ICS 35.020
CCS L78

T/CSAS

团　　体　　标　　准

T/CSAS XXXX—2025

数据安全风险评估实施指南

Implementation guide for risk assessment of Data Security

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

四川省网络空间安全协会　发 布

目　　次

前　言

本文件按照GB/T　1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由四川省网络空间安全协会提出并归口。

本文件起草单位：成都久信信息技术股份有限公司，成都市信息系统与软件评测中心，成都卓越华安信息技术服务有限公司，成都安美勤信息技术股份有限公司，杭州安恒信息技术有限公司，深信服科技股份有限公司，豪符密码检测技术有限责任公司，北京山石网科信息技术有限公司，四川智仁信息技术有限公司。

本文件主要起草人：

引　　言

数据安全风险评估实施指南旨在为指导数据安全风险评估工作，给出数据数据安全评估思路、具体的工作流程及详细的评估内容，用于发现数据安全隐患，防范数据安全风险，支撑《中国人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规落地。

数据安全风险评估实施指南

1 范围

本文件规定了开展数据安全风险评估的基本概念、基本原则、实施流程、评估方法、评估内容及工具等。

本文件适用于数据处理者、第三方机构开展数据安全评估工作，指导数据安全风险评估的组织、实施、验收等工作。

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 43697-2024 数据安全技术 数据分类分级规则 术语

3 术语和定义

下列术语和定义适用于本文件。

GB/T 43697-2024界定的以及下列术语和定义适用于本文件。

3.1 数据 data

任何以电子或者其他方式对信息的记录。

[来源：GB/T 43697—2024，3.1]

3.2 重要数据 key data

特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

注：仅影响组织自身或公民个体的数据一般不作为重要数据。

[来源：GB/T 43697—2024，3.2]

3.3 核心数据 core data

对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的，一旦被非法使用或共享，可能直接影响政治安全的重要数据。

注：核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉，重要民生，重大公共利益的数据，经国家有关部门评估确定的其他数据。

[来源：GB/T 43697—2024，3.3]

3.4 一般数据 general data

核心数据、重要数据之外的数据。

[来源：GB/T 43697—2024，3.4]

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识别的自然人有关的各种信息.

[来源：GB/T 43697—2024，3.5]

3.6 敏感个人信息 sensitive personal information

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

[来源：GB/T 43697—2024，3.6]

3.7 数据处理者 data processor

在数据处理活动中自主决定处理目的、处理方式的组织、个人。

[来源：GB/T 43697—2024，3.11]

3.8 数据处理活动 data processing activities

数据的收集、存储、使用、加工、传输、提供、公开、删除等活动。

3.9 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。

3.10 数据安全评估机构 assessment organization of data security

从事数据安全评估活动的机构。

4 数据安全风险评估概述

4.1 评估的原则目的

4.1.1 评估目的

数据安全风险评估以预防为主、主动发现、积极防范为原则，围绕数据处理活动对可能影响数据的保密性、完整性、可用性、合规性进行风险评估，掌握数据安全总体状况，发现数据隐患并提出防护措施。

4.1.2 评估的基本原则

——实施的基本原则：

a) 标准性原则：评估应遵循国家、地方、行业相关标准和规定；
b) 可控性原则：应严格按照相关标准的项目管理方法对服务过程、人员和工具进行控制，确保评估过程中的人员、技术和工具的可控；

4.2 评估的基本内容

数据安全风险评估在信息调研基础之上主要围绕数据安全管理、数据处理活动、数据安全技术、个人信息保护开展评估，数据安全评估内容见图1。

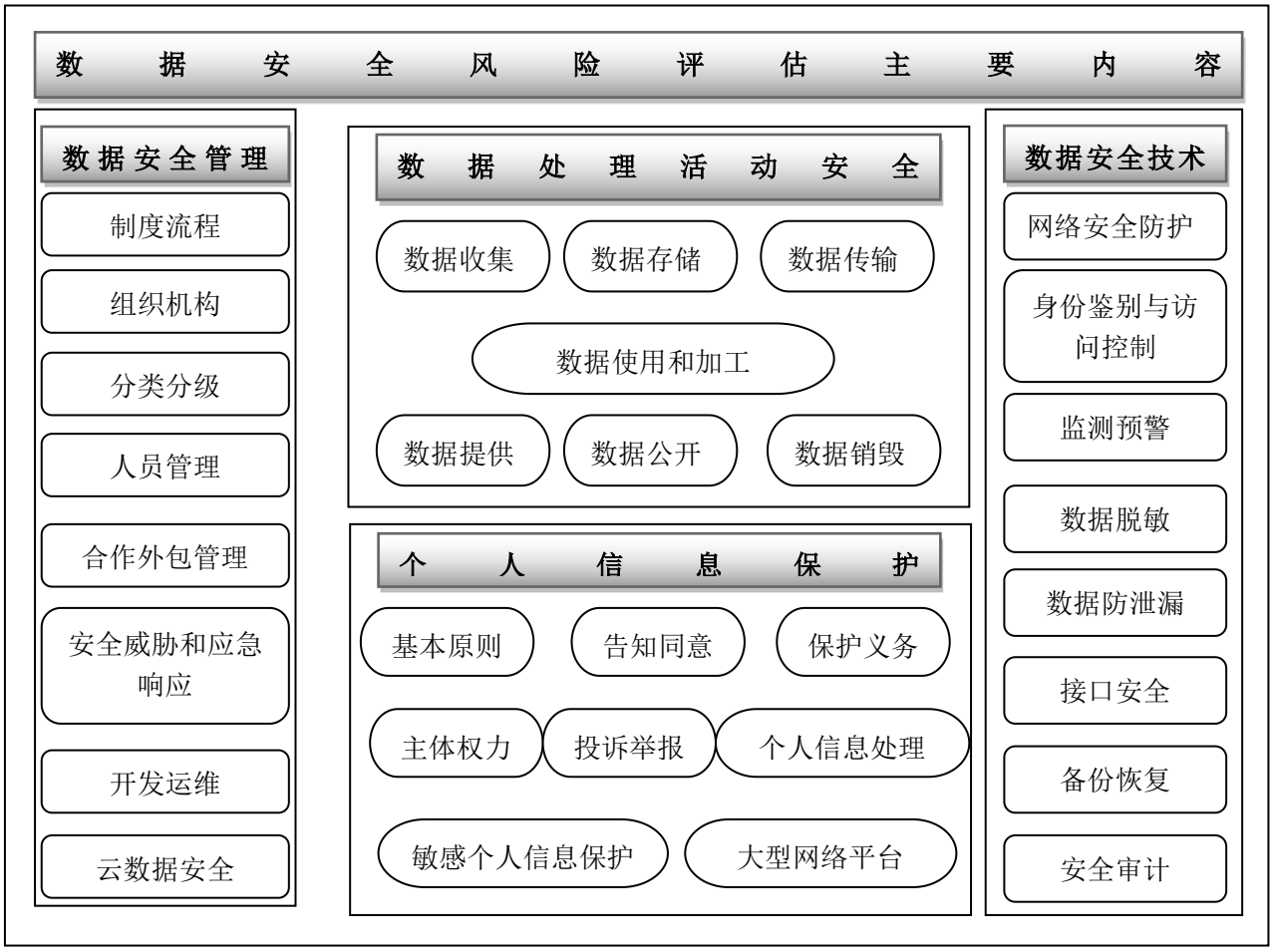

图 1　数据安全风险评估主要内容

4.3 评估流程

数据安全风险评估的实施流程主要包括评估准备、信息调研、风险识别、综合分析、评估总结5个阶段，具体实施步骤见图2。

图 2　数据安全风险评估流程

4.4 风险评估手段

开展数据安全风险评估时，综合采取一下手段进行风险评估：

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) 文档查阅：查验数据安全管理制度、风险评估报告、网络安全等级测评报告等相关材料及制度、责任落实的证明材料；
c) 安全核查：核查网络环境、数据库、业务应用系统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、渗透测试等手段核查数据资产情况、检验防护措施有效性。

5 数据安全风险评估的阶段性工作

5.1 评估准备阶段

5.1.1 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，全面摸清数据类型、数据规模、数据分布、数据应用等基本情况，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、个人信息保护情况进行安全评估，识别可能影响国家安全、公共利益、或个人、组织合法权益的风险评估，发现存在的安全问题和风险隐患，督促数据处理者建立健全数据安全管理制度、技术改进安全措施落地、封堵安全漏洞，促进完善数据安全保护措施，进一步提升数据安全和个人信息保护能力。

5.1.2 确定评估范围

根据组织工作需要和评估目标，确定数据安全评估对象、范围、边界，明确评估涉及到的数据资产、数据处理活动、业务和信息系统、相关人员和内外部组织等情况。

当针对组织全部的数据和数据处理活动开展数据安全风险评估时，应根据需要采取“全面摸排”和“中重点评估”。

a) 全面摸排：全面摸排组织数据安全的整体情况，摸清组织的数据资产类型、数据资产规模、数据处理活动、数据分类分级情况、所涉及的业务和信息系统以及涉及到的业务场景和业务流程等；
b) 重点评估：结合数据分类分级选择重点评估对象，将涉及个人信息、重要数据、核心数据的所有处理活动，可以抽样选择其他典型一般数据的处理活动作为重点评估对象开展数据安全风险评估工作；对于未开展数据分类分级工作的情况，可以结合业务和信息系统的重要性和敏感程度，选择核心业务或重点信息系统的数据或数据处理活动作为重点评估对象。

5.1.3 组建评估团队

数据安全风险评估实施团队应由被评估组织、评估机构等共同组成数据安全风险评估小组，评估机构应该根据评估范围、涉及到的行业领域特征、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，被评估方应建立专项团队，成员一般由数据安全负责人、运维人员、开发人员、业务人员、项目协调人员等组成。

为确保数据安全风险评估工作顺利有效进行，评估方和被评估方应采取合理的项目管理机制，主要相关成员角色与职责说明如表1和表2所示。

表 1 评估机构角色与职责说明

评估机构人员角色	工作职责

项目组长	是数据安全风险评估实施方的管理者、责任人、具体工作职责包括： 1、 应根据项目实际情况组建项目实施团队； 2、 应根据项目情况与被评估方一起确定评估目标和评估范围，并组织项目成员一起对被评估方的数据资产类型、数据资产规模、数据处理活动、数据分类分级情况、

表 1 评估机构角色与职责说明（续）

	所涉及的业务和信息系统以及涉及到的业务场景和业务流程等情况进行全面调研； 3、 应给根据确定的评估范围、目标及调研情况，组织编写数据安全风险评估目标； 4、 应根据评估内容制定评估计划，并根据团队成员实际情况进行分工； 5、 在评估实施阶段时，对实施过程的质量、进度等进行监督、协调、控制，确保各个阶段工作有效实施； 6、 组织阶段性会议，对阶段性的工作想被评估方汇报和沟通，及时商讨项目进展情况以及发生和可能发生的问题； 7、 组织项目成员对风险评估的工作成果进行汇总，整理问题及风险清单，编写《风险评估报告》与《风险整改建议》等项目成果； 应负责向被评估方解答项目成果中有关技性细节问题，并组织项目验收。
项目评估成员	是负责数据安全风险评估工作实施的人员，具体工作职责包括： 1、 根据评估的目标、范围的确定以及评估方的数据资产类型、数据资产规模、数据处理活动、数据分类分级情况、所涉及的业务和信息系统以及涉及到的业务场景和业务流程等情况参与数据安全风险评估的方案编制； 2、 遵循《数据安全风险评估方案》，对数据安全管理、数据安全处理活动、数据安全技术、个人信息保护进行风险评估，并形成《问题清单》、《风险清单》； 3、 对评估工作中遇到的问题及时向项目组长进行汇报。
质量控制员	是负责数据安全风险评估中质量的人员，具体工作职责包括： 1、 监督审计各阶段工作实施的进度与时间进度，对可能影响项目进度的问题及时告知项目组长； 2、 负责对项目过程文档进行管控。

表 2　被评估方组成成员角色及职责

被评估方人员角色	**工作职责**
数据安全负责人	是数据安全风险评估中被评估方的总体负责人，具体工作内容包括： 1、 组织项目成员，配合评估工作各个阶段工作； 2、 组织项目成员，对项目实施过程实施方提交的评估信息、数据资产及文档进行确认； 3、 组织项目成员对评估机构提交的《评估评估报告》与《安全整改建议》等项目成果进行审阅并确认； 4、 授权各个阶段的负责人； 5、 对数据安全风险评估工作进行验收。
项目协调人员	由数据安全负责人进行授权，负责各级部门之间的沟通，技术协调、调动相关部门资源的协调，以确保数据安全风险评估工作顺利开展。

注：当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。

5.1.4 开展前期准备

表 3 前期工作内容

工作安排	具体内容
制定工作计划	数据安全风险评估的工作内容主要包括： 1、 评估项目概述 2、 评估目的 3、 评估要求 4、 评估内容 5、 工作流程 6、 项目组织 7、 进步安排 8、 工作联络单 9、 会议记录单
确定评估依据	数据安全风险评估依据包含但不限于： 1、 法律法规：《网络安全法》《数据安全法》《个人信息保护法》等； 2、 部门规章制度：网信部门及主监部门数据安全规章、规范性文件 3、 地方政策：地方数据安全政策规定和监管要求； 4、 相关标准：数据安全国家标准、行业标准、团体标准等；
确定评估内容	结合评估目标、范围、依据，结合被评估方的实际情况，确定每个评估对象适用内容： 1） 应该围绕数据安全管理、数据处理过程、数据安全技术等方面进行评估； 2） 涉及个人信息的，应在 1）的基础之上，对个人信息进行开展风险评估。
建立评估文档	数据安全风险评估的评估文档应包括但不限于： 1、 数据安全风险评估调研表 2、 技术测试工具 3、 项目配置清单 4、 风险告知清单等
制定评估方案	组织项目成员编制数据安全风险评估方案，主要内容包括但不限于： 1、 评估概述 2、 评估范围 3、 评估人员 4、 评估依据 5、 评估对象情况 6、 评估方法及工具说明 7、 评估活动管理

5.2 信息调研

数据安全风险评估信息调研根据全面摸排的原则进行调研，主要对数据处理者调研、业务和信息系统调研、数据资产调研、数据处理活动调研、已有安全措施调研，具体调研内容单不限于见表4。

表 4 信息调研内容

	调研信息	具体调研内容
数据处理者调研	组织基本信息	单位名称、组织机构代码、办公地址、法定代表人、经营范围、数据安全负责人及岗位情况、联系方式等
	单位性质	例如：党政机关、事业单位、企业、医疗等
	是否属于特定数据类型数据处理者	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；
	所属行业领域	明确组织所性的行业领域，为明确数据安全风险评估的依据做准备；
	业务运营地区	开展数据处理活动所在国家和地区等；
	主要业务范围、业务规模等	明确组织的业务范围和业务规模，为后续风险评估的范围和边界提供基础信息；
	许可证情况	数据处理相关服务取得行政许可的情况；
	实际控制人	被评估单位的资本组成和实际控制人情况；
	境外资产参与情况	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。
业务和信息系统调研	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；
	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；
	业务涉及个人信息	重要数据或核心数据处理情况；个人信息具体类型
	业务为政务部门或境外用户提供服务情况	描述业务为政务部门或境外用户提供服务情况
	信息系统、App 和小程序情况及使用范围	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；
	数据中心和云平台使用情况	描述组织业务在本地 IDC 或云平台使用的情况，是否涉及使用国外云平台（如 AWS、微软云等）
	接入的外部第三方产品、服务或 SDK 的情况	特别针对 APP 使用的第三方 SDK，包括名称、版本、提供方、使用目的、合同协议，是否明确调用或传输的数 据类型、数据字段等。
数据资产调研	数据资产情况	包括数据资产类型、数据范国、数据规模、数据形态、数据存储分布、元数据等；
	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；
	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；
	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；
	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

表 4　信息调研内容（续）

		务流转及与信息系统的对应关系等；
	其他数据资产	
数据处理活动调研	数据收集情况	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；
	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；
	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；
	数据加工使用情况	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；
	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；
	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；
	数据销毁情况	如数据删除情形、删除方式、数据归档、介质销毁等；
	数据处境情况	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。
已有安全措施调研	已有评估	对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；
	组织人员	数据安全管理组织、人员及制度情况；
	安全设备	防火墙、入侵检测、入侵防御等网络安全设备管理、策略、安全配置执行情况；
	身份鉴别	身份鉴别与访问控制情况；
	漏洞管理与修复	网络安全漏洞管理、执行情况及漏洞修复情况；
	远程管理	VPN、零信任接入等远程管理软件的用户及管理情况
	口令技术	办公终端、设备、系统、服务器、数据库及用户的账号口令管理情况；

	安全技术	加密、脱敏、去标识化等安全技术应用情况；
	安全事件	3 年内发生的网络和数据安全事件、攻击威胁情况。如事件名称、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。

5.3 风险识别

数据安全风险识别从数据安全管理、数据处理活动、数据安全技术、个人信息保护情况等方面，通过访谈、现场核查等手段进行风险识别。

5.3.1 数据安全管理

数据安全管理的风险识别的具体内容见表5。

表 5 数据安全管理风险识别主要内容

类别	子项	评估内容
安全管理制度	数据安全制度体系	a） 数据安全总体方针和安全策略，数据安全工作的目标、范围和原则等制定情况； 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、数据安全风险评估、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。
	数据安全制度落实	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。
	重要数据处理者	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； c） 重要数据保护目录情况，重要数据分类分级情况； d） 数据安全宣传教育情况；

类别	子项	评估内容
		e） 数据安全应急演练情况，数据安全事件处置情况。
安全组织机构	数据安全组织架构	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。
	数据安全岗位设置	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。
分类分级管理	数据资产管理	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。
	数据分类分级制度	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。
	数据分类分级保护	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。

类别	子项	评估内容
人员安全管理	人员录用	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。
	保密协议	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。
	转岗离岗	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。
	数据安全培训	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。
合作外包管理	合作方管理机制	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。
	合作协议约束	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。

类别	子项	评估内容
	外包人员访问权限	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。
	第三方接入与数据回收	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。
	政务数据委托处理	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。
安全应急管理	安全威胁和事件	识别安全威胁和安全事件情况，包括但不限于： a)近 3 年发生的网络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、发生的原因、外部威胁、事件级别、处置措施、整改措施等，重大事件需要提供事件调查评估报告，

类别	子项	评估内容
	安全应急管理	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。
开发运维管理	开发运维管理	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。
云数据安全	云计算服务使用方时	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。

类别	子项	评估内容
	云计算服务提供方时	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 24 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。

5.3.2 数据处理活动

数据处理活动的风险识别主要内容见表6。

表 6 数据处理活动风险识别主要内容

类别	子项	评估内容
数据收集	数据收集合法正当性	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。

类别	子项	评估内容
	通过第三方收集数据	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。
	数据质量控制	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。
	数据收集方式	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。
	数据收集设备及环境安全	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
数据存储	数据存储适当性	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。

类别	子项	评估内容
	逻辑存储安全	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。
	存储介质安全	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。
数据传输	传输链路安全性	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。
	传输链路可靠性	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。

类别	子项	评估内容
数据使用和加工	数据使用和加工合法性	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。
	数据正当使用	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。
	数据导入导出	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。

类别	子项	评估内容
	数据处理环境	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。
	数据使用和加工安全措施	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。
数据提供	数据提供合法正当必要性	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。
	数据提供管理	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。

类别	子项	评估内容
	数据提供技术措施	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。
	数据接收方	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。
	数据转移安全	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。
	数据出境安全	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。

类别	子项	评估内容
数据公开	数据公开适当性	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。
	数据公开管理	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。
数据删除	数据删除管理	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。
	存储介质销毁	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。

类别	子项	评估内容
其他	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。

5.3.3 数据安全技术

数据安全技术的风险识别的主要内容见表7。

表 7 数据安全技术风险识别主要内容

类别	子项	评估内容
网络安全防护	网络安全防护	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。
身份鉴别与访问控制	身份鉴别	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。

类别	子项	评估内容
	访问控制	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。
	授权管理	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。
监测预警	监测预警	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。
数据脱敏	数据脱敏	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。

类别	子项	评估内容
数据防泄漏	数据防泄漏	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。
数据接口安全	对外接口安全	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。
	接口安全控制	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。
数据备份恢复	数据备份恢复	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。
安全审计	审计执行	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。
	日志留存记录	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；

类别	子项	评估内容
		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。
	行为审计	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。

5.3.4 个人信息保护

个人信息保护风险识别主要内容见表8。

表 8 个人信息保护风险识别主要内容

类别	子项	评估内容
个人信息处理基本原则	合法、诚信原则	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
	正当、必要原则	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。

类别	子项	评估内容
	个人信息告知	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。
	个人信息同意	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。
个人信息处理	个人信息保存	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。
	个人信息共同处理	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。
	个人信息委托处理	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。
	个人信息转移	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。

类别	子项	评估内容
	向他人提供个人信息	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。
	自动化决策	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。
	个人信息公开	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。
敏感个人信息处理	通用规则	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。
	人脸识别数据安全	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。

类别	子项	评估内容
个人信息主体权利	个人信息的查阅、复制、可携带	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。
	个人信息的更正、补充	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。
	个人信息的删除	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。
	其他个人信息权利	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。
个人信息安全义务	个人信息保护措施	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。

类别	子项	评估内容
	个人信息保护负责人	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。
	个人信息保护影响评估	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。
	个人信息安全应急	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。
个人信息投诉举报	个人信息投诉举报	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。
大型网络平台个人信息保护	大型网络平台个人信息保护	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。

5.4 综合分析

基于5.3章节梳理得出基础上形成问题列表，开展风险分析，并视情况对风险分析进行评价，提出整改建议。

5.4.1 问题清单梳理

基于5.3章节，对每个子项的核查结果形成问题清单，问题清单可以包含单不限于见表9。

表 9 问题清单

序号	问题类别	问题项	风险编号	问题描述

例 1	数据安全管理问题	管理制度流程	A1	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

5.4.2 风险分析与评价

基于5.4.1章节梳理得出的问题清单，综合分析可能存在的安全风险，基于实际情况对的梳理的问题进行风险分析和评价，风险分析主要考虑风险一旦发生可能对本单位、本行业以及国家、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分析。（可以参考《GB/T 20948-2022 信息安全技术 信息安全风险评估方法》、GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南》）。

风险影响程度分析方法见表10、表11、表12但不限于。

表 10 影响范围赋值分析

影响范围赋值	
分值	说明
4	业务时段内影响全部业务
3	影响波及关键的系统，或业务时段内影响部分关键业务。
2	影响波及不涉及到关键业务或系统
1	影响单个非重要业务或单个系统受到影响

表 11 严重程度赋值分析

严重程度范围赋值	
分值	说明
4	导致企业经营中断；重大财务损失；受到行政处罚或诉讼；退市处罚；高安全级信息损毁、丢失、泄露。
3	对业务产生直接影响，降低效率；造成直接的财务损失；企业声誉受到影响；中安全级信息损毁、丢失、泄露
2	会造成系统故障，但不会影响到系统的运行效率及业务；无直接财务损失；声誉受到潜在的影响；低安全级信息损毁、丢失、泄露
1	无直接影响或损失

表 12 风险影响程度计算

影响范围	1	2	3	4

严重程度	1	1	3	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

风险发生的概率计算方法见表13、表14、表15，但不限于。

表 13 控制措施有效性分析

影响范围赋值

分值	说明
4	控制措施效果失效，易发生控制故障或发生事故。在一季度内发生一次或失效发生率占该工作总数量低于 30%。

表 13　控制措施有效性分析（续）

3	控制措施部分失效，因控制措施失效，可能会产生风险。在半年内发生次数不超过一次或失效发生率占该工作总数量低于 10%。
2	控制措施基本有效，因控制措施失效产生的风险可能低。在 1 年内发生次数不超过一次或失效发生率占该工 作总数量低于 1%。
1	控制措施有效性高，因控制措施失效产生的风险可能非常低。在 3 年内发生次数不超过一次.

表 14　控制措施全面性分析

严重范围赋值	
分值	说明
4	没有制定相关管理制度也没有执行任何控制手段。
3	已制定了管理制度，但未进行实施或采取相应的控制手段。
2	未制定管理制度，但采取了控制措施。
1	制定了管理制度，并采取了相应的控制手段。

表 15　风险发生的概率赋值

影响范围	1	2	3	4
严重程度	1	1	3	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

表 16　风险值

发生概率		1	2	3	4	6	8	9	12	16
影响程度	1	1	2	3	4	6	8	9	12	16
	2	2	4	6	8	12	16	18	24	32
	3	3	6	9	12	18	24	27	36	48
	4	4	8	12	16	24	32	36	48	64
	6	6	12	18	24	36	48	54	72	96
	8	8	16	24	32	48	64	72	96	128
	9	9	18	27	36	54	72	81	108	144
	12	12	24	36	48	72	96	108	144	192
	16	16	32	48	64	96	128	144	192	256

风险值[1.32]为低风险，风险值[36，108]为中风险，风险值[128，256]为高风险。

5.4.3 风险整改建议

结合实际情况，针对发现的数据安全问题或风险，提出管理、技术等方面的问题整改或风险处置建议，风险整改建议应该是针对识别出来的安全问题或风险，具体问题针对具体对象方能完成整改。

整改建议清单见表表17.

表 17 风险整改建议

序号	评估类别	风险项	风险编号	风险描述	风险等级	改进途径	整改方案
例 1	数据安全管理问题	管理制度流程	A1	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	中	管理改进、技术改进、管理+技术改进	具体解决方案

5.5 评估总结

评估团队根据评估的实际情况编制数据安全风险评估报告（报告模板参见附录X），数据安全风险评估报告应包括：

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隐患和问题情况;

e) 风险综合分析：对数据安全问题可能带来的安全风险进行综合分析，视情从险对国家安全、公共利益、行业、组织或者个人的合法权益造成的影响程度、风险发生可能性等角度对风险进行评价；

f) 风险整改建议：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) 数据安全清单：列出完整的数据安全问题清单，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。

注：委托第三方机构开展评估或检查评估的场景：评估报告应由评估小组组长、审核人签字，并加盖评估机构。

注：涉及重要数据、个人信息、核心数据的场景：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措施等。

附 录 A
（规范性）
数据安全风险识别方法

本附录给出了常见的数据安全风险识别方法，在数据安全风险识别时候可参考表A.1的内容。

表 A.1 重点评估内容

检查项	检查点	检查类别	检查方法
用户个人信息收集	信息采集合法正当	访谈 文档检查	1)访谈相关人员，询问企业已收集哪些用户个人电子信息，了解收集目的; 2)检查用户协议内容中，是否包含收集用户个人电子信息正当、明确的目的;
		登陆检查	1)检查系统存储了哪些用户个人电子信息，并与收集目的比对看是否合理、一致; 2)查看业务系统获取用户同意的方式方法，是否是主动勾选。
	信息采集最小化原则	访谈	1）通过访谈形式获悉企业收集用户个人电子信息的类别及字段; 2）通过访谈形式了解企业收集用户个人电子信息的手段;
		安全测试	1)对于涉及到用户信息收集系统，新建测试账号，在注册，使用过程中通过代理抓包测试，分析系统收集用户信息字段; 2)与用户协议中告知部分的收集目的进行对比验证，查验是否只收集最少信息字段;
	信息采集目的用途	文档检查	1)在采集外部客户、合作伙伴等相关方的数据的过程中，是否明确采集数据的目的和用途;
		访谈 文档检查	1)访谈相关人员，询问企业收集用户个人电子信息的方式、类别、留存期限及保护措施等; 2)检查用户协议内容中，对于收集用户个人电子信息的部分，是否明确告知如下事项: a)收集用户个人电子信息的目的、方式、类别和留存时限: b）用户个人电子信息的使用范围，包括披露或向其他组织和机构提供其用户个人电子信息的范围; c)用户个人电子信息的保护措施; d)提供用户个人电子信息后可能存在的风险; e)不提供用户个人电子信息可能出现的后果 f)用户个人电子信息管理者的名称、地址、联系方式等信息; g)用户的投诉渠道;

表 A.1　重点评估内容　（续）

用户个人信息收集	信息采集目的用途	登陆检查	1）收集个人信息最小元素集中的个人信息时，是否征得了个人信息主体授权同意 2）是否明确告知信息主体在选择不同意授权情况下的影响和结果； 3)收集最小元素集之外的个人信息时，是否额外征得个人信息主体授权同意 4)收集年满 14 周岁的未成年人的个人信息前，是否征得未成年人或其监护人的明示同意； 5)不满 14 周岁的，是否征得其监护人的明示同意； 6）是否存在以改善服务质量、提升用户体验、研发新产品等为由，以默认授权、功能捆绑等形式强迫用户同意其收集个人信息；
数据使用	去标识化处理	登陆检查	1）除目的所必需外，使用个人信息时是否消除明确身份指向性，避免精确定位到特定个人； 2)使用个人信息时，是否超出与收集个人信息时所声称的目的具有直接或合理关联的范围，因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意；
		访谈	1)通过人员访谈了解企业收集个人信息后，个人信息控制者是否立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别个人的信息分开存储，并确保在后续的个人信息处理中不重新识别个人；
		访谈 登陆检查	1）通过访谈了解用户个人电子信息是否存在用户端上显示的可能,并询问显示方式； 2)涉及通过界面展示个人信息的(如显示屏幕、纸面），个人信息控制者是否对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险；
		访谈 登陆检查	1)通过访谈了解是否存在开发人员使用真实用户个人电子信息的情况发生； 2)如果使用真实用户个人信息是否具备脱敏工具；
		登陆检查	1)登录测试数据库； 2)查验测试环境中是否存在未经过模糊化处理的真实用户个人电子信息，
		登陆检查	1)新注册系统测试账户一个，填写相关用户个人电子信息并提交； 2)进入用户个人电子信息显示页面，查验相关信息的显示是否进行了模糊化处理

表 A.1　重点评估内容　（续）

	敏感数据操作权限	访谈 文档检查	1)通过访谈了解个人敏感数据操作管理制度及技术手段; 2)是否在数据分类分级定义的基础上，建立数据操作规范，明确不同数据的业务场景和操作流程，制定数据的需求、规则、方法和使用限制等;(备注:如没有接入 4A，则需要数据库自身设置访问权限控制。如果没有接入金库模式，则敏感数据访问都票要工单或纸质等授权凭证。4A 需要能够控制到数据库表级，人员权限与岗位满足"最小化"要求。)
		安全测试	1)建立测试账户尝试越权访问感信息,验证是否存在越权访问的可能

表 A.2　数据安全技术

检查项	检查点	检查类别	检查方法
数据加密	数据传输加密	访谈 文档检查	1)通过人员访谈了解企业是否梳理需要对传输通道加密的业务场景 2)是否在数据分类分级定义的基础上明确提出对相关类型、级别的数据的加密传输要求,针对数据的加密传输要求应包含对数据加密算法要求和密钥的管理要求;
		安全测试	1）是否提供对传输通道两端进行主体身份鉴别和认证的技术方案和工具; 2）是否针对关键的数据传输通道，统一部署传输通道加密方案(如采用 TL/SSL 方式); 3）是否提供对传输数据的完整性进行检测并执行恢复控制的技术方案和工具; 4)是否提供对数据传输安全策略的变更进行审核和监控的技术方案和工具，部署对通道安全配置、密码算法配置、密钥管理等保护措施进行审核及监控的技术工具; 5)是否建设密钥管理系统提供数据的加密解密、签名验签等功能，并实现对密钥的全生命周期(生成、存储、使用、分发、更新、销毁等)的安全管理，
	数据存储加密	访谈	1)通过人员访谈了解企业存储个人敏感信息时,是否采用加密等安全措施; 2）存储个人生物识别信息时，是否采用技术措施处理后再进行存储，例如仅存储个人生物识别信息的摘要
		访谈 登陆检查	1)通过访谈询问企业对数据存储已采用的技术措施， 2）登录系统数据库管理平台，查验相应存储表内的鉴权信息等敏感字段是否加密存储，

数据脱敏	数据脱敏处理	访谈 文档检查	1)通过人员访谈了解企业是否在数据分类分级定义的基础上建立数据脱敏规范，明确需要脱敏处理的应用场景和脱敏处理流程，制定数据脱敏的需求、规则、方法和使用限制等; 2)是否在数据权限和资源的申请阶段,需由该数据的安全管理岗位人员评估使用真实数据的必要性,以及确定该场景下适用的数据脱敏规则及方法，

表 A.2　数据安全技术　（续）

		登陆检查	1)通过人员访谈了解企业是否提供统一的数据脱敏工具,实现数据脱敏工具与数据权限管理平台的联动，以及数据使用前的静态脱敏; 2)是否提供面向使用者的数据脱敏定制化功能,可基于场景需求自定义脱敏规则; 3)数据脱敏后是否保留原始数据格式和特定属性,满足开发与测试需求， 4)是否提供数据脱敏处理过程的日志记录功能,满足数据脱敏处理安全审计要求;
操作权限管理	业务系统账号管理	访谈 文档检查	1)通过访谈了解企业是否建立访问控制制度,明确数据处理活动相关业务系统的账号管理访问、授权管理、数据处理操作等规程; 2)通过访谈了解数据处理活动中涉及到哪些相关业务系统; 3)检查是否制定系统的账号管理制度; 4)检查账号管理制度中是否对用户登录进行访问控制 5)检查账号管理制度中是否对密码复杂度进行要求; 6)检查账号管理制度中是否对系统账号的输入次数限制; 7）检查账号管理制度中是否对口令遗忘的申请和重置流程实施严格管理; 8)检查账号管理制度中是否对账号口令和加密密钥开展了保护工作;
		登陆检查安全测试	1)登录系统查看密码复杂度策略配置,核实是否跟账号管理制度匹配 2）登录系统查看口令输入尝试次数过多防护策略配置; 3）通过系统查验账号口令及加密密钥的是否加密存储;
		安全测试	1)新注册系统测试账户一个,检查所要填写的用户鉴权信息是否要求不小于位 8，并有复杂度要求使(用大写字母、小写字母、数字、标点及特殊字符四种字符中至少二种的组合，且与用户名无相关性; 2)新建测试账号进行测试，模拟暴力破解输入错误一定次数，验证防护手段是否真实有效; 3）模拟口令遗忘场景，验证口令重置的管理流程中是否存在业务逻辑涉及缺陷， 4）通过专业的弱口令扫描工具对调研系统及应用进行弱口令扫描，查看是否存在弱口令;

	业务系统访问授权	访谈 文档检查	1)通过访谈了解数据处理活动中涉及到哪些相关业务系统; 2）查看授权管理制度，是否控制对数据和系统物理与逻辑访问; 3）查看授权管理制度，访问授权是否以“必需知道”和“最小授权”为原则; 4)企业是否根据数据访问人员岗位职责、操作目的、所属主体等划分数据访问权限级别,在数据处理活动相关业务系统落实数据访问控制策略;
		访谈 登录检查	1)通过访谈了解数据处理活动中业务系统访问授权技术管控手段 2）查看访问授权策略配置;

表 A.2　数据安全技术　（续）

		安全测试	1)通过申请内部网络,测试访问这些业务系统是否存在未授权访问情况或者绕行访问的情况:
	运维支撑人员操作权限	访谈 文档检查	1)通过访谈形式了解运维支撑人员查询、变更数据等操作权限申请流程 2）是否按照最小够用原则进行划分;
		登录检查	1)查验运维支撑人员对数据的查询和变更等操作权限申请是否有申请及审批记录; 2)查验运维支撑人员操作数据库权限配置策略,是否提供精细化的访问控制策略;《比如细化到库、表、字段等) 3)查验运维支撑人员对数据批量导入导出、备份等操作是否有审批记录，导出数据是否采取模糊化处理;
		安全测试	1）建立测试账户尝试越权访问，验证是否存在水平和垂直越权访问的可能;
数据流动	数据流动记录	文档检查	1)针对数据流动，对不同单位间(同级单位、上下级单位、内外部单位)的数据共享有相应人工或系统记录
人员操作日志记录	重点环节日志留存管理	文档检查	1)检查是否建立数据操作日志管理制度，明确操作日志记录规范， 2)检查是否对数据收集、使用、传输、存储、共享、删除等环节的重点操作日志和系统日志进行留存管理:
	日志记录完整、准确	登陆检查 文档检查	1)查验数据采集行为日志记录是否包括采集时间、对象存储地址、采集指示等关键字段， 2）查验数据共享转移等操作日志记录是否包括操作人员、操作对象、操作时间和操作内容等关键字段 3)查验删除数据和销毁电子信息存储介质过程日志记录是否包括执行时间、参与人员、处理方式等，
	日志留存时间要求	访谈	1)通过访谈了解上述日志记录留存时间，是否不低于 180 天;
		登陆检查	1)检查上述各类日志留存时间配置策略; 2)检查是否能够查询 180 天以前的日志记录;

数据备份与恢复	数据备份与恢复	访谈 文档检查	1)通过访谈了解企业是否在数据分类分级定义的基础上建立数据存储几余策略和管理制度，以满足数据服务可靠性、可用性等数据安全保护目标; 2)是否建立数据复制、备份与恢复的操作规程，明确定义数据复制、备份和恢复的范围、频率、工具、过程 日志记录规范、数据保存时长等， 3)是否建立数据复制、数据备份与恢复的定期检查和更新工作程序，包括数据副本更新频率、保存期限等， 确保数据副本或备份数据的有效性;

表 A.2　数据安全技术　（续）

数据备份与恢复	数据备份与恢复	登陆检查	1)是否建立了用于数据备份、恢复的统一技术工具，并将具体的备份的策略固化到工具中，保证相关工作的 的自动化执行; 2)是否建立备份数据的安全管理技术手段,包括但不限于对备份数据的访问控制、压缩或加密管理、完整性 和可用性管理; 3》是否定期开展备份数据的可用性测试，留存测试结果;
安全风险监测	企业内部数据安全风险监测	文档检查	1)查看重点针对业务支撑类后台系统，及数据安全评估类(云计算、大数据、物联网、网厅掌厅、用户广告精准推送、即时通信、涉及数据对外的合作)业务的基于日志亩计报告。
数据安全事件溯源	数据安全事件溯源记录	登陆检查	1)通过日志审计是否发现安全事件，溯源需要可定位到账号。
数据接口安全	接口安全	访谈 文档检查	1)通过访谈了解企业是否制定数据接口调用安全控制策略,明确规定使用数据接口的安全限制和安全控制措施，如身份鉴别、授权策略、访问控制机制、签名、时间戳、安全协议等 2）是否建立数据接口调用的安全规范，包括接口名称、接口参数、接口安全要求等: 3）是否与数据接口调用方签署 7 合作协议，在合作协议中明确了对数据的使用目的、供应方式、保密约定及 数据留存期限等; 4)定期对本企业对外数据接口进行清查,对不符合要求的对外数据接口立刻予以关停;(备注:接口范围重点针对业务支撑类后台系统，及数据安全评估类(云计算、大数据、物联网、网厅掌厅、用户广告精准推送、即时通信、涉及数据对外的合作)业务的对外接口(包括对其它省移动公司、专业公司、集团公司、外部厂商或机构、公众进行开放的接口)。)

		文档检查 安全测试	1）是否统一收集数据接口调用的相关记录日志，并建立相应针对数据接口调用的审计工具 2)是否对大数据平台与应用内跨安全域间的接口调用采用安全通道、加密传输等安全机制
		安全测试	1)是否提供对数据接口调用的安全限制和安全控制措施，如身份鉴别、授权策略、访问控制机制、签名、时间戳、安全协议等，并对数据接口调用的参数进行限制，一但发现异常会触发告警机制 2)对数据接口执行技术测试，确认安全控制措施的有效性，并检查是否存在安全漏洞;

表 A.3　数据安全制度建设

检查项	检查点	检查类别	检查方法
分类分级	数据分类分级策略和标准	访谈 文档检查	1) 通过人员访谈了解企业是否具备数据分级分类管理制度; 2)检查是否对数据进行分类分级管理，制定数据分类分级原则、定义和方法，针对具体的关键业务场景制定数据安全分类分级的细则， (备注:各单位需要制定独立的分类分级规范制度。各单位可以复用集团已发布的《中国移动大数据安全管控分类分级实施指南》，但需要根据各自的数据库表等字段，依据集团规范做相应字段映射，并形成数据资产分类分级清单。各单位也可以根据实际情况新制定自有可落地实施的分类分级规范。）
	针对性的安全管理及技术保障策略	文档检查	1)需要在分类分级规范制度中根据不同级别明确差异化管控的措施，管控措施达到可实操的程度
		登陆检查	1)是否建立数据的安全分类分级标识工具,基于数据资产安全分类分级策略对数据进行自动的分类分级标识实现数据标识结果的发布和亩核等: 2）检查是否依据数据资产分类分级要求建立相应的标记策略、访问控制、数据加解密、数据脱敏等安全管理 71 和控制措施,(备注:2019年，针对分类分级技术手段方面建设方面(如在数据库中针对不同级别打上分类标签等)暂不做要求,但针对分类分级管理手段方面(如个人信息未经用户授权不得对外开放等)的要求需要实际落实。针对同一条记录各字段属性级别不一样的情况,采取就高不就低的原则进行管控。）

检查项	检查点	检查类别	检查方法
安全评估	数据安全评估整体要求	访谈 文档检查	1)通过访谈了解企业是否具备数据安全评估制度，主要针对企业整体数据安全保护工作情况开展评估，评估内容包括但不限于数据安全风险情况、数据合规使用提供情况、数据安全保障措施合规与完善程度、合作方数据安全保护水平，对发现的问题及时整改。 2)企业是否根据制度要求，提供本年度企业整体数据安全保护工作评估报告，识别数据安全存在风险，数据合规使用提供情况，数据安全保护措施合规及匹配性分析，合作方数据安全保护水平，及对发现的问题整改落实情况
	重点业务评估定期评估	访谈 文档检查	1)检查企业是否落实工业和信息化部互联网新技术新业务安全评估有关办法和标准要求，结合业务类型和场景，将数据安全作为安全评估重点内容。每年至少定期组织开展一次数据安全评估，评估对象是否包含但不限于云计算、大数据、物联网、网掌厅、即时通信、用户广告精准推送等及涉及数据对外合作的业务； 2)查看企业全量业务系统清单，查验上述涉及到重点业务系统评估报告，及相关评估过程记录。

表 A.3　数据安全管理制度　（续）

监测巡查	数据安全日常监测巡查	文档检查	1)检查企业是否建立数据安全日常监测巡查制度(制度中要定义正常操作的范围、日志记录的规则、审计策略等)，定期《至少每月执行一次》开展企业内部数据安全风险监测巡查；
		登陆检查	1)查看操作日志审计策略（模型)是否完善，是否能够发现非授权访问、批量复制或转移敏感数据等，审计过程形成的记录应能对安全事件的处置、应急响应和事后调查提供支撑； 2)查看日常监测巡查记录及对异常情况处置证明材料；

应急响应	应急预案及演练	访谈 文档检查	1）通过访谈了解企业是否制定数据安全应急响应预案，（备注:如果预案是集团单位下发指导性文件，各省单位要编制操作手册或细则。如单位组织角色及分工等,应急上报实施流程等需要各单位根据实际情况细化。） 2）通过查验企业数据安全应急预案，核实是否明确目的、依据、范围、原则、事件分级和分类、组织结构及职责、预防和预警机制、应急处置、应急响应保障措施等; 3）检查是否根据业务场景制定特定事件应急响应流程《个人信息泄露等》，及时配套相关安全保障措施。 4）检查企业是否根据应急预案要求，制定演练计划并定期组织演练，保存演练记录，
	数据安全事件处置	访谈 文档检查	1)访谈了解企业是否发生数据安全相关事件。 2)检查是否在发生数据安全事件时及时按照应急响应制度和应急预案实施应急措施; 3)检查在发生数据安全事件时是否及时将事件情况、应急措施以及可能造成的影响等向电信主管部门报告: 4)检查在发生用户个人信息泄露、毁损和丢失时，是否及时以邮件、信函、电话、推送通知等方式通知可能受到影响的用户，难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息，提醒用户采取防范措施; 5)检查告知内容是否包括但不限于:a.安全事件的内容和影响;b.已采取或将要采取的处置措施,c.个人信息主体自主防范和降低风险的建议;d.针对个人信息主体提供的补救措施，e.个人信息保护负责人和个人信息保护工作机构的联系方式;

表 A.3　数据安全管理制度　（续）

数据安全监督检查	数据安全监督检查制度	访谈 文档检查	1)通过访谈了解企业是否建立内部数据安全监督检查制度,定期对企业数据安全管理情况和落实效果进行监督检查，及时督促问题整改,《备注:是指省公司对地市公司、省公司内部的监督检查机制，确保发现问题及时整改，没有遗留问题。监督检查至少一年执行一次。) 2》通过访谈了解企业在监督检查过程中对违反企业数据安全管理制度的行为是否进行责任追究，对违规行为造成数据安全事件进行处罚; 3)查阅数据安全监督检查制度是否跟访谈结果一致; 4)查阅年度数据安全监督检查记录、检查过程中发现问题整改记录、责任追究处罚记录等证明文件
投诉处理	数据安全投诉处理制度	访谈 文档检查	1)通过访谈了解企业是否制定数据安全投诉处理制度; 2)查阅数据安全投诉处理制度是否明确举报投诉处理机构和人员、投诉处理流程和要求等; 3》核实投诉处理答复时间要求是否限制在自接到投诉之日起十五日内;
	公开举报投诉渠道	文档检查	1)核实企业是否建立数据安全举报投诉渠道并对外公布,举报投诉渠道应至少包括以下一种:电子邮件、电话、传真、在线客服、在线表格;备注(1、数据安全投放举报可以采用 10086、10010、10000 中的具体的分类举报渠道，但还需要在线上(官方网站 P)和线下营业厅公开明示举报电话。也可以在官方网站公示具体的投诉举报电子邮箱或设胃明显的投诉举报信息提交窗口(可提交投诉举报人、问题、建议等内容)。投诉举报提示信息需要点明是针对数据安全并涵盖个人信息，不可只针对个人信息。)
	有效举报线索处置和记录	文档检查	1)查阅举报投诉处理记录,核实企业是否按照安全投诉处理制度针对有效举报线索依法依规开展处置和记录,并自接到投诉之日起十五日内答复投诉人;
教育培训	数据安全教育培训制度	访谈 文档检查	1)通过访谈了解企业是否制度数据安全教育培训管理规章制度,并明确培训周期、培训人员、培训内容; 2)查阅数据安全教育培训制度,核实培训周期要求是否为每年至少开展 1 次，培训人员要求是否覆盖数据安全责任人、数据安全管理责任部门全体人员、相关部门配合落实数据安全管理工作的人员;培训内容要求是否台含但不限于数据安全管理与用户个人信息保护相关法律法规、标准制度、安全责任以及安全评估、技术防护应急演练等相关知识技能;
	数据安全教育培训周期	文档检查	1)查阅数据安全培训记录《培训通知、培训课件、培训签到、培训考核等》，核实企业是否按照培训制度要求每年至少开展 1 次数据安全教育培训;

表 A.3　数据安全管理制度　（续）

	数据安全教育培训人员	文档检查	1)查阅数据安全教育培训签到考核记录,核实培训人员是否按照培训制度要求，覆盖数据安全责任人、数据安全管理责任部门全体人员、相关部门配合落实数据安全管理工作的人员;
	数据安全教育培训内容	文档检查	1)查阅数据安全教育培训课件,核实数据安全教育培训内容是否包含但不限于数据安全管理与用户个人信息保护相关法律法规、标准制度、安全责任以及安全评估、技术防护、应急演练等相关知识技能于

表 A.4　组织机构

检查项	检查点	检查类别	检查方法
机构职责	明确数据安全文档检查管理	文档检查	1)通过访谈了解企业内部是否以管理文件形式明确数据安全管理责任部门，负责统筹数据安全和用户个人信息保护工作; 2)查阅相关管理文件，核验牵头责任部门是否唯一;数据安全牵头部门及其责任，是否通过正式文件进行明确，包括不限于 OA 发文、纸质发文、公司领导办公会决议等; 3)查阅企业内部相关管理文件是否与访谈结果一致;
	明确部门管理职责	文档检查	1)查阅企业部门职责说明文件,核实企业数据安全管理责任部门岗位职责是否明确，是否包含但不限于以下内容:包括但不限于制定数据安全管理整体方针策略，协调建立数据安全技术保障措施，牵头做好数据安全事件应急处置，组织开展数据安全评估、教育培训等工作。《备注:如果集团的规范、指南、方法等已达到省公司或专业公司可落地执行的程度，则省公司或专业公司可以直接复用无需另行制定。否则,需要针对职责分工工作流程等诸多细节根据公司实施情况进行补充规定《补充制定具体操作层面的实施细则、操作手册或规范等 2)企业是否能提供本年度的数据安全总体工作计划、数据安全技术保障措施建设规划、数据安全应急事件处置方案、年内组织开展的数据安全评估报告和教育培训记录等证明文件;
岗位人员	人员配备	访谈 文档检查	1)通过访谈了解企业数据安全专职或兼职人员数量; 2)牵头部门、各执行部门都需要有数据安全管理岗位人员配备; 3)对于人员配备，需要通过 OA 公文或管理文件附件，正式明确数据安全岗位人员姓名、岗位职责描述，具体承担落实数据安全管理相关工作;
	数据安全岗位职责	访谈 文档检查	1) 通过访谈了解企业内部是否明确数据安全专职人员职责; 2) 查阅企业内部相关管理文件，针对牵头部门、各执行部门数据安全管理岗位人员的职责是否进行区分。数据安全人员职责是否包含但不限于以下内容:数据安管理制度执行落实、权限管理、安全审计、应急响应约据安全事件处胃和信息报送等工作; 3) 查阅数据安全管理岗位人员是否针对以上工作职责进行落实并提供相关过程证明文件。

附 录 B

（资料性）

数据安全风险评估报告模板

报告编号：xxxxxxxxxxx-xxxx-xxxx

数据安全风险评估报告

被评估单位：	XXXXXXXXXXXXXXXXXXX
评估单位：	XXXXXXXXXXXXXXXXXXX
评估时间：	XXXXXXXXXXXXXXXXXXX

文档信息

报告名称			
报告编号			
文档版本编号		分发份数	

分发控制				
编号	接收人	文档权限	与文档的主要关系	分发份数
1				
2				

修订记录

修订次序	章节号	修订内容	修订原因	修订人	日期

声明

本报告测评结论的有效性建立在被评估单位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测对象当时的安全状态有效。当评估工作完成后，由于被评估对象发生变更而涉及到的系统构成组件（或子系统）本报告不再适用。

本报告中给出的评估结论不能作为对被评估对象内部部署的相关系统构成组件（或产品）的评估结论。

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。

XXXXXXXXXXXXXXXXX

（加盖单位公章）

XXXX 年 XX 月 XX 日

<table>
<tr><td colspan="6">被评估单位</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮政编码</td><td></td></tr>
<tr><td rowspan="3">联系人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>所属部门</td><td></td><td>办公电话</td><td colspan="2"></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮件</td><td colspan="2"></td></tr>
<tr><td colspan="6">评估单位</td></tr>
<tr><td>单位名称</td><td colspan="3"></td><td>机构代码</td><td></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮政编码</td><td></td></tr>
<tr><td rowspan="3">联系人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>所属部门</td><td></td><td>办公电话</td><td colspan="2"></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮件</td><td colspan="2"></td></tr>
<tr><td rowspan="3">审核批准</td><td>评估组长</td><td></td><td>编制日期</td><td colspan="2"></td></tr>
<tr><td>审核人</td><td></td><td>审核日期</td><td colspan="2"></td></tr>
<tr><td>批准人</td><td></td><td>批准日期</td><td colspan="2"></td></tr>
</table>

1. 评估概述

1.1 评估目的

1.2 评估依据

1.3 评估过程

填写说明：评估时间安排

1.4 评估人员

序号	姓名	技术职称/资质	承担工作/角色
1.			总工程师/技术负责人
2.			质量负责人
3.			项目经理
4.			工程师
5.			工程师
6.			工程师
7.			商务协调

1.5 评估时间安排

1、XXXX 年 XXXX 月 XXXX 日～XXXX 月 XXXX 日，评估准备过程。

2、XXXX 年 XXXX 月 XXXX 日～XXXX 月 XXXX 日，方案编制过程。

3、XXXX 年 XXXX 月 XXXX 日～XXXX 月 XXXX 日，现场实施过程。

4、XXXX 年 XXXX 月 XXXX 日～XXXX 月 XXXX 日，分析与报告编制过程

2. 评估对象描述

按照 5.1 章节调研出来的信息说明被评估对象的基本情况

2.1 数据处理者的基本情况

单位全称		简称	
单位情况简介	//描述单位具体职能、职责//		
单位性质	□党府机关 □国家重要行业、重要领域或重要企事业单位 □社会团体□企事业单位□其它类型		
数据处理者类型	□政务数据处理者 □大型网络平台运营者 □关键基础设置运营者 □其它类型		

业务运营地区（含内部业务部门）	//开展数据处理活动所在国家和业务地区//						
主要业务范围、业务规模等							
数据是否处境	//涉外供应商数据处理相关服务取得行政许可的情//						
单位地址							
邮政编码					**组织机构代码**		
数据安全负责人姓名		**电话**		**传真**		**电子邮件地址**	
数据安全负责人部门		**负责人岗位**					
联系人/协调人		**电话**		**职务/职称**		**电子邮件地址**	
上级主管部门							

2.2 业务和信息系统

业务名称	
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	
业务涉及个人信息、重要数据或核心数据处理情况	
业务为政务部门或境外用户提供服务情况	
业务数据相关信息系统接入的外部第三方产品、服务或 SDK 的情况	
数据中心和使用云平台情况	
业务流程图	

2.3 数据资产

序号	信息系统	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	数据来源	数据分级

2.4 数据处理活动

序号	系统名称	数据项	数据采集	数据存储						传输方式		数据使用		数据加工	数据提供	数据公开	数据销毁	
				存储方式	数据中心	存储系统	外部存储机构	存储地点	存储期限	传输途径	传输协议	使用目的	使用范围				情形	方式

2.5 已有安全措施情况

2.6 数据安全风险识别

依据 5.3 章节，按照表格内容进行评估，具体说明问题。

3. 综合分析

3.1 风险分析

3.2 风险评价

3.3 整改建议

附录

可附上证据材料

参 考 文 献

[1] GB/T 20948—2022 信息安全技术 信息安全风险评估方法
[2] GB/T 43697—2024 数据安全技术 数据分类分级规则
[3] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南