

SZSD

数 字 山 东 工 程 标 准

SZSD 0068—2024

数据安全评估规范

data security management evaluation specification

2024 - 04 - 15 发布

2024 - 06 - 01 实施

山东省大数据局 发 布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 评估流程 2

 4.1 评估启动条件 2

 4.2 评估准备阶段 3

 4.3 方案编制阶段 3

 4.4 现场评估阶段 3

 4.5 报告编制阶段 4

5 基础性评估 4

 5.1 数据识别 4

 5.2 分类分级 4

 5.3 风险防控 5

 5.4 审计追溯 5

6 数据安全技术防护评估 5

 6.1 数据收集 5

 6.2 数据存储 6

 6.3 数据使用 6

 6.4 数据加工 6

 6.5 数据传输 6

 6.6 数据提供 7

 6.7 数据公开 7

 6.8 信息发送 7

 6.9 个人信息处理 7

 6.10 投诉举报处理 8

 6.11 访问控制与审计 8

 6.12 数据删除、匿名化处理 8

7 数据安全运行管理评估 8

 7.1 数据安全责任人 8

 7.2 人力资源保障与考核 9

 7.3 事件应急处置 9

 7.4 体系资质 9

8 评估方法 10

 8.1 访谈 10

 8.2 核查 10

 8.3 测试 10

8.4 专家评审..... 10

9 评估报告..... 10

附录 A（资料性） 数据安全评估指标 11

附录 B（资料性） 数据安全评估报告模板..... 15

参考文献..... 17

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。

本文件由山东省大数据协会提出。

本文件由山东省大数据局归口并组织实施。

本文件起草单位：山东省大数据协会、山东中创软件工程股份有限公司、山东高速信息集团有限公司、北明成功软件（山东）有限公司、烟台东方智能技术有限公司、山东铁路投资控股集团有限公司、青岛盈康一生控股有限公司、山东完途数据技术有限公司、盈康生命科技股份有限公司、万链指数（青岛）信息科技有限公司、青岛场外市场清算中心有限公司、青岛巨商汇网络科技有限公司。

本文件主要起草人：卢钦刚、梁声新、简文鹏、范正翔、张朝伦、刘婷、赵子钰、王乐凯、李嵩、王德建、张青、彭寿钧、李杰、宋增磊、程龙、郑虎刚、乔庆学、吕海涛、陈美洁、王仕林、李琛琛、冯伟、张磊、孙剑、陈文芳。

本文件为首次制定。

数据安全评估规范

1 范围

本文件规定了数据安全评估的评估流程、基础性评估、数据安全技术防护评估、数据安全运行管理评估、评估方法、评估报告等内容。

本文件适用于网络运营者、第三方评估机构等进行数据安全评估工作，为监管部门进行数据安全评估提供参考。

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 5271.1-2000 信息技术 词汇 第1部分：基本术语
GB/T 20984-2022 信息安全技术 信息安全风险评估方法
GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
GB/T 25069-2022 信息技术 术语
GB/T 33770.2-2019 信息技术服务 外包 第2部分：数据保护要求
GB/T 35273-2020 信息安全技术 个人信息安全规范
GB/T 41479-2022 信息安全技术 网络数据处理安全要求
ISO/IEC 27001:2013 信息技术 安全技术 信息安全管理体系 要求

3 术语和定义

GB/T 25069-2022、GB/T 35273-2020、GB/T 41479-2022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。

[来源：GB/T 41479-2022，定义3.1]

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。

[来源：GB/T 41479-2022，定义3.4]

3.3

数据处理 data processing

数据操作的系统执行。

[来源：GB/T 5271.1-2000，定义01.01.06]

3.4

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：GB/T 41479-2022，定义3.5]

3.5

个人信息 personal information

以电子或者其他方式记录的与已识别或者可以识别自然人有关的各种信息。

注1：个人信息包括姓名、出生日期、公民身份号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和內容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：不包括匿名化处理后的信息。

[来源: GB/T 41479-2022, 定义3.6]

3.6

敏感个人信息 sensitive personal information

一旦泄露或者非法使用, 容易导致自然人的尊严受到侵害或者人身、财产安全受到危害的个人信息。

注: 敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息, 以及不满十四周岁未成年人的个人信息。

[来源: GB/T 41479-2022, 定义3.7]

3.7

个人信息主体 personal information subject

个人信息已识别或者可识别的自然人。

[来源: GB/T 41479-2022, 定义3.8]

3.8

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, 定义3.9]

3.9

私人信息 private information

个人发送给特定对象不可转发给其他人的信息。

[来源: GB/T 41479-2022, 定义3.10]

3.10

数据接收方 data receiver

数据处理中接收数据的组织或者个人。

[来源: GB/T 41479-2022, 定义3.11]

3.11

匿名化 anonymization

个人信息经过处理无法识别特定自然人且不能复原的过程。

[来源: GB/T 41479-2022, 定义3.13]

3.12

数据脱敏 data desensitization

对某些敏感信息通过一定规则进行数据的变形, 实现敏感隐私数据的可靠保护。

[来源: YD/T 3802-2020, 定义3.1.14]

4 评估流程

4.1 评估启动条件

对数据收集、存储、使用、加工、传输、提供、公开等处理活动的安全技术和管理评估, 应满足下列情形:

- a) 网络运营者开拓新的具有收集、使用用户个人信息功能的业务, 或设计开发新的存储用户个人信息和核心网络数据的业务支撑系统时, 应开展数据安全评估;
- b) 网络运营者验收新的存储用户个人信息和核心网络数据的业务支撑系统时, 应开展数据安全评估;
- c) 网络运营者运营具有收集、使用用户个人信息功能的业务, 或存储用户个人信息和核心网络数据的业务支撑系统时, 应定期开展数据安全评估;
- d) 业务运营阶段, 在数据承载环境发生较大变化时开展评估, 如数据采集渠道变更、数据存储系统升级改造、数据处理技术变更等;
- e) 网络运营者应在开展数据重要操作 (如开放数据对外接口、数据共享、数据转移、数据加工、数据出境等) 前对涉及到的数据相关管理措施、技术措施开展评估;

- f) 业务运营阶段，在管理责任主体变更时，应开展数据安全评估；
- g) 行业主管部门要求网络运营者进行周期性数据安全评估的，应定期开展数据安全评估；
- h) 在遇到客户严重投诉或发生重大网络安全事件后，应开展数据安全评估；
- i) 满足国家法律法规有关情形时，应开展数据安全评估。

4.2 评估准备阶段

4.2.1 工作启动

评估机构根据委托评估协议书，组建数据安全评估项目组，包括评估管理单位、责任单位、开发运营单位，编制项目计划书，收集被评估单位及评估对象的基本情况。

4.2.2 信息收集和分析

评估机构通过查阅评估对象提交的资料(可使用填写调研表的方式)，收集被评估单位的管理架构、技术体系、数据构成、数据安全管理制度、数据安全设备部署等情况。

4.2.3 工具和表单准备

评估项目组成员应根据评估对象有针对性的准备评估工具(包括：漏洞扫描工具、渗透测试工具、性能测试工具、协议分析工具等)，准备评估所需表单模板(包括：风险告知书、会议记录表单、会议签到表、评估调研表单等)。

4.3 方案编制阶段

4.3.1 评估对象确定

分析被评估单位的业务及流程，确定评估对象的名称、存储信息、用途、管理人员等信息，以及本次评估中数据涉及的生命周期阶段和各阶段涉及的应用、系统、平台范围。

注：数据评估对象可以为具有收集、使用用户个人信息功能的业务，涉及存储用户个人信息和核心网络数据的业务支撑系统等，例如，评估范围可界定为行业热点业务、业务支撑网运营管理系统、大数据分析系统等。

4.3.2 评估工具确定

使用评估工具开展必要测试，评估工具包括但不限于：漏洞扫描工具、渗透测试工具、协议分析工具等。

4.3.3 评估指导书编制

参照GB/T 41479第4章内容明确的评估内容以及附录A，编制数据安全评估指导书，包括评估项、评估方法、操作步骤和预期结果等内容。

4.3.4 评估方案编制

根据评估对象相关情况，拟定评估工作计划，编制评估方案，评估方案应包括但不限于以下内容：项目概述、评估对象、评估内容、评估依据标准、评估工具及方法等。

4.4 现场评估阶段

4.4.1 现场评估准备

评估相关方确认现场评估需要的各种资源，包括评估配合人员、相关表格和文件、评估环境等。确认评估对象中的关键数据已经进行了备份。

4.4.2 现场评估实施和结果记录

评估人员根据评估指导书实施现场评估工作，获取相关证据和信息，形成评估结果，并对评估项是否符合评估标准进行判定。

注：现场评估结束后，评估人员与评估配合人员须及时确认评估工作是否对评估对象及所在系统产生负面影响。

4.4.3 结果确认和资料归还

将评估过程中得到的证据记录进行确认，并将评估过程中借阅的文档归还。

4.5 报告编制阶段

4.5.1 数据安全基本情况

对被评估单位的基本情况简要描述，根据现场评估阶段获取的评估证据信息，从数据安全基础、数据安全技术防护、数据安全运行管理三方面，对评估对象的数据安全管理现状进行概况总结，重点描述被评估单位已采取的安全保障措施。

4.5.2 数据安全管理评估流程及内容

对数据安全管理评估工作的组织开展情况进行概括性总结，包括评估人员组成、评估依据、评估流程、评估工作内容等。

4.5.3 问题总结

对数据安全管理评估工作中得出的问题进行总结，指出评估对象目前存在的安全问题隐患，分析可能对评估对象、被评估单位、社会及国家造成的安全危害。

4.5.4 整改建议

针对评估对象可能面临的所有安全风险，根据数据安全管理相关标准、规范要求，结合被评估单位目前已采取的安全保障措施，提出合理、可行的风险规避及改进建议。

4.5.5 评估报告编制

形成数据安全管理评估报告。数据安全管理评估报告格式应符合附录B，内容应包括但不限于以下组成部分：

- a) 概述，包括被评估网络运营者数据安全管理情况、被评估业务或系统平台具体功能及数据安全情况等；
- b) 数据安全管理评估内容流程，包括评估人员组成、评估依据、评估过程、评估工作主要内容和相关事项等；
- c) 问题总结，根据评估结论梳理评估指标项中不合规项，指出数据安全中存在的问题；
- d) 整改建议，依据存在问题逐项提出针对性整改建议；
- e) 结果确认及签字(建议盖章)。

5 基础性评估

5.1 数据识别

5.1.1 评估依据

应符合GB/T 41479-2022中4.1的相关要求。

5.1.2 评估内容

查验网络运营者是否能够正确识别数据安全中涉及的数据，包括个人信息、重要数据和其他数据，形成数据保护目录，并及时更新。

5.2 分类分级

5.2.1 评估依据

应符合GB/T 41479-2022中4.2的相关要求。

5.2.2 评估内容

查验网络运营者是否按照相关国家标准，根据合同规定和业务运营需要，对所识别的数据进行分类分级管理。

5.3 风险防控

5.3.1 评估依据

应符合GB/T 41479-2022中4.3的相关要求。

5.3.2 评估内容

5.3.2.1 查验网络运营者开展数据处理时，是否按照合同约定履行数据安全保护义务，开展数据处理活动时是否加强风险监测，发现数据安全缺陷、漏洞等风险时，是否采取加密、脱敏、备份、访问控制、审计等技术或者其他必要措施，加强数据安全防护，保护数据免受露、窃取、篡改、损毁、不正当使用等。

5.3.2.2 查验网络运营者是否对重要数据和敏感个人信息进行重点保护，是否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风险评估报告。风险评估报告应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。

5.3.2.3 查验网络运营者是否建立了数据安全管理和评价考核制度，制定数据安全保护计划，开展安全风险评估，及时处置安全事件，组织开展教育培训。

5.4 审计追溯

5.4.1 评估依据

应符合GB/T 41479-2022中4.4的相关要求。

5.4.2 评估内容

查验网络运营者是否对数据处理的全生存周期进行记录，确保数据处理可审计、可追溯。

6 数据安全技术防护评估

6.1 数据收集

6.1.1 评估依据

应符合GB/T 41479-2022中5.2的相关要求。

6.1.2 评估内容

查验网络运营者为提供服务而必需处理个人信息时是否遵循合法、正当、必要的原则，是否收集与其提供的服务无直接或无合理关联，或超出个人信息主体明示同意期限的个人信息。具体内容如下：

a) 是否制定和公开个人信息保护策并严格遵守，个人信息保护政策是否符合 GB/T 35273-2020 中 5.5 要求；

b) 收集个人信息前，是否明示个人信息保护政策，并征得个人信息主体同意；

注：GB/T 35273-2020 中5.6 规定的情形除外。

c) 改变处理个人信息的目的、类型、范围、用途的，是否及时告知个人信息主体，修改个人信息保护政策，并重新征得个人信息主体同意，涉及个人信息保护政策变动的是否修改个人信息保护政策；

d) 是否明示所提供产品或服务的类型，以及该产品或服务所必需的个人信息，不应因用户不同意或撤回同意，提供该产品或服务所必需个人信息以外的信息，而拒绝提供该产品或服务；

e) 是否仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为目的，强制要求、误导用户同意收集个人信息；

f) 收集敏感个人信息前，是否取得个人信息主体的单独同意，确保单独同意是在完全知情的基础上自主给出的、具体的清晰明确的意愿表示；

g) 收集不满十四周岁未成年人个人信息前，是否取得未成人的父母或其他监护人的单独同意；

h) 从个人信息主体以外的其他途径获得个人信息的，是否了解个人信息来源、个人信息提供方已获得的个人信息处理授权同意范围，并按照本文件的要求履行安全保护义务。

6.2 数据存储

6.2.1 评估依据

应符合GB/T 41479-2022中5.3的相关要求。

6.2.2 评估内容

6.2.2.1 查验网络运营者是否对数据存储活动采取安全措施，包括：

- a) 存储重要数据和个人信息等敏感网络数据，是否采用加密、安全存储、访问控制、安全审计等安全措施；
- b) 存储重要数据和个人信息，是否超过与重要数据和个人信息主体约定的存储期限或个人信息主体授权同意有效期；
- c) 存储个人生物特征识别信息的，是否遵守 GB/T 35273-2020 中 6.3 b)的要求及生物特征识别信息保护相关国家标准要求。

6.2.2.2 数据接收方存储数据时，是否按要求采取安全措施并以合同进行约定。

6.3 数据使用

6.3.1 评估依据

应符合GB/T 41479-2022中5.4的相关要求。

6.3.2 评估内容

6.3.2.1 定向推送及信息合成

查验网络运营者在为用户提供定向推送或信息合成服务时是否满足以下要求：

- a) 网络运营者利用个人信息和算法为用户提供定向推送信息服务时，是否提供了非定向推送信息的服务选项；
- b) 在向个人信息主体提供新闻、博客类信息服务的过程中，网络运营者利用算法自动合成文字图片、音视频等信息时，是否明确告知了用户。

6.3.2.2 第三方应用管理

网络运营者是否对接入或入其产品或服务的第三方应用加强了数据安全保护管理，包括：

- a) 是否通过合同等形式明确双方的数据安全保护责任和义务；
- b) 是否监督第三方应用运营者加强数据安全保护管理，发现第三方应用没有落实安全管理责任的，是否及时督促整改，必要时停止接入；
- c) 网络运营者知道或者应知道第三方应用利用其平台侵害用户民事权益时，是否采取必要措施；
- d) 是否对接入或嵌入的第三方应用开展技术检测，确保其数据处理行为符合双方约定要求，对审计发现超出双方约定的行为及时停止接入。

6.4 数据加工

6.4.1 评估依据

应符合GB/T 41479-2022中5.5的相关要求。

6.4.2 评估内容

网络运营者在开展转换、汇聚、分析等数据加工活动的过程中，是否存在可能危害国家安全公共安全、经济安全和社会稳定的情况。

6.5 数据传输

6.5.1 评估依据

应符合GB/T 41479-2020中5.6的相关要求。

6.5.2 评估内容

网络运营者是否对数据传输活动采取安全措施，包括但不限于：

- a) 传输重要数据和敏感个人信息时，是否采用加密脱敏等安全措施；
- b) 向数据接收方传输数据时，是否按要求采取安全措施并以合同进行约定。

6.6 数据提供

6.6.1 评估依据

应符合GB/T 41479-2020中5.7的相关要求。

6.6.2 评估内容

6.6.2.1 向他人提供

网络运营者向他人提供数据前，是否进行了安全影响分析和风险评估，可能危害国家安全、公共安全、经济安全和社会稳定的，不应向他人提供。要求如下：

- a) 向他人提供个人信息，是否向个人信息主体告知接收方的名称、联系方式、处理目的、处理方式、个人信息的种类、存储期限，并取得个人信息主体同意；
- b) 共享、转让重要数据，是否与数据接收方通过合同等形式明确双方的数据安全保护责任和义务，采取加密、脱敏等措施保障重要数据安全；
- c) 委托第三方开展数据处理活动的，是否通过合同等形式明确约定委托处理的目的期限处理方式、数据的种类、保护措施、双方的权利和义务，以及第三方返还或删除数据的方式等，要求第三方以合同中约定的形式返还、删除接收和产生的数据，并对数据处理活动进行监督；
- d) 发生收购、兼并、重组、破产时，数据接收方是否继续履行了相关数据安全保护义务；没有数据接收方的，是否删除了数据。

6.6.2.2 数据出境

数据出境要求如下：

- 网络运营者向境外提供个人信息或者重要数据的，是否遵循国家相关规定和相关标准的要求；
- 境内用户在境内访问境内网络的，其流量是否路由至境外。

6.7 数据公开

6.7.1 评估依据

应符合GB/T 41479-2020中5.8的相关要求。

6.7.2 评估内容

网络运营者利用所掌握的数据资源，公开市场预测、统计等信息时，是否危害了国家安全、公共安全、经济安全和社会稳定。

6.8 信息发送

6.8.1 评估依据

应符合GB/T 41479-2020中5.9的相关要求。

6.8.2 评估内容

即时通信等社交平台运营者是否为用户提供发送私人信息和可转发信息的选项，并按照以下方式处理：

- a) 是否对以私人选项发送的信息予以严格保护，不提供转发功能；
- b) 是否对以可转发选项发送的信息，或者转发此类信息的，同时发送信息始发者在该平台上的账号名称，该账号名称唯一且不可更改。

6.9 个人信息处理

6.9.1 评估依据

应符合GB/T 41479-2020中5.10的相关要求。

6.9.2 评估内容

网络运营者是否建立渠道和机制，及时响应个人信息主体查阅、复制、更正、删除其个人信息及注销账号的请求，是否对请求设置不合理条件，是否遵守GB/T 35273-2020中8.7有关响应个人信息主体请求的要求。

6.10 投诉举报处理

6.10.1 评估依据

应符合GB/T 41479-2020中5.11的相关要求。

6.10.2 评估内容

投诉、举报受理处置应评估以下内容：

- 网络运营者是否建立投诉、举报受理处置制度；
- 收到通过其平台编造、传播虚假信息，发布侵害他人名誉、隐私、知识产权和其他合法权益信息，以及假冒、仿冒、盗用他人名义发布信息的投诉、举报的，自接受投诉举报起，受理时间是否超过3天；
- 受理后是否进行调查取证，对于查实的编造、传播虚假信息，发布侵害他人名誉、隐私、知识产权和其他合法权益信息，以及假冒、仿冒、盗用他人名义发布信息的投诉、举报，是否依法采取停止传输、消除等处置措施。

6.11 访问控制与审计

6.11.1 评估依据

应符合GB/T 41479-2020中5.12的相关要求。

6.11.2 评估内容

查验网络运营者开展数据处理活动时，是否采取以下措施：

- 是否基于数据分类分级，明确相关人员的访问权限，防止非授权访问；
- 对重要数据、个人信息的关键操作（例如批量修改、拷贝、删除、下载等），是否设置内部审批和审计流程，并严格执行。

6.12 数据删除、匿名化处理

6.12.1 评估依据

应符合GB/T 41479-2020中5.13的相关要求。

6.12.2 评估内容

6.12.2.1 符合GB/T 35273-2020中8.3的要求或符合下情形时，网络运营者是否及时对个人信息做删除或匿名化处理：

- 个人信息超出双定期限；
- 网络产品和服务停止运营；
- 个人信息主体注销账号，或者当用户撤回同意。

6.12.2.2 存储重要数据和个人信息的介质进行报废处理时，网络运营者是否采用物理损毁等方式销毁介质，以确保重要数据和个人信息不能被恢复。

7 数据安全运行管理评估

7.1 数据安全责任人

7.1.1 评估依据

应符合GB/T 41479-2020中6.1的要求。

7.1.2 评估内容

网络运营者开展经营和服务活动，处理重要数据和敏感个人信息的，是否明确数据安全责任人，并为其提供必要的资源保障，保证其独立履行职责。数据安全责任人是否具备数据安全专业知识和相关管理工作经历，参与有关数据处的重要决策，履行以下职责：

- 是否组织确定数据保护目录，制定数据安全保护计划并督促落实；
- 是否组织开展数据安全影响分析和风险评估，督促整改安全隐患；
- 是否依法向有关部门报告数据安全保护和事件处置情况；
- 是否组织受理和处置数据安全投诉、举报。

7.2 人力资源保障与考核

7.2.1 评估依据

应符合GB/T 41479-2020中6.2的相关要求。

7.2.2 评估内容

在人力资源保障与考核方面，网络运营者是否满足以下内容：

- 是否明确数据安全保护岗位及职责，并提供人力资源保障；
- 是否建立人力资源考核制度，明确数据安全考核指标和问责机制，对相关人员特别是重要岗位人员的履职情况是否进行考核。出现数据安全重大事件时，是否对直接负责的主管人员和其他直接责任人员进行问责。

7.3 事件应急处置

7.3.1 评估依据

应符合GB/T 41479-2020中6.3的相关要求。

7.3.2 评估内容

7.3.2.1 网络运营者是否建立数据安全事件应急响应机制，并根据数据安全计划的变化而及时调整，确保数据安全事件得到及时有效处置。

——应急响应机制是否包括：

- 数据安全事件分级，
- 启动条件，
- 启动所需的资源，如人员、设备、场所、工具、资金等，
- 流程、人员安排和操作手册；

——是否配备应急响应所需的资源，确保应急响应机制能够有效实施；

——是否制定应急演练计划，按计划或者在应急响应机制发生变化后，组织开展应急演练，检验和完善应急响应机制，提高实战能力。

7.3.2.2 发生数据安全事件时，网络运营者是否立即启动应急响应机制，采取相应的补救和防范措施。涉及个人信息的，是否及时以电话、短信、邮件或者信函等方式告知个人信息主体，同时对可能危害国家安全、公共安全、经济安全和社会稳定的按相关要求向有关部门报告。

7.4 体系资质

7.4.1 评估依据

数据和信息安全应符合GB/T 22239-2019、GB/T 20984-2022、ISO/IEC 27001:2013等相关标准的要求。

7.4.2 评估内容

网络运营者是否按GB/T 22239-2019和GB/T 20984-2022定期开展等级保护测评和信息安全风险评估，网络运营者是否获得信息安全管理体制资质，信息安全管理体制建设是否按照ISO/IEC 27001组织实施。

8 评估方法

8.1 访谈

评测人员与网络运营者相关人员（个人、群体）进行交流、讨论等活动，获取相关证据，了解与评估项相关的信息。

8.2 核查

8.2.1 文档审查

核查与数据安全治理评估内容相关的制度、策略、方针、计划、操作规程、记录文档等证明性文档是否齐备，本文件第7章中的各要素是否齐全。

8.2.2 现场观察

根据评估对象的实际情况，评估人员到达数据处理现场通过实地观察人员行为、技术设施和物理环境状况判断数据处理人员的安全意识、业务操作、管理程序、系统物理环境等方面的安全情况，参照附录A，评估其是否符合本文件第7章的相关要求。

8.2.3 配置核查

利用上机验证的方式核查应用系统、主机系统、数据库系统以及各设备的配置是否正确，是否与文档、相关设备和部件保持一致，并如实记录核查结果。

8.3 测试

8.3.1 根据评估指导书，利用技术工具对评估范围内的目标系统进行测试，包括基于网络探测和基于设备扫描的漏洞测试、渗透测试、功能测试、性能测试、入侵检测、协议分析等。

8.3.2 备份测试结果。

8.4 专家评审

报告编制阶段召开专家评审会，对评估实施过程及评估意见、评估整改落实情况进行核验，确认评估网络运营者或评估对象是否已经配套数据安全治理措施和数据安全技术措施，满足数据安全基线要求等。

9 评估报告

根据评估情况出具数据安全治理评估报告，评估报告模板见附录B。

附 录 A
(资料性)
数据安全评估指标

数据安全评估指标如下表A. 1所示。

表A. 1 数据安全评估指标

序号	评估项	评估指标	评估要点	指标说明
1	基础性评估	数据识别	数据识别准确性	正确识别数据安全评估中涉及的数据，包括个人信息、重要数据和其他数据。
2			数据保护目录	数据保护目录形成并及时更新。
3		分类分级	一致性	是否按照相关国家标准，根据合同规定和业务运营需要。
4			分类分级管理台账	是否有数据分类分级管理台账。
5		风险防控	风险监测和防控措施	网络运营者开展数据处理时，是否按照合同约定履行数据安全保护义务，开展数据处理活动时是否加强风险监测，发现数据安全缺陷、漏洞等风险时，是否采取加密、脱敏、备份、访问控制、审计等技术或者其他必要措施，加强数据安全防护，保护数据免受露、窃取、篡改、损毁、不正当使用等。
6			重要数据和敏感个人信息重点保护	网络运营者是否对重要数据和敏感个人信息进行重点保护，是否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风险评估报告。风险评估报告应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。
7			数据安全管理和评价考核制度	网络运营者是否建立了数据安全管理和评价考核制度，制定数据安全保护计划，开展安全风险评估，及时处置安全事件，组织开展教育培训。
8		审计追溯	数据处理全生命周期记录	是否有数据处理全生命周期记录相关文件。
9	数据安全技 术防护评估	数据收集	个人信息保护政策	是否制定和公开个人信息保护策并严格遵守，个人信息保护政策是否符合 GB/T 35273-2020中5.5要求；是否明示个人信息保护政策；涉及个人信息保护政策变动的是否修改个人信息保护政策；是否明示所提供产品或服务的类型，以及该产品或服务所必需的个人信息，不应因用户不同意或撤回同意，提供该产品或服务所必需个人信息以外的信息，而拒绝提供该产品或服务；是否仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为目的，强制要求、误导用户同意收集个人信息。
10			个人信息收集记录	是否收集与其提供的服务无直接或无合理关联，或超出个人信息主体明示同意期限的个人信息。
11			个人信息主体知情情况	收集个人信息前，是否明示个人信息保护政策，并征得个人信息主体同意，改变处理个人信息的目的、类型、范围、用途的，是否及时告知个人信息主体，修改个人信息保护政策，并重新征得个人信息主体同意；收集敏感个人信息前，是否取得个人信息主体的单独同意，确保单独同

序号	评估项	评估指标	评估要点	指标说明
				意是在完全知情的基础上自主给出的、具体的清晰明确的意愿表示；收集不满十四周岁未成年人个人信息前，是否取得未成人的父母或其他监护人的单独同意。
12			个人信息获取途径	从个人信息主体以外的其他途径获得个人信息的，是否了解个人信息来源、个人信息提供方已获得的个人信息处理授权同意范围，并按照本文件的要求履行安全保护义务。
13		数据存储	数据存储安全措施	存储重要数据和个人信息等敏感网络数据，是否采用加密、安全存储、访问控制、安全审计等安全措施。
14			数据存储有效期	存储重要数据和个人信息，是否超过与重要数据和个人信息主体约定的存储期限或个人信息主体授权同意有效期。
15			个人生物特征识别信息存储	是否遵守 GB/T 35273-2020 中 6.3 b) 的要求及生物特征识别信息保护相关国家标准要求。
16			数据接收方约定	数据接收方存储数据时，是否按要求采取安全措施并以合同进行约定。
17		数据使用	定向推送或信息合成服务	网络运营者利用个人信息和算法为用户提供定向推送信息服务时，是否提供了非定向推送信息的服务选项；在向个人信息主体提供新闻、博客类信息服务的过程中，网络运营者利用算法自动合成文字图片、音视频等信息时，是否明确告知了用户。
18			第三方应用数据安全	是否通过合同等形式明确双方的数据安全保护责任和义务；是否监督第三方应用运营者加强数据安全，发现第三方应用没有落实安全管理责任的，是否及时督促整改，必要时停止接入；网络运营者知道或者应知道第三方应用利用其平台侵害用户民事权益时，是否采取必要措施；是否对接入或嵌入的第三方应用开展技术检测，确保其数据处理行为符合双方约定要求，对审计发现超出双方约定的行为及时停止接入。
19		数据加工	安全威胁情况	网络运营者在开展转换、汇聚、分析等数据加工活动的过程中，是否存在可能危害国家安全公共安全、经济安全和社会稳定的情况。
20		数据传输	内部传输安全保护措施	传输重要数据和敏感个人信息时，是否采用加密脱敏等安全措施。
21			对外传输安全保护措施	向数据接收方传输数据时，是否按要求采取安全措施并以合同进行约定。
22		数据提供	安全影响分析和风险评估	
23			个人信息主体知情情况	向他人提供个人信息，是否向个人信息主体告知接收方的名称、联系方式、处理目的、处理方式、个人信息的种类、存储期限，并取得个人信息主体同意。
24			数据安全保护措施和职责、义务	共享、转让重要数据，是否与数据接收方通过合同等形式明确双方的数据安全保护责任和义务，采取加密、脱敏等措施保障重要数据安全。
25			第三方安全保护措施	委托第三方开展数据处理活动的，是否通过合同等形式明确约定委托处理的目的期限处理方式、数据的种类、保护措施、双方的权利和义务，以及第三方返还或删除数据的方式等，要求第三方以合同中约定的形式返还、删除接收和产生的数据，并对数据处理活动进行监督。
26			数据所有者变更	发生收购、兼并、重组、破产时，数据接收方是否继续履行了相关数据安全保护义务；没有数据接收方的，是否删除了数据。
27			数据出境	网络运营者向境外提供个人信息或者重要数据的，是否遵循国家相关规定和相关标准的要求；境内用户在境内访问境内网络的，其流量是否路由至境外。

序号	评估项	评估指标	评估要点	指标说明
28		数据公开	安全威胁情况	网络运营者利用所掌握的数据资源，公开市场预测、统计等信息时，是否危害了国家安全、公共安全、经济安全和社会稳定。
29		信息发送	私人信息	即时通信等社交平台运营者是否对以私人选项发送的信息予以严格保护，不提供转发功能。
30			可转发信息	即时通信等社交平台运营者是否对以可转发选项发送的信息，或者转发此类信息的，同时发送信息始发者在该平台上的账号名称，该账号名称唯一且不可更改。
31		个人信息处理	个人信息主体请求响应机制	网络运营者是否建立渠道和机制，及时响应个人信息主体查阅、复制、更正、删除其个人信息及注销账号的请求，是否对请求设置不合理条件，是否遵守GB/T 35273-2020中8.7有关响应个人信息主体请求的要求。
32		投诉举报处理	投诉、举报受理处置制度	网络运营者是否建立投诉、举报受理处置制度。
33			投诉、举报受理时限	收到通过其平台编造、传播虚假信息，发布侵害他人名誉、隐私、知识产权和其他合法权益信息，以及假冒、仿冒、盗用他人名义发布信息的投诉、举报的，自接受投诉举报起，受理时间是否超过3d。
34			处置措施	受理后是否进行调查取证，对于查实的编造、传播虚假信息，发布侵害他人名誉、隐私、知识产权和其他合法权益信息，以及假冒、仿冒、盗用他人名义发布信息的投诉、举报，是否依法采取停止传输、消除等处置措施。
35		访问控制与审计	访问权限	是否基于数据分类分级，明确相关人员的访问权限，防止非授权访问。
36			内部审批和审计	对重要数据、个人信息的关键操作(例如批量修改、拷贝、删除、下载等)，是否设置内部审批和审计流程，并严格执行。
37		数据删除、匿名化处理	个人信息超出双方约定期限	
38			网络产品和服务停止运营	
39			账号注销、权限撤回	个人信息主体注销账号，或者当用户撤回同意。
40			存储介质销毁	存储重要数据和个人信息的介质进行报废处理时，网络运营者是否采用物理损毁等方式销毁介质，以确保重要数据和个人信息不能被恢复。
41	数据安全运行管理评估	数据安全责任人	岗位能力	网络运营者开展经营和服务活动，处理重要数据和敏感个人信息的，是否明确数据安全责任人，并为其提供必要的资源保障，保证其独立履行职责。数据安全责任人是否具备数据安全专业知识和相关管理工作经历，参与有关数据处理的重要决策。
42			岗位职责	数据安全责任人是否履行以下职责： 组织确定数据保护目录，制定数据安全保护计划并督促落实； 组织开展数据安全影响分析和风险评估，督促整改安全隐患； 依法向有关部门报告数据安全保护和事件处置情况； 组织受理和处置数据安全投诉、举报。
43		人力资源保障与考核	数据安全保护岗位	是否明确数据安全保护岗位及职责，并提供人力资源保障。
44			人力资源考核制度	是否建立人力资源考核制度，明确数据安全考核指标和问责机制，对相关人员特别是重要岗位人员的履职情况是否进行考核。出现数据安全重大事件时，是否对直接负责的主管人员和其他直接责任人员进行问责。

SZSD 0068—2024

序号	评估项	评估指标	评估要点	指标说明
45		事件应急处置	数据安全事件应急响应机制	应急响应机制是否包括：数据安全事件分级，启动条件，启动所需的资源，如人员、设备、场所、工具、资金等，流程、人员安排和操作手册。
46			配备应急响应所需的资源	是否配备应急响应所需的资源，确保应急响应机制能够有效实施。
47			应急演练计划	是否制定应急演练计划，按计划或者在应急响应机制发生变化后，组织开展应急演练，检验和完善应急响应机制，提高实战能力。
48			数据安全事件处置记录	发生数据安全事件时，网络运营者是否立即启动应急响应机制，采取相应的补救和防范措施。涉及个人信息的，是否及时以电话、短信、邮件或者信函等方式告知个人信息主体，同时对可能危害国家安全、公共安全、经济安全和社会稳定的按相关要求向有关部门报告。
49		体系资质	等级保护测评、信息安全风险评估	按GB/T 22239-2019和GB/T 20984-2022定期开展等级保护测评和信息安全风险评估。
50			信息安全管理体系	应获得信息安全管理体系资质，信息安全管理体系建设按照ISO/IEC 27001组织实施。

附 录 B
(资料性)
数据安全评估报告模板

(封面)

(企业简称) 数据安全评估报告

业务名称: XXX

(企业名称)

年 月 日

1. 业务/平台/企业数据安全管理基本情况

简要描述被评估单位基本情况、评估对象运行环境以及评估对象数据安全现状……

2. 数据安全管理评估内容和流程

描述评估人员组成、评估依据、评估过程、评估工作主要内容和相关事项……

3. 数据安全管理存在的问题

……

4. 整改建议

……

5. 整改落实情况

……

6. 评估结论

……

7. 评估结果签字确认表（需盖章）

……

参 考 文 献

- [1] GB/T 35273-2017 信息安全技术 个人信息安全规范
 - [2] JR/T 0223-2021 金融数据安全 数据生命周期安全规范
 - [3] YD/T 3802-2020 电信网和互联网数据安全通用要求
 - [4] YD/T 3956-2021 电信网和互联网数据安全评估规范
 - [5] DB11/T 1918-2021 政务数据分级与安全保护规范
 - [6] DB33/T 2488-2022 公共数据安全体系评估规范
-