ICS 35.240.60
CCS R 07

JT

中华人民共和国交通运输行业标准

JT/T XXXX—XXXX

交通运输数据安全风险评估指南

Guidelines for transportation data security risk assessment

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国交通运输部　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。

本文件由交通运输信息通信及导航标准化技术委员会提出并归口。

本文件起草单位：交通运输部科学研究院、中电长城网际系统应用有限公司、北京中安星云软件技术有限公司。

本文件主要起草人：黄海涛、王涛、尚赞娣、黄莉莉、曹剑东、淡雅静、郑强、郑金、杨洪路、白紫秀、刘娜、任江、吕晓婷、王思源、张平、郭亚茹、王娜、吴聪雷。

交通运输数据安全风险评估指南

1 范围

本文件提供了交通运输数据安全风险评估的指导和建议，并给出了交通运输数据安全风险评估的原则、框架、方法、启动条件和流程。

本文件适用于交通运输行业数据处理者及第三方评估机构开展数据安全风险评估工作，交通运输行业管理部门开展数据安全检查评估工作参照使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

交通运输数据 transportation data

交通运输建设、运营、服务及管理等单位在履行各级职责过程中直接或通过第三方依法采集、产生、获取的，以电子或者其他方式记录的各类信息。

[来源：JT/T 747.4—2020，3.1，有修改]

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

评估域 evaluation domain

实现同一安全评估目标的一系列数据安全风险评估项的集合。

注：一个评估域中包含一个或多个评估子域。

3.4

数据处理活动 data processing activity

数据收集、存储、使用、加工、传输、提供、公开、出境、删除等活动。

3.5

数据安全风险 data security risk

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

3.6

数据安全风险评估 data security risk assessment

对数据和数据处理活动的安全风险和违法违规问题进行检测评估的过程。

3.7

合理性 rationality

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

3.8

安全措施 security measure

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

3.9

业务 business

组织为实现某项发展战略而开展的运营活动。

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，有修改]

3.10

风险源 risk source

可能导致危害数据和数据处理的保密性、完整性、可用性和合理性等事件的原因、条件、情形或行为。

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

4 缩略语

下列缩略语适用于本文件。

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

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

DBA：数据库管理员(Database Administrator)

DDos：分布式拒绝服务攻击(Distributed Denial of Service Attack)

IPSec：IP网络安全性协议（Internet Protocol Security）

PIA：个人信息保护影响评估(Privacy Impact Assessment)

SQL：结构化查询语言(Structured Query Language)

SSL：安全套接字层协议（Secure Sockets Layer）

SSH：安全外壳协议（Secure Shell）

TLS：传输层安全性协议（Transport Layer Security）

5 原则

5.1 客观公正原则

交通运输数据（以下简称“数据”）安全风险评估（以下简称“风险评估”）过程中，根据被评估方实际情况做出判断和真实的评价，不宜夸大或掩盖发现的问题，不宜根据个人主观意愿或他人意见做出评价。

5.2 可重复可再现原则

对于相同风险评估内容和风险评估要求，在相同风险评估环境下，采用同样风险评估方法对同一被评估方的风险评估实施过程进行重复操作，得到相同风险评估结果。

5.3 最小影响原则

在风险评估过程中尽量小地影响被评估方现有业务和信息系统正常运行，最大程度地降低对被评估方造成的干扰和风险。

5.4 保密原则

参与方对风险评估所涉及的被评估方商业信息、客户信息、技术文件等进行严格保密。

6 框架

风险评估框架（见图1）用于识别、执行、分析和评价数据面临的绝大部分安全风险，主体内容由下列部分组成：

a) 风险评估对象基本信息；
b) 风险评估对象所属行业类目；
c) 数据处理活动、数据安全管理、数据安全技术和个人信息保护四个评估域及其评估子域；
d) 风险分析和评价。

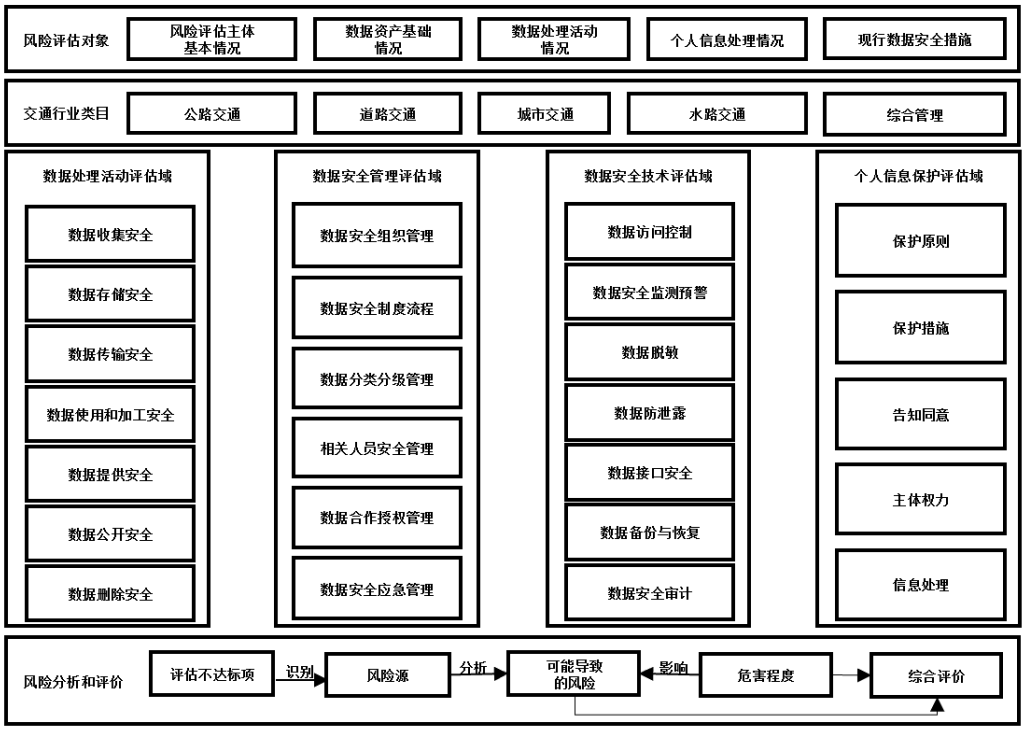

图1 风险评估框架

7 方法

7.1 人员访谈

采取调查问卷、现场面谈或远程会议等形式对被评估方相关人员进行访谈，对被评估的数据、数据处理活动和数据安全实施情况等进行了解、分析和取证。

7.2 文档审核

通过对数据安全的管理制度、安全策略、流程机制、合同协议、设计开发和测试文档、运行记录、安全日志等进行审核、查验、分析，以便了解被评估方的数据安全实施情况。

7.3 系统核查

通过查看被评估方数据安全相关网络、系统、设备的配置、功能或界面，验证数据处理系统和数据安全技术工具使用情况。

7.4 技术测试

通过手动测试或自动化工具验证被评估方数据安全措施有效性，发现可能存在的数据安全风险。

8 启动条件

以下五种情形，宜进行风险评估：

a) 按照对应管理办法开展检查的机构，或未进行过数据安全自评工作的机构；
b) 在国家及行业主管部门的相关要求发生变化时，或在业务模式、信息系统、运行环境发生重大变更时，或发生了重大数据安全事件；
c) 重要数据和个人信息的使用、共享、交易、委托等处理活动发生变化，包括活动主体、处理方式、关键流程等发生变化；
d) 数据处理者开展高风险数据处理活动前，包括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，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，新技术应用可能带来数据安全风险的，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，以及法律法规或有关部门规定的情形；
e) 对于已经做过风险评估的评估主体，当其评估对象的数据范围、数据处理活动、环境、相关方等发生变更时。

9 流程

9.1 通则

风险评估流程分为准备、实施、分析和评价、总结四个阶段，各阶段间为强逻辑关联，宜按照先后工作顺序依次执行，见图 2。

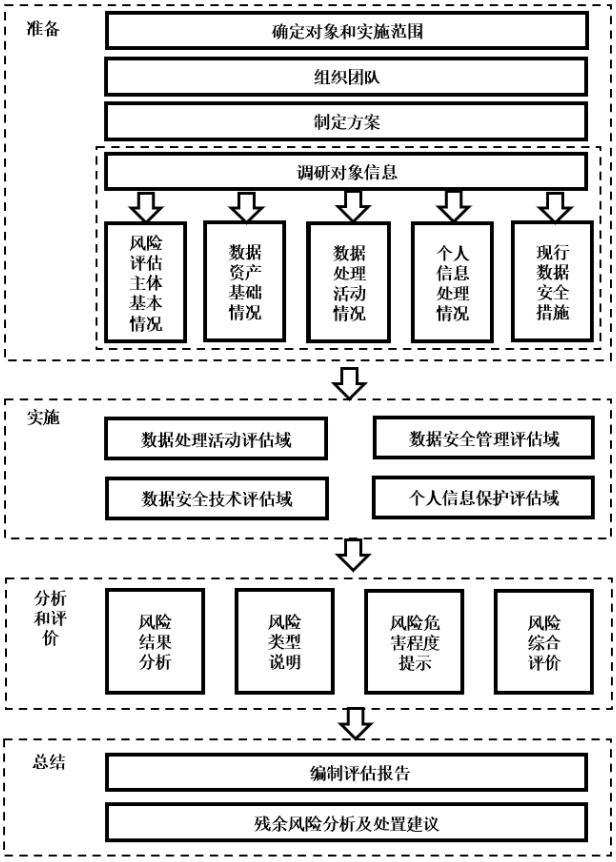

图2　风险评估流程

9.2 准备

9.2.1　确定对象和实施范围

风险评估对象范围信息包括下列内容：

a)　风险评估的主体、范围和边界；
b)　风险评估工作涉及的数据资产、业务和信息系统；
c)　风险评估涉及的数据处理活动情况；
d)　风险评估工作涉及的人员和内外部组织等。

9.2.2　组织团队

风险评估团队宜有明确的组织结构、负责人、成员，包括各自的职责分工确定清晰。

9.2.3　制定方案

风险评估方案主体由下列内容组成：

a)　整体风险评估工作概述，评估对象、评估目标、评估范围、基础信息、评估依据等；
b)　风险评估的内容和方法，评估流程、实施内容、评估准则、使用方法等；
c)　风险评估实施计划，评估具体实施进度安排、人员安排、配套管理等。

9.2.4　调研对象信息

9.2.4.1　风险评估主体基本情况

通过访谈、检查文档材料等方式，对风险评估主体基本情况进行调研，见表1。

表1　风险评估主体基本情况调研

序号	调研内容	调研指标
1	所属交通业务域	a)　公路交通域； b)　水路交通域； c)　道路交通域； d)　城市交通域； e)　综合管理域
2	单位类型性质	a)　党政机关； b)　事业单位； c)　国有及国有控股企业； d)　社会团体； e)　民营企业； f)　其他
3	处理数据级别	a)　一般数据； b)　重要数据； c)　核心数据； d)　自定义分级； e)　未分级
4	处理数据的量级	a)　GB级； b)　PB级； c)　EB级； d)　其它
5	处理的数据范围	a)　全国； b)　省级； c)　市级； d)　其它
6	主要涉及数据处理活动	a)　数据收集情况； b)　数据存储情况； c)　数据传输情况； d)　数据使用和加工情况； e)　数据提供情况； f)　数据公开情况； g)　数据删除情况
7	网络和信息系统基本情况	a)　网络拓扑图； b)　信息系统名称及作用说明； c)　信息系统责任部门； d)　数据使用部门； e)　信息系统主要业务流程；
注：表中GB级、PB级、EB级指得是计算机存储单位，1GB（Gigabyte)=1024MB，1PB（Petabyte）=1024TB，1EB（Exabyte）=1024PB		

9.2.4.2　数据资产基础情况

针对风险评估范围内的数据资产基础情况进行调研，见表2。

表2　数据资产基础情况调研

序号	调研内容	调研指标
1	是否能提供结构化和非结构化数据资产清单	a)　是； b)　否
2	是否完成数据分类分级	a)　是； b)　否
3	数据分级要素是否包含交通运输数据规模、数据精度、数据深度	a)　是； b)　否

表2　数据资产基础情况调研（续）

序号	调研内容	调研指标
4	是否有处理重要数据，重要数据在业务和信息系统的分布情况	a）　是，搜集处理重要数据的系统、重要数据种类、数据规模、业务领域等； b）　否
5	是否有处理核心数据，核心数据在业务和信息系统的分布情况	a）　是，搜集处理核心数据的系统、数据种类、数量； b）　否

9.2.4.3　数据处理活动情况

针对风险评估范围内的信息系统涉及的数据处理活动开展调研，见表3。

表3　数据处理活动情况调研

序号	调研内容	调研指标
1	数据收集情况	a）　数据收集渠道； b）　数据收集方式； c）　数据范围； d）　数据收集目的； e）　数据收集频率； f）　外部数据源清单； g）　合同协议
2	数据存储情况	a）　数据存储方式； b）　存储系统（如数据库、大数据平台、云存储、网盘、存储介质等）； c）　存储主要数据库类型； d）　外部存储机构； e）　存储地点； f）　存储期限； g）　备份冗余策略情况
3	数据传输情况	a）　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）； b）　传输协议； c）　内部数据共享； d）　数据接口情况
4	数据使用和加工情况	a）　数据使用目的； b）　数据使用方式； c）　数据使用范围； d）　数据使用场景； e）　数据使用的类型
5	数据提供情况	a）　数据提供对象； b）　数据提供的目的； c）　数据提供的方式； d）　数据提供的类型与级别； e）　数据接收方信息； f）　提供数据量级
6	数据公开情况	a）　数据公开的目地； b）　数据公开方式； c）　对象范围； d）　数据公开对象； e）　数据公开量级
7	数据删除情况	a）　是否定期删除数据； b）　数据删除场景； c）　数据删除方式； d）　删除的数据级别

9.2.4.4 个人信息处理情况

针对风险评估范围内的个人信息处理情况进行调研，见表4。

表4 个人信息处理情况调研

序号	调研内容	调研指标
1	是否处理个人信息	a) 是； b) 否
2	是否运营互联网平台	a) 是； b) 否
3	处理的个人信息量级	a) GB级； b) PB级； c) EB级
4	个人信息收集目的	a) 行业监管； b) 生产开发； c) 业务运转； d) 委托处理； e) 其他
5	处理的个人信息规模	a) 100万以下； b) 100万至1000万； c) 1000万以上
6	处理的个人信息范围	a) 全国； b) 省级； c) 市级； d) 单一机构； e) 多机构
7	是否利用个人信息进行自动化决策	a) 是； b) 否
8	是否处理敏感个人信息	a) 是； b) 否
9	是否利用个人信息进行自动化决策	a) 是； b) 否
10	处理的敏感个人信息类型	a) 14周岁以下个人信息； b) 生物识别信息； c) 医疗健康信息； d) 行踪轨迹信息； e) 金融信息； f) 特定身份信息； c) 其他
注：表中GB级、PB级、EB级指得是计算机存储单位，1GB (Gigabyte)=1024MB，1PB（Petabyte）=1024TB，1EB（Exabyte）=1024PB		

9.2.4.5 现行数据安全措施

针对风险评估范围内现行数据安全措施情况进行调研，见表5。

表5 现行数据安全措施情况调研

序号	调研内容	调研指标
1	是否设有数据安全管理机构，相关人员及制度情况	a) 是； b) 否
2	防火墙、入侵检测、入侵防御等网络安全设备及策略情况	a) 防火墙设备清单； b) 入侵检测设备清单； c) 入侵防御设备清单

表5　现行数据安全措施情况调研（续）

3	加密、脱敏等数据安全技术应用情况	a）　数据加密产品清单； b）　数据脱敏产品清单； c）　数据库访网关产品清单
4	3年内是否发生的网络和数据安全事件，事件的处置情况	a）　是； b）　否

9.3 实施

9.3.1　数据处理活动评估域

9.3.1.1　数据收集安全评估子域

数据收集安全评估子域内容见表6。

表6　数据收集安全评估子域

序号	风险评估项	风险评估方法	结果判定
1	是否存在窃取或者以其他非法方式获取数据	人员访谈 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　访谈相关人员，了解数据收集方式，确认不存在窃取或其他方式非法获取数据； b）　通过手动或自动化工具进行技术测试，验证不存在窃取或非法获取数据的可能
2	是否在法律、行政法规规定的目的和范围内收集、使用数据	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　访谈相关人员，了解数据收集流程，确认符合法律法规要求的目的和范围； b）　查阅数据收集设备或信息系统的相关建设文档，确认符合法律法规要求的收集方式
3	是否通过合同，协议等合法方式，从外部机构采集有交通运输数据	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　访谈相关人员，确认存在通过合同协议从外部机构采集数据，并确定采集方式、范围、目的等都遵照合同协议进行； b）　查阅相关合同协议文件，确定已经明确数据收集的范围、采集方式、采集目的和授权同意情况
4	是否对外部数据源和外部收集交通运输数据进行鉴别和记录	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　访谈相关人员，确认对外部数据源进行鉴别和记录，并确定鉴别方式； b）　查阅外部数据源采集文件，确定具备对外输数据源收集行为进行鉴别与记录方案； c）　通过查看被评估采集系统，操作验证针对外部数据源进行数据收集的过程具有鉴别行为与日志记录； d）　查看外部数据采集记录，对外部数据源和外部收集数据的合法性、安全性、可靠性和授权同意情况进行审核

表6　数据收集安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
5	是否制定数据质量管理制度，明确数据质量管理要求	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确定已经制定有完善的数据质量管理制度； b) 查阅数据质量管理相关文件，确定文件中明确有数据质量管理的详细要求
6	是否存在采集终端数据泄露风险	系统核查 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查看被评估数据收集终端，操作数据收集，检测不存在数据泄露情况； b) 通过手动测试或自动化工具进行技术测试，验证采集终端或设备不存在安全漏洞
7	是否存在采集数据被未授权篡改、污染原始数据风险	系统核查 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查看数据收集系统，操作进行数据收集，检测不存在未经授权数据篡改情况； b) 通过手动测试或自动化工具进行技术测试，验证不存在未经授权污染原始数据的风险
8	是否制定安全管理和操作规范、是否对数据清洗、转换和加载等行为提出明确要求	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 访谈相关人员确认存在安全管理和相应操作规范，确认对数据清洗、转换和加载等行为提出相关要求； b） 查阅安全管理、操作规范相关文件，确认数据清洗、转换和加载等相关文件是否完善
9	是否制定对异常数据质量、对异常数据及时告警或更正采取手段的措施	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 访谈相关人员确认对异常数据及异常数据及时告警采取更正等相关措施或手段； b） 查阅异常数据处理相关文件，确定对异常数据的处理流程、方法、过程等情况
10	是否收集数据监控、过程记录以及安全措施应用等情况	人员访谈 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 查看数据监控系统，查看确认存在过程记录以及安全措施应用等情况； b） 访谈相关人员，确认有进行收集数据监控等
11	是否对数据的真实性、准确性、完整性进行检验	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 查看数据审计系统，调查确认有对数据的真实性、准确性、完整性进行校验； b） 访谈DBA相关人员，确认进行数据安全配型，有对数据真实性、准确性、完整性进行校验； c） 查看相关数据安全管理文档，调研有存在有对数据的真实性、完整性、准确性有备案的文件

表6　数据收集安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
12	是否测试自动化工具收集数据对网络服务的影响	人员访谈 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 访问相关人员，确认采用自动化工具对外部数据进行访问和收集； b） 检查相关报告，确认测试自动化采集工具对网络服务的性能、功能带来的影响情况
13	采用自动化工具收集数据时，是否违反法律、行政法规或行业自律公约情况，是否侵犯他人知识产权等合法权益情况	人员访谈 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 访问相关人员，调研使用自动化工具有无违反相应法律法规； b） 核查自动化工具，调查违犯收集数据等情况； c） 通过手动对自动化工具进行测试，调查违法收集数据等情况
14	采用自动化工具收集数据时，是否明确数据收集范围、数量和频率，是否收集与提供服务无关数据的情况	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 访问相关人员，在使用自动化工具时，有明确收集收集范围、数量和频率； b） 查看自动化工具使用文档，调研收集与提供服务无关数据的情况
15	采用人工方式采集数据时，是否对数据采集人员严格管理，是否要求对采集数据直接报送到相关人员或系统，是否在采集任务完成后及时删除采集人员留存的数据	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 访问数据采集人员，确认受到严格管理，是否经过相关的专业培训； b） 查看审阅数据收集相关文档，调查要求对采集数据直接报送到系统，存在采集人员的留存的数据
16	是否对人工采集数据环境进行安全管控情况	人员访谈 系统核查 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 访谈数据采集人员，是否对人工采集数据环境进行安全管控； b） 风险评估人员查看人工采集数据环境，确认安全管控方式包括通过人员权限管控、信息碎片化等方式； c） 通过技术测试，对管控方式有效性进行验证
17	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，是否留存敏感跟个人信息或重要数据	系统核查 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 审阅App、Web相关系统，检查有存在缓存数据、个人信息等重要敏感数据； b） 利用自动化工具或手动对App、Web等客户端进行技术测试，确认没有存在缓存数据、个人敏感数据等

9.3.1.2　数据存储安全评估子域

数据存储安全评估子域具体内容见表7。

表7　数据存储安全评估子域

序号	风险评估项	风险评估方法	结果判定
1	是否根据相应的数据类别和级别采取相应的存储方式和安全措施，如加密存储、去标识化存储等	文档审核 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关文档，确认根据数据分类分级要求，所对应数据采取不同的存储方式进行了策略指定； b) 通过手动测试或自动化工具进行技术测试，查验数据已进行加密处理，去标识化等步骤
2	是否明确数据备份与恢复的策略和操作规程	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确认已制定有数据备份和恢复的操作规程以及策略文档； b) 查阅相关文档，审验内容中对于数据备份和恢复的策略和操作，具有清晰的流程界定、参数说明、操作指南等细则
3	是否对数据处理活动涉及到的系统进行安全防护，能够具备网络攻击等事件的防护能力	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确认具备了安全措施，并了解具体的安全能力； b) 查阅相关合同协议文件，确认所提供的安全设备符合国家相关法律法规，确认设备功能与安全能力能够对应，并处于正常工作状态
4	是否采用技术手段对存储数据进行备份，并定期对备份数据的有效性进行验证	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关规范说明，确认存在数据备份的技术操作环节，具备定期备份的机制； b) 通过进行相关系统操作，查验数据备份系统的操作流程正确，规范、有效，最终可以满足数据备份要求
5	是否对数据存储系统进行访问权限管理，根据数据的类别和级别以及访问人员应用的角色进行权限的分配和管理	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确定系统访问有权限划分，是根据角色的不同匹配对应的权限； b) 查阅系统文档，对访问权限的管理，角色分配的机制，具有详细说明与操作方式，参数指导等细则； c) 通过查看被评估系统，操作验证系统具备对数据类别和级别进行权限分配和管理的能力
6	是否采取一定措施确保数据存储的完整性，存储交通运输重要及以上数据时，是否采用密码技术、权限控制等技术措施保证数据完整性	文档审核 系统核查 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅系统文档，对数据存储完整性措施、密码技术、权限控制技术等具有详细说明与操作方式，配置指导等细则； b) 通过进行相关系统操作，确认系统采取了相应措施确保数据完整性； c) 通过手动测试或自动化工具进行技术测试，查验数据进行完整性处理的实施情况

表7　数据存储安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
7	在我国境内产生的交通运输数据是否都在我国境内存储，国家及行业主管部门另有规定的除外	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅相关文档，确认根据数据分类分级要求，所对应数据采取不同的存储方式进行了策略指定； b）　通过手动测试或自动化工具进行技术测试，查验数据已进行加密处理，去标识化等步骤
8	是否定期检测逻辑存储系统安全漏洞，是否针对安全漏洞进行修复与处置	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　访谈相关人员，确认已制定有数据备份和恢复的操作规程以及策略文档； b）　查阅相关文档，审验内容中对于数据备份和恢复的策略和操作，具有清晰的流程界定、参数说明、操作指南等细则
9	是否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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅相关产品文档，确认设备功能具备对操作人员行为限制策略； b）　系统核查验证，设备处于正常工作状态，文档中记录的功能均能实现
10	是否定期开展数据存储灾难恢复演练，对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试结果	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅系统文档，确定制定了数据存储灾难恢复演练，且对关键技术进行验证和记录
11	是否落实数据存储安全策略和操作规程的建设情况，存储位置、期限、方式是否适当	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅系统文档，确定制定了数据安全存储安全策略和操作规程； b）　访谈相关人员，确认数据的存储位置、期限和存储方式的适当性
12	永久存储数据类型是否必要	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅系统文档，明确了永久存储的数据类型及对应的使用场景； b）　访谈业务相关人员，确认永久存储数据的必要性
13	云存储的安全性是否有保障	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　检查云上数据梳理情况，内容包括数据存放路径，数据量、获取方式以及丢失影响等； b）　将备份数据存放在云外存储介质当中，检查备份策略的设置合理，历史备份任务的记录完整； c）　具有云存储数据恢复与恢复演练相关的制度，内容包括恢复演练周期、流程，以及应急恢复流程、操作指南等

表7　数据存储安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
14	是否落实数据数据库账号权限管理、访问控制、日志管理、加密管理、版本升级等建设情况，是否监测逻辑存储系统的安全漏洞，是否实施限制数据库管理、运维等人员操作行为，是否根据安全级别对数据分级差异化存储	人员访谈 系统核查 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 通过自动化工具或手动测试方式，对数据库账号权限管理、访问控制、日志管理、加密管理等进行测试，确认逻辑存储系统u无漏洞； b） 访问相关人员，有被限制了操作行为； c） 通过相关系统操作，核实系统有根据安全级别对数据分级进行差异化存储
15	是否明确对存储介质存储数据的安全要求，是否对存储介质进行定期或随机性安全检查情况，是否对存储介质访问和使用行为的记录进行审计	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 核查相应存储介质系统，调研其安全检查情况； b） 查阅系统文档，查阅存储介质摆放情况和使用行为记录

9.3.1.3　数据传输安全评估子域

数据传输安全评估子域具体内容见表8。

表8　数据传输安全评估子域

序号	风险评估项	风险评估方法	结果判定
1	是否根据国家相关法律法规中关于数据传输的相关要求，制定数据分类分级传输管理规定，并根据管理规定设计相应的数据传输策略，保证数据传输的合理性	人员访谈 文档审核 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，了解传输管理规定根据数据分类分级规定制定了对应的策略，可以保障传输的合理性； b) 查阅系统文档，确定按照相关法律法规要求，制定了数据分类分级方法和策略； c) 通过手动测试或自动化工具进行技术测试，根据管理办法中的策略，检测在数据传输过程中的应用效果
2	是否采取认证、鉴权和加密等安全措施，对数据传输的过程和内容进行安全保护，防止数据在传输过程中被窃取和泄露，保护数据传输的保密性	人员访谈 文档审核 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确认对于数据传输过程采取了加密措施，防止被窃取或泄露； b) 查阅系统文档，确定采取了相应安全传输措施，以防止数据被窃取或泄露； c) 通过手动测试或自动化工具对数据传输的格式和内容有加密进行检测，确认配置传输协议加密识别规则可行
3	是否采取完整性校验算法对数据传输的发送和接收进行校验，防止数据在传输过程中被篡改和破坏，保护数据传输的完整性	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，了解加密机制中使用的算法，确认算法提供的效验满足保护数据完整性的要求； b) 查阅相关合同协议文件，确定密码设备符合国家相关规定，所使用的算法符合相关法规，包括但不限于SSL、TLS、IPSec、SSH

表8　数据传输安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
4	针对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	文档审核 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 查阅系统文档，确定使用了安全的加密算法，以确保数据传输的安全性； b） 通过手动测试或自动化工具对数据传输的内容进行技术测试，确认加密算法可靠性
5	是否针对数据传输、接收的情况进行记录与审计	文档审核 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 查阅系统文档，明确指定了对数据传输进行记录与审计的规定和要求； b） 通过手动测试或自动化工具进行技术测试，确认系统按照要求对传输情况进行记录与审计
6	向国家机关、行业主管和监管单位传输数据，是否按照国家及行业相关管理要求进行传输	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅系统文档，确认按照国家及行业要求,规定了相应的传输方法
7	是否存在数据传输安全策略和操作规程，是否采取安全传输协议等安全措施，是否对数据异常传输进行处置	文档审核 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 查阅系统文档，确认数据传输安全策略和操作规程； b） 通过自动化工具或手动测试方法，测试数据的异常传输处理情况，测试系统有采取安全传输协议
8	网络传输链路是否可用，是否对关键网络传输链路、网络设备节点实行冗余建设，是否建立容灾方案和宕机替代方案	文档审核 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 通过自动化工具或手动测试方法，查看网络传输链路的可用性； b） 查看系统文档，调查有相关容灾方案和宕机替代方案
9	对外部开展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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 确认对外点对点传输数据有完整审批流程； b） 查阅与外部签订的合同或数据安全责任书等文件，已明确双方数据安全责任与保护义务

9.3.1.4　数据使用和加工安全评估子域

数据使用和加工安全评估子域具体内容见表9。

表9　数据使用和加工安全评估子域

序号	风险评估项	风险评估方法	结果判定
1	数据的使用、共享、开放是否得到数据所有者的授权，流程是否合法合规	人员访谈 文档审核 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 访谈相关人员，了解数据使用具备完整的流程说明，规定了明确的授权流程，权责范围，有对应的操作细则； b） 查阅系统文档，对数据的使用，明确制定了符合国家和行业要求的的授权说明和授权流程； c） 通过手动测试或自动化工具进行技术测试，检测授权机制的执行，具有访问口令、认证方式等措施，与操作文档的内容相符

表9　数据使用和加工安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
2	数据是否分级，并对敏感数据采用对应级别保护措施	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，了解数据分级制度建立情况，确认对应不同级别数据有对应的防护措施，不同的保护手段； b) 查阅相关系统说明文档，确认实行数据分类分级措施，包括数据标签、表单等形式有明确区分的机制
3	是否存在数据资产被恶意破坏情况，例如修改/删除，导致不可用	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅资产梳理记录，根据前期信息调研的结果，确认资产完整性，系统性，查看如存在被破坏情况，需要具备情况整体说明记录； b) 通过查看系统运行情况，确认对于资产管理具备完整日志记录，保障信息可追溯
4	是否存在敏感数据未脱敏使用的情况	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确定对于敏感数据按照相关数据分级分类要求进行脱敏处理； b) 查阅资产目录，确认按照分级分类要求，个人信息等敏感数据，在使用过程中不存在明文方式
5	是否对数据的访问权限和实际访问控制情况进行定期审计，至少每半年1次对访问权限规则和已授权清单进行复核，及时清理已失效的账号和授权	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确定对数据访问权限和控制进行定期审计，并按照要求进行复核和处置； b) 查阅系统文档，明确按照分类分级要求，制定了数据访问权限的控制的审计方法及复核处置方法
6	是否针对特权账号明确安全责任人，严格限定特权账号的使用地点，并配套多因素认证措施对使用者进行实名认证	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅系统文档，明确按照分类分级要求，制定了针对特权账号的安全认证措施及责任权属； b) 通过进行相关系统操作，确认特权账号的使用采用了多因素认证措施
7	是否根据最小够用原则，明确数据导出场景、导出数据范围和相应的权限规则，并在实际数据导出时严格执行	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅系统文档，明确制定了对数据导出场景下的权限规定及对应审计措施； b) 通过进行相关系统操作，查看在进行数据导出时，确认按照权限规定进行了限制，并进行了复核措施
8	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅系统文档，制定了对存储介质的加密、使用、销毁等方案及措施； b) 通过进行相关系统操作，确认对导出数据的操作符合对应要求

表9　数据使用和加工安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
9	是否明确原始数据加工过程中的数据获取方式、访问接口、授权机制、逻辑安全、处理结果安全等内容	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅系统文档，明确制定了对数据加工过程安全内容的要求
10	是否对数据加工过程进行监督和检查，确保加工过程的数据安全性，并完整记录数据加工过程的操作日志	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅系统文档，明确制定了数据加工过程中监督和检查的方法与措施，并进行日志记录； b）　通过进行相关系统操作，确认在数据加工过程中进行了相应的监督和检查，并记录了操作日志
11	数据使用和加工应合法合规，在使用和加工数据时，是否遵守法律、尊重社会公德和伦理，遵守商业道德和职业道德	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　审核相关系统文档，查看使用数据条目没有存在违反行为； b）　访问数据使用者，调查其在使用数据时没有存在违反相关规定行为
12	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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　审核相关系统文档，查看使用数据条目没有存在违反行为； b）　访问数据使用者，调查其在使用数据时没有存在违反相关规定行为
13	是否制作、发布、复制、传播违法信息	系统核查	满足以下要求的为符合，不满足以下要求的为不符合：企业建立针对公共违法信息内容监测处置的管理机制和技术手段，能够有效识别、即时停止发布、传输法律法规禁止发布或者传播的信息内容，并依照国家相关法律法规要求留存日志信息
14	采用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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：对信息推荐算法开展定期审核、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，并留存相应记录
15	是否有数据使用加工安全策略和操作规程的建设	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：审核相关系统文档，确认已制定数据使用和加工安全策略和操作规程
16	数据使用行为是否与承诺或用户协议一致	人员访谈 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　访谈相关人员，确认业务流程中设置了一致性审核环节； b）　通过系统核查业务数据使用情况，确定数据使用行为与用户协议一致
17	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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　访谈相关人员，确认存在完整的变更个人信息使用目的或规则的流程； b）　查阅相关文档，确认实际存在隐私政策等向用户说明使用目的的文档

表9　数据使用和加工安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
18	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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 访谈相关人员，了解评估主体开展得数据技术应用情况； b） 查阅文档，确认技术应用情况的实际效果是利于促进经济社会发展
19	是否存在利用数据开展用户画像、信息推送造成用户受不公平价格待遇、平台竞争秩序受影响	系统核查	满足以下要求的为符合，不满足以下要求的为不符合：通过自动化或手动测试方法，查看是否存在信息推送、用户画像造成的不公平待遇
20	数据使用加工目的、方式、范围是否与行政许可、合同一致	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅系统文档，确定其数据使用和加工目的、方法、范围与行政许可、合同一致
21	是否存在个人信息和重要数据滥用情况	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关管理制度，明确存在个人信息与重要数据使用要求
22	是否定期对个人信息和重要数据导出行为进行安全审计	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅审计报告文档，确认对数据导出行为有专项审计，审计异常情况有及时处理
23	数据处理环境是否配备安全管控手段，并定期清查风险	系统核查 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 数据处理环境已设置身份鉴别、访问控制、隔离存储、加密、脱敏等安全措施； 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； c） 定期扫描处理环境安全漏洞，并及时处置
24	是否建设数据防泄漏	系统核查	满足以下要求的为符合，不满足以下要求的为不符合：系统已纳入数据防泄漏保护范围，制定有详细的数据防泄露规则，并已启用
25	是否建设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	系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 配备数据脱敏技术能力，具备批量自动化脱敏、脱敏策路配置、脱敏流程审批、脱敏效果验证等功能； b） 按照数据的敏感等级设置不同的脱敏规则，采用遮蔽、随机替换、溯源水印、差分隐私等脱敏算法，确保各类数据处理场景中数据脱敏的有效性和合规性

表9 数据使用和加工安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
26	是否对数据访问与操作行为的最小化授权、访问控制、审批等进行管理	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查看创建和注销账号审批记录，确认权限设置有遵循“权限明确、职责分离、知其所需、最小特权”的原则，避免非授权用户或业务访问数据，严格控制超级管理员权限账号数量，每个账号唯一对应一个用户，账号授权按照角色或用户组进行； b) 查阅相关说明文档，确认对数据安全管理人员、数据使用人员、安全审计人员的角色进行分离设置； c) 查询相关文档，确认涉及授权特定人员超权限处理数据的，由数据安全管理责任部门进行审批并记录； d) 接入数据处理活动平台系统的用户或业务进行身份接入认证及权限控制，开展账户口令及加密密钥保护工作
27	是否对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；是否对高风险行为审计及回溯	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 数据授权访问、批量导出或删除、开放共享、销毁，及数据接口调用等场景有留存记录日志，日志记录至少包括执行时间、操作账号、处理方式、授权情况、IP 地址、登录信息等； b) 有配备日志安全审计员并完成日志安全审计； c) 查看数据安全审计制度，有明确审计对象、审计内容、实施周期、结果规范、问题改进跟踪等要求
28	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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查看制定数据对外合作实施方案，方案中有明确企业对外合作中数据安全保护方式和合作方责任落实要求； b) 查看有与合作方签订数据安全协议； c) 业务合作结束后，有督促第三方依照合同约定及时关闭数据接口，删除数据； d) 有采取其他技术措施或约束手段防止受托方非法留存、扩散数据

9.3.1.5 数据提供安全评估子域

数据提供安全评估子域具体内容见表10。

表10 数据提供安全评估子域

序号	风险评估项	风险评估方法	结果判定
1	数据提供过程中，是否存在未采取保护措施，造成数据的破坏或泄露的情况	人员访谈 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确认数据提供的机制，有明确的保护机制，提供约定等详细内容； b) 通过手动测试或自动化工具进行技术测试，确认数据导出时采取了保护措施，符合传输过程的安全要求

表10　数据提供安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
2	数据提供过程中，是否存在未根据国家或行业有关要求进行分类分级管理，造成对提供数据的破坏或泄露的情况	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，明确数据输出是按照分级分类不同规定，对外提供的管理情况； b) 查阅数据，对于数据输出管理，需按照分级分类有不同的分项、操作和记录
3	数据提供过程中，是否存在未按要求进行审批的情况	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，了解数据输出的审批流程，内容有明确的分层要求，具备详细的审批记录表； b) 查阅相关合同协议文件，确定数据使用方是符合国家和行业相关法律法规的主体（自然人），协议内容中有明确的约定条款，以执行数据输出时的安全保护措施
4	涉及个人信息的数据，是否存在提供过程中未采取脱敏措施，造成个人信息泄露的情况	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅个人信息数据使用情况，文档要包含符合个保法条款所规定的各种方案记录； b) 通过查看系统使用情况，在个人信息数据导出时，有进行明文脱敏、关键信息脱敏，有按照审批流程中的规定进行导入导出
5	数据提供方和接收方，在提供前是否存在未签署流转协议，未明确安全责任等情况	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，了解数据提供的管理情况，确认有具备正规的协议文件，具体提供和协议签署的前后顺序正确、规范； b) 查阅对应文档，确认协议内容中应包含明确安全责任条款，对数据输出的各个环节都有明确的约定，尽可能规避流转途中责任不明的风险
6	对外提供的敏感数据是否进行加密及加密有效性	文档审核； 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅对应文档，明确制定了对敏感数据的加密措施； b) 通过进行相关系统操作，确认对外提供的数据进行了有效的加密措施
7	对共享数据及数据共享过程的监控审计情况	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅对应文档，明确制定了对数据共享过程的监控审计方案措施； b) 通过进行相关系统操作，确认在数据共享过程中进行了监控和审计
8	对外提供数据时是否采取签名、添加水印等安全措施	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅对应文档，明确在对外提供数据时采取了相应的安全措施； b) 通过进行相关系统操作，确认在对外提供数据时，采用了签名、水印等安全措施

表10　数据提供安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
9	针对数据提供是否具有跟踪记录数据流量、接收者信息及处理操作信息的手段，记录日志是否完备、是否能够支撑数据安全事件溯源	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅对应文档，明确已依据分类分级要求，制定了能够支撑安全事件溯源的数据跟踪全流程记录方案与措施； b)　通过进行相关系统操作，确认在数据提供过程中，完整的跟踪记录了数据流转信息
10	数据的接收方是否存在诚信问题、违法违规问题、境外政府机构合作关系、被中国政府制裁等	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅数据接收方的资质与企业诚信档案，明确接收方不存在诚信、违法违规问题及境外机构合作关系等； b)　访谈相关人员，确认按照相关规定对数据接收方的资质及诚信问题进行核实及审计
11	数据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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅对应文档，明确数据接收方依据分类分级要求制定了保障数据安全的管理措施和技术措施； b)　访谈相关人员，确认对数据方制定的安全管理措施进行了审核评估
12	是否存在提供超时、超量、超数据类型向数据接收方提供合同约定外数据的情况	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅对应文档，明确制定数据提供的期限、范围、类型及其他约定内容的约束规定； b)　访谈相关人员，确认在数据提供过程中，不存在提供超出合同约定的情况，以及对应的审计措施执行情况
13	数据对外提供的目的、方式、范围的是否合法、正当、必要	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅相关技术文档与合同，确定数据提供目的、方式与范围，有提前告知用户，征得用户同意； 访谈相关人员，明确向第三方提供数据是为满足业务所必须
14	数据提供的依据和目的是否合理、明确	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关技术文档，明确向第三方提供数据是为满足业务所必须
15	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关技术文档，明确对外提供的个人信息和重要数据范围，是限于实现处理目的的最小范围
16	是否建设数据提供安全策略和操作规程	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关制度文档，确认已建立完善数据提供的安全策略与操作规程
17	数据对外提供是否进行审批	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关审批记录，确认数据对外提供的审批情况
18	对外提供数据前，是否进行风险评估和个人信息保护影响评估	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关评估记录与报告，确认在对外提供数据前进行风险评估

表10　数据提供安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
19	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是否进行风险评估	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关评估记录与报告，确认在开展相关活动前进行风险评估
20	是否向境外执法机构提供境内数据	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 访谈相关人员，确认在向境外执法机构提供境内数据前，收到境内执法部门提出的提供要求； b） 查阅文档，确认留存相关部门的要求文件
21	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：确认存在相关评估报告与批准的报告
22	数据对外提供的安全保证措施是否有效	系统核查	满足以下要求的为符合，不满足以下要求的为不符合：通过进行相关技术操作，确认数据得到安全保障
23	数据提供是否存在多方安全计算、联邦学习等技术	技术测试	满足以下要求的为符合，不满足以下要求的为不符合：通过自动化或手动测试方法，验证数据提供技术中的多方安全计算、联邦学习等技术的应用安全情况
24	数据接收方处理目的、方式、范围是否合法、正当、必要	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关技术文档与合同，确认数据接收方处理数据的目的、方式和范围，判断其是合法
25	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关记录文档，确认对合作方进行背景调查和安全资质审查，综合评估第三方的数据安全保障能力
26	是否对接收方数据使用、再转移、对外提供和安全保护进行监督	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅数据安全责任协议，确认对接收方明确对数据安全保护方式和责任落实要求
27	数据进行转移时，是否向有关主管部门报备	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查看报备记录，确认数据转移前向主管部门报备
28	是否制定数据转移方案	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查看相关文档，确认制定有数据转移方案
29	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查看相关文档，确认对数据接收方数据安全保障能力进行评估的记录
30	没有接收方的，是否对相关数据进行妥善删除	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 查阅相关文档，有对数据删除操作进行记录，包括删除时间、删除内容、删除方式等必要内容； b） 核查系统没有留存有该部分数据
31	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关文档，确认有梳理数据出境场景，并覆盖全部业务场景与产品类别
32	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关文档，确认有梳理数据出境线路，并覆盖公网出境、专线出境等情形

表10　数据提供安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
33	涉及数据出境的，是否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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关文档，确认是按照规定开展出境风险评估、个人信息保护认证以及标准合同的签订

9.3.1.6　数据公开安全评估子域

数据公开安全评估子域具体内容见表11。

表11　数据公开安全评估子域

序号	风险评估项	风险评估方法	结果判定
1	在数据公开前，是否评估数据公开影响	人员访谈 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　访谈相关人员，确认在数据公开前，已评估数据公开的影响； b)　通过手动测试或自动化工具进行技术测试，验证在数据公开前已对数据公开影响进行风险评估
2	数据公开过程是否开展日志记录	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　访谈相关人员，确认在数据公开过程中展开日志记录工作； b)　查阅信息系统的相关建设文档，确认该设备或信息系统在数据公开的过程中进行了日志记录工作
3	是否对数据公开所面临的风险进行安全评估	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　访谈相关人员，确认设备或系统对数据公开所面临风险进行风险评估； b)　查阅信息系统的相关建设文档，确认该设备或信息系统在数据公开所面临的风险进行安全的风险评估
4	是否制定针对数据公开可能引发安全事件的应急响应预案	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅信息系统的相关建设文档，确认该设备或信息系统制定了针对数据公开可能发生得安全事件的应急响应预案； b)　通过查看被评估设备或信息系统，执行相应操作，查看安全事件应急响应预案情况
5	数据公开前，对公开数据是否对国家安全及公共利益产生重大影响进行审核或风险评估	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　访谈相关人员，确认该设备或系统在数据公开前，已对公开该数据对国家安全及公共利益产生重大影响进行审核评估； b)　查阅信息系统的相关建设文档，确认该设备或信息系统在数据公开前，对公开该数据对国家安全及公共利益产生重大影响进行了审核评估

表11　数据公开安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
6	是否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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅信息系统的相关建设文档，明确制定了对数据公开的要求与方法，包括脱敏、添加水印、防爬取和权限控制等措施； b)　通过查看被评估设备或信息系统，执行相应操作，查看对公开数据的脱敏、防爬等控制效果
7	针对公开的数据是否会存在聚合性风险	人员访谈	满足以下要求的为符合，不满足以下要求的为不符合：访谈相关人员，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，不能推断出涉密信息、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
8	数据公开目的、方式、范围是否适当，是否与行政许可、合同授权一致	人员访谈	满足以下要求的为符合，不满足以下要求的为不符合：访谈相关人员，调研数据公开目的、方式、范围具体情况，结合行政条款和法律法规，综合合同授权判断其一致性
9	是否存在数据公开的安全制度、策略、操作规程和审核留存	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅信息系统相关建设文档，确认其数据公开的相关安全制度，存在相应的处理和操作规程，存在流程审核审批文档
10	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	人员访谈	满足以下要求的为符合，不满足以下要求的为不符合：通过访谈相关主管部门和个人，确认主管部门负责人收到相应的申请记录和其批准情况，确认个人同意授权提供个人信息
11	是否处置因法律法规、监管政策的更新，而不宜公开的已公开数据	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　对相关系统操作，检查不宜公开的数据； b）　通过查阅信息系统相关建设文档，查看其不宜公开数据的处置记录

9.3.1.7　数据删除安全评估子域

数据删除安全评估子域具体内容见表12。

表12　数据删除安全评估子域

序号	风险评估项	风险评估方法	结果判定
1	是否依照数据分类分级规定建立数据删除策略和管理制度	文档审核 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅信息系统的相关建设文档，明确依据分类分级规定，制定数据删除管理办法； b)　通过手动测试或自动化工具进行技术测试，按照分级分类要求，对于数据删除操作进行策略查验，确认相关执行有效

表12　数据删除安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
2	是否建立用户数据删除需求的响应机制	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，对于数据删除需求的响应有建立相关机制，机制运行应用的情况； b) 查阅数据，对于需求响应的删除操作，档案应包含需求输入审批、记录、执行等详细信息
3	是否建立数据删除有效性的验证机制	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，了解数据删除操作后有效性验证机制情况，采用方式和确认结果； b) 查阅相关合同协议文件，确定需要删除的数据不违背国家行业相关法规，协议约定中明确了数据删除的需求
4	是否建立用户或业务变更时的数据删除机制	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关文档，查验条款中有对用户业务变更时的数据删除机制，有对应变更规定，相关内容有包含需求变更、策略变更、有效性验证变更等细则； b) 通过查看系统使用情况，确认业务变更或用户角色变化时，对应的数据删除机制有具备相应的调整，调整后的策略中体现的用户和业务有也发生对应的调整
5	是否建立数据删除审计机制	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确认在数据删除管理规定中，具备第三方审查的环节； b) 查阅数据，明确文档内容中对于第三方的设立、要求有明确的细则，对于审查的范围、机制、权力和义务有明确的规定
6	针对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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确认委托第三方数据处理结束后，对数据进行了删除或返还操作； b) 查阅相关文档，明确制定了针对委托第三方进行数据处理结束后的删除或返还方案措施
7	是否进行数据删除的有效性、彻底性验证，是否存在多副本未彻底删除的情况	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确认在进行数据删除操作时，对删除结果进行了验证； b) 查阅相关文档，依据分类分级要求，明确制定了相应删除验证措施
8	是否存在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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关文档，确认制定了针对数据删除安全的策略和操作规程，制定了数据毁灭方式和销毁要求的操作规程
9	是否按照法律法规、合同约定、隐私政策等及时删除数据	人员访谈	满足以下要求的为符合，不满足以下要求的为不符合：访谈相关人员，确认其数据的删除方式符合法律法规和合同约定以及隐私政策

表12　数据删除安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
10	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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 访谈相关人员，明确其数据存储最后期限，明确哪些数据未进行删除以及未进行删除的原因； b） 查阅相关文档，查看数据删除记录和存储记录，确定数据存储期限
11	缓存文件是否及时删除	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 查阅相关技术文档，确认已制定缓存文件处置机制，包括缓存时间、缓存位置等； b） 查看系统缓存位置，核查到期缓存文件有已及时删除
12	是否存在存储介质销毁管理制度和审批机制	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关文档，确认存在存储介质销毁管理制度和审批机制
13	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	文档审核 人员访谈	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 查阅相关文档，确定介质销毁的策略和操作规程具体内容，确定其有明确各类介质的销毁流程和方式，确定文档中有记录存储介质使用的记录； b） 通过访谈相关介质销毁人员，调查其介质销毁具体情况，有妥善处置销毁存储介质
14	是否存在存储介质销毁过程的监控、记录，是否对被销毁的存储介质进行数据恢复验证	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 通过相关系统操作，确定系统中有存在存储介质销毁过程的监控和记录； b） 查看销毁记录，销毁存储介质的手段满足无法恢复数据的要求

9.3.2　数据安全管理评估域

9.3.2.1　数据安全组织管理评估子域

数据安全组织管理评估子域具体内容见表13。

表13　数据安全组织管理评估子域

序号	风险评估项	风险评估方法	结果判定
1	是否设立由交通运输机构高级管理层组成的数据安全领导小组，总体负责数据安全工作的统筹组织、指导推进和协调落实，明确数据安全管理部门，协调机构内部数据安全管理资源调配	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a） 查阅数据安全管理委员会领导小组相关制度及工作文件，确认领导小组由本机构高级管理层构成； b） 查阅相关制度文件，确认领导小组的工作职责已主要涵盖总体负责数据安全工作的统筹组织、指导推进和协调落实、协调本机构内部数据安全管理资源调配等，并且已明确数据安全管理部门

表13　数据安全组织管理评估子域（续）

序号	风险评估项	风险评估方法	结果判定
2	是否设立数据安全管理委员会，成员应至少包括主要部门的主要负责人，负责数据安全相关工作的实施、相关政策和制度的制定评审工作，保障数据安全管理工作所需资源，并设立数据安全管理专职岗位，负责日常数据安全管理工作	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全管理委员会相关制度及工作文件，确认委员会成员至少包括信息科、业务科室、法务、合规、风险管理、稽核审计等相关部门的主要负责人； b) 查阅相关制度文件，确认委员会的工作职责已主要涵盖负责数据安全相关工作的实施、相关政策和制度的制定评审工作，保障数据安全管理工作所需资源等； c) 查阅相关制度文件，确认已设立数据安全管理专职岗位，且其职责为日常数据安全管理工作； d) 访谈数据安全管理专职岗位人员，确认日常工作已落实到人、岗位职责明确
3	是否制定、发布和更新本机构数据安全管理制度、规程与细则，并定期审核和修订	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅本机构数据安全管理制度、规程与细则等相关文件，确认其完备性； b) 查阅相关制度、规程与细则的审核及更新记录，确认已定期审核和修订
4	是否针对业务部门、信息系统建设部门、信息系统运维部门设置数据安全人员，人员对数据安全管理要求执行是否到位	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅关于设立数据安全岗位作为数据安全管理执行层的制度文件，确认其包括业务部门、信息系统建设部门和信息系统运维等数据安全管理与安全应用相关部门； b) 访谈数据安全管理专职人员，确认其对数据安全管理要求执行到位、岗位职责明确
5	数据安全岗位人员是否已根据数据安全相关策略和规程，落实本部门数据安全防护措施	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅本部门数据安全防护措施落实的相关工作材料，确认其符合数据安全相关策略和规程； b) 访谈相关人员，确认本部门实际落实的数据安全防护措施与数据安全相关政策和规程一致
6	数据安全管理责任部门是否落实监督检查和考核问责制度要求	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全管理制度，确认已制定监管监察和考核问责制度要求； b) 访谈相关部门人员，确认工作落实到人，了解监督监察和考核问责流程与制度一致
7	针对特权账户所有者、关键数据处理岗位等数据安全关键岗位是否设立双人双岗	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关制度文件，确认针对特权账户所有者、关键数据处理岗位等数据安全关键岗位要设立双人双岗； b) 访谈特权账户所有者、关键数据处理岗位等数据安全关键岗位人员，确认实际落实的人员岗位设立与制度和政策相一致

9.3.2.2 数据安全制度流程评估子域

数据安全制度流程评估子域具体内容见表14。

表14 数据安全制度流程评估子域

序号	风险评估项	风险评估方法	结果判定
1	组织是否建立数据访问权限管理、数据安全合规性评估、数据全生命周期管理、数据合作方管理、数据安全应急响应等制度	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关记录与相关政策和规程一致； b) 查阅相关制度文件，确认组织已经建立数据访问权限管理、数据安全合规性评估、数据全生命周期管理、数据合作方管理、数据安全应急响应等制度
2	是否针对数据活动，制定需遵循的数据格式、数据定义等规范性要求	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈数据安全相关人员，确认其掌握数据格式、数据定义的规范性要求； b) 查阅相关制度文件，确认针对数据活动已经制定需遵循的数据格式、数据定义等规范性要求； c) 查阅数据库设计文档，确认针对数据活动制定数据格式、数据定义等规范要求； d) 查阅数据库表，确认字段数据类型、数据格式、取值范围、表存储方式等与设计文档一致
3	是否建立数据资产管理台账	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全制度流程相关体系文件，确认建立数据资产管理台账的制度措施； b) 查阅文档，确认有数据资产管理台账
4	是否建立数据分级分类方法，并按照规定执行数据分类分级管理	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅数据安全制度流程相关体系文件，确认已定义数据分级分类方法，并基于规则实行分类分级
5	是否按照分类分级策略形成数据资产清单	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全管理制度，确认在数据资产梳理过程中，已经按照分类分级策略形成数据资产清单； b) 访谈相关人员，了解数据分类分级策略流程，确认在相关制度及流程范围内进行
6	是否建立数据分级保护规程	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关制度文件，确认建立数据分级保护规程
7	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅数据安全记录文件，确认按照数据安全制度的要求进行文档记录。具备操作规程、记录表单等制度落实证明材料，记录完整
8	是否对有关制度的有效性进行定期评价与更新，确保基于数据分级的数据安全制度体系能覆盖数据全生命周期	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅数据安全相关记录文件，确认有对有关制度的有效性进行定期评价与更新

表14　数据安全制度流程评估子域（续）

序号	风险评估项	风险评估方法	结果判定
9	数据安全管理制度内容是否符合国家和行业数据安全法律法规和监管要求	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅数据安全管理相关制度文件，确认其符合国家和行业数据安全法律法规和监管要求
10	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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部的相关政策文件、责任分配记录、事件处理报告等文档，确认已明确建立并实施了网络安全责任制和数据安全责任制； b) 对于发生的网络安全和数据安全事件，有明确的记录显示责任人已被识别、追究，并采取了相应的处理措施； c) 访谈数据安全管理专职岗位人员，确认网络安全责任制、数据安全责任制已落实到人、岗位职责明确
11	数据安全制度的制定、评审、发布流程建设情况	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部的数据安全制度相关文件，确认存在明确的数据安全制度制定、评审、发布流程； b) 流程文件中详细描述制度的起草、审核、批准、发布和更新的步骤，以及各步骤的责任主体和时间要求，并且有明确的发布记录
12	向有关部门报送评估报告情况时，风险评估报告是否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	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅报送的风险评估报告，确认报告中包含了对处理的重要数据种类和数量的详细描述，全面记录了数据处理活动的各个环节，如数据的收集、存储、使用、传输、公开和删除等； b) 确认报告中详细列出了在数据处理过程中识别出的数据安全风险，并针对每项风险提出了相应的预防和应对措施

9.3.2.3　数据分类分级管理评估子域

数据分类分级管理评估子域具体内容见表15。

表15　数据分类分级管理评估子域

序号	风险评估项	风险评估方法	结果判定
1	是否建立数据资产管理制度，是否具备数据资产清单	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关制度文件，确认已经建立数据资产管理机构、有健全的数据资产管理体系制度； b) 查阅数据安全记录文件，确认有数据资产清单

表15　数据分类分级管理评估子域（续）

序号	风险评估项	风险评估方法	结果判定
2	数据资产的梳理是否能够覆盖数据库，大数据存储组件，云上对象等数据	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈数据安全相关人员，了解数据资产梳理流程，确认掌握数据收集对象及范围，有都遵照制度要求进行； b) 查阅相关制度文件，确认数据资产的梳理能够覆盖数据库、大数据存储组件、云上对象存储或网盘等存储工具； c) 查阅相关制度文件，确认数据资产的梳理能够覆盖个人计算机、U 盘、光盘等存储媒体中的数据
3	是否通过数据资产管理工具形成了支持即时更新的数据资产清单	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅通过本机构数据资产管理工具，对数据处理者、业务和信息系统、数据资产、数据处理活动、安全措施等情况，形成数据资产清单； b) 查阅变更数据收集信息，确认数据资产清单即时更新、维护
4	是否采用技术手段定期对数据资产进行扫描，是否能够发现识别常见个人信息	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关技术文档，确认有对数据资产定期扫描的设计； b) 通过系统核查数据资产，确认不能发现识别常见的个人信息
5	数据资产管理工具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	文档审核 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据资产报告或有关材料，确认数据标识结果正确发布； b) 检查数据资产管理工具具有录入安全等级识别规则、识别规则合并分组、指定识别数据源，绑定识别规则组等功能； c) 检查数据资产管理工具具有建立识别任务进行自动化标识能力，并能够对识别结果评审确认，结果保存
6	是否按照国家和行业的数据分类分级保护要求，建立单位数据分类分级保护制度，制定数据分类和分级方法	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全管理制度，确认按照国家和行业的数据分类分级保护要求，建立单位数据分类分级保护制度，制定数据分类和分级方法； b) 访谈相关人员，了解数据分类分级保护要求，确认实际落实的数据分级分类保护制度与相关政策一致
7	是否在相关制度中明确了数据分类管理、分级保护策略	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全管理制度，确认具备数据分类管理、分级保护策略； b) 访谈数据安全相关人员，了解数据分类管理、分级保护策略流程，责任落实到位、确认与相关制度一致

表15　数据分类分级管理评估子域（续）

序号	风险评估项	风险评估方法	结果判定
8	服务器、数据库、端口、数据资源在互联网的暴露及管理情况	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 审核相关网络架构文档、安全策略文件、系统配置记录以及安全审计报告，确认服务器、数据库、端口和数据资源的互联网暴露情况得到了妥善管理； b) 访谈网络管理员、安全团队和相关技术人员，确认他们对服务器、数据库、端口和数据资源的互联网暴露情况有清晰的了解，并能够描述当前的管理措施
9	软硬件资产维护、报废、销毁管理情况等	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部的软硬件资产管理政策、维护、报废和销毁的流程和程序，确认文档详细记录资产的生命周期管理，包括定期维护计划、报废标准、销毁方法和记录； b) 访谈相关管理人员和技术维护人员，确认能够清晰描述实际操作流程，提供实际执行的案例，证明这些政策得到了有效执行
10	数据分类分级变更和审核流程情况	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部的数据分类分级文档资料，确认存在明确定义的数据分类分级变更流程，包括变更请求的提出、审批、实施和记录，流程文档应详细说明变更的触发条件、责任人、审批层级、实施步骤以及变更后的数据安全管理措施； b) 确认存在变更记录、审批文件和更新后的数据分类分级清单等文档，表明该数据分类分级变更流程得到了有效执行
11	个人信息分类分级管理情况	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部的数据安全管理制度和相关政策文件，确认已经建立了个人信息的分类分级管理体系； b) 确认个人信息的分类分级管理体系中详细描述个人信息的分类标准、分级依据、管理措施以及相应的保护要求
12	是否对处理的个人信息和重要数据进行明确标识	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部的数据安全管理制度文档，确认组织已经建立了对个人信息和重要数据的明确标识制度； b) 制度中应包含标识的具体方法、标识的类型（如敏感、非敏感、公开、内部等）、标识的实施流程以及标识的维护和更新机制

表15　数据分类分级管理评估子域（续）

序号	风险评估项	风险评估方法	结果判定
13	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	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部的数据安全政策、流程文档和技术规范，确认已经根据数据的敏感性和重要性级别，建立了相应的安全措施； b) 确认安全措施涵盖数据的收集、存储、使用、传输、处理、共享和销毁等全流程，并与数据级别的安全要求相匹配； c) 确认措施详细描述了每个级别数据的安全控制措施，如访问控制、加密、审计日志、数据脱敏等
14	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	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部的数据管理政策、数据分类目录、安全措施文档以及实施记录，确认已经根据国家或行业的重要数据目录和相关规定，制定了对重要数据进行了识别和风险评估的方案文档； b) 确认文档中详细列出被评估为重要数据的类别、数量、存储位置和使用情况，并描述了针对这些数据实施的重点保护措施，如加强访问控制、实施数据加密、进行定期安全审计等
15	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	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部的核心数据管理政策、核心数据目录、管理流程和实施记录，确认组织已经依据相关的核心数据目录或规定，对核心数据进行了准确评估，并实施了严格的管理措施； b) 确认管理措施中详细说明了核心数据的识别标准、管理流程、保护措施，以及定期的审计和监控记录

9.3.2.4　相关人员安全管理评估子域

相关人员安全管理评估子域具体内容见表16。

表16　相关人员安全管理评估子域

序号	风险评估项	风险评估方法	结果判定
1	员工录用前是否进行必要的背景调查	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安记录文件，确认员工已经进行必要的背景调查，并有记录； b) 查阅相关制度文件，确认在员工录用前要进行必要的背景调查； c) 访谈相关人员，确认在录用前接受过公司的背景调查

表16　相关人员安全管理评估子域（续）

序号	风险评估项	风险评估方法	结果判定
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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈数据安全岗位相关人员，确认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； b) 查阅记录文件，确认有与所有涉及数据服务的人员签订了安全责任承诺或保密协议，与数据安全关键岗位人员签订了数据安全岗位责任协议，记录完整有效
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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关制度文件，确认已制定在重要岗位人员调离或终止劳动合同前，要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； b) 查阅保密承诺书，确认重要岗位离职人员签订保密承诺书； c) 访谈保密办相关责任人，了解重要岗位人员离职流程，确认与制度文件相一致
4	数据处理关键岗位人员录用，是否对其数据安全意识或专业能力进行考核	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全记录文件，确认数据处理关键岗位人员有录用考核历史文档记录； b) 查阅相关制度文件，确认对数据处理关键岗位人员在录用时，进行安全意识考核； c) 访谈数据安全处理关键岗位人员，确认其在录用时已进行过数据安全意识或专业能力考核
5	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据权限文件，确认转岗或离岗人员相关数据操作权限已变更或终止，明确责任人数据保护管理权限和保密责任； b) 核查相关系统，确认已转岗或离岗人员，系统操作权限已变更或终止
6	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据权限文件，确认对终止劳动合同人员，相关数据操作权限已终止并收回； b) 查阅终止劳动合同人员的交接文档等证明材料，确认已明确告知其继续履行有关信息的保密义务要求； c) 核查相关系统，确认对终止劳动合同的人员，系统操作权限已终止
7	是否制定数据安全培训计划，并定期更新培训计划	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关文档，确认有数据安全培训计划文件，且定期更新； b) 查阅相关制度文件，确认有数据安全培训计划且要实时更新

表16　相关人员安全管理评估子域（续）

序号	风险评估项	风险评估方法	结果判定
8	是否对全体人员开展数据安全意识教育培训，并保留相关记录	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关记录，确认有对全体人员开展数据安全意识教育培训的记录文件
9	是否每年至少1次对数据安全岗位人员进行专项培训，是否定期对关键岗位人员进行数据安全技能考核	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据，确认每年至少 1 次对数据安全岗位人员进行专项培训的培训记录，有定期对关键岗位人员进行数据安全技能考核的记录文件； b) 访谈相关人员，确认数据安全岗位人员有参加过每年至少1次的专项培训，确认关键岗位人员有进行数据安全技能考核
10	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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅内部审核员工手册、工作纪律规定、数据安全政策等相关文档，确认已制定了明确的工作纪律和工作要求； b) 确认文档中详细列出了所有禁止的行为，包括未经授权的数据访问、数据泄露、数据篡改等，并包含了相应的违规后果和处罚措施； c) 访谈数据安全相关员工，确认员工清楚了解并能够详细说明组织对数据安全方面的工作纪律和禁止行为，员工应能够列举具体的禁止行为，如未经授权的数据访问、数据泄露、数据篡改等，并应知晓违反这些规定的后果

9.3.2.5　数据合作授权管理评估子域

数据合作授权管理评估子域具体内容见表17。

表17　数据合作授权管理评估子域

序号	风险评估项	风险评估方法	结果判定
1	受托方是否建立数据合作方安全管理机制，是否明确数据合作中数据安全保护方式和合作方责任落实要求	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关制度文件，确认已建立数据合作授权安全管理机制，且明确数据合作中数据安全保护方式和合作方责任落实要求
2	是否会对数据合作方的数据安全能力进行评估或监督，确保合作方的保护能力与面临的数据安全风险相符	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关制度文件，确认对数据合作方的数据安全能力要进行评估或监督； b) 查阅相关制度文件，确认已建立合作方的保护能力要与面临的数据安全风险相符的规定； c) 访谈数据安全相关人员，确认其了解对数据合作方数据安全能力评估或监督的方法

表17　数据合作授权管理评估子域（续）

序号	风险评估项	风险评估方法	结果判定
3	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	文档审核 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅相关制度，确认已建立合作方接入的系统、使用的技术工具要进行技术检测； b）　登陆相关系统，应用技术工具、渗透测试等手段检测防护措施有效性，确认没有引入木马、后门
4	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	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅相关制度，确认建立合同协议约定提供的数据范围、提供目的、传输方式、安全措施等条款对接收、使用本单位数据的合作方的数据使用行为进行约束； b）　查阅相关合同、协议文件，确认对接收、使用本单位数据的合作方的数据使用行为进行约束
5	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	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅制度文档，确认有相关规定，合作协议中要明确数据处理目的、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； b）　查阅相关合作协议，确认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
6	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	人员访谈 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　访谈相关数据管理人员，了解合作方数据回收流程，确认在合作结束后进行了回收，并对数据进行删除； b）　核查相关系统，确认在合作结束后，向合作方提供的数据已无法访问并操作系统
7	合作服务到期后，是否进行对账号注销	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅相关制度文件，确认建立合作服务到期后，账号注销管理制度； b）　查阅数据文件，确认在合同服务到期后，合作方账号已注销； c）　核查相关系统，确认在合同服务到期后，合作方账号已无法访问并操作系统
8	合作方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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅相关制度文件，确认建立合作方人员对数据与系统的访问、修改权限要限于最小必要范围； b）　查阅数据文件，确认合作方人员数据与系统的访问、修改权限限于最小必要范围； c）　核查相关系统，确认合作方人员对数据与系统的访问、修改权限限于最小必要范围

表17　数据合作授权管理评估子域（续）

序号	风险评估项	风险评估方法	结果判定
9	能够在测试环境下或使用的测试数据，是否向合作方人员开放了生产环境权限或真实数据	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关制度文件，确认建立在测试环境下或使用的测试数据，不能向合作方人员开放生产环境权限或真实数据； b) 查阅测试数据文件，确认没有向合作方人员开放生产环境权限或真实数据； c) 核查相关系统，确认在测试环境下或使用的测试数据，没有向合作方人员开放了生产环境权限或真实数据
10	是否对合作方人员数据导出操作、数据外发操作、访问敏感数据操作的情况进行监督管理	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关制度文件，确认建立对合作方人员数据导出操作、数据外发操作、访问敏感数据操作的情况进行监督管理的制度； b) 核查相关系统，确认对合作方人员数据导出操作、数据外发操作、访问敏感数据操作的情况有进行日志记录
11	外部授权人员现场服务安全管理情况	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅外包服务合同、安全管理协议、访问控制记录、培训记录和现场服务报告等文档，确认组织对外包人员在现场服务期间的安全管理进行了严格的规定和监督； b) 访谈负责现场服务管理的内部人员、外包服务提供商的管理人员以及直接参与现场服务的外包人员，确认组织已经建立了有效的外包人员现场服务安全管理体系，相关人员应能够详细说明外包人员的身份验证、访问权限控制、安全培训、现场行为监控等安全措施的实施情况
12	对合作服务商的技术依赖程度，对授权处理数据的控制和管理能力	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅与合作服务商的合同、数据管理政策、安全协议等相关文档，确认组织对合作服务商的技术依赖程度在可接受范围内，并且具备对授权处理数据的有效控制和管理能力； b) 合同协议文档中应详细描述数据授权处理的流程、数据访问和处理的权限设置、数据保护措施、以及数据泄露或安全事件的应急响应计划； c) 访谈负责合作管理的内部人员、服务商的代表以及数据安全团队，确认组织对合作服务商的技术依赖程度在可控范围内，并且具备对委托处理数据的有效控制和管理能力

表17　数据合作授权管理评估子域（续）

序号	风险评估项	风险评估方法	结果判定
13	外部授权人员远程访问操作系统或数据的情况	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部相关安全管理制度和操作规程文档，确认明确规定了外部授权人员远程访问操作系统或数据的条件、权限、操作流程以及必要的安全措施； b) 通过对相关系统操作，确认实施对外部人员远程访问操作系统或数据的严格管理； c) 访谈外部人员及相关管理人员，了解外部人员远程访问操作系统或数据的实际操作情况，确认所有远程访问活动均遵循了组织的安全政策和程序
14	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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关的批准文件、合同协议以及监督记录，确认在委托他人建设、维护电子政务系统以及存储、加工政务数据的过程中，遵循了组织的批准程序，检查合同或服务协议中明确规定了受托方的数据安全保护责任和义务； b) 访谈负责电子政务系统建设和维护的管理人员、合同管理人员以及数据安全负责人，了解在委托外部方进行电子政务系统建设、维护以及政务数据的存储和加工过程中，遵循了组织的内部批准程序，确认有明确的审批流程记录，包括审批人员、审批时间、审批内容等
15	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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅与政务数据受托方签订的合同文件、数据安全协议、以及相关的法律法规，确认受托方有明确的义务和责任来保护政务数据的安全，且合同中有关于数据保护、数据使用限制、数据存储期限、数据销毁等方面的具体条款； b) 访谈受托方的数据安全负责人、数据管理人员以及相关业务人员，确认受托方在处理政务数据时严格遵守了法律、法规的规定和合同约定，且有明确的数据安全政策和程序，并得到了有效执行
16	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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅电子政务系统相关的服务或系统安全文档，评估相关服务或系统具备必要的安全措施，确认文档中详细描述了安全控制措施，且这些措施符合电子政务系统的管理和安全要求； b) 访谈电子政务系统的技术负责人、安全管理人员以及服务提供商的代表，了解他们对于系统安全措施的认识和执行情况，询问服务或系统已经实施了必要的安全控制

9.3.2.6 数据安全应急管理评估子域

数据安全应急管理评估子域具体内容见表18。

表18 数据安全应急管理评估子域

序号	风险评估项	风险评估方法	结果判定
1	是否制定数据安全事件应急预案，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	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关文档，确认数据安全应急预案文档，定义了数据安全事件类型，明确不同类别事件处置流程和方法； b) 查阅相关制度文件，确认已制定数据安全事件应急预案，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
2	是否定期针对不同类型事件开展数据安全应急演练活动，并留存记录	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关记录，确认有数据安全应急演练活动记录文档； b) 查阅相关制度文件，确认建立定期针对不同类型事件开展数据安全应急演练活动； c) 访谈数据安全相关人员，确认其了解数据安全应急演练活动流程
3	近 3 年发生的数据安全事件，是否进行了有效处置、记录、整改和上报	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关制度文件，确认近3年如果发生数据安全事件，进行有效处置、记录、整改和上报
4	发生大规模用户个人信息泄露、毁损和丢失时，是否采取合理、有效方式告知用户	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关制度文件，确认在发生大规模用户个人信息泄露、毁损和丢失时，会采取合理、有效方式告知用户
5	近 2 年的数据安全投诉举报，是否进行了有效处置、记录和整改，是否存在侵害用户个人权益的情况	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查询相关文档记录，确认近2年如果有数据安全事件的举报，其对应处置有效，没有包含对于个人信息权益的侵害情况
6	开展数据处理活动是否进行安全风险监测，发现数据安全缺陷、漏洞等风险时，是否立即采取补救措施	文档审核 技术测试	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关制度文件，确认建立开展数据处理活动进行安全风险监测，发现数据安全缺陷、漏洞等风险时，立即采取补救措施等制度； b) 对相关系统进行应用技术工具、渗透测试等方法，确认在发现数据安全缺陷、漏洞等风险时，通过采取补救措施已得到控制，排除安全缺陷，修复漏洞
7	是否建立数据安全应急处置机制，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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关制度，确认建立数据安全应急处置机制，发生数据安全事件时要立即采取处置措施，按照规定及时告知用户并向有关主管部门报告

9.3.3 数据安全技术评估域

9.3.3.1 数据访问控制评估子域

数据访问控制评估子域具体内容见表19。

表19　数据访问控制评估子域

序号	风险评估项	风险评估方法	结果判定
1	是否建立与数据类别级别相适应的访问控制机制情况，并限定用户可访问数据范围	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅数据分类分级文档，确认已对数据类别与级别进行明确划分，且按照级别不同划分对应的访问控制要求； b)　风险评估人员通过查看信息系统，验证可根据用户权限及数据敏感级别限定访问数据范围
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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅信息系统设计文档，确认已制定数据访问前的身份认证措施策略； b)　风险评估人员通过查看信息系统，验证对系统数据访问前必须通过身份认证，不存在非授权访问的可能
3	数据访问权限与访问者的身份是否存在关联	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　访谈相关人员并查阅业务系统相关制度，确认数据访问权限与身份角色存在对应关联关系； b)　查阅数据安全相关制度与信息系统设计文档，确认具备数据访问权限与访问者身份关联机制； c)　风险评估人员通过查看信息系统，确认已制定针对不同身份用户的不同数据访问权限，且身份与访问权限对应关系与制度文档一致
4	是否具有数据访问权限申请、审批机制	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅数据安全相关制度与信息系统设计文档，确认具备数据访问申请与审批机制； b)　风险评估人员通过查看信息系统，验证系统具备数据访问权限申请与审批能力
5	是否以满足业务实际需要的最小化权限原则进行授权	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅相关制度文档，确认已依据“业务必需、最小权限”的原则，根据各用户的职责设计用户访问控制权限； b)　风险评估人员通过查看信息系统，验证系统的相关配置，确认用户访问控制权限的配置与设计文档一致
6	针对系统管理员、安全管理员、安全审计员等人员角色是否进行分离设置和对应权限设置	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅相关制度文档，确认已依据“权限分离”的原则对管理审计人员进行分离设置，并根据各自职责设计权限范围； b)　风险评估人员通过查看信息系统，验证系统的相关配置，确认各管理审计人员的访问控制权限的配置与设计文档一致

表19　数据访问控制评估子域（续）

序号	风险评估项	风险评估方法	结果判定
7	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅相关制度文档，确认已依据“最少够用、职权分离”的原则，设计和更新权限分配表； b）　风险评估人员通过查看信息系统，验证系统的相关配置，确认权限分配原则与设计文档一致
8	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅相关制度文档，确认已制定对离职人员账号回收、沉默账号、权限违规变更等安全问题的方案技术与措施； b）　风险评估人员通过查看信息系统，验证系统的相关配置，确认系统在离职人员账号回收、沉默账号、权限违规变更等安全问题的处置响应与设计文档一致

9.3.3.2　数据安全监测预警评估子域

数据安全监测预警评估子域具体内容见表20。

表20　数据安全监测预警评估子域

序号	风险评估项	风险评估方法	结果判定
1	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅数据安全相关制度与信息系统设计文档，确认已按照要求对各类数据访问操作进行日志记录、符合安全监控与信息报告要求； b）　风险评估人员通过查看信息系统，验证系统的数据访问操作日志记录与监控配置，确认安全检测预警和信息报告机制的配置与设计文档一致
2	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅数据安全相关制度与信息系统设计文档，明确系统设计中涵盖异常行为检测能力，能够对异常行为事件进行识别、发现、跟踪和监控； b）　风险评估人员通过查看信息系统，验证系统具备异常行为检测能力，能够对异常行为事件进行识别、发现、跟踪和监控，且与设计文档一致

表20　数据安全监测预警评估子域（续）

序号	风险评估项	风险评估方法	结果判定
3	是否具备对批量传输、下载、导出等敏感数据操作的安全监控和分析能力，并对数据异常访问和操作进行告警	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　访谈相关人员并查阅业务系统相关制度，确认在进行敏感数据操作时，能够实现对数据异常访问进行告警； b）　查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备对敏感数据操作的告警能力； c）　风险评估人员通过查看信息系统，验证系统的相关功能，确认敏感数据操作告警与设计文档一致
4	是否具备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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备对异常流量和行为进行告警的能力； b）　风险评估人员通过查看信息系统，验证系统的相关功能，确认对异常流量和行为进行告警功能与设计文档一致
5	是否具备风险信息的获取、分析、研判、通报、处置能力	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备风险信息全流程跟踪能力； b）　风险评估人员通过查看信息系统，验证系统的相关功能，确认风险信息全流程跟踪功能与设计文档一致
6	是否记录数据操作过程及关键数据要素，在出现数据泄露事件后能跟据泄露的数据进行溯源	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅数据安全相关制度与信息系统设计文档，明确系统设计具备数据溯源的能力； b）　通过查看信息系统，验证系统的相关功能，确认数据溯源功能与设计文档一致
7	是否具备数据安全缺陷、漏洞等风险的监测预警能力	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a）　查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备数据安全监测预警能力； b）　风险评估人员通过查看信息系统，验证系统的相关功能，确认数据安全监测预警功能与设计文档一致

9.3.3.3　数据脱敏评估子域

数据脱敏评估子域具体内容见表21。

表21　数据脱敏评估子域

序号	风险评估项	风险评估方法	结果判定
1	是否具备数据脱敏能力，脱敏规则、脱敏方法和脱敏数据的使用是否符合管理要求	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备数据脱敏相关配置能力； b) 查看信息系统，验证系统的相关功能，确认数据脱敏相关配置与设计文档一致
2	是否对进行数据脱敏处理的应用场景、处理流程及操作进行记录	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备数据脱敏场景、流程、操作等记录能力； b) 查看信息系统，验证系统的相关功能，确认数据脱敏处理的应用场景、处理流程及操作记录与设计文档一致
3	是否具备静态数据脱敏和动态数据脱敏技术能力	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员并查阅业务系统相关制度，确认静态与动态数据脱敏能力情况； b) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备静态数据脱敏和动态数据脱敏技术能力； c) 通过查看信息系统，验证系统的相关功能，确认静态数据脱敏和动态数据脱敏技术能力建设情况与设计文档一致
4	开发测试、人员信息公示等应用场景的数据脱敏效果是否符合管理要求	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备开发测试、人员信息公示等应用场景脱敏能力； b) 通过查看信息系统，验证系统的相关功能，确认开发测试、人员信息公示等应用场景的数据脱敏效果与设计文档及预期一致
5	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备匿名化处理后信息仍被识别的风险保护措施； b) 通过查看信息系统，验证系统的相关功能，确认系统具备匿名化处理后信息仍被识别的风险保护措施的能力

9.3.3.4　数据防泄露评估子域

数据防泄露评估子域具体内容见表22。

表22　数据防泄漏评估子域

序号	风险评估项	风险评估方法	结果判定
1	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备对系统关键环节进行监控并报告敏感信息的能力； b) 通过查看信息系统，验证系统的相关功能，确认系统具备对网络、邮件、终端等关键环节进行监控并报告敏感信息的功能
2	针对市场上售卖组织业务数据，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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，确认没有进行数据售卖； b) 通过公开渠道，未能查询到组织业务信息
3	数据防泄漏技术措施是否具有有效性	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员并查阅业务系统相关制度，确认数据泄露技术措施时效性情况； b) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中数据防泄漏技术措施的时效性情况； c) 通过查看信息系统，验证系统的相关功能，确认系统数据防泄漏技术措施的时效性

9.3.3.5　数据接口安全评估子域

数据接口安全评估子域具体内容见表23。

表23　数据接口安全评估子域

序号	风险评估项	风险评估方法	结果判定
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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备对违规接入的限制能力、对接口调用的监控和处理能力； b) 查看信息系统，验证系统的相关功能，确认系统对违规接入的限制、对接口调用的监控和处理效果与设计文档及预期一致
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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备应对安全密钥被破解的能力； b) 通过查看信息系统，验证系统的相关功能，确认系统在安全密钥被破解时，应对能力与设计文档及预期一致

表23　数据接口安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
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	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员并查阅业务系统相关制度，确认在各安全等级系统间、跨区域系统间数据流动的安全控制措施情况； b) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备在各安全等级系统间、跨区域系统间数据流动的安全控制措施； c) 通过查看信息系统，验证系统的相关功能，确认系统在各安全等级系统间、跨区域系统间数据流动时的安全控制措施及能力与设计文档及预期一致
4	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备接口安全控制策略设置能力； b) 通过查看信息系统，验证系统的相关功能，确认系统在接口安全控制策略配置方面的功能与设计文档及预期一致
5	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中有涉及个人信息和重要数据传输接口实施调用审批能力； b) 通过查看信息系统，验证系统的相关功能，确认系统在对涉及个人信息和重要数据的传输接口实施调用审批方面的功能与设计文档及预期一致
6	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备定期清查数据接口的规范和处置措施； b) 通过查看信息系统，验证系统的相关功能，确认系统对接口进行定期清查，对不符合要求的接口进行了关停
7	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中对敏感数据的接口调用制定了相应的安全措施； b) 风险评估人员通过查看信息系统，验证系统的相关功能，确认系统在对敏感数据接口调用时采取了安全措施
8	数据接口是否具备身份鉴别、访问控制、授权策略、接口签名、安全传输协议等防护能力	系统核查	满足以下要求的为符合，不满足以下要求的为不符合： 通过查看信息系统，验证系统的相关功能，确认系统在数据接口层面设置了身份鉴别、访问控制等参数配置项

表23　数据接口安全评估子域（续）

序号	风险评估项	风险评估方法	结果判定
9	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	系统核查	满足以下要求的为符合，不满足以下要求的为不符合： 通过查看信息系统，验证系统的相关功能，确认系统对接口访问进行了日志记录，对接口异常事件进行了告警通知

9.3.3.6　数据备份与恢复评估子域

数据备份与恢复评估子域具体内容见表24。

表24　数据备份与恢复评估子域

序号	风险评估项	风险评估方法	结果判定
1	数据备份恢复策略和操作规程是否建设落实	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备数据备份恢复策略和操作规程的能力； b) 通过查看信息系统，验证系统相关功能，确认系统在数据备份恢复策略和操作规程方面，功能、设计文档及预期一致
2	是否定期开展数据备份恢复工作	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备定期开展数据备份恢复工作的能力； b) 通过查看信息系统，验证系统相关功能，确认系统在定期开展数据备份恢复工作方面的功能与设计文档及预期一致
3	备份和归档数据访问控制措施的有效性	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员并查阅业务系统相关制度，确认系统备份和归档数据访问控制措施的有效性情况； b) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中备份和归档数据访问控制措施的有效性能力； c) 通过查看信息系统，验证系统的相关功能，确认系统备份和归档数据访问控制措施的时效性
4	是否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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备定期检查和验证数据完整性和可用性的能力； b) 通过查看信息系统，验证系统的相关功能，确认系统具备定期检查和验证数据完整性和可用性的功能与设计文档一致

表24　数据备份与恢复评估子域（续）

序号	风险评估项	风险评估方法	结果判定
5	是否定期开展灾难恢复演练	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备定期开展灾难恢复演练的能力； b) 访谈相关人员并查阅业务系统相关制度，确认灾难恢复演练的实施情况有按照演练预案执行； c) 通过查看信息系统，验证系统的相关功能，确认系统具备定期开展灾难恢复演练的能力，且与设计文档一致

9.3.3.7　数据安全审计评估子域

数据安全审计评估子域具体内容见表25。

表25　数据安全审计评估子域

序号	风险评估项	风险评估方法	结果判定
1	是否具备安全审计能力	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备审计实施能力； b) 查看信息系统，验证系统的相关功能，确认系统审计实施的能力与设计文档一致
2	审计策略和要求的合理性、有效性是否符合管理要求	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中审计策略和要求的合理性、有效性情况； b) 通过查看信息系统，验证系统的相关功能，确认系统中审计策略和要求的合理性、有效性与设计文档一致
3	对数据的访问权限和实际访问控制是否进行定期审计，审核用户实际使用权限与审批时的目的是否保持一致，并是否及时清理已过期的账号和授权	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员并查阅业务系统相关制度，确认系统具备定期审计的情况及审批与实际使用权限的一致性问题、清理过期账号和授权能力的情况； b) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备对于定期审计的情况及审批与实际使用权限一致性问题的处理、清理过期账号和授权的能力； c) 通过查看信息系统，验证系统的相关功能，确认系统审计实施的能力、一致性问题、清理过期账号和授权等与设计文档一致
4	是否针对特权用户进行安全审计，审计情况是否具备完整记录	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备对于特权用户安全审计情况的能力； b) 通过查看信息系统，验证系统的相关功能，确认系统中对于特权用户安全审计情况的能力与设计文档一致

表25　数据安全审计评估子域（续）

序号	风险评估项	风险评估方法	结果判定
5	是否对数据授权访问、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审计	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据安全相关制度与信息系统设计文档，明确系统设计中具备重点环节进行日志留存管理的能力； b) 通过查看信息系统，验证系统的相关功能，确认系统中对于重点环节进行日志留存管理的能力与设计文档一致
6	日志审计内容，是否至少包括执行时间、操作账号、处理方式、授权情况、IP 地址、登录信息	系统核查	满足以下要求的为符合，不满足以下要求的为不符合： 通过查看信息系统，验证系统的相关功能，确认系统中日志审计的内容包括执行时间、操作账号、处理方式、授权情况、IP地址、登录信息等条目
7	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	系统核查	满足以下要求的为符合，不满足以下要求的为不符合： 通过查看信息系统，验证系统的相关功能，确认系统中日志记录的内容能够对识别追溯数据操作和访问行为提供支撑
8	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	系统核查	满足以下要求的为符合，不满足以下要求的为不符合： 通过查看信息系统，验证系统的相关功能，确认系统对日志进行了定期备份
9	是否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，对数据库、数据接口的访问和操作行为，对数据批量复制、下载、导出、修改、删除等高风险行为，对个人信息处理活动合规性进行审计	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 通过查看审计报告，验证审计工作对相关行为进行了审计与追溯； b) 通过查看信息系统，验证系统的相关功能，确认系统中审计策略和要求的合理性、有效性与设计文档一致

9.3.4　个人信息保护评估域

9.3.4.1　保护原则评估子域

保护原则评估子域具体内容见表26。

表26　保护原则评估子域

序号	风险评估项	风险评估方法	结果判定
1	处理个人信息是否具有明确、合理的目的	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：通过查阅个人信息收集使用规则与系统功能说明，确认处理个人信息具有明确、合理的目的
2	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	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅个人信息收集使用规则，确认处理个人信息与目的直接相关； b) 通过访谈相关人员，确认处理个人信息方式为对个人权益影响最小的方式
3	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查看信息系统，确认实际收集的个人信息类型、申请打开可收集使用个人信息的权限等与收集使用规则中相关内容一致； b) 查阅相关文档，确认收集个人信息遵循“最小够用”原则

表26　保护原则评估子域（续）

序号	风险评估项	风险评估方法	结果判定
4	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	系统核查	满足以下要求的为符合，不满足以下要求的为不符合：通过查看信息系统，确认不同意处理个人信息，不影响其使用现有业务功能或相关服务
5	是否存在隐瞒产品或服务所收集个人信息功能的情况	系统核查	满足以下要求的为符合，不满足以下要求的为不符合：通过查看信息系统与个人信息收集规则，确认所列收集个人信息功能与实际一致
6	是否存在通过误导、欺诈、胁迫等方式处理个人信息的情况	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅个人信息隐私政策、用户协议、数据处理流程及相关操作记录，评估个人信息处理过程中不存在误导、欺诈或胁迫等不当行为，确认用户在充分知情的情况下自愿提供信息，数据处理遵循了法律法规和行业标准； b) 通过进行相关操作，检查用户交互日志、数据处理记录和系统配置，确认个人信息收集和使用过程中不存在误导、欺诈或胁迫行为，评估用户同意的真实性，确保信息处理活动遵循用户授权且符合法律法规要求
7	是否存在非法收集、使用、加工、传输他人个人信息的情况	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部的隐私政策、用户协议、数据处理流程记录和相关内部管理制度，确认个人信息的收集、使用、加工和传输遵循了法律法规和用户授权； b) 通过进行相关操作，检查系统在个人信息处理活动中，没有未经授权或超出授权范围的行为
8	是否存在非法买卖、提供或者公开他人个人信息的情况	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 审查相关操作手册、交易记录和审计报告，确保没有非法买卖、提供或公开个人信息的行为，核实所有个人信息处理活动均遵循法律法规和内部数据保护政策，且有适当的监控和审计机制以防止和检测潜在的非法活动； b) 通过进行相关操作，验证系统安全措施能够有效防止未授权的数据访问和传输，存在监控机制来检测和记录任何潜在的违规活动
9	是否从事危害国家安全、公共利益的个人信息处理活动	系统核查	满足以下要求的为符合，不满足以下要求的为不符合：通过查看信息系统，确认不同意处理个人信息，不影响其使用现有业务功能或相关服务
10	个人信息处理活动是否具备《中华人民共和国个人信息保护法》规定的合法性事由	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关设计文档，确认个人信息收集规则与功能，符合《中华人民共和国个人信息保护法》的相关规定

表26　保护原则评估子域（续）

序号	风险评估项	风险评估方法	结果判定
11	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部的个人信息隐私政策、用户协议、数据处理流程及相关操作记录，评估个人信息处理过程中不存在误导、欺诈或胁迫等不当行为，确认用户在充分知情的情况下自愿提供信息，数据处理遵循了法律法规和行业标准； b) 通过进行相关操作，检查用户交互日志、数据处理记录和系统配置，确认个人信息收集和使用过程中不存在误导、欺诈或胁迫行为，评估用户同意的真实性，确保信息处理活动遵循用户授权且符合法律法规要求
12	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织内部的隐私政策、用户协议、数据处理流程记录和相关内部管理制度，确认个人信息的收集、使用、加工和传输遵循了法律法规和用户授权； b) 通过进行相关操作，检查系统在个人信息处理活动中，没有未经授权或超出授权范围的行为
13	接收方是否继续履行个人信息处理者的义务	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：审查相关操作手册、交易记录和审计报告，确保没有非法买卖、提供或公开个人信息的行为，核实所有个人信息处理活动均遵循法律法规和内部数据保护政策，且有适当的监控和审计机制以防止和检测潜在的非法活动
14	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅信息推送和商业营销政策，确认在自动化决策基础上，为用户提供了不基于个人特征的推送选项，及为用户提供了明确的拒绝接收个性化推送的途径； b) 检查系统相应用户界面，确认系统提供了基于非个人特征的信息推送选项，且允许用户拒绝或退出个性化推送，并确认这些选择得到执行
15	是否明确对自动化决策方式予以说明	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅相关文档，确认其隐私政策、用户协议或相关服务条款中对自动化决策的方式、目的、逻辑和可能产生的后果进行了明确说明； b) 通过系统核查，检查系统中相应的用户界面，确认以清晰准确的形式，提供了对自动化决策方式的明确说明

表26 保护原则评估子域（续）

序号	风险评估项	风险评估方法	结果判定
16	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	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅数据使用政策、隐私政策和服务条款等文档，确认组织在处理个人自行公开或其他已经合法公开的个人信息时，遵循了合理的范围限制； b) 查阅数据使用政策、隐私政策和服务条款等文档，确认文档中明确了个人拒绝处理其信息的权利，以及组织如何响应和执行个人的拒绝请求
17	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 通过文档审核，检查处理已公开但可能对个人权益产生重大影响的个人信息时，制定了获取个人明确同意政策和流程； b) 通过系统核查，确认在处理可能对个人权益产生重大影响的已公开个人信息时，系统提供了用户界面或交互流程以获取用户的明确同意

9.3.4.2 保护措施评估子域

保护措施评估子域具体内容见表27。

表27 保护措施评估子域

序号	风险评估项	风险评估方法	结果判定
1	个人信息保护内部管理制度和操作规程的建设落实情况	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅文档存在个人信息保护相关管理制度与操作规程； b) 风险评估人员通过访谈相关人员，已落实相关管理制度与操作规程
2	对个人信息分类管理实施情况及效果	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅文档，确认在制度中明确个人信息分类，并已梳理系统个人信息分类清单
3	是否存在加密、去标识化等安全技术措施应用	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅业务系统相关制度，确认存在加密、去标识化等安全技术措施的应用； b) 通过查看信息系统，确认加密、去标识化等安全技术措施已覆盖个人信息
4	是否合理确定个人信息处理的操作权限	人员访谈 文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 通过查阅账号权限管理制度，确认其中对于岗位账号的匹配机制； b) 通过对相关人员访谈，确认了解自我岗位的账号权限； c) 通过查看信息系统，未发现超范围授权情况

表27　保护措施评估子域（续）

序号	风险评估项	风险评估方法	结果判定
5	个人信息安全事件应急预案制定及组织实施情况	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 通过查阅个人信息安全事件应急预案，确认应急预案已制定； b) 通过人员访谈与应急演练记录核查，确认已在本年度进行个人信息安全事件应急演练，并保存有应急演练报告
6	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	系统核查	满足以下要求的为符合，不满足以下要求的为不符合：通过查看信息系统，确认在展示、委托处理、提供、公开等环节，已对个人信息直接标识符进行了去标识化处理
7	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：通过文档审核，确认制定了定期进行个人信息处理合规审计的政策和程序，确认有记录显示已经执行了这些审计活动，包括审计报告、发现的问题、采取的纠正措施以及后续的跟踪和改进
8	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：通过文档审核，确认根据国家网信部门的规定，设置了个人信息保护负责人，并确认组织有明确的政策和流程，确保个人信息保护负责人能够有效地监督个人信息的处理活动
9	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：通过文档审核，确认在其官方网站、用户协议、隐私政策或其他公开渠道上公布了个人信息保护负责人的姓名和联系方式，以及组织能按照国家网信部门的要求，将个人信息保护负责人的相关联系信息报送至相应的监管机构
10	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风险评估	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：通过文档审核，确认在进行敏感个人信息处理、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、以及向境外提供个人信息等活动前，进行了个人信息保护影响风险评估
11	个人信息保护影响风险评估内容是否符合《中华人民共和国个人信息保护法》第56条规定	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：通过文档审核，确认个人信息保护影响风险评估内容全面覆盖了《中华人民共和国个人信息保护法》第56条所规定的各个方面
12	是否对个人信息处理情况进行记录，个人信息保护影响风险评估报告和处理情况记录是否至少保存三年	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：通过文档审核，确认建立了个人信息处理活动的记录系统，且按照《中华人民共和国个人信息保护法》的规定，对个人信息保护影响风险评估报告和个人信息处理情况进行了记录，确认记录内容遵循完整性、准确性和可追溯性，且记录的保存期限满足至少三年的要求

表27　保护措施评估子域（续）

序号	风险评估项	风险评估方法	结果判定
13	个人信息安全事件应急预案制定及组织实施情况	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 通过文档审核，确认制定了个人信息安全事件应急预案，且该预案包含了对各种可能发生的个人信息安全事件的响应措施，确认存在应急预案的培训、演练和定期更新文档记录； b) 查阅对应工作台账及记录，确认已进行了应急预案的培训、演练和定期更新
14	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	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 通过文档审核，确认制定了相应的预案和补救措施以应对可能发生个人信息泄露、篡改、丢失的场景； b) 查阅对应工作台账及记录，确认在发生个人信息安全事件后，能迅速启动应急预案，执行必要的流程和补救措施
15	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅对应工作台账，确认在发生个人信息安全事件时，能按照法律法规的要求及时通知了所涉及的个人，并向网信部门报告，且事件通知的内容包括了信息种类、事件原因、可能造成的危害、已采取或建议采取的补救措施，以及个人信息处理者的联系方式等

9.3.4.3　告知同意评估子域

告知同意评估子域具体内容见表28。

表28　告知同意评估子域

序号	风险评估项	风险评估方法	结果判定
1	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 通过查看信息系统，确认首次运行或用户注册时主动提示用户阅读隐私政策； b) 通过查阅隐私政策，确认隐私政策中包含收集使用个人信息规则的内容； c) 通过查阅隐私政策，确认隐私政策文本文字显示方式不会造成阅读困难； d) 通过查阅隐私政策，确认隐私政策中逐一列出收集使用个人信息的目的、方式、范围等
2	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅隐私政策，确认隐私政策应对App运营者基本情况进行描述，内容包括公司名称、注册地址、个人信息保护相关负责人联系方式

表28　告知同意评估子域（续）

序号	风险评估项	风险评估方法	结果判定
3	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	文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅隐私政策，确认对每个业务功能都说明其所收集的个人信息类型，未出现多个业务功能对应一类个人信息的情况； b) 查阅隐私政策，确认每个业务功能在说明其所收集的个人信息类型时，在隐私政策中逐项列举，未使用“等、例如”等方式概括说明； c) 过查阅隐私政策，确认隐私政策对个人信息存放地域（国内、国外）；存储期限（法律规定范围内最短期限或明确的期限）、超期处理方式进行明确说明
4	个人信息处理规则是否告知个人行使《中华人民共和国个人信息保护法》规定权利的方式和程序	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查看信息系统，确认首次运行或用户注册时主动提示用户阅读隐私政策； b) 查阅隐私政策，确认隐私政策中逐一列出收集使用个人信息的目的、方式、范围等
5	告知事项发生变更的，是否将变更部分告知个人	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅隐私政策，确认隐私政策中对于事项变更时告知个人，有明确说明内容； b) 通过系统核查，验证隐私政策内容发生变化时有通知个人的记录
6	个人信息处理规则是否便于查阅和保存	系统核查	满足以下要求的为符合，不满足以下要求的为不符合：通过系统核查，验证个人信息处理规则的显示方式、保存方式易于辨认，设置位置明显，操作方便
7	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅隐私政策，确认隐私政策中对于紧急情况下对于个人信息的处理方式，有明确说明内容； b) 通过系统核查，验证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，个人信息处理者在紧急情况消除后及时告知
	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查看信息系统，确认当信息系统打开系统权限时（不包括用户自行在系统设置中打开权限的情况），信息系统说明该权限将收集个人信息的目的； b) 查看信息系统，确认收集个人敏感信息时，信息系统通过弹窗提示等明显方式向用户明示收集、使用个人信息的目的、方式、范围； c) 查阅个人信息处理记录，确认处理个人信息前有取得个人同意，由个人在充分知情的前提下自愿、明确作出选择

表28 告知同意评估子域（续）

序号	风险评估项	风险评估方法	结果判定
8	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查看信息系统，确认已建立便捷的撤回同意方式； b) 查看个人信息处理记录，确认撤回同意后，不再处理相应的个人信息； c) 查看个人信息处理记录，确认撤回同意不影响撤回前基于同意的个人信息处理
9	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查看信息系统，确认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，及时更新隐私政策，用户打开信息系统第一时间推送，用户点击同意后开始处理个人信息； b) 查看个人信息处理记录，确认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，有重新取得个人同意

9.3.4.4 主体权力评估子域

主体权力评估子域具体内容见表29。

表29 主体权力评估子域

序号	风险评估项	风险评估方法	结果判定
1	个人信息处理者是否为个人提供查阅其个人信息的途径，能及时提供个人信息查阅	系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查看信息系统，确认向用户提供访问所持有的关于该用户的个人信息、信息来源和所用于的目的等信息的方法； b) 进行相关操作，确认系统所提供的查阅个人信息方法及时准确
2	是否为个人提供复制其个人信息的途径，是否能及时个人信息复制	系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查看信息系统，确认为用户提供获取个人信息副本的途径； b) 经过相关操作，确认提供的方法及时有效
3	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查看信息系统，确认根据用户请求，为用户提供获取个人信息副本的方法； b) 查看技术规范书，确认技术可行的前提下，可直接将个人信息副本传输给指定的个人信息处理者
4	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	系统核查	满足以下要求的为符合，不满足以下要求的为不符合：查看信息系统，确认在信息系统中提供了个人信息更正、补充的途径
5	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	人员访谈 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 通过访谈相关人员，确认更正、补充的个人信息，已及时进行核实； b) 查看信息系统，验证更正、补充的个人信息，及时在系统内进行更新

表29　主体权力评估子域（续）

序号	风险评估项	风险评估方法	结果判定
6	个人信息处理目的已实现、无法实现或者为实现处理目的最短时间。不再必要时，是否按要求删除相关个人信息	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查阅个人信息处理办法，确认规定个人信息留存时间为实现处理目的最短时间； b)　访谈相关人员，查阅删除记录，确认已及时删除不再需要的个人信息
7	在已停止提供涉及个人信息处理的产品或者服务，或者保存期限已届满时，是否按要求删除相关个人信息	人员访谈	满足以下要求的为符合，不满足以下要求的为不符合：访谈相关人员，查阅删除记录，确认已及时删除不再需要的个人信息
8	机构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	系统核查	满足以下要求的为符合，不满足以下要求的为不符合：查看信息系统，确认信息系统中提供对个人信息处理规则解释说明的途径
9	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	系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a)　查看信息系统，确认存在利用用户个人信息和算法定向推送信息情形时（包括利用个人信息和个性化推荐算法等推送新闻和信息、展示商品、推送广告等），在隐私政策中进行了相关说明； b)　查看信息系统，确认为用户提供拒绝接收定向推送信息，或停止、退出、关闭相应功能的机制，或不基于个人信息和个性化推荐算法等推送的模式、选项
10	自然人死亡的，其近亲属为了自身的合法、正当利益，是否能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	系统核查	满足以下要求的为符合，不满足以下要求的为不符合：查看信息系统，确认建立便捷的近亲属对死者相关个人信息进行查阅、复制、更正、删除的途径
11	是否存在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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：数据处理记录、审计报告、合规性评估文件以及与个人信息处理相关的政策和程序，确认不存在个人信息处理者在处理个人信息时违反了法律、行政法规或与个人信息主体的约定
12	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：通过文档审核，确认制定明确的个人行使权利的申请受理和处理流程，确认组织在拒绝个人行使权利请求时，有明确的政策或程序来说明拒绝的理由，且这些理由合理、合法

9.3.4.5　信息处理评估子域

信息处理评估子域具体内容见表30。

表30　信息处理评估子域

序号	风险评估项	风险评估方法	结果判定
1	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅个人信息保护类制度文件，确认文件中明确个人信息保存的期限，且该期限符合实现处理目的所必要的最短时间规定； b) 查看涉及个人信息处理系统，验证系统按制度文件要求进行个人信息保存
2	是否将个人生物识别信息与个人身份信息分开存储	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅个人信息保护制度文件，确认文件中明确将个人生物识别信息与个人身份信息分开存储要求； b) 查看涉及个人信息处理系统，验证系统中已将个人生物识别信息与个人身份信息分开存储
3	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅涉及个人信息处理系统相关设计文件，确认文件明确处理个人信息时已与受托人约定处理目的、期限、处理方式等； b) 查看涉及个人信息处理系统，验证系统已按设计文件要求与受托人约定个人信息处理目的、处理方式、保护措施等，且系统对个人信息处理活动进行监督记录
4	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	人员访谈 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确认在执行过程中个人信息均按照与委托人约定的目的、方式进行处理； b) 查看涉及个人信息处理系统，验证系统是按照与委托者约定的目的和方式进行的个人信息处理
5	个人信息公开是否取得个人单独同意	人员访谈 文档审核	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，查阅相关制度文件，确认文件中明确有个人信息公开需取得委托人同意流程设计； b) 查看文档，确认已公开的个人信息均取得对应委托人的知情同意书
6	处理不满14周岁未成年人个人信息时，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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅个人信息保护制度规范，其中针对不满14周岁的未成年人个人信息制定有专项信息处理规则； b) 查看涉及个人信息处理系统，验证系统中不满14周岁未成年人个人信息处理是按制度规范要求进行处理，且具备未成年人信息处理知情同意书

表30　信息处理评估子域（续）

序号	风险评估项	风险评估方法	结果判定
7	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅数据保护政策、数据处理协议以及相关的隐私政策，确认敏感个人信息的处理是基于特定的目的，并且这些目的具有充分的必要性，且文档中详细说明了对敏感个人信息采取的保护措施
8	处理敏感个人信息是否取得个人的单独同意	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅隐私政策、用户协议、数据处理记录等文档，确认其中明确规定了对个人敏感信息处理的同意获取流程，并且有明确的个人同意记录； b) 通过系统核查，检查系统有明确的用户界面或交互流程，确认用户在系统处理其敏感信息前提供明确的同意
9	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅涉及个人信息处理系统相关设计文件，确认文件明确处理个人信息时与受托人约定处理目的、期限、处理方式；等； b) 查看涉及个人信息处理系统，验证系统已按设计文件要求与受托人约定个人信息处理目的、处理方式、保护措施等，且系统对个人信息处理活动进行监督记录
10	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 访谈相关人员，确认在执行过程中个人信息均按照与委托人约定的目的、方式进行处理； b) 查看涉及个人信息处理系统，验证系统是按照与委托者约定的目的和方式进行的个人信息处理
11	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅相关制度文件，确认如果涉及敏感个人信息处理，有取得相关许可的证明
12	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	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：查阅组织的数据保护政策、数据处理协议以及相关的隐私政策，确认敏感个人信息的处理是基于特定的目的，并且这些目的具有充分的必要性，且文档中详细说明了对敏感个人信息采取的保护措施
13	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织的业务操作手册、用户协议、隐私政策以及其他相关政策文件，确认开展业务活动时提供了多种身份鉴别方式，以及用户拒绝使用人脸识别时的替代方案； b) 通过系统核查，检查业务系统中的身份验证流程和用户界面，确认提供了除人脸识别之外的其他身份鉴别方式，确认在用户拒绝使用人脸识别时，系统继续提供服务而不进行频繁的授权申请或提示

表30　信息处理评估子域（续）

序号	风险评估项	风险评估方法	结果判定
14	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	文档审核 系统核查	满足以下所有列项的为符合，不满足以下列项中一项或多项的为不符合： a) 查阅组织的数据管理政策、隐私政策以及相关的技术规范，确认在身份鉴别过程中收集和使用的人脸相关数据在操作完成后被及时删除，且存在定期的数据清理和审计流程来确保政策的执行； b) 通过系统核查，检查业务系统审计日志，确认执行了数据的删除操作
15	是否满足人脸识别有关政策规定	文档审核	满足以下要求的为符合，不满足以下要求的为不符合：通过文档审核，检查关于敏感个人信息处理操作的技术规范，确认符合人脸识别相关政策规定，包括但不限于人脸识别技术的使用目的、使用范围、数据保护措施、用户同意获取、数据存储和处理的安全性要求等

9.4 分析和评价

9.4.1　评估结果风险分析

在风险评估结果的基础上，从影响数据保密性、完整性、可用性和数据处理合理性角度，分别从数据处理活动、数据安全管理、数据安全技术和个人信息保护四个评估域，对风险评估不符合项进行风险源识别和风险类型分析，常见风险源见附录A，共计归纳169项，可能导致的安全风险见附录B，共计归纳21个类型。

9.4.2　风险危害程度分析

风险危害程度评价，从数据安全风险一旦发生，对国家安全、公共利益或者个人、组织合法权益造成的危害程度进行评价，主要考虑数据价值、风险隐患严重程度两个因素。其中数据价值主要从数据分级角度衡量数据价值，数据级别越高代表数据价值越高。风险隐患严重程度，主要考虑不同风险危害对数据、数据处理活动带来的损害程度，例如违法违规类风险的严重程度可能比数据安全风险的严重程度高。

在综合分析数据价值、风险隐患严重程度的基础上，将风险危害程度从低到高分为很低、低、中、高、很高5个级别。风险危害程度按照就高从严、整体分析原则评价，如果该风险涉及多个数据资产，应对数据进行累加判断。数据安全风险危害程度见附录C。

9.4.3　风险综合评价

针对不同的评估不符合项，识别对应风险源，分析可能导致的数据安全风险，并对其危害程度做综合分析，形成风险评估综合评价表，示例见表31。根据评价表中的结果，参考计算公式得出评价分值，数据安全风险评分方法见附录D。

示例:

表31　风险评估综合评价

序号	评估不达标项	风险源	可能导致的风险	危害程度
1	数据采集没有相关合同协议	a）窃取或者以其他非法方式获取数据； b）数据完成采集后，未按照合同要求使用数据，将数据用于“大数据杀熟”，违反法律、行政法规规定的目地和范围	违法违规利用数据	高
2	在邮件、网络传输接口、终端等关键环节，没有部署数据防泄漏设备	a）数据收集来源被盗，收集的数据被仿冒、伪造； b）采集数据遭投毒，导致数据不可用	数据泄露风险	中

9.5 总结

9.5.1 编制报告

9.5.1.1 风险评估报告概述

报告概述内容包括：

a) 风险评估工作组织情况，包括风险评估时间安排、参与人员、前置准备、方案表述等；
b) 风险评估工作概述，包括风险评估目的及依据，风险评估对象和范围，风险评估结论概要；
c) 风险评估主体的基本信息，数据资产情况、风险评估对象系统情况、现有安全措施等情况；
d) 风险评估主体真实性承诺。

9.5.1.2 风险评估分析及评价

整体风险评估分析及评价的内容包括：

a) 风险评估详细结果，对风险评估实施工作的主体内容做情况汇总，对于数据处理活动安全、数据安全管理、数据安全技术、个人信息保护四个评估域，厘清具体风险评估不符合项；
b) 风险综合分析，基于风险评估结果，进行对应风险源识别和风险类型说明，给出风险危害程度参考，分别列出高、中、低风险数目，对于不同级别的数据安全风险分别进行情况详述；
c) 《数据安全风险综合分析表》及量化评分。

9.5.1.3 报告附件

风险评估执行过程中的重要文档附在报告后作为组成部分，包括：

a) 风险评估不符合项详情表；
b) 风险处置建议表；
c) 风险评估过程的关键记录和证据。

9.5.2 残余风险分析及处置建议

风险评估人员结合最终风险评估报告内容，依据风险评估主体实际情况，提供对应风险处置措施意见，预判措施有效性和残余风险，形成记录，常见风险处置建议见附录E。

附 录 A
（资料性）
常见风险源

常见风险源见表A.1～表A.4。

表A.1 数据处理活动评估域常见风险源

评估子域	风险评估项	风险源类型	常见风险源
数据收集安全	收集过程	恶意攻击	恶意代码注入、数据无效写入、账号操控
		数据泄露	敏感数据丢失
		数据质量低	数据无效写入、无作为或操作失误
		篡改	数据污染、非法数据源投毒
		越权或滥用	数据分类分级或标记错误、采集数据过度获取
		抵赖	采集数据难以追溯定责
		管理不到位	数据收集频次、内容混乱
		违法违规获取数据	数据窃取、超范围收集
		社会工程学	网络钓鱼
	安全管理	管理不到位	人员误操作、提供虚假数据、未取得采集对象同意、未申明采集数据使用范围等
	承载数据平台/系统	软硬件故障、物理环境影响等	采集设备、采集接口等脆弱性被利用，其他方面参考等级保护测评和风险评估的结果
数据传输安全	传输过程	数据泄露	数据窃取、旁路攻击、网络监听、数据从高安全区域传输到低安全区域、重要数据明文传输
		篡改	数据篡改、数据传输缺乏完整性验证、伪装通信代理或通信对端等数据篡改
		恶意攻击	传输两端发起端与接收端不一致、病毒感染、网络拒绝、传输数据劫持、伪造网络凭证、窃取应用程序访问令牌、使用替代身份验证材料、撞库攻击、重定向攻击、恶意代码注入
	安全管理	管理不到位	知情同意、运维管理人员误操作、数据传输不合法等，其他参考等级保护测评和风险评估 (管理内容) 的结果
	承载数据平台/系统	软硬件故障、物理环境影响等	网络堵塞、终端拒绝、缺乏冗余线路设计、未使用加密通道传输数据、使用弱加密算法加密、传输过载或超过传输通道承载能力等数据无法传输或丢失；其他方面参考等级保护测评、密码评估和风险评估的 (技术内容) 结果

表A.1　数据处理活动评估域常见风险源（续）

评估子域	风险评估项	风险源类型	常见风险源
数据存储安全	存储过程	数据泄露	数据窃取、数据不可控、存储数据丢失、未授权爬取
		篡改	数据篡改、数据破坏
		越权或滥用	数据分类或标记错误、权限滥用、过多特权账号、 非授权访问或数据误操作
		恶意攻击	恶意代码执行、SQL注入、盗取应用程序访问令牌、撞库攻击
		抵赖	审计线索不足
	安全管理	管理不到位	内部人员误操作、存储平台权限管理失效；缺少对第三方云平台、数据中心等的管控；其他可参考等级保护测评和风险评估 (管理内容) 的结果
	承载数据平台/系统	软硬件故障、物理环境影响等	物理环境及设备故障、网络故障、备份失效、物理环境变化、 自然灾害等；缺乏存储容错与灾备机制等；其他方面可参考等级保护测评、密码评估和风险评估的 (技术内容) 结果
数据使用和加工安全	使用和加工过程	恶意攻击	注入攻击、恶意盗取、中间人攻击
		数据窃取	在使用加工过程中缺少监督管控机制，导致数据窃取
		抵赖	数据抵赖
		越权或滥用	违反法律、行政法规规定的目的和范围使用加工数据，数据越权使用、使用权限混乱、数据过度获取、信任滥用威胁、分析结果滥用、违规操作
		数据泄露	数据不可控、敏感元数据未脱敏使用，去标识化或匿名化策略失效，对不同来源的数据整合后使得敏感数据被还原、泄露
		违法违规违约加工使用数据	未按有关规定或约定期限要求，超期使用有关数据；违规利用数据进行“大数据杀熟”、违规舆论引导等违法违规行为
		无作为或操作失误	错误处理敏感数据
	安全管理	管理不到位	内部人员误操作、恶意授权等；其他可参考等级保护测评和风险评估 (管理内容) 的结果
	承载数据平台/系统	软硬件故障、物理环境影响等	数据处理设备故障等；其他方面可参考等级保护测评、密码评估和风险评估的 (技术内容) 结果

表A.1 数据处理活动评估域常见风险源（续）

评估子域	风险评估项	风险源类型	常见风险源
数据公开安全	数据公开过程	违反相关法规政策要求	国家和行业发布新的法律法规和行业规章，调整了数据公开的方式、受众范围、访问权限，导致公开目录未及时更新，或已公开的数据与现行法律法规和行业规章的要求不一致
		数据公开评估能力缺失	缺少相关手段评估已公开数据或将公开数据，对国家安全、公共利益或者个人、本单位合法权益造成影响
		缺少数据防爬取手段	缺少公开的数据异常访问或异常操作检测手段， 如已公开的数据被超过设定阈值的频率访问，或访问操作超出设定的访问权限 (如增加、删除、 编辑、读取、导出等)，或访问人群超出设定的受众范围，或访问已公开数据的身份鉴权失效；缺少公开数据反爬取手段
	安全管理	管理不到位	数据公开的管理制度缺少或不完善，未对数据公开的方式、受众范围、访问权限，以及数据内容审核及审批制度、数据发布应急处理流程的情况做出明确规定；本单位的数据公开情况底数不清，未形成数据公开目录；本单位的数据公开制度更新，调整了数据公开的方式、受众范围、访问权限，导致公开目录未及时更新，或已公开的数据与制度要求不一致
	承载数据平台/系统	软硬件故障、物理环境影响等	数据公开相关软硬件故障或物理损毁；其他方面可参考等级保护测评、密码评估和风险评估的(技术内容) 结果
数据提供安全	数据提供过程	数据泄露	未对数据进行去标识化等脱敏处理、数据提供过程缺少有效数据传输安全保护机制、接收方未对接收到的数据进行访问控制或有效保护
		违反数据合法合规提供原则	数据提供不具备正当、合法目的，提供个人信息缺少用户的单独同意，超出约定的处理目的、方式或范围处理数据，接收方缺少对接收数据存储期限、存储地点和到期后处理方式的明确规定
		越权或滥用	共享权限混乱、数据过度获取、数据不可控
		恶意攻击	中间人攻击、篡改攻击、重放攻击、数据信息监听、资源劫持、网络拒绝、撞库攻击
		篡改	数据篡改
		恶意代码和病毒	恶意加密 (勒索病毒等) 、病毒横向蠕动
	安全管理	管理不到位	缺少对数据提供的安全管理制度、内部人员权限管理失效、访问控制失效等；其他可参考等级保护测评和风险评估 (管理内容) 的结果
	承载数据平台/系统	软硬件故障、物理环境影响等	终端拒绝、数据未加密、数据交换设备故障等；其他方面可参考等级保护测评、密码评估和风险评估的 (技术内容) 结果
数据删除安全	删除过程	数据泄露	数据到期未删除、数据未有效删除、残余数据利用、残余介质利用或丢失、资源劫持、容器和资源发现、匿名化策略失效、数据删除不彻底
	安全管理	管理不到位	缺少数据销毁机制、违反法律法规相关规定等；其他可参考等级保护测评和风险评估(管理内容)的结果
	承载数据平台/系统	软硬件故障、物理环境影响等	数据销毁设备故障等；其他方面可参考等级保护测评、密码评估和风险评估的 (技术内容)结果

表A.2　数据安全管理评估域常见风险源

风险源类型	常见风险源
数据安全组织管理不当	关键岗位数据安全管理职责不清晰
	数据涉敏岗位职权不分离
	违反法律、行政法规规定非法开展个人信息处理活动
数据安全制度流程存在缺陷	缺少数据安全总体策略、方针、目标和原则
	数据安全相关制度内容不满足国家和行业数据安全法律法规和监管要求
	数据安全管理制度的制定、评审、发布、缺少定期审核和更新机制
数据分类分级管理缺失或执行不到位	数据资产梳理更新不及时，对应防护措施不能落实
	数据分类分级方法不准确，存在错误分类分级数据
	存在静默数据资产
	存在高危权限账户
相关人员安全管理不到位	有预谋或以利益为目的窃取或者破坏数据
	滥用权限非正常访问、修改、窃取数据
	员工数据安全意识薄弱
	人员能力与岗位要求不匹配
数据合作方安全管理不到位	数据被合作方非法扩大目的使用
	合作方数据泄露
	数据合作管理混乱，存在数据违规合作风险
	数据实际合作内容和协议中不匹配，数据超种类、超数量供应
数据安全应急制度和响应方案存在缺陷	数据安全应急处置分工不清，责任不明
	缺乏针对性的应急处置措施和统一协调
	缺乏应急处置实践经验
	应急处置策略和方法缺乏依据，随意性强
	既有应急处置机制无法适应新情况
	人工进行安全事件的判定和闭环
	人员能力得不到保证
	安全事件的发生和影响，无法得到有效缓解和避免

表A.3　数据安全技术评估域常见风险源

风险源类型	常见风险源
安全监测预警与安全审计缺陷	未对本单位电子数据流转的全过程进行监控与审计
	物理介质传递等过程中的视频监控等记录材料不完整
	缺少在线监测手段及时发现数据传输、共享等情况下的网络攻击风险
	高安全等级区域内缺少视频监控等基础安全设施，或者设备未正常运行
	缺少对异常行为事件的发现和监测能力
	缺少对日常行为的监测预警能力
	单位缺少对非法内联和非法外联的网络行为的分析、监测预警、阻断或限制以及行为记录等的技术手段，或相关监测系统未正常运行
	单位缺少对数据操作、泄露数据的追溯能力
	缺少对数据安全监测情况的定期跟踪评估
	数据安全组织机构管理不完善，缺少监督机制
	数据安全审计相关岗位及人员设置不健全
	数据安全审计岗位未签署责任协议或协议内容不符合安全要求
	缺少对数据安全审计岗位及人员的定期审查机制
	数据安全审计相关制度文件不健全或未起到应有的作用
	缺少统一有效的数据安全审计管理系统
	未形成定期数据安全审计机制
	缺少对第三方接入产品和服务的安全审计和监测措施
	本单位存在数据访问权限和实际访问控制情况不一致的情况，未及时发现并清理已失效的账号和授权
	缺少对特权账号操作行为的审计措施，或审计记录存在被删除或篡改的可能性缺少对数据加工过程的监督和审计措施
	通过安全运维管理平台等访问或操作数据时，未经过安全审计记录，可能存在违反数据安全保护要求的情况
	缺少对数据委托行为的审计记录，可能存在委托处理的数据超过安全等级要求，或者数据未经脱敏、标记等安全风险
	与委托方通过在线方式进行数据传递时，缺少相应的审计记录措施
	缺少对数据外部共享场景的安全审计措施
	数据销毁过程管理措施不完善
数据访问控制措施不到位	盗用账号窃取数据
	脱库、撞库等数据窃取
	使用共享账号篡改、窃取数据
	使用程序账号篡改、窃取数据
	使用多余账号、过期账号篡改、窃取数据
	使用多余权限、过期权限篡改、窃取数据
	内部恶意人员非法篡改、窃取数据

表A.3 数据安全技术评估域风险源（续）

风险源类型	常见风险源
数据防泄漏手段缺失或不到位	被采集数据的范围和边界不明确，未采取必要控制措施
	内外部数据传输未考虑使用加密措施确保传输过程的安全
	未部署相关设备监测网络可用性及防范数据泄漏风险
	对数据存储媒体的访问和使用未进行有效管控
	对数据分布式处理过程缺乏有效管控
	对导入导出过程中数据的安全性未进行管控
	缺乏对数据和存储媒体的安全销毁手段
	缺乏对终端设备上数据和数据操作进行管控
	缺乏对数据的访问和操作的有效监控和审计
	终端数据未纳入单位数据资产清单
	终端未采取准入控制、终端鉴别等安全技术措施，无法防止非法或未授权终端接入内部网络
	使用内部无线网络传输数据，未采取相应安全措施防范数据泄露、防范恶意代码传播等，例如允许移动智能终端在内网和互联网之间无任何安全措施情况下交叉使用
	未建立数据访问权限申请和审核批准机制，或者实际操作与申请审批结果不一致
	未采用专用终端设备操作数据
	专用终端设备未经审批授权就开通使用
	通过专用终端设备访问数据时，未采取技术手段限制获取数据的范围，包括但不限于数据对象、数据量等，或者未对获取的数据采取安全措施，例如脱敏处理等，导致生产数据未经过安全处置
	对接入单位内部、开发测试等环境的内外部终端设备，缺少统一的安全管控措施，例如未安装统一的终端安全管理软件等
	未采取终端合规检查、终端安全状态监测等技术手段，防止终端设备的操作系统管理权限被非法破解，进而成功接入单位内部网络
	终端设备鉴别强度低，未通过多因素认证、设备证书等技术手段，增强对使用者身份的标识和验证
	未采取智能化分析等技术手段，动态调整终端设备的管控策略
	未定期开展日志信息分析工作，或者分析结果未形成总结报告
	缺少对异常行为的应急处置能力
数据脱敏缺陷	脱敏后的数据被恶意复原
	数据脱敏未覆盖到所有数据使用场景
	脱敏后的数据影响业务正常使用
接口安全风险	API存在漏洞被攻击导致数据被非法获取，攻击手法包括但不限于：重放攻击、注入攻击、DDoS等
	API鉴权失效，包括但不限于：用户身份鉴权失效、对象级别的鉴权失效和功能级别的鉴权失效等
	API敏感数据展示不当，通过API接口直接获取未脱敏或伪脱敏数据
	API过量数据暴露，API接口接收到参数请求后，后台服务器未做筛选，便将大量数据返回至前端，造成敏感数据泄露
	API被第三方非法留存数据，第三方通过频繁访问合作接口，私自过量缓存、获取数据
	数据备份策略不当，包括备份间隔时间过长或备份数据不全面
	备份数据损坏，包括备份存储介质故障损坏、被病毒攻击等
	数据备份恢复操作日志丢失，造成数据无法恢复

表A.4　个人信息保护评估域常见风险源

风险源类型	常见风险源
未公开收集使用规则	App中没有隐私政策，或者隐私政策中没有收集使用个人信息规则
	App首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则
	隐私政策等收集使用规则难以访问，如进入App主界面后，需多于4次点击等操作才能访问到
	隐私政策等收集使用规则难以阅读，如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等
未明示收集使用个人信息的目的、方式和范围	未逐一列出App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等
	收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用户阅读等
	申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解
	有关收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解，如使用大量专业术语等
未经用户同意收集使用个人信息	征得用户同意前就开始收集个人信息或打开可收集个人信息的权限
	用户明确表示不同意后，仍收集个人信息或打开可收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用
	实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围
	以默认选择同意隐私政策等非明示方式征求用户同意
	未经用户同意更改其设置的可收集个人信息权限状态，如App更新时自动将用户设置的权限恢复到默认状态
	利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项
	以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限，如故意欺瞒、掩饰收集使用个人信息的真实目的
	未向用户提供撤回同意收集个人信息的途径、方式
	违反其所声明的收集使用规则，收集使用个人信息
违反必要原则，收集与其提供的服务无关的个人信息	收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关
	因用户不同意收集非必要个人信息或打开非必要权限，拒绝提供业务功能
	App新增业务功能申请收集的个人信息超出用户原有同意范围，若用户不同意，则拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外
	收集个人信息的频度等超出业务功能实际需要
	仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息
	要求用户一次性同意打开多个可收集个人信息的权限，用户不同意则无法使用
未经同意向他人提供个人信息	既未经用户同意，也未做匿名化处理，App客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息
	既未经用户同意，也未做匿名化处理，数据传输至App后台服务器后，向第三方提供其收集的个人信息
	App接入第三方应用，未经用户同意，向第三方应用提供个人信息
未按法律规定提供删除或更正个人信息功能或未公布投诉、举报方式等信息	未提供有效的更正、删除个人信息及注销用户账号功能
	为更正、删除个人信息或注销用户账号设置不必要或不合理条件
	虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需人工处理的，未在承诺时限内（承诺时限不宜超过15个工作日，无承诺时限的，以15个工作日为限）完成核查和处理
	更正、删除个人信息或注销用户账号等用户操作已执行完毕，但App后台并未完成的
	未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不宜超过15个工作日，无承诺时限的，以15个工作日为限）受理并处理的

附 录 B
（资料性）
数据安全风险类型

数据安全风险的类型见表B.1。

表B.1 数据安全风险类型

序号	风险类型	内容
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、人员操作失误作或有意盗取等，导致数据被未授权泄露、访问从而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从而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、数据质量下降等从而影响数据可用性、准确性的风险
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，导致数据被丢失、难以恢复等从而影响数据可用性的风险
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，或缺乏有效安全措施、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
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权	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合法权利
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
19	数据处理抵赖	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	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	其他	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
（资料性）
数据安全风险危害程度

数据安全风险的危害程度说明见表C.1。

表C.1 数据安全风险危害程度

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	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
		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
		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
		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	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
		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	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
		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	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
		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	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
		严重影响人民群众的日常生活秩序
		严重影响各级政务部门履行公共管理和服务职能
		严重影响法治和社会伦理道德规范
	中	对人民群众的日常生活秩序造成一般影响
		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
		直接影响公共场所的活动秩序、公共交通秩序

表C.1 数据安全风险危害程度表（续）

影响对象	危害程度	参考说明
公共利益	很高	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
		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
		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	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
		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
		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

附 录 D
（资料性）
数据安全风险评分方法

按照9.4.4 数据安全风险危害程度定性分析方法，表 D.1以百分制给出数据安全风险危害程度等级得分区间，结合实际情况，得出风险危害程度的分值。

表 D1 数据安全风险危害程度等级得分区间

等级	得分
很高	[80%, 100%]
高	[60% 80%)
中	[40%, 60%)
低	[20%, 40%)
很低	[0%, 20%)

根据公式D.1，计算每一个风险评估不符合项的量化分值（Ci），根据公式D.2，以所有风险评估不符合项的量化分值（C_1、C_2、…、C_n）累加后得出最终风险评分（R），R值越大代表风险越高。计算公式如下：

$$Ci=Li*0.5 \quad \cdots\cdots (D.1)$$

式中：

Ci ——第i个风险评估不符合项量化分值；

Li ——第i个风险评估不符合项对应的风险危害程度得分。

$$R=\sum_{i=1}^{n} Ci \quad \cdots\cdots (D.2)$$

式中：

Ci ——第i个风险评估不符合项量化分值；

n ——具体风险评估不符合项的个数。

附 录 E
（资料性）
数据安全风险常见处置方法

数据安全风险常见处置方法见表E.1～表E.4。

表E.1 数据处理活动风险常见处置方法

数据处理活动	安全处置措施
数据收集	通过合同协议等方式，约定从外部机构采集的数据范围、收集方式、安全措施
	明确数据采集渠道，规范数据收集格式、流程方法，采取措施保持数据源正式有效及采集过程的安全可控
	建立数据源管理的机制，包括明确人员、梳理检查、制定制度、整改及定期检查 等方面内容
	对外部数据源和外部收集数据进行鉴别和记录
	制定数据质量管理制度，明确数据质量管理要求
	采取技术工具对数据质量的一致性、完整性、准确性等属性进行监控和管理
数据存储	制定数据备份与恢复策略，采用技术手段对存储数据进行备份，定期对备份数据的有效性进行验证
	针对数据分类分级情况建立不同的数据存储安全防护机制，如设置不同业务数据的存储合理时间、分开存储、划分逻辑区域采取不同安全措施
	采用技术手段对存储数据进行备份，定期对备份数据的有效性进行验证
	对重要数据进行加密后存储，并建立有安全的密钥管理体系保证数据存储机密性安全；采用完整性校验算法对存储数据进行完整性校验，及时发现数据存储过程被篡改和破坏的情况，保护数据存储的完整性
	建立第三方云平台、数据中心等外部提供者数据存储约束与控制措施，并定期对措施有效性进行验证
	针对数据分类分级情况建立不同的数据存储安全防护机制，如设置不同业务数据的存储合理时间、分开存储、划分逻辑区域采取不同安全措施
数据传输	在数据分类分级的基础上，根据业务场景，进行数据加密后传输或采用加密传输通道，防止数据在传输过程中被窃取和泄露，保护数据传输的机密性
	建立完整性校验机制对数据传输过程进行校验，防止数据在传输过程中被篡改和破坏，保护数据传输的完整性
	采用技术手段对传输通道两端主体进行身份鉴别
	对关键的网络传输链路、网络设备节点实行冗余建设，建立灾难和宕机替代方案； 建立有数据传输的接口管理，并对接口的数据传输建立日志记录与监控审计体系
	根据国家相关法律法规中关于数据传输的相关要求，制定数据分类分级传输管理规定，并根据管理规定涉及相应的数据传输策略，保证数据传输的合理性
数据使用和加工	对数据使用环境进行保护，通过账号管理、访问控制策略、鉴权及审计策略对数据使用、加工环境约束
	加工过程中涉及的应用平台、数据库、服务器等环境应采用身份鉴别技术，且用户身份标识具有唯一性，用户身份鉴别信息具有复杂度要求并要求定期更换具有登录失败处理功能，配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施
	相关环境保持日志开启审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息,具体安全要求参考等级保护相关标准实施
	通过用户隐私协议、合同、安全附加条款等途径获取对数据使用加工的授权，确保对涉及数据的使用加工行为具备充分授权，使用加工目的具备充分授权
	数据使用权限应进行定期复核，确保授权人员仍属于合理使用范围，此外应定期检查审计日志，或采用基于规则的事件告警服务，对越权访问行为进行监控
	通过需求评估、PIA评估等管理流程，确保数据使用加工目的的合法性和正当性，确保数据使用加工目的符合法律法规要求、不明显违背数据来源和业务所处环境道德伦理和公序良俗
	定期对业务场景进行及授权情况进行复核，确保业务场景变化仍处于授权范围内，业务环境仍对数据有明确需求，满足正当合理必要原则
	结合场景对通过匿名化、去标识化的手段对使用加工数据进行脱敏，确保使用加工过程中涉及的数据集是实现使用加工目的的最小的数据集
	定期对去标识化或匿名化策略有效性进行评估，监控相关技术手段的安全性是否仍然满足安全要求，并根据评估结果判断是否进行策略更新

表E.1 数据处理活动风险常见处置方法（续）

数据处理活动	安全处置措施
数据使用和加工	对数据使用加工结果进行评估，避免产出数据还原脱敏前原始信息
	对于加工结果数据进行重新分类定级，并在分类定级过程中确认是否包含原始数据，并结合加工结果应用场景判断是否授权充分。具备留存和使用条件
	通过数据申请、授权管理方式确保使用加工过程中涉及的数据是必要的，确保使用加工过程中涉及的数据集是实现使用加工目的的最小的数据集
	在申请加工数据前对数据加工使用逻辑进行确认，对于中间数据、过程数据所处环境进行监控，避免非必要的数据留存
	对于加工结果数据进行重新分类定级，并结合加工结果应用场景判断数据承载环境是否满足安全要求
	开展算法评估工作，确保加工过程中使用的算法与预期一致
数据提供	通过合同协议等方式，约定提供的数据范围、提供目的、传输方式、安全措施
	向涉及提供个人信息的主体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，并取得个人的单独同意
	通过合同协议等方式，约定接收方在约定的处理目的、处理方式和个人信息的种类等范围内处理个人信息
	通过合同协议等方式，约定接收方变更原先的处理目的、处理方式的，应重新取得个人同意
	接收方缺少对接收数据存储期限、存储地点和到期后处理方式的明确规定
	制定数据提供管理制度，规范数据提供流程与技术保障措施
	提供方对提供的数据进行了去标识化等脱敏处理
	提供数据过程中的数据传输采用加密措施
	接收方对接收到的数据进行访问控制
数据公开	建立数据主动公开管理制度和操作规范，明确发布数据使用者和发布者的权利和义务的情况
	建立数据公开的管理措施与机制，包括数据公开的方式、受众范围、访问权限，以及数据内容审核及审批制度、数据公开应急处理流程的情况，确保公开内容可以公开且符合法律法规要求
	提供数据发布清单，包括公开数据摘要、数据格式、更新频率等内容，以及使用条件等的设置情况
	建立定期审核检查制度，对已公开的数据进行监控，确定符合本单位数据公开安全管理规定
	定期审核已公开数据，对照国家和行业更新的相关法律法规和行业规章，评估数据公开发布带来的数据安全风险
	采用自动和人工审计相结合的手段，对重要数据和个人信息等高风险数据的在线访问操作进行监控
	具备对异常或高风险数据访问操作的自动化识别和实时预警能力；在数据公开展示重要数据和个人信息时宜具备数据脱敏处理能力，展示界面复制、打印等可将展示数据导出的限制等情况
	对数据公开所面临的风险进行安全评估，对公开的个人信息开展个人信息保护影响评估
	对公开数据增加数据水印
数据删除	对于通过物理介质销毁完成的数据删除，应建立流程，对物理销毁过程进行监控、复核、验证
	定期组织对删除数据所使用技术的评估、确保通过匿名化或物理手段删除的数据仍无法被还原
	通过数据血缘、密钥管理、可信执行环境及数据隔离等技术手段保持对原始数据流转的追踪，确保数据删除在环境中能被完整执行，并能够提供证明，确保数据已被完整删除或匿名化处理
	对于数据主体主张删除后仍需保留以满足法律法规要求的场景，通过数据隔离、可信执行环境、密钥管理等技术拆分数据归档环境，以确保根据法律法规的要求能对数据进行还原，同时无人能独立接触到归档数据

表E.2 数据安全管理风险常见处置方法

数据安全管理	安全处置措施
资产管理	建立数据资产管理制度，明确数据资产管理统一规范要求
	建立数据资产清单，并进行定期更新
	建立数据资产变更记录，对数据资产使用、留存及报废等状态进行登记，并针对已形成的数据资产清单定期更新数据资产变更记录
组织管理	建立数据安全管理委员会领导小组
	建立数据安全管理部门，牵头承担组织内部数据安全管理工作
	指定组织最高管理者或授权代表担任数据安全负责人，负责统筹协调和落实数据安全管理相关工作
	根据职责分离原则设置数据安全管理的岗位和人员
	当组织处理个人信息达到国家网信部门规定数量时，指定个人信息保护负责人
人员管理	员工录用前进行必要的背景审查
	数据服务人员签订安全责任协议和保密协议
	员工入职时按照最小必要原则分配初始权限
	员工离岗和转岗时，及时终止或变更数据操作权限
	制定数据安全培训计划，并按计划开展数据安全培训，保留相关培训记录
	定期对关键岗位人员进行审查和数据安全能力考核
分类分级	及时更新数据资产清单，并与保护措施关联
	制定精细分类分级标准，采用就高原则
	定期监测梳理数据资产，清除静默资产
	重要数据使用最小化授权，数据行为监测
应急响应	设定专职岗位和人员，明确具体岗位的工作内容
	根据不同事件类型，明确相应的处置方法和流程
	形成预案，并定期开展演练
	应符合相应法律、法规，并结合自身业务特点
	应结合不断出现的安全事件和政策变化进行完善和调整
	采取专用工具或系统辅助进行安全事件的分析、处置，提高响应的质量、速度
	应定期开展应急处置机制的宣贯，进行技能培训
	应分析安全事件的深层次原因，并相应进行安全加固和改造
数据合作方	与数据合作方签订协议、合同等，其中明确数据的使用目的、使用场景、供应方式、安全保护约定、安全责任义务等
	设立数据合作场景中的安全风险评估机制，明确评估的频率、内容，形成数据合作风险评估报告，及时整改并采取措施
	建立组织数据合作的相关技术工具，对数据合作目录、数据源数据字典等进行审查记录
	通过数据内容识别、数据交换检测等技术工具，保证数据实际合作内容和协议中保持 一致
投诉举报机制	建立个人信息保护和数据安全投诉、举报渠道
	明确处理投诉、举报的部门、人员和处理流程
	公布受理投诉、举报的响应时间和处理进度，对处理结果有明确回复和说明
数据安全制度	设定清晰明确的数据安全总体策略、方针、目标和原则
	数据安全相关制度内容逐一落实国家和行业数据安全法律法规和监管要求
	建立健全数据安全管理制度的制定、评审、发布、定期审核和更新机制
密钥管理	制定并实施有效的密钥管理制度
	制定并实施有效的密钥使用权限分配方案
	采用符合密码相关国家和行业标准的密钥生成模块
	使用安全的密钥分发和传输方案
	采用符合密码相关国家和行业标准的密钥存储模块
	使用安全的临时密钥协商协议
	使用安全的密钥更新和恢复方案
	对过期和需撤销的密钥立即终止使用并执行有效的密钥销毁措施

表E.3　数据安全技术风险常见处置方法

数据安全技术	安全处置措施
监控与审计	本单位电子数据的保存、查阅、复制等操作均由专人审批，且有审批记录，流转记录完整、审计记录合规
	通过物理介质传递数据时，在传递过程中采用了视频监控等安全措施，确保物理介质安全到位，传递过程中物理介质未离开相关责任人、监控设备等的监视及控制范围
	当通过自动化手段传输、共享数据时，采取了流量监控等手段，有效防范网络监听、接口滥用等网络攻击
	在数据存储系统所部署的高安全等级机房或区域内，部署了电子门禁、视频监控等安全措施，鉴别、记录和控制人员出入
	采用人工或信息系统和产品等方式，实现了对异常行为事件的识别、发现、跟踪和监控等安全防护，包括但不限于IP 、账号、数据、使用场景等内容
	对数据运行情况进行在线实时监测和预警，监测指标包括但不限于对数据访问、传输或下载的授权、次数、频率、总量等
	采取流量分析等技术实现了对数据收集、传输、处理、分析等关键环节的数据流动监测分析，包括但不限于流动类型、流动范围、数据载体、日均量级、数据账号访问情况、数据流向等信息，并对数据流动异常情况或异常数据访问行为（例如不安全的采集设备与采集内容、非授权时段访问重要数据、未授权访问、数据流向未经授权、频繁访问、超量数据传输等进行告警和记录。监测预警系统具备触发监测阈值时的预警机制及安全保护措施，相关操作均有日志记录
	形成预警响应，以及阻断等应急处置能力
	具备主动发现非授权接入和非法外联的设备和策略配置的技术手段
	单位具备对数据操作过程及关键数据要素，在安全事件发生后进行数据溯源的能力，包括但不限于从数据类型、数据量级、数据特征等维度进行数据标记和跟踪，支持从接口、IP 、账号、时间等方面进行溯源分析，以定位追踪到相关责任人
	本单位安全监测情况纳入年度数据安全评估内容
	数据安全组织机构中包含负责数据安全审计的部门
	本单位设置了数据安全审计相关岗位
	数据安全审计岗位设立了专人专岗，且审计岗位与管理、操作等其他岗位实行了职责分离
	签署了数据安全审计岗位责任协议，且协议内容符合安全要求
	本单位定期对数据安全审计岗位人员行为进行安全审查
	本单位制定数据安全审计相关制度和策略，且制度文件完整有效，包括但不限于审计周期、审计方式、审计形式等内容，以及日志的存储、分析和检查等要求
	以数据为中心开展安全审计，包括采集、传输、存储、使用、删除、销毁等阶段。审计范围覆盖至每个有权使用数据的用户，包括数据库管理员、数据库用户、操作系统管理员、操作系统用户、存储介质管理员、业务管理员、业务使用者、存储介质用户等。审计记录包括时间、用户、IP地址、操作对象、操作内容、操作行为和操作结果等相关信息
	对审计记录实施了安全保护，防止未授权的访问和输出。审计记录的留存时间不少于6个月
	单位建立数据安全审计系统，执行单位审计策略，对日志进行统一管理和处理，包括提供对审计记录的统计、查询、分析及报表生成等功能，形成审计报告反馈相关部门
	本单位定期开展数据安全审计工作，包括内部审计或第三方审计等，根据发现的问题和风险反馈情况，制定整改方案并实施
	单位内部审计部门负责对整改工作进行有效监督，包括但不限于指导发现整改情况的追踪、报告管理、问题管理等
	对第三方接入产品和服务的数据处理活动进行审计和记录，确认其能够落实安全管理要求和责任，并对第三方接入产品和服务的数据处理活动进行必要的监测
	本单位对数据的访问权限和实际访问控制情况进行定期审计，包括审计策略、审计周期和审计内容等，每年对访问权限规则和已授权清单进行复核，及时清理已失效的账号和授权
	对特权账号的访问过程和操作记录进行了审计和记录，记录要素完整详尽，且特权账号无法对操作日志进行修改和删除
	对数据加工的过程进行监督和审计记录
	通过安全运维管理平台等访问或操作数据时，应对其相关行为进行审计记录
	对委托处理数据的行为进行审计记录，包括但不限于数据级别、数据片段信息等

表E.3 数据安全技术风险常见处置方法（续）

数据安全技术	安全处置措施
监控与审计	通过信息系统 (包括API 、前置机等) 与委托方进行数据传递时，对数据的外发与回传过程的关键节点进行审计，包括设置安全审计策略、审计周期和审计内容等
	当存在数据外部共享的业务场景时，对数据共享进行安全审计，审计内容包括但不限于数据使用对象、使用期限、使用范围、操作记录、存储方式、到期处置情况等内容
	对数据销毁全过程进行了审计记录和定期检查，审计记录包括但不限于存储介质类别、介质编号、介质所属部门、销毁服务机构、介质应用系统、数据类型、数据安全等级、销毁方式、销毁地点、销毁时间、执行人、监督人等；检查内容包括但不限于存储介质销毁台账与实际情况的一致性，销毁审批手续履行情况，销毁过程记录要素的完备性，对销毁效果的评估等
鉴别与访问控制	采用口令、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身份鉴别，且其中一种鉴别技术至少使用密码技术来实现
	对用户、登录的进程/应用进行身份标识和鉴别，用户身份标识具有唯一性，身份鉴别信息具有复杂度并且定期更新
	指定专门的部门或人员，对用户身份及数据权限的策略、技术能力进行统一管理
	制定身份标识与鉴别、访问控制与权限管理等方面管理制度，明确对身份标识与鉴别、访问控制及权限的分配、变更、撤销等权限管理的要求
	授予管理用户所需的最小权限，实现管理用户的权限分离
	建立系统账户、数据权限的申请审批流程
	定期删除或停用多余的、过期的账户及数据权限
	建立组织统一的身份与访问管理系统，支持人员、数据资源、应用系统的统一纳入
	访问控制的粒度达到主体为用户级，客体为系统、文件、数据库表级或字段
防泄漏	应明确数据的知悉范围和所采取的相应控制措施
	采用适当的加密算法、设备等保护措施，确保传输通道和传输内容的安全
	采用负载均衡、防入侵攻击、数据防泄漏检测与防护等设备进行安全监测
	对终端及网络存储设备的访问和使用场景进行管控
	对外部服务组件注册与使用审核、分布式处理节点间可信连接认证、节点和用户安全属性周期性确认、数据文件标识和用户身份鉴权、数据副本节点更新检测及防止数据泄漏等方面进行管控
	数据导入导出过程中对数据自身的可用性和完整性构成的危害进行管控
	建立对数据和数据载体的销毁规程和彻底删除机制
	明确终端安全配置管理和管理规范，部署终端的防泄漏监测工具
	针对数据生命周期中未授权访问、数据滥用、数据泄漏进行监控和审计
终端数据管理	对本机构内部办公终端中产生、交换、归档的电子数据进行盘点、梳理与分类，纳入统一的数据资产清单
	部署了终端安全管控系统，且配置了相关安全策略，如网络准入控制、多因素终端鉴别等，并且安全策略运行有效
	终端安全管控系统 (服务器) 所配置的安全策略与实际管控终端数量、安全接入要求一致
	在内网和互联网交叉使用移动智能终端时，采取了相应的技术防护措施，例如防范数据泄漏、防恶意代码等，且相关要求已明确在数据安全管理制度中
	采用固定处理终端对信息系统或数据库等进行数据访问等相关操作
	内外部终端设备已采取安全措施，包括但不限于网络准入、防病毒、操作系统补丁、文件输入输出审计等管控措施，且安全策略均正常运行
	通过专用终端获取数据的操作被成功记录，包括网络、主机、数据库等设备的审计日志中
	内外部终端设备接入单位内部、开发测试等环境的申请、准入操作及变更记录，与实际终端数量和被批准的安全策略一致
	单位网络或数据安全管理相关制度规程中，已制定明确的接入申请审批流程，申请表中包括但不限于接入原因、接入时间、申请部门、使用人员、审批人员、途径、接入点以及采取的技术隔离手段等信息
	终端设备通过互联网接入单位内网时，在边界网络区域处采取技术隔离措施，例如代理或前置机等，避免直接访问内部网络
	单位具备根据终端常用位置和目前位置、设备属性、安全状态、访问行为等信息进行动态授权的防护能力

表E.3　数据安全技术风险处置方法（续）

数据安全技术	安全处置措施
终端数据管理	定期对终端设备的日志信息进行分析，包括但不限于结合业务操作日志、系统运行日志、上网行为等日志记录，对数据异常使用、用户异常行为等进行分析，形成数据安全分析报告
	能够及时对可疑的异常情况进行处置
数据脱敏	梳理组织脱敏的各种场景，围绕数据可用性和安全性两方面进行调研确认
	制定组织统一的数据脱敏管理制度，包括脱敏的原则、方法、策略等
	组织建立统一的数据脱敏工具，实现数据脱敏工具与数据权限管理系统、堡垒机系统等的联动或组合使用
	根据具体的数据使用场景采用数据动态脱敏工具或数据静态脱敏工具，不限于生产测试、数据运维、数据分析、数据交换等
	使用数据脱敏工具，保证脱敏后的数据和原始数据之间的逻辑关系保持一致

表E.4　个人信息保护安全风险常见处置方法

个人安全保护	安全处置措施
保护原则	制定和公开个人信息保护政策并严格遵守
	个人信息保护政策满足GB/T 35273中有关个人信息保护政策的要求
	收集个人信息的方式合法，收集的个人信息范围、种类、数量、频率等属性满足最小必要原则
保护措施	传输和存储个人敏感信息时，采用加密存储、去标识化存储等安全措施，并制定备份与恢复策略
告知同意	收集个人信息前，明示个人信息保护政策、数据收集的目的、类型、范围、用途信息，并征得个人信息保护主体同意
	改变处理个人信息的目的、类型、范围、用途的，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修改个人信息保护政策
	收集个人敏感信息前，告知个人信息主体收集目的并取得明示同意，确保明示同意是在完全知情基础上自主给出、具体、清晰、明确的意愿表示
	收集不满14周岁未成年人个人信息前，征得其监护人的明示同意
主体权力	建立公开的个人信息权益投诉、维权渠道，保障个人信息主体的合法权益
	基于个人同意处理个人信息的，信息处理者提供便捷的撤回同意的方式
个人信息处理	制定个人信息分类分级管理措施

参 考 文 献

[1] GB/T 20984 信息安全技术 信息安全风险评估方法
[2] GB/T 31509 信息安全技术 信息安全风险评估实施指南
[3] GB/T 35273 信息安全技术 个人信息安全规范
[4] GB/T 36073 数据管理能力成熟度评估模型
[5] GB/T 37378 交通运输 信息安全规范
[6] GB/T 37988 信息安全技术 数据安全能力成熟度模型
[7] GB/T 39335 信息安全技术 个人信息安全影响评估指南
[8] GB/T XXXXX 信息安全技术 数据安全风险评估方法
[9] JT/T 747.4 交通运输信息资源目录体系 第4部分：公路水路信息资源分类
[10] YD/T 3801 电信网和互联网数据安全风险评估实施方法
[11] T/ISC-0011 数据安全治理能力评估方法
[12] ISO/IEC 27005 Information security, cybersecurity and privacy protection—Guidance on managing information security risks
[13] NIST SP800-30 Guide for Conducting Risk Assessments
[14] 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
[15] 《互联网信息服务算法推荐管理规定》(国家互联网信息办公室 工业和信息化部 公安部 国家市场监督管理总局 令 第9号)
[16] 《交通运输部办公厅关于印发<公路水路交通运输数据分类分级指南>的通知》(交办科技〔2022〕44号)
[17] 张涛，马海群，刘硕，等.英国国家数据安全治理：制度、机构及启示[J].信息资源管理学报，2022,12(6):44-57.
[18] 李艳，章时雨，季媛媛,等.全球数据安全：认知、政策与实践[J].信息安全与通信保密,2021(7):2-10.

交通运输行业标准

交通运输数据安全风险评估指南

（征求意见稿）

编制说明

标准起草组

2024 年 5 月

目　录

一、工作简况

（一）任务来源

根据《交通运输部关于下达2023年交通运输标准化计划（第二批）的通知》（交科技函〔2023〕654 号）安排，制订《交通运输数据安全风险评估指南》，计划编号为JT 2023-117。本标准由交通运输信息通信及导航标准化技术委员会（以下简称“标委会”）提出并归口管理，交通运输部科学研究院牵头承担编制工作。

（二）主要工作过程

1.研究立项阶段

2023年1月～2023年5月，开展标准计划项目建议研究。通过互联网、文献数据库、国家政策法规等途径获取文献资料，了解最新的相关政策法规和技术方法；通过对相关管理单位和部门的走访调研，了解行业内外数据安全标准化工作现状、数据安全管理开展情况和标准化需求；通过对数据安全相关企业和厂商的走访调研，了解前沿的数据安全技术；同时收集了国家、其他行业和地方政府数据安全风险评估相关资料，研究确定标准的整体框架。

2023年6月，召开了标准编制工作方案讨论会议，制定了标准编制工作方案。

2023年7月～2023年9月，起草组基于前期调研情况，确定了标准的技术内容、适用范围和体系框架，编制形成草案初稿，提交标准计划立项申请。

2023年10月，通过交通运输部科技司组织的2023年第二批标准制修订计划立项答辩。

2023年12月，标准通过立项审核，交通运输部正式下达标准编制计划。

2.起草阶段

2023年11月～2024年2月，交通运输部科学研究院成立标准起草组，起草组根据正在制定的国家标准GB/T XXXXX—XXXX《信息安全技术 数据安全风险评估方法》，以及国家和其他行业与数据安全相关的最新法律法规及标准规范，

结合我国交通运输行业数据资源现状和数据安全管理需求，对标准草案中数据安全风险评估原则、评估框架、评估方法、评估启动条件、评估流程等内容进一步修改完善。

2024 年 3 月～2024 年 4 月，秘书处审核了标准的各项内容，提出了有关修改建议。起草组根据意见完善了标准内容，形成了正式的标准征求意见稿。

（三）标准起草单位、主要起草人员及其所做的具体工作

本标准的起草单位为：交通运输部科学研究院、中电长城网际系统应用有限公司、北京中安星云软件技术有限公司。

本标准主要起草人为：黄海涛、王涛、尚赞娣、黄莉莉、曹剑东、淡雅静、郑强、郑金、杨洪路、白紫秀、刘娜、任江、吕晓婷、王思源、张平、郭亚茹、王娜、吴聪雷。任务分工见表 1。

表 1 标准主要起草人及任务分工

序号	姓名	单位	主要工作
1	黄海涛	交通运输部科学研究院	总体负责确定标准编写的总体思路、框架、内容；负责前期立项申请、组织召开评审会、推进工作进度；负责标准第 1～6 章编写、标准编制说明编写等
2	王涛	交通运输部科学研究院	为标准文档框架和技术内容提供指导；参与标准第 5 章编写
3	尚赞娣	交通运输部科学研究院	对标准框架、思路、文本质量等进行审核
4	黄莉莉	交通运输部科学研究院	为标准文档框架和技术内容提供指导；参与标准第 6 章编写
5	曹剑东	交通运输部科学研究院	对标准文本的质量和技术进行审核
6	淡雅静	中电长城网际系统应用有限公司	参与标准框架制定，负责标准第 7～8 章、9.5 章条编写
7	郑强	北京中安星云软件技术有限公司	组织开展标准文本中涉及技术工具的调研；负责标准第 9 章编写
8	郑金	北京中安星云软件技术有限	负责标准文本中评估项与风险源关系验证，技

序号	姓名	单位	主要工作
		公司	术逻辑分析；负责 9.4 章条编写
9	杨洪路	交通运输部科学研究院	参与标准第 7 章编写
10	白紫秀	交通运输部科学研究院	参与标准第 8 章编写
11	刘娜	交通运输部科学研究院	参与标准第 9 章编写
12	任江	中电长城网际系统应用有限公司	为标准文档框架和技术内容提供指导
13	吕晓婷	中电长城网际系统应用有限公司	负责标准文本格式修订，参与标准 9.3 章条编写
14	王思源	交通运输部科学研究院	参与标准 9.5 章条编写
15	张平	交通运输部科学研究院	参与标准附录编写
16	郭亚茹	交通运输部科学研究院	参与标准附录编写
17	王娜	交通运输部科学研究院	参与标准附录编写
18	吴聪雷	中电长城网际系统应用有限公司	组织开展标准文本中涉及技术工具的调研；参与标准 9.3 章条编写

二、标准编制原则和确定标准主要内容的依据

（一）编制原则

1.服务应用原则

本标准的制定为交通运输行业开展数据安全风险评估工作提供指导，帮助行业管理部门掌握数据安全总体状况，有效识别数据安全管理、数据处理活动等环节的数据安全风险和违法违规问题，为进一步健全数据安全管理制度和技术措施，提高数据安全治理能力和防护能力奠定基础。

2.协调性原则

本标准的制定参考了国内已发布的数据安全相关法律法规，其中，术语、部分技术内容引用了已发布的GB/T 20984—2022《信息安全技术 信息安全风险评估方法》、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》等标准。本标准所提出的核心思想、概念、准则、建议等，均与我国现行的《中华人民共和国网络安全法》（2016）、《中华人民共和国数据安全法》（2021）、《中华人民共和国个人信息保护法》（2021）等法律法规、标准规范、政策文件相协调。

3.实践性原则

本标准注重对于风险评估实施的可操作性，通过实践执行了解交通运输行业的数据安全风险现状，为提升交通运输行业数据安全风险防范能力提供有效方法措施。

（二）标准主要内容的确定依据

1.范围

本标准提供了交通运输数据安全风险评估的指导和建议，并给出了交通运输数据安全风险评估的框架、原则、方法、启动条件和流程。

本标准适用于交通运输行业数据处理者及第三方评估机构开展数据安全风险评估工作，交通运输行业管理部门开展数据安全检查评估工作参照使用。

2.规范性引用文件

本标准规范性引用主要参考了以下文件内容：

GB/T 25069　信息安全技术　术语

3.术语和定义

本标准新增的术语及定义包括：交通运输数据、数据安全、评估域、数据处理活动、数据安全风险、数据安全风险评估、合理性、安全措施、业务、风险源。GB/T 25069界定的术语和定义适用于本标准。其中，交通运输数据的定义主要参考了JT/T 747.4-2020，评估域的定义主要参考了GB/T 37988-2019，数据安全、数据处理活动、数据安全风险、数据安全风险评估、合理性、风险源、安全

措施等术语的定义主要参考了 TC260-PG-20231A，业务的定义主要参考了 GB/T 20984。

4. 缩略语

本标准给出以下缩略语，分别是：

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

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

DBA：数据库管理员(Database Administrator)

DDos：分布式拒绝服务攻击(Distributed Denial of Service Attack)

IPSec：IP 网络安全性协议（Internet Protocol Security）

PIA：个人信息保护影响评估(Privacy Impact Assessment)

SQL：结构化查询语言(Structured Query Language)

SSL：安全套接字层协议（Secure Sockets Layer）

SSH：安全外壳协议（Secure Shell）

TLS：传输层安全性协议（Transport Layer Security）

5. 原则

本标准参考了 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》和 GB/T 20984—2022《信息安全技术 信息安全风险评估方法》，综合考虑数据安全风险评估的实践特性以及实施过程中的核心元素，给出了风险评估四项原则，分别是：客观公正原则、可重复可再现原则、最小影响原则和保密原则。

6. 框架

基于数据安全风险评估的基本逻辑，本标准明确整体风险评估工作所包含的各阶段以及各阶段之间的逻辑从属关系，给出风险评估中涉及的主要要素和内容。

本标准参考 GB/T 37988—2019《信息安全技术 数据安全能力成熟度模型》

中的“实践域”原理，提出了“评估域”的概念，具体划分为数据处理活动、数据安全管理、数据安全技术、个人信息保护等四个评估域。起草组从可操作性和落地性方面，考虑到数据处理活动、数据安全管理、数据安全技术、个人信息保护等维度涉及的具体风险评估项、适用方法都不一样，对于技术手段运用的程度也不尽相同，用“评估域”更能体现本标准的特征。

本标准参照 GB/T XXXXX—XXXX《信息安全技术 数据安全风险评估方法》的风险程度说明，提出了风险评估不符合项、风险来源、风险描述三者相关联的风险评估结果，并给出了风险评估结果与安全风险等级相对应的评价体系。

7. 方法

本标准通过前期调研，以及学习国家相关法律法规和其他行业相关政策文件标准规范，参考 GB/T XXXXX—XXXX《信息安全技术 数据安全风险评估方法》，给出四种风险评估方法，分别是：人员访谈、文档审核、系统核查和技术测试。

8. 启动条件

本标准遵循《中华人民共和国数据安全法》（2021），参照网络安全等级保护的执行思路，结合数据安全防护的特性，给出五种风险评估启动条件，首先，执行相关政策法规要求，其次，在政策法规要求发生变化、数据处理活动发生变化、数据进行高风险活动、数据主体发生变更时，宜开展数据安全风险评估工作。

9. 流程

按照评估工作的基本流程，结合本标准风险评估框架的理论体系，风险评估工作分为四个阶段，分别是：风险评估准备、风险评估实施、风险评估分析和评价、风险评估总结。

（1）准备

风险评估准备工作，除组建风险评估团队和制定风险评估方案两项工作外，核心是对风险评估对象进行信息调研，包括评估主体基本情况、数据资产基础情况、数据处理活动情况、个人信息处理情况和现行得数据安全措施。

①确定评估对象和实施范围

参考 GB/T XXXXX—XXXX《信息安全技术 数据安全风险评估方法》，提出确

定风险评估对象和实施范围应考虑数据资产、数据处理活动、业务、信息系统、人员和内外部组织等因素，具体内容的确定参照了 JT/T 747.4 和《交通运输部办公厅关于印发<公路水路交通运输数据分类分级指南>的通知》（交办科技〔2022〕44 号)。

②制定风险评估方案

根据确定的风险评估对象和范围，制定风险评估方案，确定风险评估的内容和方法，包括风险评估流程、实施内容、评估准则、使用方法等，以及基本调研情况，制定风险评估实施计划，包括风险评估具体实施进度安排、人员安排、配套管理等。

③调研评估对象信息

通过学习网络安全风险评估实施的具体办法等实践指引，参考 GB/T XXXXX—XXXX《信息安全技术 数据安全风险评估方法》主要内容，本标准以表格形态列出需要调研的信息内容。首先对风险评估主体的基本情况进行调研，包括行业类目、数据规模、数据范围等；其次，对数据资产基本情况进行调研，包括数据种类、分级分类情况、数据量级等，对具体涉及的数据处理活动情况进行调研，包括收集、存储、传输、使用和加工、提供、公开和删除 7 个环节的基本情况，再对个人信息处理情况进行调研，包括使用目的、范围、运用的技术策略等基本情况；最后，对现有的安全措施情况做调研，包括常规安全检查工具的使用、是否出现过重大安全事故等基本情况。

（2）实施

起草组通过对 GB/T 20984—2022《信息安全技术 信息安全风险评估方法》、GB/T 35273—2020《信息安全技术 个人信息安全规范》、GB/T XXXXX—XXXX《信息安全技术 数据安全风险评估方法》、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》等标准规范学习，发现上述文件在风险评估操作这部分，对于具体的风险评估实践形式没有详细说明，比如，面对不同的评估域采用什么样的风险评估方法，是单一式还是组合式，对于风险评估项的安全指标如何设定，导致可操作性和落地性不强。

起草组对如何能够呈现更明确的实践属性，对于风险评估内容如何能够清

晰明了的进行判定，判定结果又如何与评价体系进行关联等问题，经过反复讨论与调研后，提出具体风险评估内容以表格形式呈现，对每个评估域再分成若干子域，一个评估子域对应一张表格，列清风险评估项，明确对应的风险评估方法和判定条件。

① 数据处理活动评估域

本标准定义了 7 个评估子域，风险评估项分布如下：数据收集安全评估子域，17 个风险评估项；数据存储安全评估子域，15 个风险评估项；数据传输安全评估子域，9 个风险评估项；数据使用和加工安全评估子域，28 个风险评估项；数据提供安全评估子域，34 个风险评估项；数据公开安全评估子域，11 个评估项；数据删除安全评估子域，14 个风险评估项。

② 数据安全管理评估域

本标准定义了 6 个评估子域，风险评估项分布如下：数据安全组织管理评估子域，7 个风险评估项；数据安全制度流程评估子域，12 个风险评估项；数据分类分级管理评估子域，16 个风险评估项；相关人员安全管理评估子域，10 个风险评估项；数据合作授权管理评估子域，16 个风险评估项；数据安全应急管理评估子域，7 个风险评估项。

③ 数据安全技术评估域

本标准定义了 7 个评估子域，风险评估项分布如下：数据访问控制评估子域，8 个风险评估项；数据安全监测预警评估子域，7 个风险评估项；数据脱敏评估子域，5 个风险评估项；数据防泄露评估子域，3 个风险评估项；数据接口安全评估子域，9 个风险评估项；数据备份与恢复评估子域，5 个风险评估项；数据安全审计评估子域，9 个风险评估项。

④ 个人信息保护评估域

本标准定义了 5 个评估子域，风险评估项分布如下：保护原则评估子域，18 个风险评估项；保护措施评估子域，15 个风险评估项；告知同意评估子域，10 个风险评估项；主体权力评估子域，12 个风险评估项；信息处理评估子域，16 个风险评估项。

（3）分析和评价

本标准提出风险评估结果与风险等级综合分析的评价体系，风险评估结果由风险评估不符合项、风险识别和风险分析三元素组成，其识别原理从影响数据保密性、完整性、可用性和数据处理合理性角度出发。依照上述的风险评估实施结果，将不符合项一一识别出常见的风险来源，分析其风险类型。分别给出附录A和B作为对应参考。

① 评估结果风险分析

本标准中将第 9.3 章的风险评估实践结果，对于不符合项逐条进行对应风险源识别，以评估域的划分进行风险内容的详细说明与对应参照，具体分布如下：数据处理活动评估域，48 条；数据安全管理评估域，26 条；数据安全技术评估域，64 条；个人信息保护评估域，31 条，风险来源可能导致得风险类型共计归纳 21 项。

②风险危害程度分析

本标准参考 GB/T XXXXX—XXXX《信息安全技术 数据安全风险评估方法》中对风险等级的说明，在综合分析数据价值、风险隐患严重程度的基础上，将风险危害程度从低到高分为很低、低、中、高、很高 5 个级别，并以附录 C 对数据安全风险危害程度进行说明。

② 风险综合评价

基于上述风险评估结果的风险分析，本标准提出包含风险评估不符合项、风险源识别、风险类型分析和风险危害程度的评价体系，以表格形式进行示例说明。为了帮助被评估主体更直观的了解整体风险评估情况，本标准以附录 D 给出了量化评分的计算参考公式

（4）总结

本标准根据风险评估分析和评价结果，对风险评估对象的整体数据安全风险评估情况进行报告编制，主要内容包括风险评估发现的问题、对应的风险描述及程度、残余风险分析并给出处置建议。

① 编制评估报告

风险评估报告的内容由报告概述、风险评估分析及评价、附件三部分组成，概述部分主要是陈述风险评估主体的基本信息情况，风险评估人员与方案说明，

对于风险评估工作的主体内容情况，包括四个评估域的具体风险评估结果；基于风险评估结果，结合风险源识别和风险类型，对风险危害程度进行评价，列出高等级数据安全风险、中等级数据安全风险、低等级数据安全风险情况，说明高、中、低风险数目，填写“数据安全风险综合评价表”，将风险评估项列表和其他关键记录文件作为附件，形成完整的数据安全风险评估报告。

② 残余风险分析及处置建议

本标准主要是指导交通运输行业开展数据安全风险评估工作，尽可能全面的帮助数据处理者了解自身存在的数据安全风险现状，对于风险处置不列入本标准重点表述内容，起草组以附录形式给出了常见的建议措施，供风险评估主体参考。

10. 附录

本标准共给出了五个附录，均为资料性，分别是：

附录 A 常见风险源，按照数据处理活动、数据安全管理、数据安全技术和个人信息保护四个评估域，以表格形式列出常见风险源，共计一百六十九项；

附录 B 数据安全风险类型，以表格形式列出常见数据安全风险类型，共计归纳二十一项；

附录 C 数据安全风险危害程度，主要参考 GB/T XXXXX—XXXX《信息安全技术 数据安全风险评估方法》，对数据安全风险危害程度的五个等级进行描述；

附录 D 数据安全风险评分方法，参考 GB/T XXXXX—XXXX《信息安全技术 数据安全风险评估方法》，对风险量化评分给出计算公式；

附录 E 数据安全风险常见处置方法，按照数据处理活动、数据安全管理、数据安全技术和个人信息保护四个评估域，以表格形式列出常见处置方法，共计一百七十一项。

三、主要试验的分析综述报告、技术经济论证或预期效果

（一）技术经济论证

根据本标准提出的数据安全风险评估流程、内容和方法，对山东省交通运输厅的 OA 办公系统、公路水路建设市场综合服务管理系统、道路客运联网售票系统、超限运输许可管理系统和重点营运车辆动态信息公共服务平台等 5 个信息系统的数据资源以及涉及的数据处理活动进行了风险评估，有效识别出数据安全管理和数据处理活动中的安全风险，并给出相应的处置建议，最终形成《山东省交通运输厅重点系统数据安全风险评估报告》报中共山东省委国家安全委员会办公室。

（二）预期效果

本标准是贯彻落实总体国家安全观和《数据安全法》（中华人民共和国国务院令 2021 年第 84 号）的具体体现，是提升交通运输行业数据安全防护能力的重要举措，是指导交通运输行业开展数据安全风险评估的重要依据。本标准能帮助行业管理部门掌握数据安全总体状况，有效识别数据安全管理、数据处理活动等环节中的数据安全风险和违法违规问题，为进一步健全数据安全管理制度和技术措施，提高数据安全治理能力和防护能力奠定基础，从而切实加强行业数据安全保护，为促进数字交通发展、加快建设交通强国筑牢数据安全屏障。

四、采用国际标准和国外先进标准的程度

本标准未采用国际标准。

五、与有关的现行法律法规和强制性国家标准的关系

本标准与现行法律、法规，以及现有国家标准、行业标准无冲突和矛盾。标准的部分内容与现行有效的标准保持一致，引用标准中标注年份的，则以该标准为依据；没有标注年份的，则以该标准的最新版为依据。具体为：

1.对数据安全、数据处理的定义与《中华人民共和国数据安全法》（2021）的描述保持一致。

2.数据安全评估方法、流程等与 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》和 GB/T XXXXX—XXXX《信息安全技术 数据安全风险评估方法》保持一致。

六、重大分歧意见的处理经过和依据

本标准在编制过程中，未出现重大分歧意见。

七、标准过渡期的建议

根据本标准升级现有系统相关功能需要两个月，标准宣贯一个月，因此建议标准发布后三个月实施。

本标准发布后建议主管部门通过多种形式组织宣贯、培训，加强标准贯彻落实，并于 1 年内通过开展数据安全检查评估工作进行推广应用，发挥本标准的规范作用。

八、废止现行有关标准的建议

本标准为新制定的标准规范，无废止现行的有关标准。

九、其他应予说明的事项

在本标准编制过程中，目前未接到任何涉及相关专利或知识产权争议的信息、文件。