健康特别严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒等严重影响公众健康的事件。
	高	1.直接危害公共健康和安全，如严重影响疫情防控、传染病的预防监控和治疗等。 2.可能导致重大突发公共卫生事件（Ⅱ级），造成社会公众健康严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒等严重影响公众健康的事件。 3.导致一个或多个地市大部分地区的社会公共资源供应较长期中断，较大范围社会成员（如100万人以上）无法使用公共设施、获取公开数据资源、接受公共服务。
	中	对公共利益产生一般危害，影响小范围社会成员使用公共设施、获取公开数据资源、接受公共服务等。
组织权益	中	可能导致组织遭到监管部门严重处罚（包括取消经营资格、长期暂停相关业务等），或者影响重要/关键业务无法正常开展的情况，造成重大经济或技术损失，严重破坏机构声誉，企业面临破产。
	低	可能导致组织遭到监管部门处罚（包括一段时间内暂停经营资格或业务等），或者影响部分业务无法正常开展的情况，造成较大经济或技术损失，破坏机构声誉。
	很低	可能导致个别诉讼事件，或在某一时间造成部分业务中断，使组织的经济利益、声誉、技术等轻微受损。
个人权益	中	个人信息主体可能会遭受重大的、不可消除的、可能无法克服的影响，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害。如遭受无法承担的债务、失去工作能力、导致长期的心理或生理疾病、导致死亡等。
	低	个人信息主体可能遭受较大影响，个人信息主体克服难度高，消除影响代价较大。如遭受诈骗、资金被盗用、被银行列入黑名单、信用评分受损、名誉受损、造成歧视、被解雇、被法院传唤、健康状况恶化等。
	很低	个人信息主体可能会遭受困扰，但尚可以克服。如付出额外成本、无法使用应提供的服务、造成误解、产生害怕和紧张的情绪、导致较小的生理疾病等。
注：数据处理者可根据数据对自身的价值、重要性，结合风险源的严重程度，将仅影响组织权益、个人权益等的风险危害程度自行定为或调整为“很高”“高”等级别，及时进行风险处置。		

9.2.3 风险发生可能性分析

风险发生可能性分析，主要考虑风险源发生频率、安全措施有效性和完备性、风险源关联性等因素。

分析方法如下：

a) 风险源发生频率，可从被评估对象发生相关数据安全事件的次数及频率、同行业或业务模式相似的单位发生相关数据安全事件的次数及频率、相似数据安全事件发生次数及频率、轻微安全问题累

计发生次数等方面，综合分析同类风险源发生可能性，一般风险源或安全事件发生频率越高，风险发生可能性越高；

b）安全措施有效性、完备性，主要通过识别数据安全措施应对风险源的有效性、全面性等，核心数据、重要数据及相关数据处理活动，需采取更严格的安全防护措施才能降低风险发生可能性；

c）风险源关联性，主要通过风险源清单关联分析，发现多个风险源组合后可能引发数据安全风险，则将其与其他风险源合并分析，综合判断风险发生可能性。在综合分析风险源发生频率、安全措施有效性和完备性、风险源关联性的基础上，将数据安全风险发生的可能性划分为3个不同的等级，等级1-3级，从低到高分别对应低、中、高 ，如表2 所示。等级越高代表措施完备性、有效性越低，风险越可能发生。如需进行定量分析，可参考附录 C.2 。

表 2 风险发生可能性等级参考

等级	风险发生可能性描述
高	涉及违法违规行为、缺少数据安全措施或安全措施有效性较弱，被评估对象或同类组织多次高频发生相关风险源，或容易与其他风险源结合引发风险，风险隐患发生可能性高（例如出现频率高、在大多数情况下几乎不可避免、可以证实经常发生过）。
中	有一定数据安全措施，但有效性不足，被评估对象或同类组织发生相关风险源，或有一定概率与其他风险源结合引发风险，风险隐患发生可能性一般（例如出现频率中等，在某种情况下可能发生，或被证实曾经发生）。
低	数据安全措施比较到位、完备，被评估对象或同类组织很少发生相关风险源，或很难与其他风险源结合引发风险，风险隐患发生可能性低（例如几乎不可能发生，或仅可能在非常罕见和例外的情况下发生）。

9.3 数据安全风险评估

基于实际情况对数据安全风险进行评价，风险评价主要考虑风险一旦发生可能对本企业、能源领域以及对国家安全、社会公共利益、其他组织或者个人的合法权益造成的影响，以及风险发生的可能性进行综合评价。具体风险分析和评价方法，可参考数据安全风险评估方法国家标准。

数据安全风险评价结果包括：

a）重大安全风险：一般指可能直接影响国家安全的数据安全风险；

b）高安全风险：一般指可能直接影响经济运行、社会稳定、公共健康安全，以及较为广泛的公众权益，或对国家安全造成间接影响的数据安全风险；

c）中安全风险：一般指可能直接对企业合法权益造成较为严重的影响，或直接对自然人的人格尊严受到严重侵害或者人身、财产安全受到严重危害，或对经济运行、社会稳定、公众利益造成较为严重间接影响的数据安全风险；

d）低安全风险：一般指可能直接对企业合法权益造成一般影响，或直接对自然人的人格尊严受到侵害或者人身、财产安全受到危害，或对社会、公众权益有一定或较小影响的数据安全风险；

e）轻微安全风险：一般指可能直接对企业合法权益造成一般或较小影响，或对自然人人格尊严、人身安全、财产安全不造成侵害或仅产生较轻微的危害，或对小范围的组织或公民个体权益造成影响的数据安全风险。

数据处理者可根据自身情况，将仅影响组织权益、个人权益等的风险自行定为或调整为“重大”“高”等级别，及时进行风险处置。本文件提出了定性和定量评价风险的方法，表3 提供了一种风险等级定性评价方法，如需获得风险定量评价结果，可参考附录 C.3 进行风险评估。

表 3 数据安全风险评估矩阵

危害程度 可能性	很高	高	中	低	很低
高	重大安全风险	重大安全风险	中安全风险	低安全风险	轻微安全风险
中	重大安全风险	高安全风险	低安全风险	低安全风险	轻微安全风险
低	中安全风险	中安全风险	轻微安全风险	轻微安全风险	轻微安全风险

9.4 数据安全风险清单

针对各项数据安全风险完成风险评价后，整理各项风险评估结果，形成数据安全风险清单（如表4所示），列出各项风险的风险等级、危害程度、发生可能性等。

表 4 数据安全风险清单

序号	风险类型	风险源	风险源描述	风险危害程度	风险发生的可能性	风险等级	涉及的数据及类型	涉及的数据处理活动	评估情况描述

10 数据安全风险评估总结

10.1 编制评估报告

根据评估情况，评估团队编制数据安全风险评估报告（报告模板参见附录 E）。评估报告应准确、清晰地描述评估活动的主要内容（并附必要的证据或记录），提出可操作性的整改措施对策建议。风险评估报告的内容包括：

a）评估概述，包括评估目的及依据，评估对象和范围，评估结论等；

b）评估工作情况，包括评估人员、评估时间安排、评估工具和环境情况等；

c）信息调研情况，包括数据处理者、业务和信息系统、数据资产、数据处理活动、安全措施等情况，形成的数据资产清单、数据处理活动清单、数据流图等文件可视情放在报告正文或附件中；

d）数据安全风险识别，包括数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面识别的风险源情况；

e）风险分析与评价，对数据安全问题可能带来的安全风险进行综合分析与评价；

f）整改建议，针对发现的数据安全问题或风险，提出整改措施或风险处置建议；

g）数据安全风险源清单，列出完整的数据安全风险源清单，并附上关键记录和证据，若证据无法在附录中完整列出，应列出证据关键信息和序号，在提交评估报告时作为附件提交；

h）涉及重要数据、个人信息、核心数据的，应当详细列出处理的数据种类、数量（不包括数据内容本身），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；

i）委托第三方机构开展评估或检查评估的，评估报告应由评估组长、审核人签字，并加盖评估机构公章。

10.2 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。被评估方应制定数据安全风险处置方案，限期完成整改，无法及时完成整改的，应采取临时安全措施，防止数据安全事件发生。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。

10.3 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。被评估方完成整改后，评估方可开展数据安全风险复评工作，复评时可重点分析风险处置后的残余风险，以及采取额外控制措施可能导致的次生风险等。

附 录 A
（资料性）
能源大数据数据分类和分级结果示例

A.1 能源大数据数据分类和分级结果示例

序号	一级类	二级类	三级类	三级说明	数据安全定级
1	能源生产数据	煤炭及煤制品生产基础数据	煤炭生产企业信息	指煤炭生产企业的基础数据，位置数据等	重要
2			煤炭生产设施信息	指煤炭生产设施的基础数据、位置数据、产能数据等	核心
3		煤炭及煤制品生产运行数据	煤炭及煤制品生产供应链数据	指煤炭生产企业生产过程中涉及到的生产、采购、销售、库存的数据等	重要
4			煤炭及煤制品生产设备运行数据	指煤炭及煤制品生产设备运行过程中产生的数据	核心
5		天然气生产基础数据	天然气生产相关企业信息	指天然气生产企业的基础数据、位置数据等	重要
6			天然气生产设施信息	指天然气生产设施的基础数据、位置数据、产能数据等	核心
7		天然气生产运行数据	天然气生产供应链数据	指天然气生产企业生产过程中涉及到的生产、库存的数据等	重要
8			天然气生产设备运行数据	指天然气生产设备运行过程中产生的数据	核心
9		石油及石油制品生产基础数据	石油及石油制品生产企业信息	指使用及石油制品生产企业的基础数据、位置数据等	重要
10			石油及石油制品生产设施信息	指石油及石油制品生产设施的基础数据、位置数据、产能数据等	核心
11		石油及石油制品生产运行数据	石油及石油制品生产供应链数据	指石油及石油制品生产企业生产过程中涉及到的加工、生产、销售、库存的数据等	重要
12			石油及石油制品生产设备运行数据	指石油及石油制品生产设备运行过程中产生的数据	核心
13		电能生	电能生产企	指电能生产企业的基础数据、位置数据等	重要

		产基础数据	业信息		
14			电能生产设施信息	指电能生产设施的基础数据、位置数据等、装机容量、计划投产数据等	核心
15		电能生产运行数据	电能生产供应链数据	指电能生产企业生产过程中涉及到的发电、区外来电、新能源消纳、上网电价的数据等	核心
16			电能生产设备运行数据	指电能生产设备运行过程中产生的数据、如光伏逆变器负荷、并网量等	核心
17		能源生产指标数据	一次能源产量	指各类一次能源的产量数据	2
18			电力装机容量	指电力总装机容量与不同发电类型的装机容量，如煤电装机容量、风电装机量、太阳能发电装机量等	2
19			发电量	指发电总量指标与不同发电类型的发电总量，如煤电发电总量、风电发电总量、太阳能发电总量等	2
20			其他保障能力	指不同能源类型接卸、储存、运出等保障能力，如原油储备能力、煤炭接卸能力、煤炭基地运出能力等	2
21			煤电平均供电煤耗	指煤电平均供电煤耗的相关数据	2
22	能源存储数据	煤炭及煤制品存储基础数据	煤炭及煤制品存储企业信息	指煤炭及煤制品存储企业的基础数据、位置数据等	重要
23			煤炭及煤制品存储设施信息	指煤炭及煤制品存储设施的基础数据、位置数据、煤炭进出港能力、扩建的数据等	核心
24		煤炭及煤制品存储运行数据	煤炭及煤制品存储供应链数据	指煤炭及煤制品存储企业存储过程中涉及到的库存、进出港的数据等	重要
25			煤炭及煤制品存储设备运行数据	指煤炭及煤制品存储设备运行过程中产生的数据	核心
26		天然气存储基础数据	天然气存储企业信息	指天然气存储的基础数据、位置数据等	重要
27			天然气存储设施信息	指天然气存储设施的基础数据、位置数据、接卸、储备、输出的数据等	核心
28		天然气存储运行数据	天然气存储供应链数据	指天然气存储企业存储过程中涉及到的库存、接卸、外输的数据等	重要
29			天然气存储设备运行数据	指天然气存储设备运行过程中产生的数据	核心
30		石油及石油制品存储基础数据	石油及石油制品存储企业信息	指石油及石油制品存储企业的基础数据、位置数据等	重要
31			石油及石油制品存储设	指石油及石油制品存储设施的基础数据、位置数据、储备、油品类型的数据等	核心

			施信息		
32		石油及石油制品存储运行数据	石油及石油制品存储供应链信息	指石油及石油制品存储企业存储过程中涉及到的库存数据等	重要
33			石油及石油制品存储设备运行数据	指石油及石油制品存储设备运行过程中产生的数据	核心
34		电能存储基础数据	电能存储企业信息	指电能存储企业的基础数据、位置数据等	重要
35			电能存储设施信息	指电能存储设施的基础数据、位置数据、设备容量的数据等	核心
36		电能存储运行数据	电能存储设备运行数据	指电能存储设备运行过程中产生的数据、如充/放电量、蓄电池组状态、储能收益的数据等	核心
37	能源运输数据	天然气运输基础数据	天然气运输企业信息	指天然气运输企业的基础数据、位置数据等	重要
38			天然气运输管网信息	指天然气运输官网的基础数据、位置数据、长度、设施类型、管径、设计流量的数据等	核心
39		石油及石油制品运输基础数据	石油及石油制品运输企业信息	指石油及石油制品运输企业的基础数据、位置数据等	重要
40			石油及石油制品运输官网信息	指石油及石油制品运输官网的基础数据、位置数据、长度、设施类型、管径、设计流量的数据等	核心
41		电能运输基础数据	电能网络企业信息	指电能网络企业的基础数据、位置数据等	重要
42			电能输配电信息	指电能输配电的基础数据、位置数据、线路长度、变电站数量、负载能力的数据等	核心
43		能源运输指标数据	电网综合线损率	指电网综合线损相关的数据	重要
44	能源消费数据	能源消费基础数据	能源消费客户信息	指能源消费客户相关企业的基础数据、位置数据、客户档案、财务状况、企业工业产品产值、生产运行的数据等	核心
45			能源消费服务商信息	指能源消费服务商相关企业的类型、基础数据、位置数据等	重要
46		煤炭及煤制品消费运行数据	客户煤炭及煤制品消费数据	指客户在煤炭及煤制品消费过程中涉及到的购进、库存、消费的数据等	核心
47			煤炭及煤制品市场交易数据	指煤炭及煤制品市场交易过程中涉及到的期货交易、现货交易、交割周期、交易量的数据等	核心
48		天然气消费运	客户天然气消费数据	指客户在天然气消费过程涉及到的相关数据	重要

49		行数据	天然气服务设施数据	指天然气服务设施的基本数据、位置数据、燃气价格、设施检修的数据等	2
50			天然气市场交易数据	指天然气市场交易过程中涉及到的期货交易、现货交易、交割周期、交易量的数据等	3
51		石油及石油制品消费运行数据	客户使用及石油制品消费数据	指客户在石油及石油制品消费过程中涉及到的购进、库存、消费数据等	核心
52			石油服务设施数据	指石油服务设施的基础数据、位置数据、成品油价的数据等	3
53			石油及石油制品市场交易数据	指石油及石油制品市场交易过程中涉及到的期货交易、现货交易、交割周期、交易量的数据等	3
54		电能消费运行数据	客户电能消费数据	指客户在电能消费过程中涉及到的电量、负荷的数据等	核心
55			客户电能设备运行数据	指客户在电能设备运行过程涉及到的电压、功率、电能、负载、损耗、电流的数据等	重要
56			电能服务设施数据	指客户在电能服务设施运行过程中涉及到的充电桩、充电站、岸电设备位置、电能设施等的位置数据、功率、充电时长、价格、电压、利用率、维修的数据等	3
57			电力市场交易数据	指电力市场交易过程中涉及到的相关数据，如市场化用电公告的数据等	3
58		热能消费运行数据	客户热能消费数据	指客户在热能消费过程中涉及到的消费量的数据等	核心
59			客户热能设备运行数据	指客户热能设备运行过程中涉及到的流量、速度、热量、温度的数据等	重要
60		水消费运行数据	客户水消费数据	指客户在水消费过程中涉及到的用水量的数据等	核心
61			客户水设备运行数据	指客户在水设备运行过程中涉及到的流量、速度的数据等	重要
62		能源消费双碳数据	碳排放数据	指碳排放涉及到的排放量、排放强度、排放计划、盘查、碳足迹的数据等	重要
63			碳交易数据	指碳交易涉及到的交易台账、碳配额、履约情况、绿证的数据等	重要
64			碳金融数据	指碳金融涉及到的绿色债券、贷款的数据等	重要
65			碳普惠数据	指碳普惠数据涉及到的碳积分的数据等	重要
66			碳汇数据	指碳汇数据涉及到的相关数据	重要
67		能源消费指标数据	能源消费总量	指全社会用电量和不同类型能源的消费总量，如煤炭消费总量、原有消费总量的数据等	2
68			能源消费占比	指不同类型能源的消费占比，如石油消费占比、天然气消费占比的数据等	2
69			能源消费增量	指增量总量指标和不同类型能源的消费增量，如煤炭消费增量、石油消费增量的数据等	2
70			能源消费占比增量	指不同类型能源的消费占比增量，如煤炭消费占比增量、石油消费占比增量的数据等	2

71			能源消费强度	指能源总量指标维护和不同类型能源的消费强度，如煤炭消费强度、电力消费强度的数据等	2
72			能耗指标	指国家、本地区、产品/工艺/设备、行业产值、企业主要工业产品的能耗指标与单位能耗指标数据等	2
73			复工复产指数	指复工复产相关的指标数据	2
74			能源价格指数	指能源价格相关的指标数据	2
75			碳排总量	指碳排总量相关的指标数据，如碳排总量维护、碳排总量分解的数据等	2
76			碳配额	指碳排配额相关的指标数据，如碳配额管理、碳配额分解的数据等	2
77	能源行业相关数据	国土资源和能源基础数据	自然资源数据	指自然资源的基础数据，如风能资源、太阳能资源、水力资源、传统化石能源、矿产资源数据等	重要
78		国土资源和能源管理数据	新能源项目管理	指新能源项目管理涉及到的项目信息、通知、企业申报的数据等	核心
79			能源科技	指能源科技管理相关的企业基本信息、分类的数据等	核心
80			能源改革	指能源企业基于能源改革的项目主体分类、企业信息、项目信息等数据	核心
81			能源合作	指能源企业的能源合作方案、主题分类、企业项目信息等数据	核心
82			节能管理	指能源行业相关的企业如重点能耗企业的节能管理方案、能源利用效率等数据	核心
83			能耗双控	指能源行业相关的企业如重点能耗企业的能耗总量和强度双控指标、指标完成情况等数据	核心
84		工业和交通运行数据	交通运输数据	指交通运输的运行数据，如电动汽车保有量数据等	重要
85		气象水文测绘地震运行数据	气象数据	指气象的运行数据，如天气相关的数据等	重要
86		能源行业相关指标数据	宏观经济指标	指与能源行业相关的宏观经济指标，如经济 GDP、社会 CPI 等数据	2
87	能源大数据应用数据	能源大数据应用基础数据	平台用户信息	指用户注册能源大数据平台过程中产生的账号密码、企业名称、资质证书等数据	核心
88			平台数据增值产品信息	指能源大数据平台发布的数据增值产品的产品名称、价格数据等	2
89		能源大数据应	平台用户行为数据	指用户使用能源大数据中心平台过程中产生的访问数据、浏览数据等	重要

90		用运行数据	平台数据增值产品运行数据	指数据增值产品在平台运行过程中产生的浏览量、交易量数据等	重要
91			平台发布信息	指能源大数据中心平台运行过程中对外发布的平台公告、宣传活动信息、能源法规政策、能源行业资讯等数据	1

附 录 B
（规范性）
典型数据安全风险类别

本附录给出了常见数据安全风险类别，如数据泄露风险、数据篡改风险、数据破坏风险、数据丢失风险等，如表 B.1 所示。

B.1 典型数据安全风险类别

序号	风险类别	描述
1	数据泄露风险	由于数据窃取、爬取、拖库、撞库等安全威胁，或者缺乏有效的安全措施、人员操作失误或有意盗取等，导致数据泄露、恶意窃取、未授权访问等影响数据保密性的风险。
2	数据篡改风险	由于数据注入、中间人攻击等安全威胁，或者缺乏有效的安全措施、人员有意或无意操作等，导致数据被未授权篡改等影响数据完整性的风险。
3	数据破坏风险	由于拒绝服务攻击、自然灾害、嵌入恶意代码、数据污染、设备故障等安全威胁，或者缺乏有效的安全措施、人员有意或无意操作等，导致数据被破坏、毁损、数据质量下降等影响数据可用性的风险。
4	数据丢失风险	由于数据过载、软硬件故障、备份失效、链路过载等问题，或者缺乏有效的安全措施、人员有意或无意操作等，导致数据丢失、难以恢复等安全风险。
5	数据滥用风险	由于缺乏授权访问控制、权限管控等有效的安全管控措施、人员有意或无意操作等，导致数据被未授权或超出授权范围使用、加工的风险。
6	数据伪造风险	由于数据源欺骗、深度伪造等安全威胁，或者缺乏有效的安全措施、人员有意或无意操作等，导致数据或数据源被伪造、数据主体被仿冒等安全风险。
7	违法违规获取数据	违反法律、行政法规等有关规定，非法或违规获取、收集数据的风险。
8	违法违规出售数据	违反法律、行政法规等有关规定，非法或违规向他人出售、交易数据的风险。
9	违法违规保存数据	违反法律、行政法规等有关规定，非法或违规留存数据的风险，如逾期留存、违规境外存储等。
10	违法违规利用数据	违反法律、行政法规等有关规定，非法或违规使用、加工、委托处理数据的风险。
11	违法违规提供数据	违反法律、行政法规等有关规定，非法或违规向他人提供、共享、交换、转移数据的风险。
12	违法违规公开数据	违反法律、行政法规等有关规定，非法或违规公开数据的风险。
13	违法违规购买数据	违反法律、行政法规等有关规定，非法或违规购买、收受数据的风险。
14	违法违规出境数据	违反法律、行政法规等有关规定，非法或违规向境外提供数据的风险。
15	数据处理缺乏正当性	违反正当性原则，数据处理活动缺乏明确、合理的处理目的。
16	未有效个人信息主体权利	由于未采取有效的个人信息保护措施、人员操作或外部威胁等，导致未能有效保障个人信息主体的知情权、决定权、限制或者拒绝个人信息处理等个人信息主体合法权利。
17	App 违法违规收集使用个人信息	App 违反个人信息监管政策或标准规范，存在违法违规收集使用个人信息行为的风险。
18	数据处理缺乏公平公正	由于缺乏安全管控措施、人员有意或无意操作等，导致数据处理违反公平公正、诚实守信原则，侵犯其他组织或个人合法权益的风险。

序号	风险类别	描述
19	数据处理抵赖风险	由于外部攻击威胁、缺乏有效安全管控措施、人员有意或无意操作等，导致处理者或第三方否认数据处理行为或绕过数据安全措施等风险。
20	数据不可控风险	由于第三方数据安全能力不足、缺乏有效的第三方管控措施、合同协议缺失、外包人员操作等，导致委托处理或合作的第三方违反法律法规或合同协议约定处理数据，造成第三方超范围处理数据、逾期留存数据、违规再转移等数据不可控风险。
21	数据推断风险	由于未考虑数据之间的关联关系，导致从公开数据可推断出核心数据、重要数据、未公开的个人数据等，包括但不限于面向人工智能模型的推理攻击、面向基础设施的跨域推断攻击等
22	其他风险	其他可能影响国家安全、公共利益或组织、个人合法权益的数据安全风险。

附 录 C
（规范性）
数据安全风险量化分析与评估方法

C.1 数据安全风险危害程度量化分析方法

表 C.1 数据安全风险危害程度划分为5个不同的等级，等级1-5级，从低到高分别对应很低、低、中、高、很高，按照百分制给出数据安全风险危害程度量化分析方法，结合实际情况，根据得分区间给出风险危害程度得分值，得分越高代表风险危害程度越高。

表 C.1 数据安全风险危害程度等级参考

等级	标识	得分
5	很高	[80%, 100%]
4	高	[60% 80%)
3	中	[40%, 60%)
2	低	[20%, 40%)
1	很低	[0%, 20%)

C.2 数据安全风险发生可能性量化分析方法

表 C.2 数据安全风险发生的可能性划分为3个不同的等级，等级1-3级，从低到高分别对应低、中、高，按照百分比给出数据安全风险发生可能性量化分析方法，结合实际情况，根据得分区间给出风险发生可能性得分值，得分越高代表风险发生可能性越高。

表 C.2 数据安全风险发生可能性等级参考

等级	标识	得分
3	高	[75% 100%]
2	中	[30%, 75%)
1	低	[0%, 30%)

C.3 数据安全风险量化评估方法

结合 9.3 给出的数据安全风险评估方法，本节提出数据安全风险量化评估方法，结合实际情况，根据 C.1 和 C.2 给出的量化结果计算风险分值，得分越高代表风险等级越高。计算公式如下：

$$Ri = \sigma i \times Vi$$

式中：

Ri为第i个数据的风险评价分值；

σi为第i个数据危害程度赋值；

Vi为第i个数据的风险发生可能性赋值。

附 录 D
（资料性）
能源企业数据安全风险评估调研表示例

D.1 系统基本情况调研表

表 D.1 系统基本情况调研表

系统名称	xx 系统 v1.1			
系统规模	承载的主要业务			
	是否有子系统	□是□否	子系统数	____个
	业务信息类型	**公民个人信息、员工管理信息、营销管理信息、输配电管理信息、网元信息等等。（根据实际情况调整）**		
	子系统清单			
	是否跨省域	□是□否	跨省域数	____个
	跨省域名称			
	系统总用户数			
是否是涉及国家秘密的系统		□是 □否		
系统是否采用符合国家规定的专用密码产品		□是 □否		
等级保护级别		□一级 □二级 □三级 □四级		
定级情况说明		□初次定级 □重新定级 □未定级		
URL 地址		https://10.XXX.XXX.1		
IP 地址/掩码		/		
网关		/		
所属网络区域		DMZ/IDC		
操作系统及版本				
数据库及版本				
中间件				
C/S 或 B/S 模式				
涉及敏感数据类型				
数据量				
现有用户数量				
主要用户角色				
第三方运维厂商		XXX 公司		
是否开放接口进行数据共享		否		

D.2 系统网络拓扑图

网络结构图要求：

a)应该标识出网络设备、服务器设备和主要终端设备及其名称；

b)应该标识出服务器设备的IP地址；

c)应该标识网络区域划分等情况；

d)应该标识网络与外部的连接等情况；

e)应该能够对照网络结构图说明所有业务流程和系统组成；

f)如果一张图无法表示，可以将核心部分和接入部分分别划出，或以多张图表示。

D.3 系统备份恢复信息调研表

表 D.3 系统备份恢复信息调研表

序号	数据分类	数据量（单位：TB）	应用名称	库数量	备份方式	备份地址	备份频率	备注
1	结构化数据	0.2	xx 系统	1				
2	非结构化数据	1	xx 系统	1				
3	…	…	…	…	…	…	…	…

D.4 数据安全设备情况调研表

表 D.4 数据安全设备情况调研表

序号	设备名称	设备主要功能	覆盖范围
1	…	…	…

D.5 数据安全管理文档调研表

表 D.5 数据安全管理文档调研表

序号	文档要求	相关文档名称	备注
1	单位总体安全方针和政策方面的管理制度		
2	部门设置、岗位设置及工作职责定义方面的管理制度		
3	授权审批、审批流程等方面的管理制度		
4	安全审核和安全检查方面的管理制度		
5	管理制度、操作规程修订、维护方面的管理制度		
6	人员录用、离岗、考核等方面的管理制度		

序号	文档要求	相关文档名称	备注
7	人员安全教育和培训方面的管理制度		
8	第三方人员访问控制方面的管理制度		
9	工程实施过程管理方面的管理制度		
10	软件外包开发或自我开发方面的管理制度		
11	测试、验收方面的管理制度		
12	办公环境安全管理方面的管理制度		
13	资产、设备、介质安全管理方面的管理制度		
14	信息分类、标识、发布、使用方面的管理制度		
15	网络安全管理（网络配置、帐号管理等）方面的管理制度		
16	系统安全管理（系统配置、帐号管理等）方面的管理制度		
17	系统监控、风险评估、漏洞扫描方面的管理制度		
18	病毒防范方面的管理制度		
19	系统变更控制方面的管理制度		
20	密码管理方面的管理制度		
21	备份和恢复方面的管理制度		
22	安全事件报告和处置方面的管理制度		
23	应急响应方法、应急响应计划等方面的文件		
24	其他文档		

D.6 评估工具环境调研表

表 D.6 评估工具环境调研表

序号	信息采集项	资源协调（被评估系统填写）	备注说明	协调对象
1	流量分析采集	流量镜像口制作（http 流量）：*已准备*	用于流量接入，主要通过在系统上层的交换机上旁路部署数据安全风险评估工具，需要接入未加密的业务流量，不限制系统数量，尽量接入。 如单位系统均采用 https 协议进行传输；请提前准备 http 流量。	网络工程师
2	镜像流量接入方式	□光口（万兆） □电口（千兆）	确认交换机上的接口入方式：以光口（万兆）/电口（千兆）	网络工程师
3	部署方式	*云部署/本地部署*	确认系统的部署方式	网络工程师
4	镜像流量峰值	*XX b/s*	在交换机上统计业务流量的镜像流量峰值。	网络工程师
5	日均流量	*XX Gb/天*	在交换机上统计业务流量的镜像日均流量。	网络工程师

6	评估工具管理IP1	管理 IP1: 子网掩码： 网关：	该 IP 作为数据安全风险评估工具的管理 IP；请开通 22 号端口，允许 IP2 对 IP1 的 22 号端口进行访问。	网络工程师
7	测试人员 IP2	测试 IP2: 子网掩码： 网关：	该 IP 作为现场测试人员终端电脑使用 IP；需与 IP1 连通，并能访问单位系统各系统，验证风险。	
8	防火墙	防火墙策略配置，保证 IP2 可与 IP1、业务系统间可连通可访问	防火墙策略配置，保证 IP2 可与 IP1、被评估系统连通（如通过白名单访问，请提前开通访问策略）。	
9	测试账号	账号： 密码：	如需通过统一登录验证方式访问被评估系统，如堡垒机、4A 等；需提供测试账号用于风险验证。	系统管理员/运维管理员

D.7 系统相关联系人

表 D.7 系统相关联系人调研表

序号	人员名称	所属部门	职务/职称	负责范围	联系方法
1	XX	XX	系统负责人/数据库管理员……		
2					

附 录 E

（资料性）

能源企业数据安全风险评估报告示例

E.1 能源企业数据安全风险评估报告示例

能源企业数据安全风险评估报告

评估单位（盖章）：

报告时间： 年 月 日

能源企业数据安全风险评估报告

一、评估概述

1.1 评估目的

1.2 评估依据

1.3 评估对象和范围

说明评估对象的选择原则，描述评估对象和评估范围。

1.4 评估结论概要

说明数据和数据处理活动的概要情况，评估结果概要。

二、评估工作开展情况

2.1 评估人员情况

说明评估工作组织和评估团队人员情况，被评估方参与人员情况。

2.2 评估时间安排情况

说明本次评估工作的时间进度安排，描述各阶段完成的任务、工作成果和时间节点等内容。

2.3 评估工具和环境情况

说明使用的评估工具，接入的网络或系统环境、技术测试内容等情况。

三、信息调研情况

说明数据安全风险评估调研情况。

3.1 企业基本情况

说明数据处理者的机构实体基本情况。

3.2 信息系统情况

说明主营业务、信息系统、App 和网络拓扑等情况。

3.3 数据资产情况

说明数据资产、数据分类分级，涉及个人信息、重要数据、核心数据目录等情况。

3.4 数据处理活动情况

说明数据收集、数据存储、数据使用、数据加工、数据传输、数据共享、数据公开、数据删除、数据出境情况。

针对评估对象结合实际情况画出数据流转图。

3.5 安全措施情况

说明已开展的安全测评认证和核实情况，数据安全管理机构、人员及制度情况，网络和数据安全主要措施。

四、数据安全风险识别

从数据安全管理、技术、处理活动、个人信息保护等方面，说明各评估对象的风险隐患或安全问题，如有必要可附上关键证据材料。

4.1 数据安全管理风险识别

4.2 数据安全技术风险识别

4.3 数据处理活动风险识别

4.4 个人信息处理风险识别

五、风险分析与评价

针对本报告发现的问题隐患，参考附录 C 分析数据安全风险，提出整改建议。具体风险分析和评价方法，可参考数据安全风险评估方法国家标准。

5.1 风险分析与评价

5.2 整改建议

附录 XX

附录可给出完整的数据安全风险源清单，根据实际需要提供评估底稿，或者补充相应的证据材料等。

参 考 文 献

[1]GB/T 20984—2022 信息安全技术 信息安全风险评估方法

[2]GB/T 35273—2020 信息安全技术 个人信息安全规范

[3]GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

[4]GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

[5]JR/T 0223—2021 金融数据安全 数据生命周期安全规范

[6]YD/T 3801—2020 电信网和互联网数据安全风险评估实施方法

[7]T/JSIA 0001—2022 能源大数据 数据分类分级指南

[8]中华人民共和国数据安全法（2021年6月10日中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过）

[9]中华人民共和国个人信息保护法（2021年8月20日中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议通过）

[10]中华人民共和国网络安全法（2016年11月7日中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过）

[11]《App违法违规收集使用个人信息认定方法》（2019年11月28日国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、市场监管总局办公厅联合印发）

[12]《常见类型移动互联网应用程序必要个人信息范围规定》（2021年3月12日国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、市场监管总局办公厅联合印发）

[13]《电力行业网络安全管理办法》（国能发安全规〔2022〕100号）

[14]南方电网《数据安全风险评估工作指引》（办数字〔2023〕25号附件1）