TC260-PG-2023XX

网络安全标准实践指南

—网络数据安全风险评估实施指引

（征求意见稿 v1.0-202304）

全国信息安全标准化技术委员会秘书处

2023 年 4 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

本《实践指南》版权属于信安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国信息安全标准化技术委员会秘书处”。

技术支持单位

本《实践指南》得到中国电子技术标准化研究院、国家信息技术安全研究中心、国家计算机网络应急技术处理协调中心、国家工业信息安全发展研究中心等单位的技术支持。

摘　要

为指导网络数据安全风险评估工作，发现数据安全隐患，防范数据安全风险，依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规，参照数据安全相关国家标准，制定本指南。

网络数据安全风险评估应坚持预防为主、主动发现、积极防范，对数据处理者数据安全保护和数据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措施建议，提升数据安全防攻击、防破坏、防窃取、防泄露、防滥用能力。

本指南给出了网络数据安全风险评估思路、流程和方法，明确了网络数据安全风险评估步骤和工作内容，基于数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面识别、评估安全风险，适用于数据处理者自行开展安全评估或者有关主管部门组织开展检查评估。

目 录

1 范围

本指南提出了网络数据安全风险评估思路、主要工作内容、流程和方法，提出从数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面评估安全风险。

本指南适用于指导数据处理者自行开展风险评估，也可为有关主管监管部门组织开展数据安全检查评估提供参考。

2 术语定义

2.1 网络数据

一般指通过网络收集、存储、传输、处理和产生的各种电子数据，简称“数据”。

2.2 网络数据处理者

在网络数据处理活动中自主决定处理目的和处理方式的个人和组织，以下简称“数据处理者”。

2.3 网络数据安全

通过采取必要措施，确保网络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，简称“数据安全”。

2.4 网络数据安全风险评估

对网络数据安全保护和数据处理活动情况进行风险评估的过程。

2.5 网络数据处理活动

网络数据的收集、存储、使用、加工、传输、提供、公开、删除等活动。

2.6 委托处理

网络数据处理者委托个人、组织按照约定的目的和方式开展的网络数据处理活动。

2.7 共同处理

两个及以上的网络数据处理者共同决定网络数据的处理目的和处理方式的网络数据处理活动。

2.8 单独同意

网络数据处理者在开展具体网络数据处理活动时，对每项个人信息取得个人同意，不包括一次性针对多项个人信息、多种处理活动的同意。

2.9 网络数据安全风险

由于开展网络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、个人合法权益造成的影响。

2.10 合理性

数据处理活动遵守法律、行政法规，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，不得损害个人、组织的合法权益。

2.11 风险隐患

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故的原因、条件、情形或行为。

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。

2.12 安全措施

保护数据资产、抵御安全威胁、减少安全脆弱性、降低数据安全事件的影响，以及打击信息犯罪而实施的各种实践、规程和机制。

2.13 业务

组织为实现某项发展战略而开展的活动，该活动具有明确的目标，并延续一段时间。

2.14 自动化决策

通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

3 风险评估概述

3.1 评估思路

网络数据安全风险评估坚持预防为主、主动发现、积极防范，对数据处理者数据安全保护和数据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，提升数据安全防攻击、防破坏、防窃取、防泄露、防滥用能力。

网络数据安全风险评估的评估思路如图 1 所示。

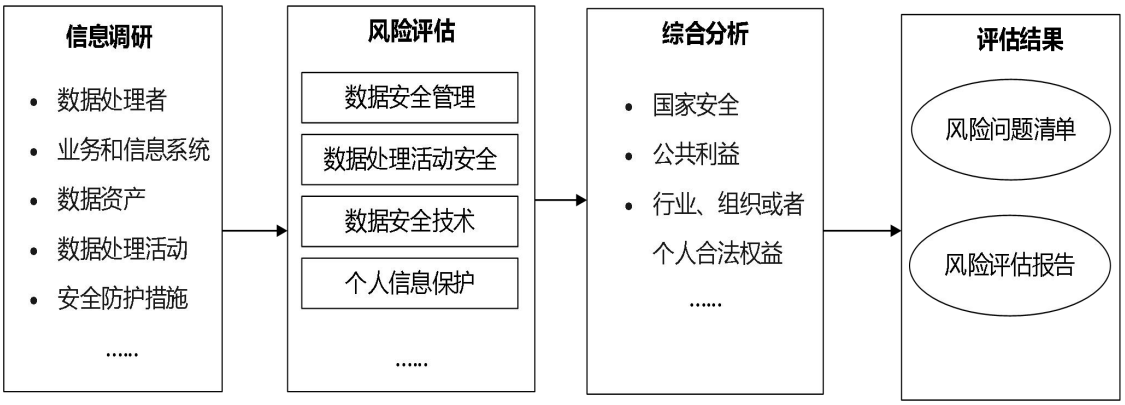

图 1 数据安全风险评估思路示意图

3.2 评估内容

网络数据安全风险评估主要围绕数据安全管理、数据处理活动安全、数据安全技术、个人信息保护等方面开展。评估内容框架如图 2 所示。

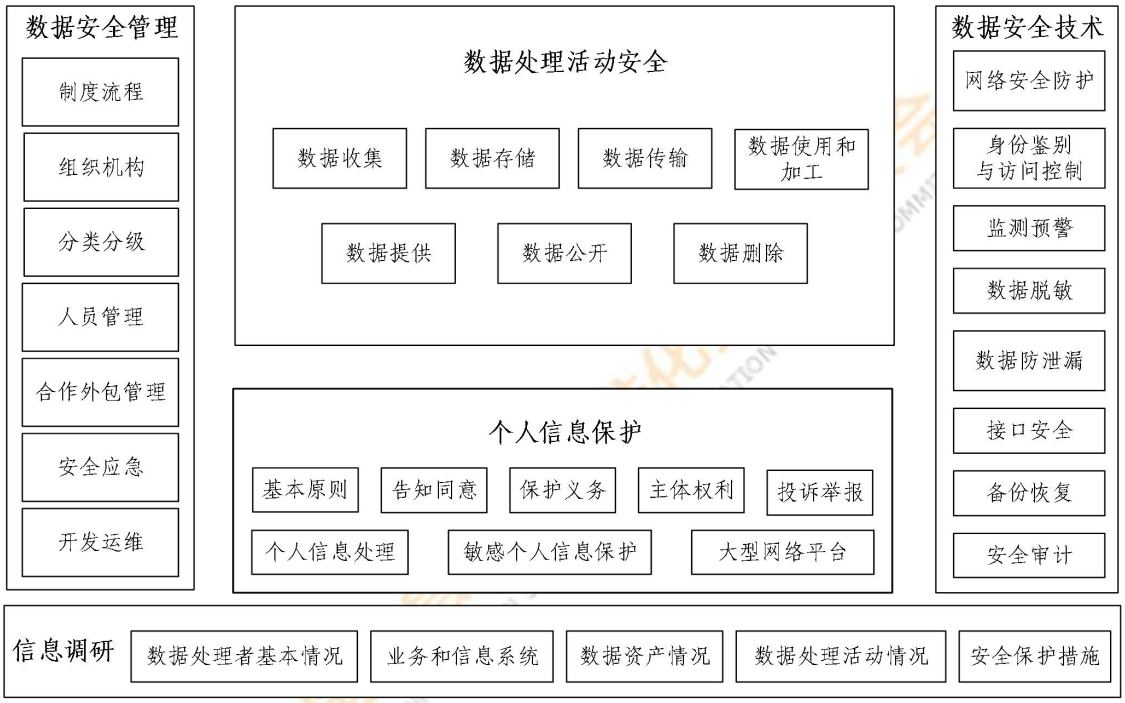

图 2 数据安全风险评估内容框架

3.3 评估流程

数据安全风险评估流程，主要包括评估准备、信息调研、风险评估、综合分析、评估总结五个阶段，评估实施流程如图 3 所示。

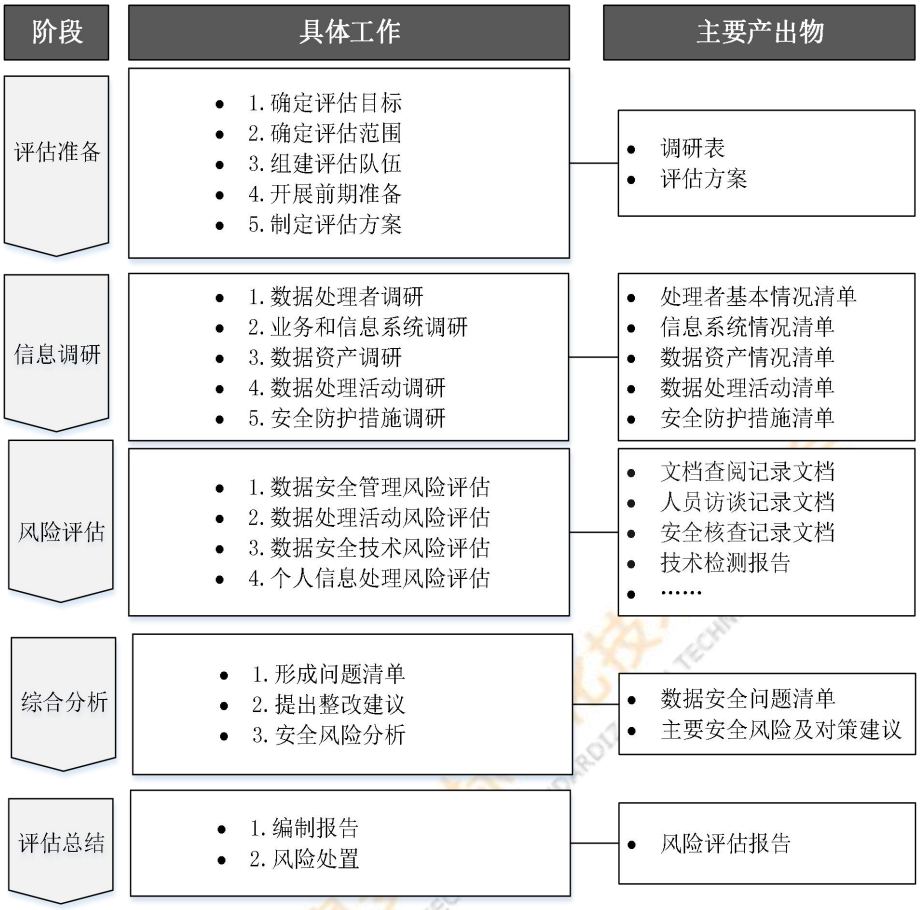

图 3 数据安全风险评估具体工作及主要产出物

数据处理者进行自评估时，可依据本指南进行风险自查，具体实施步骤如图 4 所示。

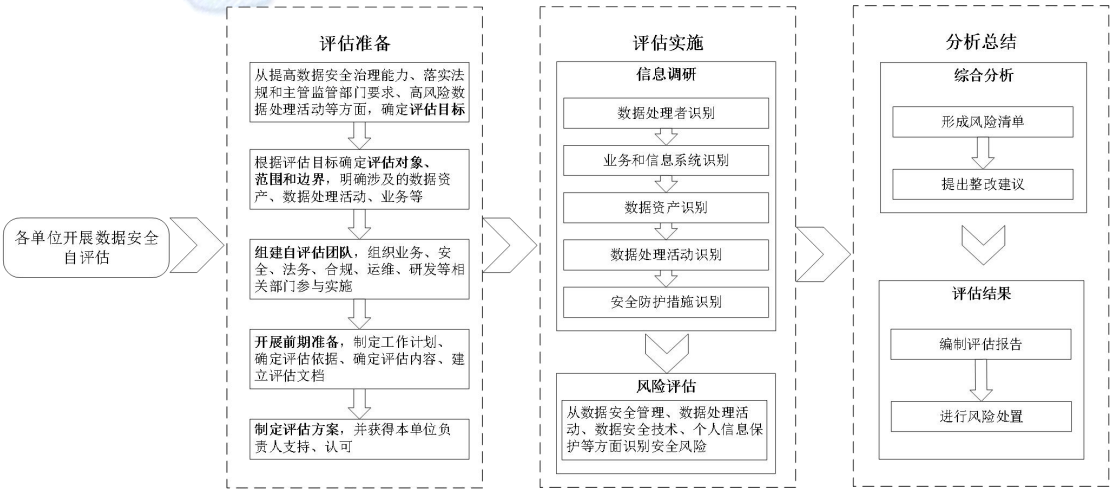

图 4 数据安全风险评估（自评估）实施流程

有关部门进行检查评估时，可参考本指南开展检查工作，具体实施步骤如图 5 所示。

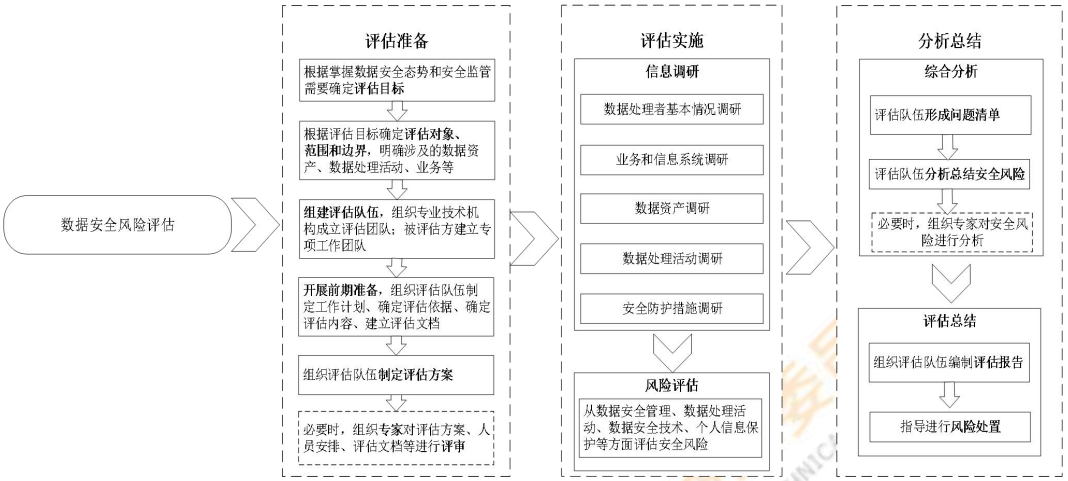

图 5 数据安全风险评估（检查评估）实施流程

3.4 评估手段

开展数据安全风险评估时，综合采取下列手段进行评估:

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。

4 评估准备

4.1 明确评估目标

为落实《数据安全法》《个人信息保护法》等法律法规要求或安

全监管需要，对数据处理者的数据安全管理、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评估，发现存在的安全问题和风险隐患，督促数据处理者健全安全制度、改进安全措施、堵塞安全漏洞，进一步提高数据安全和个人信息保护能力。

数据安全风险评估的目标，包括但不限于:

a）摸清数据种类、规模、分布等基本情况；

b）摸清数据处理活动的情况；

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隐患；

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

e）促进完善数据安全保护措施，提升数据安全保护能力。

4.2 确定评估范围

根据工作需要和评估目标，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、业务和信息系统、人员和内外部组织等。

4.3 组建评估团队

4.3.1 组建检查评估团队

根据评估范围、涉及的行业特征、专业需求，选择具备相关专业能力的评估人员组成评估队伍。评估队伍应提前完成风险评估表格、文档、检测工具等各项准备工作，并签署保密协议。

被评估方应建立专项工作团队，成员一般包括数据安全负责人和安全、法务、合规、运维、研发、业务等部门相关人员。专项工作团队应按照要求做好人员、设备、技术保障等工作，配合开展风险评估。

4.3.2 组建自评估团队

数据处理者自行开展数据安全风险评估时，可组织业务、安全、法务、合规、运维、研发等相关部门参与实施，评估组长由数据安全负责人或授权代表担任，也可委托第三方专业技术机构实施。

4.4 开展前期准备

4.4.1 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队伍按照工作要求制定评估工作计划。

4.4.2 确定评估依据

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》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、团体标准和地方标准。

开展自评估时，本单位数据安全制度规范可作为评估依据之一。

4.4.3 确定评估内容

结合评估目标、范围、依据，针对被评估方的实际情况，确定被评估方适用的评估内容。

a）数据处理者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；

b）涉及处理个人信息的，应在a）的基础上，对个人信息保护开展风险评估。

开展评估工作过程中，可依据任务要求、评估重点、监管需要等，进一步完善评估内容。

4.4.4 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。

4.5 制定评估方案

组织评估队伍编制风险评估工作方案，方案内容包括但不限于：

a）评估概述：包括评估目标、评估范围、评估依据等内容；

b）评估内容和方法：包括评估内容、评估准则、评估方法和评估工具等内容；

c）评估人员：包括评估队伍的组织结构、负责人、成员、职责分工等内容；

d）实施计划：主要包括评估具体实施进度安排、人员安排等内容；

e）工作要求：包括严格依照评估内容及标准规范，规范评估行为，按照尽量不影响被评估方正常工作的原则，制定评估工作应急保障和风险规避措施，并明确告知被评估方评估可能产生的风险，严守工作纪律和保密要求等内容。

评估队伍可邀请行业领域和数据安全、网络安全专家对风险评估方案进行评议，重点评议方案内容、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。

5 信息调研

5.1 数据处理者调研

数据处理者的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）单位性质，例如党政机关、事业单位、企业、社会团体等；

c）是否属于特定类型数据处理者，例如政务数据处理者、大型网络平台运营者、关键信息基础设施运营者等；

d）所属行业领域；

e）业务运营地区，开展数据处理活动所在行政区划等；

f）主要业务范围、业务规模等；

g）数据处理相关服务取得行政许可的情况；

h）被评估单位的资本组成和实际控制人情况；

i）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；

j）对国家安全、公共利益、公民和组织合法权益的影响。

5.2 业务和信息系统调研

业务和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）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。

5.3 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。调研内容包括但不限于:

a）数据资产概况，包括数据总量、数据资产类型、数据库表和字段规模、数据量变化情况、境外存储量、数据分布等;

b）数据分类分级情况，包括分类分级情况、是否符合国家标准和行业管理规范等;

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）其他数据情况。

5.4 数据处理活动调研

被评估方应根据评估范围绘制数据流图，或编制数据处理活动清单，清晰描述数据流转和参与主体情况。

结合被评估的业务、系统和数据资产，由被评估方配合评估队伍梳理数据处理活动清单，摸清数据处理活动，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;

h）数据出境情况，是否存在个人信息或重要数据出境，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。

5.5 安全防护措施调研

安全防护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;

b）数据安全管理机构、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）网络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;

i）3 年内发生的网络和数据安全事件及处置情况。

6 风险评估

6.1 数据安全管理风险

6.1.1 安全管理制度

6.1.1.1 数据安全制度体系

针对数据安全制度体系建设情况，应重点评估:

a）数据安全总体策略、方针、目标和原则制定情况;

b）数据安全管理工作规划或工作方案制定情况;

c）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建设情况;

d）关键岗位的数据安全管理操作规程建设情况;

e）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。

6.1.1.2 数据安全制度落实

针对被评估方数据安全制度落实情况，应重点评估：

a）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；

b）数据安全制度的制定、评审、发布流程建设情况；

c）数据安全制度的定期审核和更新情况；

d）制度发布范围是否覆盖全面，发布方式是否正规、有效；

e）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；

f）制度落实监督检查机制。

针对重要数据处理者，还应当评估以下内容：

a）对数据处理活动定期开展数据安全风险评估的情况；

b）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。

6.1.2 安全组织机构

6.1.2.1 数据安全组织架构

针对被评估方数据安全组织架构建设情况，应重点评估：

a）数据安全管理机构和职能设置情况；

b）数据安全负责人和职能设置情况；

c）单位高层人员参与数据安全决策情况；

d）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;

e）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。

6.1.2.2 数据安全岗位设置

针对被评估方数据安全岗位设置情况，应重点评估:

a）数据库管理员、操作员及安全审计人员、安全运维人员等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;

b）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;

c）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。

6.1.3 分类分级管理

6.1.3.1 数据资产管理

针对数据资产管理情况，应重点评估:

a）数据资产台账建设、更新、维护情况;

b）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、光盘等存储媒体中的数据;

c）通过数据资产管理等工具对数据资产清单及时更新、维护的情况;

d）采用技术手段定期对数据资产进行扫描的情况，及发现识别个人信息、重要数据的能力；

e）服务器、数据库、端口、数据资源在互联网的暴露及管理情况；

f）软硬件资产维护、报废、销毁管理情况等。

6.1.3.2 数据分类分级制度

针对数据分类分级制度建设情况，应重点评估：

a）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；

b）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；

c）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；

d）数据分类分级变更和审核流程情况；

e）个人信息分类分级管理情况。

6.1.3.3 数据分类分级保护

针对数据分类分级保护情况，应重点评估：

a）是否对处理的个人信息和重要数据进行明确标识；

b）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；

c）数据分类分级打标或数据资产管理工具建设情况，是否具有自动化标识能力，是否具有数据标识结果发布、审核等能力；

d）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；

e）按照相关核心数据目录或规定，评估核心数据并进行严格管理的情况。

6.1.4 人员安全管理

6.1.4.1 人员录用

针对人员录用情况，应重点评估：

a）员工录用前背景调查情况；

b）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。

6.1.4.2 保密协议

针对保密协议签订情况，应重点评估：

a）员工工作纪律和工作要求，是否对数据安全相关员工禁止行为有明确规定；

b）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；

c）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。

6.1.4.3 转岗离岗

针对人员转岗离岗管理情况，应重点评估：

a）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;

b）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。

6.1.4.4 数据安全培训

针对人员数据安全培训情况，应重点评估:

a）数据安全培训计划制定、定期更新情况;

b）对全体人员开展数据安全意识教育培训，并保留相关记录情况;

c）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。

6.1.5 合作外包管理

6.1.5.1 合作方管理机制

针对合作方管理机制建设情况，应重点评估:

a）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;

b）是否对数据合作方或外包服务机构的安全能力进行评估;

c）对外包服务机构、人员履行安全责任义务的监督检查情况;

d）外包人员现场服务安全管理情况;

e）对外包服务商的技术依赖程度，对委托处理数据的控制和管理能力。

6.1.5.2 合作协议约束

针对合作协议约束情况，应重点评估:

a）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;

b）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、保密约定及违约责任和处罚条款等;

c）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。

6.1.5.3 外包访问权限

针对外包访问权限管理情况，应重点评估:

a）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;

b）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;

c）外包人员数据导出操作或数据外发操作的监督管理情况;

d）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;

e）数据外包服务账号及访问权限管理情况;

f）外包人员远程访问操作系统或数据的情况。

6.1.5.4 第三方接入与数据回收

针对第三方接入与数据回收情况，应重点评估:

a）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，避免引入木马、后门等;

b）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;

c）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。

6.1.5.5 政务数据委托处理

涉及政务部门或针对法律、法规授权的具有管理公共事务职能的组织委托处理政务数据的情形，应重点评估:

a）委托他人建设、维护电子政务系统，存储、加工政务数据，是否经过严格的批准程序，是否以合同等手段监督受托方履行相应的数据安全保护义务;

b）政务数据受托方依照法律、法规的规定和合同约定履行数据安全保护义务的情况，是否擅自留存、使用、泄露或者向他人提供政务数据;

c）支撑电子政务相关系统运行的相关服务或系统的安全措施，是否满足电子政务系统管理和相关安全要求。

6.1.6 安全应急管理

针对安全应急管理情况，应重点评估:

a）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，明确不同类别事件的处置流程和方法;

b）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;

c）网络和数据安全事件应急演练情况;

d）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;

e）近 3 年发生的数据安全事件处置、记录、整改和上报情况;

f）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;

g）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。

6.1.7 开发运维管理

针对开发运维管理情况，应重点评估:

a）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;

b）开发程序的修改、更新、发布的批准授权和版本控制流程;

c）工程实施、验收、交付的安全管理情况;

d）对开发代码、测试数据的安全管理情况;

e）产品或业务上线前进行安全评估的情况;

f）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;

g）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；

h）对开发和运维人员行为的监督和审计情况；

i）远程运维的审批、管理和安全防护措施；

j）第三方 SDK 或开源软件的中文版运行维护、二次开发等技术资料完备性。

6.1.8 云数据安全

被评估对象使用云计算服务时，应重点评估：

a）专有云部署模式下，与云服务提供商、第三方厂商安全责任划分是否明确、合理；

b）是否明确云数据安全责任划分边界，并履行相应数据安全责任，部署与自身业务安全需求匹配的安全产品；

c）是否对云服务商的运维操作行为进行安全审计。

被评估对象是云计算服务提供方时，应重点评估：

a）公有云、社区云等不同类型云平台间隔离防护情况；

b）租户与云、云数据中心间数据传输安全防护情况；

c）云平台是否明确约定服务相关方数据安全保护角色和职责；

d）针对不同服务模式（IaaS、PaaS、SaaS）、部署模式（公有云、社区云、私有云等）、产品和服务，数据安全责任界面划定情况及合法合规性；

e）责任划分合理性，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;

f）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;

g）云上收集租户数据梳理情况，是否包含对重要数据、个人信息等内容的梳理，收集方式是否安全合理，是否存在超范围收集;

h）云上承载用户个人信息、重要数据情况，是否对重要数据、敏感个人信息实施增强的安全防护;

i）产品安全配置情况，数据安全产品、数据库、网络等产品的配置是否合理，产品基线安全配置、默认安全配置是否合理，是否存在数据泄露风险;

j）第三方组件安全核查、漏洞修复情况，是否及时对第三方组件进行安全核查、对漏洞更新补丁，是否满足云服务商漏洞修复时间要求;

k）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;

l）云平台提供的基础数据安全防护能力是否能提供有效安全防护;

m）是否对用户使用云产品或服务的高危操作进行显著提示，明确说明相关操作可引发的安全风险;

n）对云上租户的账号管理措施的部署情况及安全性;

o）是否设置保障租户数据安全的相关制度规定、安全措施;

p）约定服务到期、欠费、提前终止等情形下，数据返还、删除

等情况;

q）数据备份和恢复机制是否完善，数据备份策略、备份周期、备份存储等是否符合安全需要;

r）承载重要数据的云平台，开展数据安全风险评估工作情况。

6.2 数据处理活动风险

6.2.1 数据收集

6.2.1.1 数据收集合法正当性

针对数据收集合法正当性情况，应重点评估:

a）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;

b）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。

6.2.1.2 通过第三方收集数据

重点评估从外部机构采集数据的安全情况:

a）通过合同协议等合法方式，约定从外部机构采集的数据范围、收集方式、使用目的和授权同意情况;

b）对外部数据源和外部收集数据进行鉴别和记录的情况;

c）数据的真实性及来源的可靠性;

d）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的情况。

6.2.1.3 数据质量控制

针对数据质量控制情况，应重点评估:

a）数据质量管理制度建设情况，对采集数据质量和管理措施是否进行明确要求;

b）安全管理和操作规范对数据清洗、转换和加载等行为是否进行明确要求;

c）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;

d）收集数据监控、过程记录等情况，以及安全措施应用情况;

e）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;

f）对外部数据源和外部收集数据的真实性和可靠性进行鉴别和校验的情况。

6.2.1.4 收集方式

针对数据收集方式，应重点评估:

a）采用自动化工具访问、收集数据的，违反法律、行政法规或者行业自律公约情况，侵犯他人知识产权等合法权益情况;

b）采用自动化工具收集时，对数据收集范围、数量和频率的明确情况，收集与提供服务无关数据的情况;

c）采用自动化工具收集数据以及该方式对网络服务的性能、功能带来的影响情况;

d）通过人工方式采集数据的，是否对数据采集人员严格管理，要求将采集数据直接报送到相关人员或系统，采集任务完成后及时删除采集人员留存的数据。

6.2.1.5 数据收集设备及环境安全

针对数据收集设备及环境安全情况，应重点评估：

a）采集终端数据泄露风险，检测采集终端或设备的安全漏洞，是否存在数据泄露风险；

b）人工采集数据泄露风险，通过人员权限管控、信息碎片化等方式，对人工采集数据环境进行安全管控情况；

c）客户端敏感信息留存风险，检测 App、Web 等客户端完成相关业务后，是否及时对缓存数据进行清理，是否留存敏感个人信息或重要数据。

6.2.2 数据存储

6.2.2.1 数据存储适当性

针对数据存储适当性，应重点评估：

a）数据存储安全策略和操作规程的建设落实情况；

b）存储位置、期限、方式的适当性；

c）永久存储数据类型的必要性；

d）云存储的安全性。

6.2.2.2 逻辑存储安全

针对逻辑存储安全情况，应重点评估：

a）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;

b）检测逻辑存储系统安全漏洞，查看安全漏洞修复、处置情况;

c）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;

d）脱敏后的数据与可用于恢复数据的信息分开存储的情况;

e）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;

f）数据存储在第三方云平台、数据中心等外部区域的安全管理、访问控制情况;

g）根据安全级别、重要性、量级、使用频率等因素，对数据分域分级差异化存储安全管控情况。

6.2.2.3 存储介质安全

针对存储介质安全情况，应重点评估:

a）存储介质（含移动存储介质，下同）的使用、管理及资产标识情况;

b）存储介质安全管理规范建设情况，是否明确对存储介质存储数据的安全要求;

c）对存储介质进行定期或随机性安全检查情况;

d）存储介质访问和使用行为的记录和审计情况。

6.2.3 数据传输

6.2.3.1 传输链路安全性

针对数据传输链路安全性，应重点评估:

a）数据传输安全策略和操作规程的建设落实情况;

b）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;

c）个人信息和重要数据传输进行完整性保护情况;

d）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;

e）数据传输、接收的记录和安全审计情况;

f）采取安全传输协议等安全措施情况;

g）数据异常传输检测发现及处置情况。

6.2.3.2 传输链路可靠性

针对数据传输链路的可靠性，应重点评估:

a）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;

b）点对点传输中是否存在传输经过第三方、被第三方缓存情况。

6.2.4 数据使用和加工

6.2.4.1 数据使用和加工合法性

针对数据使用和加工合法性，应重点评估:

a）使用和加工数据时，遵守法律、行政法规，尊重社会公德和伦理，遵守商业道德和职业道德等情况;

b）是否存在危害国家安全、公共利益的数据使用和加工行为，损害个人、组织合法权益的数据使用和加工行为;

c）是否制作、发布、复制、传播违法信息;

d）应用算法推荐技术提供互联网信息服务的，是否按照《互联网信息服务算法推荐管理规定》开展定期审核、评估、验证数据处理机制机理、模型、数据和应用结果等相关工作。

6.2.4.2 数据正当使用

针对数据正当使用情况，应重点评估:

a）数据使用加工安全策略和操作规程的建设落实情况;

b）数据使用是否获得数据提供方、数据主体等相关方授权;

c）数据使用行为与承诺或用户协议的一致性;

d）除为实现法定职责或依法开展数据共享等情况外，变更个人信息使用目的或规则时,是否以合理明确的方式再次征得用户明示同意;

e）开展数据处理活动以及研究开发数据新技术，是否有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理;

f）使用数据开展用户画像、信息推送、内容呈现等业务，造成用户受不公平的价格待遇、平台公共竞争秩序受影响、平台内劳动者正当权益受损害等风险情况;

g）数据使用加工目的、方式、范围，与行政许可、合同授权等的一致性;

h）是否存在个人信息和重要数据滥用情况。

6.2.4.3 数据导入导出

针对数据导入导出情况，应重点评估:

a）数据导出安全评估和授权审批流程建设情况;

b）导入导出审计策略和日志管理机制建设情况;

c）是否进行严格的导出权限管理并记录了完整的导出操作;

d）是否对导出数据的存储介质提出了严格的加密、使用、销毁要求并进行落实;

e）定期对个人信息和重要数据导出行为进行安全审计情况。

6.2.4.4 数据处理环境

针对数据处理环境安全情况，应重点评估:

a）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;

b）大数据平台等处理组件按照基线要求进行安全配置、配置核查情况;

c）处理环境中的安全漏洞情况，已发现漏洞的处置情况。

6.2.4.5 数据使用和加工安全措施

针对数据使用和加工安全措施情况，应重点评估:

a）在数据清洗、转换、建模、分析、挖掘等加工过程中，对数据特别是个人信息和重要数据的保护情况;

b）数据防泄漏措施建设情况;

c）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;

d）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;

e）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;

f）数据加工过程中对个人信息、重要数据等敏感数据的操作行为记录、定期审计情况;

g）高风险行为审计及回溯工作开展情况;

h）委托加工数据的，是否明确约定受托方的安全保护义务，并采取技术措施或其他约束手段防止受托方非法留存、扩散数据。

6.2.5 数据提供

6.2.5.1 数据提供合法正当必要性

针对数据提供合法正当必要性，应重点评估:

a）数据对外提供的目的、方式、范围的合法性、正当性、必要性;

b）数据提供的依据和目的是否合理、明确;

c）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;

d）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。

6.2.5.2 数据提供管理

针对数据提供管理情况，应重点评估:

a）数据提供安全策略和操作规程的建设落实情况;

b）数据对外提供的审批情况;

c）对外提供数据前，数据安全风险评估情况和个人信息保护影响评估情况;

d）与接收方签订合同协议情况，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;

e）开展共享、交易、委托处理、向境外提供数据等高风险数据处理活动前的安全评估情况;

f）向境外执法机构提供境内数据的情况;

g）核心数据跨主体流动前是否经国家数据安全工作协调机制评估和批准。

6.2.5.3 数据提供技术措施

针对数据提供技术措施情况，应重点评估:

a）对外提供的敏感数据是否进行加密及加密有效性;

b）对共享数据及数据共享过程的监控审计情况;

c）对外提供数据时采取签名、添加水印等安全措施情况;

d）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;

e）数据对外提供的安全保障措施及有效性;

f）多方安全计算、联邦学习等安全技术应用情况。

6.2.5.4 数据接收方

针对数据接收方情况，应重点评估:

a）数据接收方的诚信状况、违法违规情况、境外政府机构合作关系、被中国政府制裁等情况;

b）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；

c）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；

d）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；

e）对接收方数据使用、再转移、对外提供和安全保护的监督情况。

6.2.5.5 数据转移安全

针对因兼并、重组、破产等原因向外转移数据，或承接其他数据处理者转移数据等场景，重点评估：

a）是否向有关主管部门报告；

b）是否制定数据转移方案；

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

d）没有接收方的，对相关数据删除处理情况。

6.2.5.6 数据出境安全

针对数据出境安全情况，重点评估：

a）数据出境场景梳理是否合理、完整，是否覆盖全部业务场景和产品类别；

b）出境线路梳理是否合理、完整，是否覆盖公网出境、专线出境等情形；

c）涉及数据出境的，按照有关规定开展数据出境安全评估、个人信息保护认证、个人信息出境标准合同签订的情况;

d）针对公网出境场景，监测核查实际出境数据是否与申报内容一致。

6.2.6 数据公开

6.2.6.1 数据公开适当性

针对数据公开适当性，应重点评估:

a）数据公开目的、方式、范围的适当性;

b）数据公开目的、方式、范围与行政许可、合同授权的一致性;

c）公开的数据内容与法律法规要求的符合程度;

d）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;

e）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。

6.2.6.2 数据公开管理

针对数据公开管理情况，应重点评估:

a）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;

b）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;

c）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;

d）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;

e）对公开数据的脱敏处理、防爬取、数字水印等控制措施。

6.2.7 数据删除

6.2.7.1 数据删除管理

针对数据删除管理情况，应重点评估:

a）数据删除流程和审批机制的建设落实情况;

b）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;

c）是否按照法律法规、合同约定、隐私政策等及时删除数据;

d）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;

e）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;

f）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;

g）缓存数据的删除情况。

6.2.7.2 存储介质销毁

针对存储介质销毁情况，应重点评估:

a）存储介质销毁管理制度和审批机制的建设落实情况;

b）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；是否依据存储内容重要性、存储介质使用寿命，明确存储介质销毁方法；是否妥善处置销毁的存储介质；

c）存储介质销毁过程的监控、记录情况；

d）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。

6.2.8 其他

对于人脸、步态、基因、声纹、即时通信、快递物流、网上购物、网络支付服务、网络音视频、汽车、网络预约汽车服务等数据处理活动的评估，可参照相应国家标准、行业标准的具体细化要求评估风险。

6.3 数据安全技术风险

6.3.1 网络安全防护

针对网络安全防护情况，应重点评估：

a）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；

b）网络隔离、边界防护等措施的有效性；

c）安全策略和配置核查情况；

d）身份鉴别、访问控制、权限管理情况；

e）安全漏洞发现及常见漏洞修复、处置情况；

f）异常流量、恶意代码和钓鱼邮件发现及处置情况；

g）外部攻击、内部攻击、新型攻击的发现和处置情况；

h）未授权连接内网、外网、无线网等情况；

i）通信链路、网络设备、计算设备等关键设备的冗余情况;

j）对第三方组件进行安全核查、修复、更新的情况;

k）处理重要数据、核心数据的信息系统，应当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，还应当符合关键信息基础设施安全保护要求。

6.3.2 身份鉴别与访问控制

6.3.2.1 身份鉴别

针对身份鉴别措施情况，应重点评估:

a）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;

b）身份鉴别信息是否具有复杂度要求并定期更换;

c）是否存在可绕过鉴别机制的访问方式;

d）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;

e）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;

f）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。

6.3.2.2 访问控制

针对访问控制措施情况，应重点评估:

a）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;

b）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;

c）数据访问权限与访问者的身份关联情况;

d）数据访问权限申请、审批机制的建设落实情况;

e）是否以满足业务实际需要的最小化权限原则进行授权。

6.3.2.3 授权管理

针对授权情况，应重点评估:

a）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;

b）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;

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

d）是否存在与权限申请审批结果不一致的情况;

e）是否存在多余、重复、过期的账户和角色;

f）是否存在共享账户和角色权限冲突的情况;

g）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;

h）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。

6.3.3 监测预警

针对数据安全风险监测预警情况，应重点评估:

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。

6.3.4 数据脱敏

针对数据脱敏情况，应重点评估:

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。

6.3.5 数据防泄漏

针对数据防泄漏情况，应重点评估:

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。

6.3.6 数据接口安全

6.3.6.1 对外接口安全

针对对外接口安全情况，应重点评估:

a）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;

b）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;

c）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。

6.3.6.2 接口安全控制

针对数据接口安全控制情况，应重点评估:

a）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;

b）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;

c）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;

d）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;

e）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;

f）对接口类型、名称、参数等安全要求规范情况;

g）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;

h）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。

6.3.7 数据备份恢复

针对数据备份恢复情况，应重点评估:

a）数据备份恢复策略和操作规程的建设落实情况;

b）定期开展数据备份恢复工作情况;

c）备份和归档数据访问控制措施的有效性;

d）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;

e）定期开展灾难恢复演练情况。

6.3.8 安全审计

6.3.8.1 审计执行

针对数据安全审计执行情况，应重点评估:

a）审计的实施情况;

b）审计策略和要求的合理性、有效性;

c）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;

d）特权用户安全审计情况。

6.3.8.2 日志留存记录

针对日志留存记录情况，应重点评估:

a）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;

b）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;

c）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;

d）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。

6.3.8.3 行为审计

针对数据安全行为审计情况，应重点评估:

a）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;

b）对数据库、数据接口的访问和操作行为审计情况;

c）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；

d）对个人信息处理活动的合规审计情况。

6.4 个人信息保护风险

6.4.1 个人信息处理基本原则

6.4.1.1 合法、诚信原则

针对合法、诚信原则遵守情况，应重点评估：

a）通过误导、欺诈、胁迫等方式处理个人信息的情况；

b）非法收集、使用、加工、传输他人个人信息的情况；

c）非法买卖、提供或者公开他人个人信息的情况；

d）是否从事危害国家安全、公共利益的个人信息处理活动；

e）个人信息处理活动是否具备《个人信息保护法》规定的合法性事由；

f）是否存在隐瞒产品或服务所收集个人信息功能的情况。

6.4.1.2 正当、必要原则

针对正当、必要原则遵守情况，应重点评估：

a）处理个人信息是否具有明确、合理的目的；

b）处理个人信息是否与处理目的直接相关，是否采取对个人权益影响最小的方式；

c）收集个人信息是否限于实现处理目的的最小范围，如最少类型、最低频次等；是否存在过度收集个人信息行为；

d）是否以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务，或者干扰个人正常使用服务，处理个人信息属于提供产品或者服务所必需的除外。

6.4.2 个人信息告知

针对个人信息告知情况，应重点评估:

a）在处理个人信息前，是否以显著方式、清晰易懂的语言真实、准确、完整地公开个人信息处理规则;

b）是否告知个人信息处理者的名称或姓名、联系方式，有法律、行政法规规定应当保密或者不需要告知的情形除外;

c）个人信息处理规则是否告知个人信息的处理目的、处理方式，处理的个人信息种类、保存期限;

d）个人信息处理规则是否告知个人行使《个人信息保护法》规定权利的方式和程序;

e）告知事项发生变更的，是否将变更部分告知个人;

f）个人信息处理规则是否便于查阅和保存;

g）紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者是否在紧急情况消除后及时告知。

6.4.3 个人信息同意

针对个人信息同意情况，应重点评估:

a）处理个人信息前是否取得个人同意，同意是否由个人在充分知情的前提下自愿、明确作出，法律规定的例外情形除外;

b）基于个人同意处理个人信息的，个人信息处理者是否提供便捷的撤回同意的方式，个人是否有权撤回其同意，个人撤回同意是否不影响撤回前基于个人同意已进行的个人信息处理活动的效力；

c）个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，是否重新取得个人同意。

6.4.4 个人信息处理

6.4.4.1 个人信息保存

针对个人信息保存情况，应重点评估：

a）个人信息的保存期限是否为实现处理目的所必要的最短时间，法律、行政法规另有规定除外；

b）是否将个人生物识别信息与个人身份信息分开存储。

6.4.4.2 个人信息共同处理

对于两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，重点评估：

是否约定各自的权利和义务，约定是否不影响个人向任一个人信息处理者行使权利。

6.4.4.3 个人信息委托处理

针对个人信息委托处理情况，应重点评估：

a）是否与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，是否对受托人的个人信息处理活动进行监督；

b）个人信息受托人是否按照约定处理个人信息，是否超出约定的处理目的、处理方式等处理个人信息;

c）委托合同不生效、无效、被撤销或者终止的，受托人是否将个人信息返还个人信息处理者或者予以删除，是否违规保留个人信息;

d）未经个人信息处理者同意，受托人是否转委托他人处理个人信息。

6.4.4.4 个人信息转移

因合并、分立、解散、被宣告破产等原因需要转移个人信息的，重点评估:

a）是否向个人告知接收方的名称或者姓名和联系方式;

b）接收方是否继续履行个人信息处理者的义务;

c）接收方变更原先的处理目的、处理方式的，是否重新取得个人同意。

6.4.4.5 向他人提供个人信息

向他人提供个人信息的，应重点评估:

a）是否向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类;

b）是否取得个人的单独同意;

c）接收方是否在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息；如接收方变更原先的处理目的、处理方式的，是否重新取得个人同意。

6.4.4.6 自动化决策

针对自动化决策情况，应重点评估：

a）是否保证决策的透明度和结果公平、公正，是否对个人实行不合理的差别待遇；

b）通过自动化决策方式向个人进行信息推送、商业营销等，是否同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式；

c）是否明确对自动化决策方式予以说明。

6.4.4.7 个人信息公开

针对个人信息公开情况，应重点评估：

a）个人信息公开是否取得个人单独同意；

b）是否在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息，个人明确拒绝的除外；

c）处理已公开的个人信息，对个人权益有重大影响的，是否取得个人同意。

6.4.5 敏感个人信息处理

6.4.5.1 通用规则

针对敏感个人信息处理规则，应重点评估：

a）敏感个人信息处理是否具有特定的目的和充分的必要性，是否对敏感个人信息采取严格保护措施；

b）处理敏感个人信息是否取得个人的单独同意；

c）法律、行政法规规定处理敏感个人信息应当取得书面同意的，是否取得个人的书面同意;

d）处理敏感个人信息是否向个人告知处理敏感个人信息的必要性以及对个人权益的影响;

e）处理不满 14 周岁未成年人个人信息的，是否取得未成年人的父母或者其他监护人的同意，是否制定专门的未成年人个人信息处理规则;

f）是否遵守法律、行政法规对处理敏感个人信息规定，取得相关行政许可或者作出其他限制。

6.4.5.2 人脸识别数据安全

针对人脸识别数据安全情况，应重点评估:

a）在公共场所安装图像采集、个人身份识别设备，是否为维护公共安全所必需，是否遵守国家有关规定，并设置显著的提示标识;

b）所收集的个人图像、身份识别信息，是否只用于维护公共安全的目的，未用于其他目的，取得个人单独同意的除外;

c）开展业务活动时是否限定使用人脸识别技术作为身份鉴别的唯一方式，并且当用户拒绝人脸识别方式时，是否频繁申请授权干扰用户正常使用;

d）完成身份鉴别后，应及时删除身份鉴别过程中收集、使用的人脸相关数据，通过以单独操作注册预留的、且仅用于比对的生物特征模板除外;

e）是否满足人脸识别有关政策规定。

6.4.6 个人信息主体权利

6.4.6.1 个人信息的查阅、复制、可携带

针对个人信息的查阅、复制、可携带等主体权利保障情况，应重点评估:

a）个人信息处理者是否为个人提供查阅其个人信息的途径，是否可以及时提供个人信息查阅;

b）是否为个人提供复制其个人信息的途径，是否可以及时提供个人信息复制;

c）个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者是否提供转移的方法。

6.4.6.2 个人信息的更正、补充

针对个人信息的更正、补充等主体权利保障情况，应重点评估:

a）个人信息处理者是否为个人提供请求个人信息更正、补充的途径;

b）个人请求更正、补充其个人信息的，个人信息处理者是否对其个人信息予以核实，是否及时更正、补充。

6.4.6.3 个人信息的删除

针对个人信息的删除等主体权利保障情况，应重点评估有以下情形的，个人信息处理者是否主动删除个人信息:

a）个人信息处理目的已实现、无法实现或者为实现处理目的不再必要时;

b）个人信息处理者停止提供产品或者服务，或者保存期限已届满;

c）个人撤回同意;

d）个人信息处理者违反法律、行政法规或者违反约定处理个人信息。

针对法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，重点评估个人信息处理者是否停止除存储和采取必要的安全保护措施之外的处理。

6.4.6.4 其他个人信息权利

针对个人信息主体权利保障情况，还应重点评估:

a）个人信息处理者是否为个人提供对其个人信息处理规则进行解释说明的途径;

b）通过自动化决策方式作出对个人权益有重大影响的决定，是否为个人提供解释说明的途径，个人是否有权拒绝个人信息处理者仅通过自动化决策的方式作出决定;

c）自然人死亡的，其近亲属为了自身的合法、正当利益，是否可以对死者相关个人信息进行查阅、复制、更正、删除等，死者生前另有安排的除外;

d）是否建立便捷的个人行使权利的申请受理和处理机制，拒绝个人行使权利请求的，是否说明理由。

6.4.7 个人信息安全义务

6.4.7.1 个人信息保护措施

针对个人信息保护措施部署情况，应重点评估:

a）个人信息保护内部管理制度和操作规程的建设落实情况;

b）对个人信息分类管理实施情况及效果;

c）加密、去标识化等安全技术措施应用情况;

d）是否合理确定个人信息处理的操作权限;

e）个人信息安全事件应急预案制定及组织实施情况;

f）是否在展示、委托处理、提供、公开等环节，对个人信息直接标识符进行去标识化处理;

g）是否定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

6.4.7.2 个人信息保护负责人

针对个人信息保护负责人设置情况，应重点评估:

a）处理个人信息达到国家网信部门规定数量的个人信息处理者的个人信息保护负责人设置情况，能否负责对个人信息处理活动以及采取的保护措施等进行监督;

b）是否公开个人信息保护负责人的联系方式，是否将个人信息保护负责人的姓名、联系方式等报送网信部门。

6.4.7.3 个人信息保护影响评估

针对个人信息保护影响评估开展情况，应重点评估:

a）是否在处理敏感个人信息、利用个人信息进行自动化决策、委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息、向境外提供个人信息前进行个人信息保护影响评估;

b）个人信息保护影响评估内容是否符合《个人信息保护法》第56条要求;

c）是否对个人信息处理情况进行记录，个人信息保护影响评估报告和处理情况记录是否至少保存三年。

6.4.7.4 个人信息安全应急

针对个人信息安全应急措施部署情况，应重点评估:

a）个人信息安全事件应急预案制定及组织实施情况;

b）发生或者可能发生个人信息泄露、篡改、丢失时，是否立即采取补救措施;

c）个人信息安全事件是否通知所涉及个人并报告网信部门，事件通知是否包含信息种类、原因、可能造成的危害、补救措施、个人信息处理者联系方式等。

6.4.8 个人信息投诉举报

针对个人信息投诉举报情况，应重点评估:

a）对违反个人信息保护相关规定行为的投诉举报渠道建设情况，包括是否建设便捷的投诉举报渠道，是否及时受理、处置相关投诉举报;

b）是否公布接受投诉、举报的联系方式;

c）用户投诉、举报后，是否在承诺时限内受理并处理。

6.4.9 大型网络平台个人信息保护

针对大型网络平台个人信息保护情况，应重点评估:

a）是否按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督;

b）是否遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务;

c）是否对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务;

d）是否定期发布个人信息保护社会责任报告，接受社会监督。

7 综合分析

综合汇总评估情况，梳理问题清单，提出整改建议，分析作出评估结论。

7.1 梳理问题列表

根据各个评估项的评估情况，梳理存在的安全问题，按照问题类别和问题项汇总形成问题列表。问题类别可参考第六章二级标题（6.x），问题项可参考第六章三级标题（6.x.x）给出。

7.2 问题整改建议

结合实际情况，针对存在的具体问题逐一给出整改建议，形成数据安全问题清单，如表 1 所示。

表 1 数据安全问题清单

序号	问题类别	问题项	问题描述	整改建议
1	数据安全管理问题	管理制度流程	数据安全管理制度覆盖范围不全面，工作文件印发范围未覆盖 XX 部门	科学界定文件印发范围,确保压实数据安全管理责任
2		安全组织机构	缺少数据安全管理机构，缺乏有效监督考核机制	设立专门的数据安全管理机构，建立监督考核机制，定期开展评估检查

问题清单可包括:

a）问题类别：可参考第五章评估内容，列出安全问题对应的评估内容类别，如数据安全管理问题、数据处理活动问题、数据安全技术问题、个人信息保护问题等;

b）问题项：列出数据安全问题的细分类别，如管理制度流程、安全组织架构、分类分级管理、人员安全管理等;

c）问题描述：对所列数据安全问题项的具体情况展开描述，如涉及的数据资产、数据处理活动、相关系统和业务、具体问题内容等;

d）整改建议：针对所列的数据安全问题给出管理、技术等方面的整改建议。

7.3 风险分析评价

主要从数据安全风险（可参考附录A）一旦发生，对本单位、本行业以及对国家安全、社会公共利益、其他组织或者个人的合法权益造成的危害程度进行分析。可综合分析数据安全问题清单，同时考虑数据价值、风险隐患严重程度、风险发生可能性、安全措施有效性和完备性等因素后，给出存在的主要问题、数据安全风险情况和总体评价。

可以根据实际工作情况，邀请行业领域和数据安全、网络安全等方面专家对问题清单、整改建议、风险分析、总体评价等评估结果的准确性、有效性、科学性、合理性进行评议。

如需分析风险发生的可能性、产生的危害程度，评价风险级别，可参考《信息安全技术 数据安全风险评估方法》。

8 评估总结

8.1 评估报告

根据评估情况，评估队伍编制网络数据安全风险评估报告（报告模板参见附录B）。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），针对发现的风险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;

b）评估工作情况，包括工作组织、时间安排、参与人员情况;

c）被评估方基本信息、业务和信息系统情况、数据资产情况、数据处理活动情况、安全防护措施情况;

d）数据安全管理风险评估，包括数据安全制度流程、数据安全组织、数据分类分级、人员安全管理、数据合作方管理、数据安全应急管理、开发运维等方面风险评估情况;

e）数据处理活动安全风险评估，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评估情况;

f）数据安全技术风险评估，包括网络安全防护、身份鉴别与访问控制、监测预警、数据脱敏、数据防泄漏、数据接口安全、数据备份恢复、安全审计等技术安全风险评估情况;

g）个人信息保护风险评估，包括处理个人信息时，遵循合法、诚信、正当、必要、公开、透明原则情况，个人信息同意情况，一般个人信息、敏感个人信息处理，个人信息主体权利及安全义务、投诉

举报情况、App 个人信息保护（如有）等方面风险评估情况。若不涉及个人信息处理，则不列此章节;

h）数据安全问题清单，包括问题类别、问题项、存在的安全问题、整改建议等;

i）风险总结分析，从对国家安全、公共利益、行业、组织或者个人的合法权益造成的危害程度对风险进行总结分析，给出存在的主要问题、数据安全风险情况和总体评价;

j）对策建议，针对发现的数据安全风险，提出整改措施对策建议;

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;若无法在附录中完整列出，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;

l）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（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;

m）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。

8.2 风险处置

被评估方应制定整改计划，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。

在检查评估中，被评估方完成整改后，主管监管部门可视情组织或指导被评估方开展网络数据安全风险复评估工作。

附录 A 数据安全风险示例

A.1典型数据安全风险类别

表 B.1 典型数据安全风险类别示例

序号	风险类别	描述
1	数据泄露风险	由于数据窃取、爬取、脱库、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	超范围处理数据	数据处理活动违反必要性原则，超范围或过度收集使用个人信息或重要数据的风险。

序号	风险类别	描述
16	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。
17	未有效保障个人信息主体权利	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。
18	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。
19	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。
20	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。
21	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。
22	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
23	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。

A.2数据收集常见安全风险

表 B.2 数据收集常见安全风险示例

风险名称	风险描述
采集数据泄露风险	采集过程中由于脱库等攻击或自身措施不完善等情况，造成数据窃取，引发数据泄露风险。
超范围采集风险	违背个人信息采集最小化原则，超业务所需范围采集个人信息，影响数据安全与采集的合理性。
非法获取数据风险	违反国家法律法规、监管政策，违背数据采集合法性原则进行数据采集，引发数据非法获取风险。
采集手段失效风险	由于软硬件故障、接口故障、配置失效等造成数据无法采集。
采集数据过载风险	由于数据实际采集量超过预期承载量，导致数据被覆盖或丢失。
清洗转换错误风险	由于数据清洗、转换规则、手段、方法出现问题，导致被采集的数据完整性、可用性降低。
校验失效风险	由于未进行数据校验或者校验失效，导致采集的数据完整性、可用性降低。

风险名称	风险描述
采集数据篡改风险	数据采集过程中，由于数据被未授权更改，或数据入库时污染原始数据，使得数据被篡改，降低其完整性、可用性。
采集数据污染风险	数据采集过程，由于人为故意或偶然行为，导致原始数据的完整性和真实性被损害。
采集数据破坏风险	采集过程中，由于缺少防护措施或遭受攻击，导致数据被破坏
数据错误标记风险	由于数据分类分级判断错误或打标记错误，导致数据受保护级别降低，造成数据保护措施不到位。
数据源错误风险	数据采集过程受到未授权、失效、不符合预期等问题时，导致数据完整性、可用性降低。
采集数据质量风险	采集数据不准确、不完整，因数据质量导致数据处理出错
元数据定义失当风险	元数据类型、格式定义不适宜，造成数据完整性、可用性降低。
无效数据写入风险	数据入库时，数据不符合规范或无效，造成数据完整性、可用性降低
安全验证措施缺失风险	可能发生恶意代码注入、恶意数据源引用等，进一步引发数据窃取、篡改、毁损等风险。
质量验证措施缺失风险	可能发生采集过载、清洗转换错误等，进一步导致数据篡改、丢失、毁损等风险。

A.3数据存储常见安全风险

表 B.3 数据存储常见安全风险示例

风险名称	风险描述
存储数据破坏	由于信息系统自身故障、物理环境变化、自然灾害或安装恶意代码等导致数据破坏，影响数据完整性和可用性
存储数据篡改	通过安装恶意代码等篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等，破坏数据完整性和可用性
存储数据丢失风险	硬件、软件导致存储数据丢失、海量数据归档机制（如时间隔、数据类型等）不合理，影响数据机密性、完整性、可用性。
存储数据一致性问题	软硬件、网络等原因导致数据同步过程中数据丢失，进而导致数据一致性问题。
数据备份失效	由于备份的数据无法恢复或备份策略失效，影响数据完整性、可用性。
存储数据窃取风险	在数据库服务器、文件服务器、办公终端等存储系统安装恶意代码，造成数据被窃取，影响数据机密性、完整性、可用性。
数据不可控风险	委托第三方云平台、数据中心等外部提供者存储数据，但缺少有效的约束与控制手段，影响数据机密性、完整性、可用性。

风险名称	风险描述
存储数据误操作风险	由于数据存储系统操作行为不当导致数据泄露或损坏，影响数据机密性、完整性、可用性。
数据非授权访问风险	数据被未授权客体访问，可能造成数据泄露、损坏等问题，影响数据机密性、完整性、可用性。
超期存储风险	数据存储期限超出预设合理时间，可能引发数据滥用或非法使用等问题。

A.4数据传输常见安全风险

表 B.4 数据传输常见安全风险示例

风险名称	风险描述
传输数据窃取风险	攻击者伪装成外部通信代理、通信对端、通信链路网关，通过伪造虚假请求或重定向窃取数据，影响数据机密性、完整性、可用性。
传输数据破坏风险	传输过程中数据被破坏，影响数据机密性、完整性、可用性。
传输数据篡改风险	攻击者伪装成通信代理或通信对端篡改数据，影响数据机密性、完整性、可用性。
传输数据污染风险	数据传输时，攻击者接入传输网络污染传输的数据，破坏数据完整性。
传输数据丢失风险	由于传输过载，超过传输通道的承载能力导致数据丢失，影响数据完整性、可用性。
传输手段失效风险	由于软硬件故障、接口故障、配置失效等导致数据无法传输或丢失，影响数据完整性、可用性。
数据非法传输风险	违反法律法规、制度文件要求传输数据，影响数据机密性。

A.5数据使用和加工安全风险

表 B.5 数据使用和加工常见安全风险示例

风险名称	风险描述
行为抵赖风险	缺少日志记录等手段，无法承认数据处理行为。
越权处理风险	超出授权范围的数据处理活动，影响数据机密性、完整性、可用性。
数据处理不可控风险	委托第三方机构或外部系统处理数据，没有有效的约束与控制手段，影响数据机密性、完整性、可用性。
敏感信息泄露风险	由于未对数据做适当的脱敏处理，导致敏感信息泄露，影响数据机密性。
处理结果泄露风险	对数据进行分析处理后得出的结果发生泄露，影响数据机密性。
特权账户滥用风险	由于对特权账户的分配和使用缺乏有效监管，造成数据泄露、篡改等风险，影响数据机密性、完整性、可用性。
算法推荐违法违规风险	违反《互联网信息服务算法推荐管理规定》要求，开展的违法不良信息传播、侵害用户权益、操纵社会舆论等行为
数据非法利用风险	未按照国家相关法律法规和相关数据保护要求对数据进行使用和加工，影响数据机密性、完整性、可用性。或者数据

风险名称	风险描述
	使用、加工活动可能对国家安全、公共利益或个人、组织合法权益造成危害
安全措施失当或失效风险	由于未依据数据安全加工使用过程实际安全需要或数据性质明确防护措施，引发数据安全风险。

A.6数据提供常见安全风险

表 B.6 数据提供常见安全风险示例

风险名称	风险描述
数据违规共享风险	数据共享行为违反数据共享原则或流程，影响数据机密性。
共享接口滥用风险	对共享接口的访问频次、使用量、调用时间等滥用，影响数据机密性。
共享数据篡改风险	共享过程中，数据被篡改，影响数据机密性、完整性、可用性。
共享数据泄露风险	超范围访问共享的数据，导致共享数据泄露，影响数据机密性。
共享越权风险	由于数据共享接口的管理或技术手段失效，或共享权限分配混乱，导致第三方可以获取授权之外的数据，影响数据机密性、完整性、可用性。
权力扩散风险	原数据所有方对共享后的数据的使用、再转移等缺少约束，共享的数据超出授权使用范围，影响数据机密性。
接收方违规留存风险	数据接收方违规留存数据，影响数据机密性。

A.7数据公开常见安全风险

表 B.7 数据公开常见安全风险示例

风险名称	风险描述
个人信息泄露风险	缺少数据脱敏等技术防护手段，造成数据公开后的个人信息泄露风险。
数据非法爬取风险	利用爬虫或自动化脚本对公开数据进行爬取，影响数据机密性。
数据泄露风险	因审核缺失、误判、误操作等错误公开数据，或未采取措施处置不宜公开数据，造成数据泄露。
超范围公开风险	超出预定范围公开数据，造成数据泄露。

A.8数据删除常见安全风险

表 B.8 数据删除常见安全风险示例

风险名称	风险描述
逾期留存风险	数据失效或业务关闭后，遗留了敏感数据仍然可以被访问，破坏了数据的机密性。
数据销毁不彻底风险	未按照规定的要求进行销毁，数据使用环境中存在多副本，数据销毁时存在遗留副本未被销毁，未销毁备份数据，破坏了数据的机密性。

附录 B 评估报告模板

网络数据安全风险评估报告

评估单位（盖章）：

报告时间： 年 月 日

<table>
<tr><td colspan="6">被评估方</td></tr>
<tr><td>单位名称</td><td colspan="2"></td><td colspan="2">统一社会信用代码</td><td></td></tr>
<tr><td>单位地址</td><td colspan="2"></td><td colspan="2">邮政编码</td><td></td></tr>
<tr><td>评估对象</td><td colspan="5"></td></tr>
<tr><td rowspan="2">联系人</td><td>姓名</td><td></td><td colspan="2">职务/职称</td><td></td></tr>
<tr><td>联系方式</td><td></td><td colspan="2">所属部门</td><td></td></tr>
<tr><td>真实性声明</td><td colspan="5">被评估方承诺:
提供的所有材料准确、真实、合法、有效，并愿为此承担有关法律责任。</td></tr>
<tr><td>数据安全负责人</td><td colspan="5"></td></tr>
<tr><td colspan="6">评估队伍单位信息</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="2"></td><td>邮政编码</td><td colspan="2"></td></tr>
<tr><td>联系人</td><td>姓名</td><td></td><td>联系方式</td><td colspan="2"></td></tr>
<tr><td rowspan="2">审核批准</td><td>评估组长</td><td></td><td>日期</td><td colspan="2"></td></tr>
<tr><td>审核人</td><td></td><td>日期</td><td colspan="2"></td></tr>
</table>

一、评估概述

1.1 评估目的和依据

（*说明本次评估的目的和依据*）

1.2 评估对象和范围

（*描述本次评估涉及的对象和范围*）

1.3 评估结论概要

（*数据和数据处理活动的概要情况，评估结果及处置建议概要。*）

二、评估工作开展情况

2.1 评估工作组织情况

（概要说明为开展本次评估工作，单位内部建立的组织机构及其人员构成、相关工作机制、汇报机制等工作组织情况。）

2.2 评估时间安排情况

（对本次评估工作的时间进度安排进行说明，对每个工作阶段的工作内容、消耗时间、工作结果等信息进行描述。）

2.3 参与人员情况

（对本次评估工作的参与人员和部门进行说明）

三、数据和数据处理活动基本情况

3.1 数据处理者基本情况

3.2 业务和信息系统情况

3.3 数据资产情况

3.4 数据处理活动情况

3.5 安全防护措施情况

四、数据安全风险评估

4.1 数据安全管理风险评估

4.2 数据处理活动风险评估

4.3 数据安全技术风险评估

4.4 个人信息处理风险评估

五、总结分析

5.1 数据安全问题清单

5.2 风险总结分析

5.3 对策建议

声 明

【填写说明：声明是评估机构对评估报告的有效性前提、评估结论的适用范围以及使用方式等有关事项的陈述，评估机构可参考以下建议书写内容编制。】

本报告是[被评估方名称]的网络数据安全风险评估报告。

本报告评估结论的有效性建立在被评估方提供相关证据的真实性基础之上。

本报告中给出的评估结论仅对被评估方当时的安全状态有效。当评估工作完成后，由于被评估方发生变更而涉及到的数据或数据处理活动本报告不再适用。

在任何情况下，若需引用本报告中的评估结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

单位名称（加盖单位公章）

年　　月　日