报告编号：

数据安全风险评估报告

评估单位（盖章）：

报告时间：　　年　　月　　日

声明

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

本报告是[被评估方]的网络数据安全风险评估报告。

本报告评估结论的有效性建立在被评估方提供相关证据的真实性基础之上。

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

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

单位名称（加盖单位公章）

2025 年　月　日

数据安全风险评估基本信息表

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

报告概述

[评估方]受[被评估方]的委托于 XX 年 XX 月 XX 日至 XX 年 XX 月 XX 日开展数据安全风险评估工作，对[被评估方]的 XX 系统进行数据安全风险评估，通过评估项目的实施根据被测信息系统当前的安全状况，给出评估结果并提出改进建议，为后续的整改工作提供参考依据。

本次评估工作主要采用人员访谈、文档查验、配置核查、工具测试等方法，评估范围涉及数据安全管理、数据处理活动及数据安全技术等方面。

通过对[被评估方]以及 XX 系统综合评估，评估人员发现：[被评估方]……（根据实际情况阐述被评估方在网络安全工作方面值得肯定的成绩）【示例：[被评估方]高度重视数据安全防护工作，为安全保障工作投入了大量时间、人力和精力；制定有较为完善的安全策略、安全规范及操作细则等相关管理制度；在合规管理层面完善数据安全内控管理，在技术防护层面通过防泄露、数据加密、数据脱敏等技术提升数据安全防护能力；在运营监测层面实现了数据安全风险感知】。

通过进一步评估发现，[被评估方] ……（根据实际情况阐述被评估方在网络安全工作方面存在的安全风险）

【示例：[被评估方]仍存在一些安全风险，需要进一步完善和加强。本次评估过程中归纳总结出问题项共 XX 个，其中重大安全风险 XX 个、高安全风险 XX 个、中安全风险 XX 个、低安全风险 XX 个、轻微安全风险 XX 个。其中主要问题表现为 XXXXXX。在此基础上，我们强化问题的整改跟踪并提出下一步工作建议，逐步提升数据安全保障能力，持续完善数据安全机制，确保数据安全风险可控。建议及时根据报告中提出的风险进行确认和整改】。

目录

声明 II
数据安全风险评估基本信息表 III
报告概述 IV
目录 V
1　评估概述 1
1.1　评估目的 1
1.2　评估依据 1
1.3　评估对象和范围 1
1.4　评估结论概要 1
1.5　报告分发范围 2
2　评估方法 3
2.1　评估原理 3
2.1.1　风险归类 3
2.1.2　风险危害程度分析 3
2.1.3　风险发生可能性分析 6
2.1.4　风险评价 7
2.2　评估手段 8
3　评估工作开展情况 9
3.1　评估人员情况 9
3.1.1　被评估方项目组 9
3.1.2　评估团队组成 9
3.2　评估时间安排情况 10
3.3　评估测试工具情况 11
4　信息调研情况 12
4.1　数据处理者基本情况 12
4.2　业务和信息系统情况 12
4.2.1　XX 系统 12
4.3　数据资产情况 15

4.3.1　数据资产内容.....15
4.3.2　数据分类分级情况.....15
4.4　数据处理活动情况.....16
4.4.1　数据收集.....16
4.4.2　数据存储.....16
4.4.3　数据使用.....17
4.4.4　数据加工.....18
4.4.5　数据传输.....19
4.4.6　数据提供.....19
4.4.7　数据公开.....19
4.4.8　数据删除.....20
4.4.9　数据出境情况.....21
4.5　数据流程图.....21
4.6　安全措施情况.....21
4.6.1　已开展的安全测评.....21
4.6.2　安全管理情况.....21
4.6.3　安全技术情况.....22
4.6.4　网络和数据安全事件情况.....22
5　数据安全风险识别.....23
5.1　数据安全管理风险识别.....23
5.2　数据处理活动风险识别.....23
5.3　数据安全技术风险识别.....23
5.4　个人信息处理风险识别.....24
6　风险分析与评价.....25
6.1　风险分析.....25
6.2　工具测试问题描述.....25
6.3　整改建议.....25
附录 A　数据安全风险评估记录表.....26
A.1　数据安全管理.....26

A.1.1　安全管理制度.....26
A.1.2　安全组织机构.....27
A.1.3　分类分级管理.....27
A.1.4　人员安全管理.....29
A.1.5　合作外包管理.....30
A.1.6　安全威胁和应急管理.....32
A.1.7　开发运维管理.....33
A.1.8　云数据安全.....34
A.2　数据处理活动.....36
A.2.1　数据收集.....36
A.2.2　数据存储.....38
A.2.3　数据传输.....39
A.2.4　数据使用和加工.....40
A.2.5　数据提供.....42
A.2.6　数据公开.....42
A.2.7　数据删除.....45
A.2.8　其他.....46
A.3　数据安全技术.....47
A.3.1　网络安全防护.....47
A.3.2　身份鉴别与访问控制.....48
A.3.3　监测预警.....48
A.3.4　数据脱敏.....50
A.3.5　数据防泄漏.....50
A.3.6　数据接口安全.....51
A.3.7　数据备份恢复.....51
A.3.8　安全审计.....54
A.4　个人信息保护.....55
A.4.1　个人信息处理基本原则.....55
A.4.2　个人信息告知.....55

A.4.3　个人信息同意.....56
A.4.4　个人信息处理.....57
A.4.5　敏感个人信息处理.....59
A.4.6　个人信息主体权利.....59
A.4.7　个人信息安全义务.....62
A.4.8　个人信息投诉举报.....62
A.4.9　大型网络平台个人信息保护.....63
附录 B　漏洞扫描结果记录.....65
附录 C　渗透测试结果记录.....66
C.1　XXXX 系统.....66
C.1.1　信息收集.....66
C.1.2　手工测试.....66
C.1.3　漏洞归纳.....66
附录 D　典型数据安全风险类型.....67

1 评估概述

1.1 评估目的

为落实《数据安全法》等法律法规要求或安全监管需要，对数据处理者的数据安全管理、数据处理活动和数据安全技术情况等进行安全评估，发现存在的安全问题和风险隐患，督促数据处理者健全安全制度、改进安全措施、堵塞安全漏洞，进一步提高数据安全能力。

1.2 评估依据

评估过程中主要依据的标准：

（1） 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》

（2） GB/T 45577-2025《数据安全技术 数据安全风险评估方法》

（3） GB/T 43697-2024《数据安全技术 数据分类分级规则》

（4） GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》

（5） 《政务信息化项目网络安全评估实施指南》

1.3 评估对象和范围

【评估对象选择原则：根据 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》，需将“数据”和“数据处理活动”作为评估对象。】

表 1-1 评估对象表

序号	评估对象
1	XX 数据
2	XX 数据处理活动

1.4 评估结论概要

本次评估过程中归纳总结出问题项共 XX 个，其中重大安全风险 XX 个、高安全风险 XX 个、中安全风险 XX 个、低安全风险 XX 个、轻微安全风险 XX

个

1.5 报告分发范围

本次数据安全风险评估报告正本一式 3 份，其中 [被评估方]1 份，[评估机构]1 份，被评估方同级网信部门 1 份。

2 评估方法

2.1 评估原理

2.1.1 风险归类

根据数据安全问题清单，分析数据安全风险源可能引发的安全风险，按照风险类型对风险源归类，典型数据安全风险类别见附录D。

2.1.2 风险危害程度分析

风险危害程度分析，主要分析数据的价值、重要性、规模、种类，以及数据处理目的、方式、范围等要素，综合评估数据安全风险一旦发生，对国家安全、经济运行、社会秩序、公共利益或者个人、组织合法权益造成的危害程度。风险危害程度从低到高可分为很低、低、中、高、很高 5 个级别。风险危害程度分析遵循就高从严、整体分析原则，如果该风险涉及多个数据资产，应进行累加判断，

将涉及数据的风险按照最高危害等级判断。风险危害程度评价，主要考虑数据价值、数据重要性、风险源严重程度三个因素，分析方法如下:

a）数据价值主要从数据资产的经济效益、业务效益、投入成本计量等方面分析。

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

c）风险源严重程度，主要考虑风险源对数据处理者带来的危害程度。

数据安全风险危害程度的判断标准如下表所示:

表 2-1 数据安全风险危害程度等级参考表

影响对象	危害程度	主要内容
国家安全	很高	直接危害国家安全重点领域，如政治安全。
	高	关系国家安全重点领域，或者对国土、军事、经济、文化、社会、科技、电磁空间、网 络、生态、资源、核、海外利益、太空、极地、深 海、生物、人工智能等任一领域国家 安全造成严重威胁。
	中	对国土、军事、经济、文化、社会、科技、电磁空间、网络、生态、资源、核、海外利 益、太空、极地、深海、生物、人工智能等任一领 域国家安全造成威胁。
经济运行	很高	1、直接影响涉及国家安全的行业、支柱产业和高新技术产业中的重要骨干企业、提供重 要公共产品的行业、重大基础设施和重要矿产资源行业等关系国民经济命脉行业的运行 和发展。 2、关系国民经济命脉，严重危害对社会经济发展具有重大影响的行业领域、 部门、 企业、 资 源 、 区 域 等 的 生 产 运 营 和 经 济 利 益 。 3、对一个或多个行业领域的发展态势、业务经营、技术进步、产业生态造成特别严重危 害， 如对核心业务造成重大损害，导致大面积业务中断、大量业务处理能力丧失等。 4、对一个或多个省（自治区、直辖市）的经济运行造成特别严重影响，例如导致大范围 停工停产、大规模基础设施长时间中断运行等。
	高	1、直接影响宏观经济运行状况和发展趋势，如社会总供给和总需求、国民经济总值和增长速度、国民经济主要比例关系、物价总水平、劳动就业总水平与失业率、货币发行总 规模与增长速度、进出口贸易总规模与变动等。 2、直接影响一个或多个地级市、行业内多个企业或大规模用户，对行业发展态势、技术进步和产业生态等造成严重影响，或者直接影响行业领域核心竞争力、核心业务运行、 关键产业链、核心供应链等。
	中	1、对单个行业领域发展、业务经营、技术进步、产业生态等造成一般危害，如受影响的用户和企业数量较小、生产生活区域范围较小、持续时间较短、社会负面影响较小。 2、对单个行业领域的经济运行秩序造成一般危害，如市场准入、市场行为、市场结构、 商品销售、交换关系、

影响对象	危害程度	主要内容
		生产经营秩序等。
社会秩序	很高	1、关系重要民生，直接影响人民群众重要民生保障的事项、物资、工程或项目等。 2、直接导致特别重大突发事件、特别重大群体性事件、暴力恐怖活动等，引起一个或多个省（自治区、直辖市）大部分地区的社会恐慌，严重影响社会正常运行。
	高	1、直接导致重大突发事件、重大群体性事件等，影响一个或多个地市大部分地区的社会稳定。 2、严重影响人民群众的日常生活秩序。 3、严重影响各级政务部门履行公共管理和服务职能。 4、严重影响法治和社会伦理道德规范。
	中	1、对人民群众的日常生活秩序造成一般影响。 2、直接影响企事业单位、社会团体的生产秩序、经营秩序、教学科研秩序、医疗卫生秩序。 3、直接影响公共场所的活动秩序、公共交通秩序。
公共利益	很高	1、关系重大公共利益，导致一个或多个省（自治区、直辖市）大部分地区的社会公共资源供应长期、大面积瘫痪，大范围社会成员（如1000万人以上）无法使用公共设施、获取公开数据资源、接受公共服务。 2、可能导致特别重大网络安全和数据安全事件，或者导致特别重大事故级别的安全生产事故，对公共利益造成特别严重影响，社会负面影响大。 3、可能导致特别重大突发公共卫生事件（I级），造成社会公众健康特别严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒等严重影响公众健康的事件。
	高	1、直接危害公共健康和安全，如严重影响疫情防控、传染病的预防监控和治疗等。 2、可能导致重大突发公共卫生事件（II级），造成社会公众健康严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒等严重影响公众健康的事件。 3、导致一个或多个地市大部分地区的社会公共资源供应较长期中断，较大范围社会成员（如100万人以上）无法使用公共设施、获取公开数据资源、接受公共服务。
	中	对公共利益产生一般危害，影响小范围社会成员使用公共设施、获取公开数据资源、接受公共服务等。
组织权益	中	可能导致组织遭到监管部门严重处罚（包括取消经营资格、长期暂停相关业务等），或者影响重要/关键业务无法正常开展的情况，造成重大经济或技术损失，严重破坏机构声誉，企业面临破产。

影响对象	危害程度	主要内容
	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。
注：数据处理者可根据数据对自身的价值、重要性，结合风险源严重程度，将仅影响组织权益等的风险危害程度自行定为或调整为“很高”“高”等级别，及时进行风险处置。		

2.1.3 风险发生可能性分析

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

a）风险源发生频率，可从被评估对象发生相关数据安全事件的次数及频率、同行业或业务模式相似的单位发生相关数据安全事件的次数及频率、相似数据安全事件发生次数及频率、轻微安全问题累计发生次数等方面，综合分析同类风险源发生可能性。一般风险源或安全事件发生频率越高，风险发生可能性越高。

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

c）风险源关联性，主要通过风险源清单关联分析，发现多个风险源组合后可能引发数据安全风险，则将其与其他风险源合并分析，综合判断风险发生可能性。

在综合分析风险源发生频率、安全措施有效性和完备性、风险源关联性的

基础上，将数据安全风险发生的可能性从低到高分为低、中、高 3 个级别，如下表所示。等级越高代表措施完备性、有效性越低，风险越可能发生。

表 2-2 风险发生可能性等级参考表

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

2.1.4 风险评价

风险评价一般结合评估对象实际情况，基于风险危害程度和风险发生可能性的分析结果，综合风险危害程度及风险发生可能性对安全风险进行综合评价。数据安全风险评价结果包括：

a）重大安全风险：一般指可能直接影响国家安全的数据安全风险。

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

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

d）低安全风险：一般指可能直接对企业合法权益造成一般影响，或直接对

自然人的人格尊严受到侵害或者人身、财产安全受到危害，或对社会、公众权益有一定或较小影响的数据安全风险。

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

数据处理者可根据自身情况，将仅影响组织权益、个人权益等的风险自行定为或调整为“重大”“高”等级别，及时进行风险处置。本文件提出了定性和定量评价风险的方法，表 4 提供了一种风险等级定性评价方法。

表 2-3 数据安全风险评价矩阵表

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

2.2 评估手段

开展数据安全风险评估时，综合采取下列手段进行评估：

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

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

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

3 评估工作开展情况

3.1 评估人员情况

3.1.1 被评估方项目组

- 被评估方项目组职责：

（1）向评估方介绍本单位基本业务情况、组织情况、数据情况及数据安全现状等；

（2）准备评估单位需要的资料；

（3）为评估项目实施提供支持和协调；

（4）对评估文档及评估结果进行确认签字。

- 被评估项目组人员构成：

表 3-1 被评估方项目组人员构成表

序号	部门	姓名	职务	项目角色	联系方式	备注
1						
2						

3.1.2 评估团队组成

- 评估方项目组职责：

（1）组建评估项目组；

（2）指出被评估单位应提供的基本资料（基本资料：凡涉及数据收集、传输、存储、使用和加工、提供、公开和删除等数据安全相关的制度文档；组织架构图；已开展的测评报告）；

（3）向被评估单位介绍评估工作流程和方法；

（4）了解被评估单位的数据安全现状，以及单位选定业务情况、组织情况、

数据情况等与评估相关的信息。

（5）准备评估相关文档；

（6）实施现场评估工作；

（7）编制评估报告。

- 评估项目组人员构成：

本次数据安全风险评估团队的具体角色和职责分工如下：

表 3-2 评估方项目组人员构成表

序号	姓名	人员角色	工作职责	联系方式
1				
2				

3.2 评估时间安排情况

本次评估活动分为四个阶段：评估准备阶段、信息调研阶段、风险分析阶段和报告编制阶段。各阶段的实施过程说明如下：

1．2025 年 XX 月 XX 日～XX 月 XX 日，评估准备阶段：由[被评估方]牵头组织本次数据安全风险评估工作，协调对应人员。[评估方]阶段所需材料以及各个业务部门准备材料清单。

2．2025 年 XX 月 XX 日～XX 月 XX 日，信息调研阶段：通过项目启动会[被评估方]宣贯项目背景，介绍工作内容，下发准备资料，并启动访谈调研、资料查验、技术测试，采集获取相关信息。

3．2025 年 XX 月 XX 日～XX 月 XX 日，风险分析阶段：针对目标范围包括组织层面以及 XX 个重点系统，评估小组基于获取的相关信息，通过人员访谈、资料查验、技术测试等方式进行风险发现。

4．2025 年 XX 月 XX 日～XX 月 XX 日，报告编制阶段：根据评估活动的开展情况，完成数据安全风险评估。

3.3 评估测试工具情况

本次风险评估采用的测试工具主要包括：

表 3-3 测试工具信息表

序号	工具名称	型号	系统版本	规则库版本
1				
2				

注：因测试工具系统版本和漏洞规则库版本可能更新，正式测评中使用的测试工具系统版本和漏洞规则库版本以实际为准。

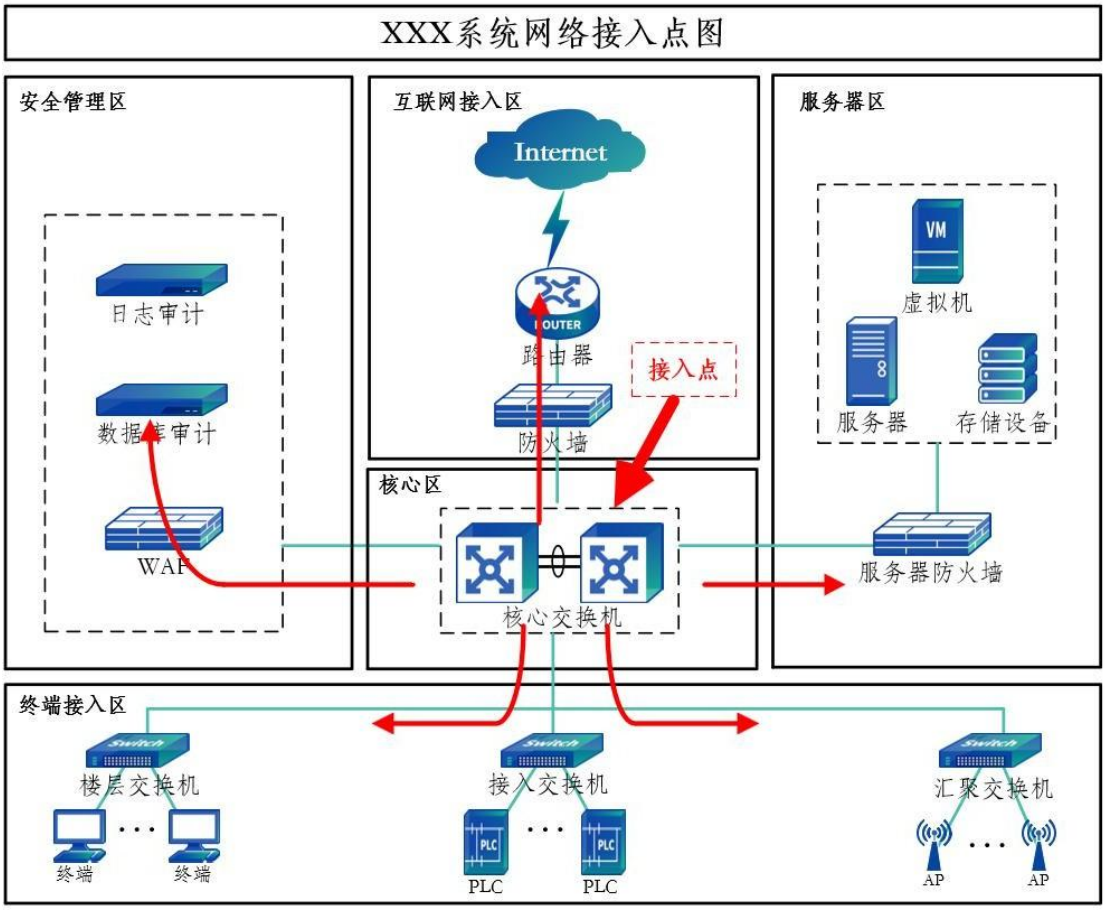

图 1 工具接入点

4 信息调研情况

4.1 数据处理者基本情况

表 4-1 数据处理者基本情况表

数据处理者基本情况表	
单位名称	
统一社会信用代码	
单位类型	☐党政机关　☐国有及国有控股企业　☐事业单位 ☐外资（含港澳台）投资企业　☐民营企业 ☐其他：
办公地址	
开展数据处理活动所在地	
法人信息	姓名：　　国籍
数据安全负责人	
经营范围	经营范围： 主营业务：
数据处理相关服务行政许可	
是否境外上市或计划赴境外上市	☐是，上市地区和交易所 ☐计划上市，计划上市地区和交易所 ☐否
人员规模	约　　人
单位所属行业	☐工业　☐电信　☐交通　☐金融　☐自然资源 ☐卫生健康　☐教育　☐科技　☐其他：
上级主管部门	

4.2 业务和信息系统情况

4.2.1 XX 系统

1、网络结构

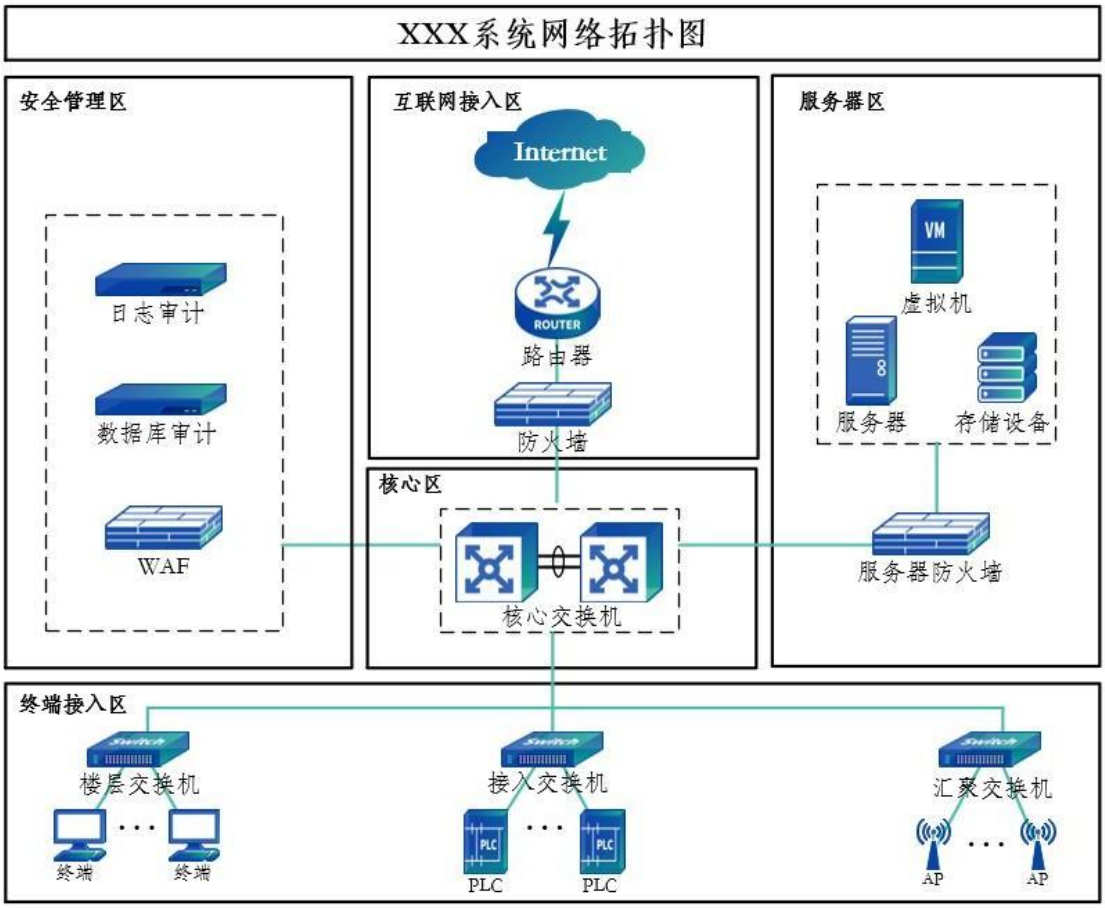

图 2 XX 系统网络拓扑图

如图 XXX 系统网络拓扑图所示，XX 系统的网络结构主要包括：非信创办公后台区、非核心业务区、办公接入区、运维后台区、数据中心互联区、下联接入区、核心交换区、网上交易区和互联网接入区。

2、业务情况

业务情况需要列举组织开展的主要业务名称，以及对应的业务功能、应用场景、业务流程、服务对象、用户规模、覆盖地域、相关部门信息。

（1）业务名称 1

介绍业务功能、应用场景、业务流程、服务对象、用户规模、覆盖地域、相关部门等情况。

（2）业务名称 2

……

3、信息系统情况

业务涉及信息系统的情况需要针对不同业务，列举所涉及的信息系统名称、系统介绍、系统功能介绍、系统的等保级别、IP 地址范围、信息系统资产表、信息系统负责人等信息，并提供网络拓扑结构图。

表 4-2 信息系统基本情况表

资产名称	系统说明	系统等保级别	系统服务对象	IP 地址	其它地址（请说明）	管理员联系方式	应用访问路径（URL）	备注

【填写说明】

（1）网络和信息系统基本情况，包括网络规模、拓扑结构、关键信息基础设施等信息系统情况及其对外连接、运营维护等情况。

（2）业务基本信息，包括业务描述、业务类型、服务对象、业务流程、用户规模、覆盖地域、相关部门等基本信息。

（3）业务涉及重要数据或核心数据处理情况； d）业务为政务部门或境外用户提供服务情况；

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

（5）接入的外部第三方产品、服务或 SDK 的情况，包括名称、版本、提供方、使用目的、合同协议等。

4.3 数据资产情况

4.3.1 数据资产内容

表 4-3 数据资产内容表

序号	数据类型	内容描述	载体形式	数据规模	存储区域/信息系统	现有管理政策	重要程度			是否涉及出境传输或访问	备注
							用途	影响	存储失效		
1											
2											

1、资产类别。梳理结构化数据资产（如数据库表等）和非结构化数据资产（如图表文件等），摸清数据底数。

2、数据资产总量、数据库表和字段规模、数据量变化情况、境外存储量、数据分布、数据存储情况等。

3、数据重要性。已完成分类分级的，介绍数据分级结果；未完成分类分级的，结合业务重要性、数据应用模式、数据敏感度等因素，描述数据重要性，给出建议的数据分级级别。

4、数据资产类型。按照分类分级情况进行梳理，如一般数据、重要数据、核心数据等级别数据，对应的种类、规模、敏感程度、行业领域、数据来源、与信息系统的对应关系。

4.3.2 数据分类分级情况

目前，XX 行业未出台明确的数据分类分级行业规范。[被评估方]参照《网络安全标准实践指南——网络数据分类分级指引》、GB/T 43697-2024《数据安全技术 数据分类分级规则》，开展数据分类分级工作。共识别出重要数据 XX 项，累计规模 XXGB，详情如下。

4.4 数据处理活动情况

4.4.1 数据收集

针对“数据资产内容”中的内容，逐项说明数据收集情况。如数据收集渠道、收集方式、数据范围、收集目的、收集频率、外部数据源、合同协议、相关系统，以及在被评估方外部公共场所安装图像采集的情况等。

表 4-4 数据情况表

序号	数据类型	内容描述	载体形式	收集方式	数据来源	业务场景	用途
1							
2							

4.4.2 数据存储

数据存储情况，如数据存储方式、数据中心、存储系统（如数据库、大数据平台、云存储、网盘、存储介质等）、外部存储机构、存储地点、存储期限、备份冗余策略等。

1、总体数据资产规模：

表 4-5 总体数据资产规模表

数据总量	日均增量	用户数据量	用户数据日均增量	统计截至时间

2、数据中心情况：单位所有境内、境外数据中心名称，及各数据中心所处地理位置、IP 地址段、规模（服务器数/存储容量）、数据服务模式（自建/租用机房/公有云/私有云）、运维方式（自主/第三方运维）、网络服务商等。

表 4-6 数据中心情况表

序号	数据中心名称	地理位置	IP 地址段	规模	数据服务模式	运维方式	网络服务商	统计截至时间

序号	数据中心名称	地理位置	IP 地址段	规模	数据服务模式	运维方式	网络服务商	统计截至时间
1								
2								

3、数据中心的存储情况：具体说明截至 2025 年 XX 月 XX 日，单位所有境内、境外的数据中心名称，及各数据中心存储的数据类型（包括但不限于用户身份数据、行为数据、音视频数据、定位数据等）、数据量、涉及的业务、数据来源（自身业务收集 /第三方共享/外部购买等），是否涉及重要数据及其数据内容或字段，（数据中心名称应与上表一致）。

表 4-7 数据中心存储情况表

序号	数据中心名称	存储数据类型	涉及业务	数据量	数据来源	重要数据情况	统计截至时间
1							
2							

4.4.3 数据使用

数据使用情况，如数据使用目的、方式、范围、场景、算法规则、相关系统和部门，应用算法推荐技术提供互联网信息服务的情况，核心数据、重要数据委托处理、共同处理的情况等。

1、请说明被评估单位在业务开展中，是否存在利用核心数据、重要数据进行算法推荐的情况？如有，请说明：

算法推荐类型（合成类/个推类/排序类/调度类等）、应用场景、用户特征使用的数据字段、数据来源（用户填写/埋点自动采集等）、调用更新频率（实时/X 分钟/X 小时/）；

表 4-8 算法推荐情况表

序号	算法推荐类型	应用场景	用户特征使用的数据字段	数据来源	调用更新频率

序号	算法推荐类型	应用场景	用户特征使用的数据字段	数据来源	调用更新频率
1					
2					

是否提供算法推荐开关、选择或删除个人特征标签的功能，以及有关操作路径。

2、大数据利用：请说明被评估单位利用收集掌握的用户数据，进行大数据关联分析后对外发布数据分析报告或支撑政府部门决策的情况。并分别说明：

各项报告的名称、发布时间、发布对象（公众/XX 企业/XX 政府部门）、报告主要内容、使用的用户数据字段、内部审批部门。

表 4-9 报告发布情况表

序号	报告名称	发布时间	发布对象	报告主要内容	使用的用户数据字段	内部审批部门
1						
2						

4.4.4 数据加工

数据加工情况，如数据清洗、转换、标注等加工情况，是否对外委托加工等。

表 4-10 数据加工情况表

序号	加工数据类型	加工目的	加工方式	加工场所	是否委托加工
1					
2					

4.4.5 数据传输

数据传输情况，如数据传输途径和方式（如互联网、VPN、物理专线等在线通道情况，采用介质等离线传输情况）、传输协议、内部数据共享、数据接口等。

表 4-11 数据传输情况表

序号	传输数据类型	源传输节点	目的传输节点	中间节点	传输途径和方式
1					
2					

4.4.6 数据提供

数据提供情况，如数据提供（数据共享、数据交易， 因合并、分立、解散、被宣告破产等原因需要转移数据等）的范围、合同协议、各数据接收方的名称、提供方式（SDK/API/系统接口/邮件等数据传输方式）、提供目的、提供频率、数据字段、数据量、涉及的业务、用户是否单独同意，对外提供的重要数据的种类、数量、范围、敏感程度、保存期限等。

表 4-12 数据提供情况表

序号	数据接收方	提供方式	提供目的	提供频率	数据字段	数据量	涉及的业务	用户是否单独同意
1								
2								

4.4.7 数据公开

数据公开情况，如数据公开的目的、方式、对象范围、受众数量、行业、组织、地域等。

表 4-13 数据公开情况表

序号	公开数据类型	目的	方式	对象范围	受众数量	其他
1						
2						

4.4.8 数据删除

1、从在线数据、离线数据两个维度，分别说明[被评估方]各类数据的留存和删除机制。具体包括：各项数据类型（[被评估方]及第三方处理数据、身份信息/位置信息行为记录）、具体字段、存储形式（在线/离线）、保存时限（X天/永久/）、触发删除操作的条件（用户主动删除/重置/注销账户/系统 定期删除）、后台删除方式（物理删除/逻辑删除）、删除后的可恢复性等。

表 4-14 数据删除情况表

序号	数据类型	具体字段	存储形式	保存时限	删除条件	删除方式	能否恢复
1							
2							

2、说明被评估单位后台系统数据删除流程。

分别说明用户注销账户、用户请求删除数据、超出数据保存期限三种场景下，后台系统删除、销毁数据的流程和系统处理措施，并以附件形式提供相应的证据材料及验证方法手段。

表 4-15 数据删除流程情况表

用户注销账户、用户请求删除数据、超出数据保存期限三种场景下数据处理措施			
删除场景	系统处理数据的措施	相关截图（正常）	相关截图（删除）

4.4.9 数据出境情况

数据出境情况，是否存在重要数据出境，如跨境业务、跨境办公、境外上市、使用境外云服务或数据中心、国际 交流合作等场景的数据出境情况。（注：数据出境方式包括但不限于使用境外云服务、 员工和用户境外远程访问、企业跨境专线、境外缓存加速、境外第三方机构认证、境外机构数据合作等。）

4.5 数据流程图

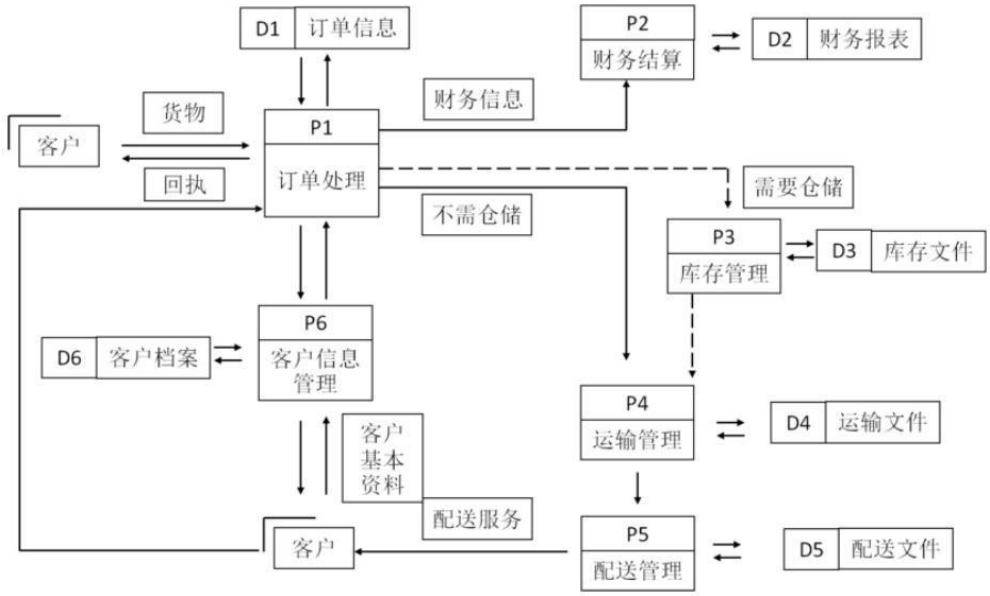

图 3 数据流程图

4.6 安全措施情况

4.6.1 已开展的安全测评

已开展的等级保护测评、风险评估、安全认证、合规审计情况核实介绍。

4.6.2 安全管理情况

数据安全管理机构、人员及制度情况介绍。

4.6.3 安全技术情况

防火墙、入侵检测、入侵防御等网络安全设备及策略情况。VPN 等远程管理软件的用户及管理情况介绍。设备、系统及用户的账号口令管理情况介绍。加密、脱敏、去标识化等安全技术应用情况。

4.6.4 网络和数据安全事件情况

三年内发生的网络和数据安全事件及处置情况。

表 4-16 网络和数据安全事件情况表

序号	事件名称	发生时间	事件内容简述	事件临时处理措施	事件最终处理措施	事件影响等级	社会面影响等级	事件结果
1								
2								

5 数据安全风险识别

5.1 数据安全管理风险识别

数据安全管理主要从安全管理制度、安全组织机构、 分类分级管理、人员安全管理、合作外包管理、安全威胁和应急管理、开发运维管理和云数据安全等方面进行评估，下表为发现的风险问题项描述。

表 5-1 数据安全管理问题表

序号	评估类	评估项	问题	问题描述	危害分析	涉及的数据及类型	涉及的处理活动
1							
2							

5.2 数据处理活动风险识别

数据处理活动主要从数据收集、数据传输、数据存储、数据使用、数据加工、数据提供、数据公开、数据删除等 环节进行评估，下表为发现的风险问题项描述。

表 5-2 数据处理活动问题表

序号	评估类	评估项	问题	问题描述	危害分析	涉及的数据及类型	涉及的处理活动
1							
2							

5.3 数据安全技术风险识别

数据安全技术主要从网络安全防护、身份鉴别与访问控制、监测预警、数据脱敏、数据防泄露和数据接口安全、备份恢复、安全审计等方面进行评估，下表为发现的风险问题项描述。

表 5-3 数据安全技术问题表

序号	评估类	评估项	问题	问题描述	危害分析	涉及的数据及类型	涉及的处理活动

序号	评估类	评估项	问题	问题描述	危害分析	涉及的数据及类型	涉及的处理活动
1							
2							

5.4 个人信息处理风险识别

个人信息处理主要从个人信息处理基本原则、个人信息处理、敏感个人信息处理、个人信息主体权利、个人信息安全义务、个人信息投诉举报、大型网络平台个人信息保护等方面进行评估，下表为发现的风险问题项描述。

表 5-4 数据安全技术问题表

序号	评估类	评估项	问题	问题描述	危害分析	涉及的数据及类型	涉及的处理活动
1							
2							

6 风险分析与评价

6.1 风险分析

通过对问题的风险类型、风险危害程度和可能性进行综合分析，当前各项安全问题的风险等级结果如下表所示。

表 6-1 数据安全风险表

序号	问题	风险类型	风险危害程度	风险发生的可能性	风险等级
1					
2					

6.2 工具测试问题描述

通过对漏洞扫描结果进行分析，XX 系统存在的主要安全漏洞汇总如下表所示：

表 6-2 主要安全漏洞汇总表

序号	安全漏洞名称	关联资产/IP	严重程度
1			
2			

6.3 整改建议

表 6-3 整改建议表

序号	问题	问题描述	危害分析	风险等级	整改建议
1					
2					

附录A　数据安全风险评估记录表

A.1 数据安全管理

A.1.1 安全管理制度

评估点	评估项	结果记录
数据安全制度体系	a）数据安全总体策略、方针、目标和原则制定情况；	
	b）数据安全管理工作规划或工作方案制定情况；	
	c）数据分类分级、数据安全评估、数据访问权限管理、数据全生命周期管理、数据安全应急响应、数据合作方管理、数据脱敏、数据加密、数据安全审计、数据资产管理、大数据平台安全等制度或要求建设情况；	
	d）关键岗位的数据安全管理操作规程建设情况；	
	e）制度内容与国家和行业数据安全法律法规和监管要求的符合情况。	
数据安全制度落实	a）网络安全责任制、数据安全责任制落实情况，网络安全和数据安全事件责任查处情况；	
	b）数据安全制度的制定、评审、发布流程建设情况；	
	c）数据安全制度的定期审核和更新情况；	
	d）制度发布范围是否覆盖全面，发布方式是否正规、有效；	
	e）数据安全制度落实情况，是否具备操作规程、记录表单等制度落实证明材料；	
	f）制度落实监督检查机制；	
	g）针对重要数据处理者，还	

评估点	评估项	结果记录
	应评估以下内容：1）对数据处理活动定期开展数据安全风险评估的情况；2）向有关部门报送评估报告情况，风险评估报告至少应包含处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。	

A.1.2 安全组织机构

评估点	评估项	结果记录
数据安全组织架构	a）数据安全管理机构和职能设置情况；	
	b）数据安全负责人和职能设置情况；	
	c）单位高层人员参与数据安全决策情况；	
	d）对组织内部的数据安全管理执行情况、数据操作行为等进行安全监督的情况；	
	e）数据安全人员和资源投入情况与组织数据安全保护需求适应性。	
数据安全岗位设置	a）数据库管理员、操作员及安全审计人员、安全运维人员、数据备份管理人员、数据恢复管理人员等；	
	b）数据安全关键岗位设置情况，及职责分离、专人专岗等原则落实情况；	
	c）业务部门、信息系统建设部门、信息系统运维部门数据安全人员设置情况， 数据安全管理要求执行情况；	
	d）特权账户所有者、关键数据处理岗位等数据安全关键岗位设立双人双岗情况。	

A.1.3 分类分级管理

评估点	评估项	结果记录
数据资产管理	a）数据资产台账建设、更新、维护情况；	
	b）数据资产梳理是否全面，是否能够覆盖数据库、大数据存储组件、云上对象存储或网盘等存储工具及办公计算机、U 盘、光盘等存储介质中的数据；	
	c）通过数据资产管理等工具对数据资产清单及时更新、维护的情况；	
	d）采用技术手段定期对数据资产进行扫描的情况，及发现识别个人信息、重要数据的能力。	
数据分类分级制度	a）数据分类分级保护制度建设情况，是否符合国家、行业和地方的数据分类分级规范要求；	
	b）数据分类分级管理情况，及核心数据和重要数据目录建立及维护情况；	
	c）是否在相关制度中明确了数据分类管理、分级保护策略，数据分类分级保护措施是否落实在数据访问权限申请、保护措施部署等方面；	
	d）数据分类分级变更和审核流程情况；	
	e）个人信息分类分级管理情况。	
数据分类分级保护	a）是否对处理的个人信息和重要数据进行明确标识；	
	b）按照数据级别建设覆盖全流程数据处理活动的安全措施情况；	
	c）数据分类分级标识或数据资产管理工具建设情况，是否具有自动化标识能力，是否具	

评估点	评估项	结果记录
	有数据标识结果发布、审核等能力；	
	d）按照相关重要数据目录或规定，评估重要数据并进行重点保护的情况；	
	e）按照相关核心数据目录或规定，评估核心数据并进行严格管理的情况。	

A.1.4 人员安全管理

评估点	评估项	结果记录
人员录用	a）重要岗位员工录用前背景调查情况；	
	b）数据处理关键岗位人员录用，对其数据安全意识或专业能力进行考核的情况。	
保密协议	a）员工工作纪律和工作要求中是否明确规定员工禁止的数据安全相关行为；	
	b）是否与所有涉及数据服务的人员签订安全责任承诺或保密协议，与数据安全关键岗位人员签订数据安全岗位责任协议；	
	c）在重要岗位人员调离或终止劳动合同前，是否明确并告知其继续履行有关信息的保密义务要求，并签订保密承诺书。	
转岗离岗	a）在人员转岗或离岗时，是否及时终止或变更完成相关人员数据操作权限，并明确有关人员后续　的数据保护管理权限和保密责任；	
	b）对终止劳动合同的人员，是否及时终止并收回其系统权限及数据权限，明确告知其继续履行有关信息的保密义务要求。	

评估点	评估项	结果记录
数据安全培训	a）数据安全培训计划制定、更新情况；	
	b）开展数据安全意识教育培训，并保留相关记录情况；	
	c）是否对数据安全岗位人员每年至少进行 1 次数据安全专项培训，对关键岗位人员进行定期数据安全技能考核情况。	

A.1.5 合作外包管理

评估点	评估项	结果记录
合作方管理机制	a）数据合作方安全管理机制建设情况，如对合作方或外包服务机构的选择、评价、管理、监督机制；	
	b）是否对数据合作方或外包服务机构的安全能力进行评估；	
	c）对外包服务机构、人员履行安全责任义务的监督检查情况；	
	d）外包人员现场服务安全管理情况；	
	e）对外包服务商的技术依赖程度，对委托处理数据的控制和管理能力。	
合作协议约束	a）服务合同、承诺及安全保密协议情况，是否通过合同协议等方式对接收、使用本单位数据的合作方的数据使用行为进行约束；	
	b）是否在合作协议中明确了数据处理目的、方式、范围，安全保护责任、数据返还或销毁要求、保密约定及违约责任和处罚条款等；	
	c）合同、协议中，数据处理者与合作方、外包服务商间的数据安全责任界定情况。	

评估点	评估项	结果记录
外包人员访问权限	a）外包人员对数据与系统的访问、修改权限是否限于最小必要范围；	
	b）能够在测试环境下或使用测试数据完成的，是否向外包人员开放了生产环境权限或真实数据；	
	c）外包人员数据导出操作或数据外发操作的监督管理情况；	
	d）外包人员对敏感数据的访问及操作能否被实时监督或监测；	
	e）数据外包服务账号及访问权限管理情况；	
	f）外包人员远程访问操作系统或数据的情况。	
第三方接入与数据回收	a）是否对合作方接入的系统、使用的技术工具进行了技术检测，或合作方提供专业第三方机构评估的数据安全报告，避免引入木马、后门等；	
	b）为完成技术或服务目的向合作方提供的数据，在合作结束后是否进行了回收，是否要求合作方对数据进行删除；	
	c）外包服务到期后，账号注销、数据回收、数据删除销毁等管理情况；	
	d）为完成技术或服务目的向合作方提供的系统权限和接口，在合作结束后是否进行了停用或下线。	
政务数据委托处理	a）委托他人建设、维护电子政务系统，存储、加工政务数据，是否经过严格的批准程序，是否以合同等手段监督受托方履行相应的数据安全保护义务；	

评估点	评估项	结果记录
	b）政务数据受托方依照法律、法规的规定和合同约定履行数据安全保护义务的情况，是否擅自留存、使用、泄露或者向他人提供政务数据；	
	c）支撑电子政务相关系统运行的相关服务或系统的安全措施，是否满足电子政务系统管理和相关安全要求。	

A.1.6　安全威胁和应急管理

评估点	评估项	结果记录
安全威胁和事件	a）近 3 年发生的网络安全或数据安全事件信息及其处置、记录、整改和上报情况，如事件名称、影响对象、发生时间和频次、发生原因、外部威胁、事件级别、处置措施、整改措施等，重大事件需提供事件调查评估报告；	
	b）近 1 年通过安全工具、日志审计、安全测评、合规自查等发现的安全威胁、违规行为及其频率统计；	
	c）实际环境中通过监测系统、检测工具等发现的攻击威胁情况；	
	d）近期公布或曝光的同行业、类似业务模式的威胁事件、威胁预警。	
安全应急管理	a）数据安全事件应急预案制定和修订情况，是否定义数据安全事件类型，明确不同类别级别事件的处置流程和方法；	
	b）数据安全应急响应及处置机制建设情况，发生数据安全事件时是否立即采取处置措施，是否按照规定及时告知用户并向有关主管部门报告；	

评估点	评估项	结果记录
	c）数据安全事件应急演练情况；	
	d）数据处理活动安全风险监测情况，发现数据安全缺陷、漏洞等风险时，是否立即采取补救措施；	
	e）安全事件对个人、其他组织造成危害的，是否将安全事件和风险情况、危害后果、已经采取的补救措施等通知利害关系人，无法通知的是否采取公告等其他方式告知；	
	f）面向社会提供服务的数据处理者是否建立便捷的数据安全相关投诉举报渠道，以及近3年的数据安全投诉举报处置、记录和整改情况，是否存在侵害用户个人信息合法权益的情况。	

A.1.7 开发运维管理

评估点	评估项	结果记录
开发运维管理	a）新应用开发审核流程建设情况，进行数据处理需求安全合规审核情况；	
	b）开发程序的修改、更新、发布的批准授权和版本控制流程；	
	c）工程实施、验收、交付的安全管理情况；	
	d）对开发代码、测试数据的安全管理情况；	
	e）产品或业务上线前进行安全评估的情况；	
	f）开发测试环境和实际运行环境的隔离情况、测试数据和测试结果的控制情况；	
	g）开发测试中使用真实个人信息、核心数据、重要数据情	

评估点	评估项	结果记录
	况，开发测试前对相关数据进行去标识化、脱敏处理（测试确需信息除外）情况；	
	h）对开发和运维人员行为的监督和审计情况；	
	i）远程运维的审批、管理和安全防护措施；	
	j）第三方 SDK 或开源软件的运行维护、二次开发等技术资料完备性。	

A.1.8 云数据安全

评估点	评估项	结果记录
云数据安全（被评估对象使用云计算服务）	a）云服务提供者、第三方厂商、云租户的安全责任划分和落实情况；	
	b）上云数据的安全审核和管理情况；	
	c）云安全产品服务的使用和配置情况；	
	d）对云上操作行为的安全审计情况；	
	e）云用户账号和权限管理情况；	
	f）私有云远程运维安全管理情况；	
	g）云上承载用户个人信息、重要数据、核心数据情况，是否对核心数据、重要数据、敏感个人信息实施增强的安全防护；	
云数据安全（被评估对象是云计算服务提供者）	a）公有云、社区云等不同类型云平台间边界防护情况；	
	b）租户与云平台、数据中心间数据传输安全防护情况；	
	c）针对不同服务模式、部署模式、产品和服务，云平台对相关方的数据安全责任界面划	

评估点	评估项	结果记录
	定情况及合法合规性；	
	d）是否通过合同协议等方式，与租户划清云数据安全责任边界，并履行相应数据安全责任；	
	e）发生数据安全风险或事件时，为租户提供事件报告、应急处置等协同保障措施情况；	
	f）收集租户数据情况，是否识别重要数据、个人信息，收集方式是否安全合理，是否存在超范围收集；	
	g）计算、存储、网络、数据库、安全等产品安全配置情况；	
	h）第三方组件安全核查、漏洞修复情况；	
	i）云产品漏洞更新和推送情况，是否会及时提供补丁推送、跟进用户漏洞更新等情况；	
	j）云平台提供的基础安全防护能力情况；	
	k）云产品对用户高风险操作的提示情况；	
	l）对云租户的身份管理和访问控制情况；	
	m）云平台保障租户数据安全的相关制度和安全措施；	
	n）约定服务到期、欠费、提前终止等情形下，云数据删除和个人信息权益保障等情况；	
	o）云数据备份和恢复机制是否完善，数据备份策略、备份周期、备份存储、数据恢复策略，恢复验证等是否符合安全需要；	
	p）云平台开展数据安全风险	

评估点	评估项	结果记录
	评估、云计算服务安全评估等情况；	
	q）云平台基础设施部署和运维情况；	
	r）云安全管理中心管控情况；	
	s）云数据迁移安全保障情况；	
	t）云平台数据出境安全情况。	

A.2 数据处理活动

A.2.1 数据收集

评估点	评估项	结果记录
数据收集合法正当性	a）数据收集的合法性、正当性，是否存在窃取、超范围收集、未经合法授权收集或者以其他非法方式获取数据的情况，数据收集目的和范围是否合法；	
	b）违反法律、行政法规关于收集使用数据目的、范围相关要求，收集数据的情况。	
通过第三方收集数据	a）通过合同协议等合法方式，约定从外部机构收集的数据范围、收集方式、使用目的和授权同意情况；	
	b）对外部数据源进行鉴别和记录的情况；	
	c）数据的真实性及来源的可靠性	
	d）对外部收集数据的合法性、安全性和授权同意情况进行审核的情况。	
数据质量控制	a）数据质量管理制度建设情况，对收集数据质量和管理措施是否进行明确要求；	

评估点	评估项	结果记录
	b）安全管理和操作规范对数据清洗、转换和加载等行为是否进行明确要求；	
	c）数据质量管理和监控的情况，对异常数据及时告警或更正采取的手段措施；	
	d）收集数据监控、过程记录等情况，以及安全措施应用情况；	
	e）采用人工检查、自动检查或其他技术手段对数据的真实性、准确性、完整性校验情况。	
数据收集方式	a）采用自动化工具访问、收集数据的，违反法律、行政法规、部门规章或协议约定情况，侵犯他人知识产权等合法权益情况；	
	b）采用自动化工具收集时，对数据收集范围的明确情况，收集与提供服务无关数据的情况；	
	c）采用自动化工具收集数据以及该方式对网络服务的性能、功能带来的影响情况；	
	d）通过人工方式采集数据的，是否对数据采集人员严格管理，要求将采集数据直接报送到相关人员或系统，采集任务完成后及时删除采集人员留存的数据。	
数据收集设备及环境安全	a）检测数据收集终端或设备的安全漏洞，是否存在数据泄露风险；	
	b）人工采集数据泄露风险，通过人员权限管控、信息碎片化等方式，对人工采集数据环境进行安全管控情况；	
	c）客户端敏感信息留存风	

评估点	评估项	结果记录
	险，检测 App、Web 等客户端完成相关业务后，是否留存敏感个人信息或重要数据。	

A.2.2 数据存储

评估点	评估项	结果记录
数据存储适当性	a）数据存储安全策略和操作规程的建设落实情况；	
	b）存储位置、期限、方式的适当；	
	c）永久存储数据类型的必要性。	
逻辑存储安全	a）数据库的账号权限管理、访问控制、日志管理、加密管理、版本升级等方面要求的落实情况；	
	b）检测逻辑存储系统安全漏洞，查看安全漏洞修复、处置情况；	
	c）实施限制数据库管理、运维等人员操作行为的安全管理措施情况；	
	d）脱敏后的数据与可用于恢复数据的信息分开存储的情况；	
	e）对敏感个人信息、重要数据进行加密存储情况及加密措施有效性；	
	f）数据存储在第三方云平台、数据中心等外部区域的安全管理、访问控制情况；	
	g）根据安全级别、重要性、量级、使用频率等因素，对数据分域分级差异化存储安全管控情况；	
	h）重要数据和核心数据存储的防勒索应对机制情况。	
存储介质安全	a）存储介质（含移动存储介	

评估点	评估项	结果记录
	质，下同）的使用、管理及资产标识情况；	
	b）存储介质安全管理规范建设情况，是否明确对存储介质存储数据的安全要求。	
	c）对存储介质进行定期或随机性安全检查情况	
	d）存储介质访问和使用行为的记录和审计情况。	

A.2.3 数据传输

评估点	评估项	结果记录
传输链路安全性	a）数据传输安全策略和操作规程的建设落实情况；	
	b）敏感个人信息和重要数据传输加密情况及加密措施有效性，是否选用安全的密码算法；	
	c）个人信息和重要数据传输进行完整性保护情况；	
	d）数据传输通道部署身份鉴别、安全配置、密码算法配置、密钥管理等防护措施情况；	
	e）数据传输、接收的记录和安全审计情况；	
	f）采取安全传输协议等安全措施情况；	
	g）数据异常传输检测发现及处置情况；	
	h）制定数据跨组织传输管理规则，及跨组织数据传输安全技术措施建立情况。	
传输链路可靠性	a）网络传输链路的可用情况，包括对关键网络传输链路、网络设备节点实行冗余建设，建立容灾方案和宕机替代方案等情况；	

评估点	评估项	结果记录
	b）点对点传输中是否存在传输经过第三方、被第三方缓存情况。	

A.2.4 数据使用和加工

评估点	评估项	结果记录
数据使用和加工合法性	a）使用和加工数据时，遵守法律、行政法规，尊重社会公德和伦理，遵守商业道德和职业道德等情况；	
	b）是否存在危害国家安全、公共利益的数据使用和加工行为，损害个人、组织合法权益的数据使用和加工行为；	
	c）是否制作、发布、复制、传播违法信息；	
	d）应用算法推荐技术、深度合成技术提供互联网信息服务、生成式 AI 技术提供服务的，是否按照《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》等规定开展相关工作。	
数据正当使用	a）数据使用加工安全策略和操作规程的建设落实情况；	
	b）数据使用是否获得数据提供方、数据主体等相关方授权；	
	c）数据使用行为与承诺或用户协议的一致性；	
	d）开展数据处理活动以及研究开发数据新技术，是否有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理；	
	e）使用数据开展用户画像、信息推送、内容呈现等业务，造成用户受不公平的价格待遇、平台公共竞争秩序受影	

评估点	评估项	结果记录
	响、平台内劳动者正当权益受损害等风险情况；	
	f）数据使用加工目的、方式、范围，与行政许可、合同授权等的一致性；	
	g）是否存在个人信息和重要数据滥用情况。	
数据导入导出	a）数据导出安全评估和授权审批流程建设情况；	
	b）导入导出审计策略和日志管理机制建设情况；	
	c）导出权限管理、导出操作记录情况；	
	d）导出数据的存储介质的标识、加密、使用、销毁管理情况；	
	e）定期对个人信息和重要数据导出行为进行安全审计情况；	
	f）对导入数据的格式、安全性和完整性校验情况。	
数据处理环境	a）数据处理环境设置身份鉴别、访问控制、隔离存储、加密、脱敏等安全措施情况；	
	b）大数据平台等处理组件按照基线要求进行安全配置、配置核查情况；	
	c）处理环境中的安全漏洞情况，已发现漏洞的处置情况。	
数据使用和加工安全措施	a）在数据清洗、转换、建模、分析、挖掘等加工过程中，对数据特别是个人信息和重要数据的保护情况；	
	b）数据防泄露措施建设情况；	
	c）数据使用加工过程中采取的数据脱敏、水印溯源等安全保护措施情况；	

评估点	评估项	结果记录
	d）数据访问与操作行为的最小化授权、访问控制、审批等管理情况；	
	e）数据使用权限管理情况，如是否存在未授权访问、超范围授权、权限未及时收回、特权账号设置不合理等情况；	
	f）数据加工过程中对个人信息、重要数据等敏感数据的操作行为记录、定期审计情况；	
	g）高风险行为审计及回溯工作开展情况；	
	h）委托加工数据的，是否明确约定受托方的安全保护义务，并采取技术措施或其他约束手段防止受托方非法留存、扩散数据。	

A.2.5 数据提供

评估点	评估项	结果记录
数据提供合法正当必要性	a）提供、委托处理、共同处理数据，以及数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要；	
	b）数据接收方的诚信、守法等情况；	
	c）数据提供是否遵守法律法规和监管政策要求，是否存在非法买卖、提供他人个人信息或重要数据行为；	
	d）对外提供的个人信息和重要数据范围，是否限于实现处理目的的最小范围。	
数据提供管理	a）数据提供安全策略和操作规程的建设落实情况；	
	b）数据对外提供的审批情况；	
	c）对外提供数据前，数据安	

评估点	评估项	结果记录
	全风险评估情况和个人信息保护影响评估情况；	
	d）签订合同协议情况，是否在合同协议中明确了处理数据的目的、方式、范围、数据安全保护措施、安全责任义务及罚则，与网络数据接收方订立或者拟订立的相关合同中关于网络数据安全的要求能否有效约束网络数据接收方履行网络数据安全保护义务；	
	e）开展共享、交易、委托处理、向境外提供数据等高风险数据处理活动前的安全评估情况；	
	f）监督数据接收方到期返还、删除数据的情况；	
	g）向境外执法机构提供境内数据的情况；	
	h）核心数据跨主体流动前是否经过国家有关部门评估。	
数据提供技术措施	a）对外提供的敏感数据是否进行加密及加密有效性；	
	b）对所提供数据及数据提供过程的监控审计情况；	
	c）对外提供数据时采取签名、添加水印、脱敏等安全措施情况；	
	d）跟踪记录数据流量、接收者信息及处理操作信息情况，记录日志是否完备、是否能够支撑数据安全事件溯源；	
	e）数据提供、委托处理、共同处理的安全保障措施及有效性，采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险；	

评估点	评估项	结果记录
	f）多方安全计算、联邦学习等技术应用安全情况。	
数据接收方	a）数据接收方的诚信状况、违法违规等情况；	
	b）数据接收方处理数据的目的、方式、范围等的合法性、正当性、必要性；	
	c）接收方是否承诺具备保障数据安全的管理、技术措施和能力并履行责任义务；	
	d）是否考核接收方的数据保护能力，掌握其发生的历史网络安全、数据安全事件处置情况；	
	e）对接收方数据使用、再转移、对外提供和安全保护的监督情况。	
数据转移安全	a）是否向有关主管部门报告；	
	b）是否制定数据转移方案；	
	c）接收方数据安全保障能力，是否满足数据转移后数据接收方不降低现有数据安全保护水平风险；	
	d）没有接收方的，对相关数据删除处理情况。	
数据出境安全	a）数据出境场景梳理是否合理、完整，是否覆盖全部业务场景和产品类别；	
	b）出境线路梳理是否合理、完整，是否覆盖公网出境、专线出境等情形；	
	c）涉及数据出境的，按照有关规定开展数据出境安全评估、个人信息保护认证、个人信息出境标准合同签订的情况；	
	d）针对公网出境场景，监测	

评估点	评估项	结果记录
	核查实际出境数据是否与申报内容一致。	

A.2.6 数据公开

评估点	评估项	结果记录
数据公开适当性	a）数据公开目的、方式、范围的适当性；	
	b）数据公开目的、方式、范围与行政许可、合同授权的一致性；	
	c）公开的数据内容与法律法规要求的符合程度；	
	d）对公开的数据进行必要的脱敏处理、数据水印、防爬取、权限控制情况；	
	e）数据公开是否会带来聚合性风险。基于被评估对象的已公开数据，结合社会经验、自然知识或其他公开信息，尝试是否可以推断出涉密信息、被评估对象其他未曾公开的关联信息，或其他对国家安全、社会公共利益有影响的信息。	
数据公开管理	a）数据公开的安全制度、策略、操作规程和审核流程的建设落实情况；	
	b）数据公开的条件、批准程序，涉及重大基础设施的信息公开是否经过主管部门批准，涉及个人信息公开是否取得个人单独同意；	
	c）数据公开前的安全评估情况，是否事前评估数据公开条件、环境、权限、内容等风险；	
	d）因法律法规、监管政策的更新，对不宜公开的已公开数据的处置情况；	
	e）对公开数据的脱敏处理、	

评估点	评估项	结果记录
	防爬取、数字水印等控制措施。	

A.2.7 数据删除

评估点	评估项	结果记录
数据删除管理	a）数据删除流程和审批机制的建设落实情况；	
	b）数据删除安全策略和操作规程，是否明确数据销毁对象、原因、销毁方式和销毁要求及对应操作规程；	
	c）是否按照法律法规、合同约定、隐私政策等及时删除数据；	
	d）委托第三方进行数据处理的，是否在委托结束后监督第三方删除或返还数据；	
	e）数据删除有效性、彻底性验证情况，以及可能存在的多副本同步删除情况；	
	f）是否明确数据存储期限，并于存储期限到期后按期删除数据，明确不可删除数据的类型及原因；	
	g）缓存数据、到期备份数据的删除情况。	
存储介质销毁	a）存储介质销毁管理制度和审批机制的建设落实情况；	
	b）介质销毁策略和操作规程，是否明确各类介质的销毁流程、方式和要求，是否妥善处置销毁的存储介质；	
	c）存储介质销毁过程的监控、记录情况；	
	d）软硬件资产维护、报废、销毁管理情况等；	
	e）介质销毁措施有效性，是否对被销毁的存储介质进行数	

评估点	评估项	结果记录
	据恢复验证；	
	f）是否按照数据分类分级，明确不同级别数据适当的删除措施，核心数据删除是否采用存储介质销毁方式。	

A.2.8 其他

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

A.3 数据安全技术

A.3.1 网络安全防护

评估点	评估项	结果记录
开发运维管理	a）网络拓扑结构、网络区域划分、IP 地址分配、网络带宽设置等网络资源管理情况；	
	b）网络隔离、边界防护等措施的有效性；	
	c）安全策略和配置核查情况；	
	d）网络访问控制、安全审计情况；	
	e）安全漏洞发现及常见漏洞修复、处置情况；	
	f）异常流量、恶意代码和钓鱼邮件发现及处置情况；	
	g）外部攻击、内部攻击、新型攻击的发现和处置情况；	
	h）未授权连接内网、外网、无线网等情况；	
	i）通信链路、网络设备、计算设备等关键设备的冗余情况；	

评估点	评估项	结果记录
	j）对第三方组件进行安全核查、修复、更新的情况；	
	k）服务器、数据库、端口、数据资源在互联网的暴露及管理情况；	
	l）处理重要数据、核心数据的信息系统，应按照有关规定满足相应网络安全等级保护要求。属于关键信息基础设施的，还应符合关键信息基础设施安全保护要求。	

A.3.2 身份鉴别与访问控制

评估点	评估项	结果记录
身份鉴别	a）建立用户、设备、应用系统的身份鉴别机制情况，身份标识是否具有唯一性；	
	b）身份鉴别信息是否具有复杂度要求并定期更换；	
	c）是否存在可绕过鉴别机制的访问方式；	
	d）登录失败时采取结束会话、限制非法登录次数、设置抑制时间和网络登录连接超时自动退出等措施的情况	
	e）当远程管理时，是否采取必要措施防止鉴别信息在网络传输中被窃听	
	f）处理重要数据的信息系统，采用口令技术、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行鉴别的情况。	
访问控制	a）建立与数据类别级别相适应的访问控制机制情况，是否限定用户可访问数据范围；	
	b）是否在数据访问前设置身份认证等措施，防止数据的非授权访问；	

评估点	评估项	结果记录
	c）数据访问权限与访问者的身份关联情况；	
	d）数据访问权限申请、审批机制的建设落实情况；	
	e）是否以满足业务实际需要的最小化权限原则进行授权。	
数据提供管理	a）数据权限授权审批流程建设落实情况，是否明确用户账号分配、开通、使用、变更、注销等安全保障要求，是否对数据权限申请和变更进行审核，是否严格控制管理员权限账号数量；	
	b）系统管理员、安全管理员、安全审计员等人员角色分离设置和权限管理情况；	
	c）系统权限分配表建设及更新情况，用户账号实际权限是否满足最少够用、职权分离原则；	
	d）是否存在与权限申请审批结果不一致的情况；	
	e）是否存在多余、重复、过期的账户和角色；	
	f）是否存在共享账户和角色权限冲突的情况；	
	g）是否存在离职人员账号未及时回收、沉默账号、权限违规变更等安全问题；	
	h）数据批量复制、下载、导出、修改、删除等数据敏感操作是否采取多人审批授权或操作监督，并进行日志审计。	

A.3.3 监测预警

评估点	评估项	结果记录
监测预警	a）安全监测预警和信息报告机制的建设落实情况，是否明	

评估点	评估项	结果记录
	确对组织内部各类数据访问操作的日志记录要求、安全监控要求；	
	b）异常行为监测指标建设情况，包括 IP 地址、账号、数据、使用场景等，对异常行为事件进行识别、发现、跟踪和监控等；	
	c）对批量传输、下载、导出等敏感数据操作的安全监控和分析的情况，是否实现对数据异常访问和操作进行告警；	
	d）对数据交换网络流量进行安全监控和分析的情况，是否具备对异常流量和行为进行告警的能力；	
	e）风险信息的获取、分析、研判、通报、处置工作开展情况；	
	f）数据安全缺陷、漏洞等风险的监测预警能力建设情况。	

A.3.4 数据脱敏

评估点	评估项	结果记录
数据脱敏	a）数据脱敏规则、脱敏方法和脱敏数据的使用限制情况；	
	b）需要进行数据脱敏处理的应用场景、处理流程及操作记录情况；	
	c）静态数据脱敏和动态数据脱敏技术能力建设情况；	
	d）开发测试、人员信息公示等应用场景的数据脱敏效果验证情况；	
	e）对匿名化或去标识化处理的个人信息重新识别出个人信息主体的风险分析情况，是否采取相应的保护措施。	

A.3.5 数据防泄露

评估点	评估项	结果记录
数据防泄露	a）数据防泄露技术手段部署情况，能否对网络、邮件、终端等关键环节进行监控并报告敏感信息的外发行为；	
	b）市场上售卖组织业务数据的情况，查看是否能通过公开渠道、开源网站查询到组织业务信息，如代码、数据库信息等；	
	c）数据防泄露技术措施有效性。	

A.3.6 数据接口安全

评估点	评估项	结果记录
对外接口安全	a）面向互联网及合作方数据接口的接口认证鉴权与安全监控能力建设情况，是否能够限制违规接入，是否能对接口调用进行必要的自动监控和处理；	
	b）应用程序编程接口（API）密钥及密钥安全存储措施设置情况，能否避免密钥被恶意搜索或枚举；	
	c）不同安全等级系统间、不同区域间跨系统、跨区域数据流动的安全控制措施情况。	
接口安全控制	a）接口安全控制策略设置情况，是否规定使用数据接口的安全限制和安全控制措施，明确包括接口名称、接口参数等内容的数据接口安全要求；	
	b）是否对涉及个人信息和重要数据的传输接口实施调用审批；	
	c）是否定期对接口（特别是对外数据接口）进行清查，清	

评估点	评估项	结果记录
	查不符合要求的接口是否立即关停；	
	d）涉及敏感数据的接口调用是否具备安全通道、加密传输、时间戳等安全措施；	
	e）数据接口部署身份鉴别、访问控制、授权策略、接口签名、安全传输协议等防护措施情况；	
	f）对接口类型、名称、参数等安全要求规范情况；	
	g）与接口调用方是否明确数据的使用目的、供应方式、保密约定及数据安全责任等情况；	
	h）是否对接口访问做日志记录，同时对接口异常事件进行告警通知的情况。	
数据提供技术措施	a）对外提供的敏感数据是否进行加密及加密有效性；	
	b）对所提供数据及数据提供过程的监控审计情况；	
	c）对外提供数据时采取签名、添加水印、脱敏等安全措施情况；	
	d）跟踪记录数据流量、接收者信息及处理操作信息情况，记录日志是否完备、是否能够支撑数据安全事件溯源；	
	e）数据提供、委托处理、共同处理的安全保障措施及有效性，采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险；	
	f）多方安全计算、联邦学习等技术应用安全情况。	

评估点	评估项	结果记录
数据接收方	a）数据接收方的诚信状况、违法违规等情况；	
	b）数据接收方处理数据的目的、方式、范围等的合法性、正当性、必要性；	
	c）接收方是否承诺具备保障数据安全的管理、技术措施和能力并履行责任义务；	
	d）是否考核接收方的数据保护能力，掌握其发生的历史网络安全、数据安全事件处置情况；	
	e）对接收方数据使用、再转移、对外提供和安全保护的监督情况。	
数据转移安全	a）是否向有关主管部门报告；	
	b）是否制定数据转移方案；	
	c）接收方数据安全保障能力，是否满足数据转移后数据接收方不降低现有数据安全保护水平风险；	
	d）没有接收方的，对相关数据删除处理情况。	
数据出境安全	a）数据出境场景梳理是否合理、完整，是否覆盖全部业务场景和产品类别；	
	b）出境线路梳理是否合理、完整，是否覆盖公网出境、专线出境等情形；	
	c）涉及数据出境的，按照有关规定开展数据出境安全评估、个人信息保护认证、个人信息出境标准合同签订的情况；	
	d）针对公网出境场景，监测核查实际出境数据是否与申报内容一致。	

A.3.7 数据备份恢复

评估点	评估项	结果记录
数据备份恢复	a）数据备份恢复策略和操作规程的建设落实情况；	
	b）数据备份的方式、频次、保存期限、存储介质等情况；	
	c）提供本地或异地数据灾备功能情况；	
	d）定期开展数据备份恢复工作情况；	
	e）备份和归档数据访问控制措施的有效性；	
	f）定期采取必要的技术措施查验备份和归档数据完整性和可用性情况	
	g）定期开展灾难恢复演练情况。	

A.3.8 安全审计

评估点	评估项	结果记录
人员录用	a）审计的实施情况；	
	b）审计策略和要求的合理性、有效性；	
	c）对数据的访问权限和实际访问控制情况进行定期审计的情况，审核用户实际使用权限与审批时的目的是否保持一致，并及时清理已过期的账号和授权；	
	d）特权用户安全审计情况。	
日志留存记录	a）对数据授权访问、收集、批量复制、提供、公开、销毁、数据接口调用、下载、导出等重点环节进行日志留存管理情况；	
	b）日志记录内容，是否包括执行时间、操作账号、处理方式、授权情况、IP 地址、登录	

评估点	评估项	结果记录
	信息等；	
	c）日志记录是否能够对识别和追溯数据操作和访问行为提供支撑；	
	d）是否定期对日志进行备份，防止数据安全事件导致日志被删除；	
	e）日志保存期限是否符合法律法规要求，如网络日志是否保存六个月以上。	
行为审计	a）对网络运维管理活动、用户行为、网络异常行为、网络安全事件等审计情况；	
	b）对数据库、数据接口的访问和操作行为审计情况。	
	c）对数据批量复制、下载、导出、修改、删除等高风险行为的审计情况；	
	d）对个人信息处理活动的合规审计情况。	

A.4 个人信息保护

A.4.1 个人信息处理基本原则

评估点	评估项	结果记录
合法、诚信原则	a）通过误导、欺诈、胁迫等方式处理个人信息的情况；	
	b）非法收集、使用、加工、存储、传输个人信息的情况；	
	c）非法买卖、提供或者公开他人个人信息的情况；	
	d）是否从事危害国家安全、公共利益的个人信息处理活动；	
	e）个人信息处理活动是否具备《个人信息保护法》规定的合法性事由；	
	f）是否存在隐瞒产品或服务	

评估点	评估项	结果记录
	所收集个人信息功能的情况；	
	g）移动互联网应用（如 App、SDK、小程序等）是否存在违法违规收集使用个人信息或侵害用户权益行为。	
正当、必要原则	a）处理个人信息是否具有明确、合理的目的；	
	b）处理个人信息是否与处理目的直接相关，是否采取对个人权益影响最小的方式；	
	c）收集个人信息是否限于实现处理目的的最小范围，如最少类型、最低频次等；是否存在过度收集个人信息行为；	
	d）是否以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务，或者干扰个人正常使用服务，处理个人信息属于提供产品或者服务所必需的除外。	

A.4.2 个人信息告知

评估点	评估项	结果记录
个人信息告知	a）在处理个人信息前，是否以显著方式、清晰易懂的语言真实、准确、完整地公开个人信息处理规则；	
	b）是否告知个人信息处理者的名称或姓名、联系方式，有法律、行政法规规定应保密或者不需要告知的情形除外；	
	c）个人信息处理规则是否告知个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；	
	d）个人信息处理规则是否告知个人行使《个人信息保护法》规定权利的方式和程序；	
	e）告知事项发生变更的，是	

评估点	评估项	结果记录
	否将变更部分告知个人；	
	f）个人信息处理规则是否便于查阅和保存；	
	g）紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者是否在紧急情况消除后及时告知。	

A.4.3 个人信息同意

评估点	评估项	结果记录
个人信息同意	a）处理个人信息前是否取得个人同意，同意是否由个人在充分知情的前提下自愿、明确作出，法律规定的例外情形除外；	
	b）基于个人同意处理个人信息的，个人信息处理者是否提供便捷的撤回同意的方式，个人是否有权撤回其同意，个人撤回同意是否不影响撤回前基于个人同意已进行的个人信息处理活动的效力；	
	c）个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，是否重新取得个人同意。	

A.4.4 个人信息处理

评估点	评估项	结果记录
个人信息保存	a）个人信息的保存期限是否为实现处理目的所必要的最短时间，法律、行政法规另有规定除外；	
	b）是否将个人生物识别信息与个人身份信息分开存储。	
个人信息公共处理	对于两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的， 重点评估:	

评估点	评估项	结果记录
	是否约定各自的权利和义务，约定是否不影响个人向任一个人信息处理者行使权利。	
个人信息委托处理	a）是否与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，是否对受托人的个人信息处理活动进行监督；	
	b）个人信息受托人是否按照约定处理个人信息，是否超出约定的处理目的、处理方式等处理个人信息；	
	c）委托合同不生效、无效、被撤销或者终止的，受托人是否将个人信息返还个人信息处理者或者予以删除，是否违规保留个人信息；	
	d）未经个人信息处理者同意，受托人是否转委托他人处理个人信息。	
个人信息转移	a）是否向个人告知接收方的名称或者姓名和联系方式；	
	b）接收方是否继续履行个人信息处理者的义务	
	c）接收方变更原先的处理目的、处理方式的，是否重新取得个人同意。	
向他人提供个人信息	a）是否向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类；	
	b）是否取得个人的单独同意；	
	c）接收方是否在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。如接收方变更原先的处理目的、处理方式的，是否重新取得个	

评估点	评估项	结果记录
	人同意。	
自动化决策	a）是否保证决策的透明度和结果公平、公正，是否对个人实行不合理的差别待遇；	
	b）通过自动化决策方式向个人进行信息推送、商业营销等，是否同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式；	
	c）对应用算法推荐技术提供互联网信息服务的情形，是否以显著方式告知用户其提供算法推荐服务的情况，并以适当方式公示算法推荐服务的基本原理、目的意图和主要运行机制等。	
个人信息公开	a）个人信息公开是否取得个人单独同意；	
	b）是否在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息，个人明确拒绝的除外；	
	c）处理已公开的个人信息，对个人权益有重大影响的，是否取得个人同意。	

A.4.5 敏感个人信息处理

评估点	评估项	结果记录
通用规则	a）敏感个人信息处理是否具有特定的目的和充分的必要性，是否对敏感个人信息采取严格保护措施；	
	b）处理敏感个人信息是否取得个人的单独同意；	
	c）法律、行政法规规定处理敏感个人信息应取得书面同意的，是否取得个人的书面同意；	
	d）处理敏感个人信息是否向	

评估点	评估项	结果记录
	个人告知处理敏感个人信息的必要性以及对个人权益的影响；	
	e）处理不满 14 周岁未成年人个人信息的，是否取得未成年人的父母或者其他监护人的同意，是否制定专门的未成年人个人信息处理规则；	
	f）是否遵守法律、行政法规对处理敏感个人信息规定；	
生物特征识别信息安全	a）在公共场所安装图像采集、个人身份识别设备，是否为维护公共安全所必需，是否遵守国家有关规定，并设置显著的提示标识；	
	b）所收集的个人图像、身份识别信息，是否只用于维护公共安全的目的，未用于其他目的，取得个人单独同意的除外；	
	c）开展业务活动时是否限定使用人脸识别技术作为身份鉴别的唯一方式，并且当用户拒绝人脸识别方式时，是否频繁申请授权干扰用户正常使用；	
	d）完成身份鉴别后，应及时删除身份鉴别过程中收集、使用的人脸相关数据，仅用于比对的生物特征模板或法律法规另有规定的除外；	
	e）是否满足人脸识别有关政策规定；	
	f）对于步态、基因、声纹等其他生物特征信息安全，可参照相应国家标准、行业标准的具体细化要求评估风险。	

A.4.6 个人信息主体权利

评估点	评估项	结果记录

评估点	评估项	结果记录
个人信息的查阅、复制、可携带	a）个人信息处理者是否为个人提供查阅其个人信息的途径，是否可及时提供个人信息查阅；	
	b）是否为个人提供复制其个人信息的途径，是否可及时提供个人信息复制；	
	c）个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者是否提供转移的方法。	
个人信息的更正、补充	a）个人信息处理者是否为个人提供请求个人信息更正、补充的途径；	
	b）个人请求更正、补充其个人信息的，个人信息处理者是否对其个人信息予以核实，是否及时更正、补充；	
个人信息的删除	a）个人信息处理目的已实现、无法实现或者为实现处理目的不再必要时；	
	b）个人信息处理者停止提供产品或者服务，或者保存期限已届满；	
	c）个人撤回同意；	
	d）个人信息处理者违反法律、行政法规或者违反约定处理个人信息。	
其他个人信息权利	a）个人信息处理者是否为个人提供对其个人信息处理规则进行解释说明的途径；	
	b）通过自动化决策方式作出对个人权益有重大影响的决定，是否为个人提供解释说明的途径，个人是否有权拒绝个人信息处理者仅通过自动化决策的方式作出决定；	
	c）自然人死亡的，其近亲属	

评估点	评估项	结果记录
	为了自身的合法、正当利益，是否可对死者相关个人信息进行查阅、复制、更正、删除等，死者生前另有安排的除外；	
	d）是否建立便捷的个人行使权利的申请受理和处理机制，拒绝个人行使权利请求的，是否说明理由。	

A.4.7 个人信息安全义务

评估点	评估项	结果记录
个人信息保护措施	a）个人信息保护内部管理制度和操作规程的建设落实情况；	
	b）对个人信息分类管理实施情况及效果；	
	c）加密、去标识化等安全技术措施应用情况；	
	d）是否合理确定个人信息处理的操作权限；	
	e）个人信息安全事件应急预案制定及组织实施情况；	
	f）是否在展示、公开等环节，对个人信息直接标识符进行去标识化处理；	
	g）是否定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。	
个人信息保护负责人	a）处理个人信息达到国家网信部门规定数量的个人信息处理者的个人信息保护负责人设置情况，能否负责对个人信息处理活动以及采取的保护措施等进行监督；	
	b）是否公开个人信息保护负责人的联系方式，是否将个人信息保护负责人的姓名、联系方式等报送网信部门。	

评估点	评估项	结果记录
个人信息保护影响评估	a）是否在处理敏感个人信息、利用个人信息进行自动化决策、委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息、向境外提供个人信息前进行个人信息保护影响评估；	
	b）个人信息保护影响评估内容是否符合《个人信息保护法》第 56 条要求；	
	c）是否对个人信息处理情况进行记录，个人信息保护影响评估报告和处理情况记录是否至少保存三年；	
个人信息安全应急	a）个人信息安全事件应急预案制定及组织实施情况；	
	b）发生或者可能发生个人信息泄露、篡改、丢失时，是否立即采取补救措施；	
	c）个人信息安全事件是否通知所涉及个人并报告有关部门，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。	

A.4.8 个人信息投诉举报

评估点	评估项	结果记录
个人信息投诉举报	a）对违反个人信息保护相关规定行为的投诉举报渠道建设情况，包括是否建设便捷的投诉举报渠道，是否及时受理、处置相关投诉举报；	
	b）是否公布接受投诉、举报的联系方式；	
	c）用户投诉、举报后，是否在承诺时限内受理并处理。	

A.4.9 大型网络平台个人信息保护

评估点	评估项	结果记录
大型网络平台个人信息保护	a）是否按照国家规定建立健全个人信息保护合规制度体系，是否成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；	
	b）是否遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；	
	c）是否对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；	
	d）是否定期发布个人信息保护社会责任报告，接受社会监督。	

附录B　漏洞扫描结果记录

附录 B 表-1 漏洞扫描结果主要安全漏洞示例表

序号	安全漏洞名称	关联资产	严重程度	漏洞描述	解决办法
1					
2					

附录C　渗透测试结果记录

C.1 XXXX 系统

C.1.1 信息收集

C.1.2 手工测试

C.1.2.1SQL 注入漏洞

（1）测试方法:

（2）测试链接:

（3）测试结果:

C.1.2.2XSS 漏洞

（1）测试方法:

（2）测试链接:

（3）测试结果:

C.1.2.3……

C.1.3 漏洞归纳

附录D　典型数据安全风险类型

附录 D 表-1 典型数据安全风险类别示例表

序号	风险类别	描述
1	数据泄露风险	由于数据窃取、爬取、脱库、撞库等安全威胁，或者缺乏有效的安全措施、人员操作失误或有意盗取等，导致数据泄露、恶意窃取、未授权访问等影响数据保密性的风险
2	数据篡改风险	由于数据注入、中间人攻击等安全威胁，或者缺乏有效的安全措施、人员有意　或无意操作等，导致数据被未授权篡改等影响数据完整性的风险
3	数据破坏风险	由于拒绝服务攻击、自然灾害、嵌入恶意代码、数据污染、设备故障等安全威胁，或者缺乏有效的安全措施、人员有意或无意操作等，导致数据被破坏、毁损、数据质量下降等影响数据可用性的风险
4	数据丢失风险	由于数据过载、软硬件故障、备份失效、链路过载等问题，或者缺乏有效的安全措施、人员有意或无意操作等，导致数据丢失、难以恢复等安全风险
5	数据滥用风险	由于缺乏授权访问控制、权限管控等有效的安全管控措施、人员有意或无意操作等，导致数据被未授权或超出授权范围使用、加工的风险
6	数据伪造风险	由于数据源欺骗、深度伪造等安全威胁，或者缺乏有效的安全措施、人员有意或无意操作等，导致数据或数据源被伪造、数据主体被仿冒等安全风险
7	违法违规获取数据	违反法律、行政法规等有关规定，非法或违规获取、收集数据的风险，包含违法违规购买数据的情况
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

序号	风险类别	描述
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主体权利	由于未采取有效的个人信息保护措施、人员操作或外部威胁等，导致未能有效保障个人信息主体的知情权、决定权、限制或者拒绝个人信息处理等个人信息主体合法权利
18	App 违法违规收集使用个人信息	App 违反个人信息监管政策或标准规范，存在违法违规收集使用个人信息行为的风险
19	数据处理缺乏公平公正	由于缺乏安全管控措施、人员有意或无意操作等，导致数据处理违反公平公正、诚实守信原则，侵犯其他组织或个人合法权益的风险
20	数据处理抵赖风险	由于外部攻击威胁、缺乏有效安全管控措施、人员有意或无意操作等，导致处理者或第三方否认数据处理行为或绕过数据安全措施等风险
21	数据不可控风险	由于第三方数据安全能力不足、缺乏有效的第三方管控措施、合同协议缺失、外包人员操作等，导致委托处理或合作的第三方违反法律法规或合同协议约定处理数据，造成第三方超范围处理数据、逾期留存数据、违规再转移等数据不可控风险
22	数据推断风险	由于未考虑数据之间的关联关系，导致从公开数据可推断出核心数据、重要数据、未公开的个人数据等，包括但不限于面向人工智能模型的推理攻击、面向基础设施的跨域推断攻击等
23	其他风险	其他可能影响国家安全、公共利益或组织、个人合法权益的数据安全风险