ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 45577—2025

数据安全技术　数据安全风险评估方法

Data security technology—Risk assessment method for data security

2025-04-25 发布　　2025-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

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

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国电子技术标准化研究院、国家信息技术安全研究中心、国家计算机网络应急技术处理协调中心、国家工业信息安全发展研究中心、中央网信办数据与技术保障中心、中国信息安全测评中心、国家信息中心、中国科学院信息工程研究所、公安部第三研究所、北京市政务信息安全保障中心、中国网络安全审查认证和市场监管大数据中心、中国科学技术大学、中国科学院软件研究所、阿里云计算有限公司、北京快手科技有限公司、蚂蚁科技集团股份有限公司、华为技术有限公司。

本文件主要起草人：杨建军、姚相振、张宇光、胡影、陈琦、杨韬、林星辰、陈特、卢磊、林志强、姜松浩、上官晓丽、任英杰、朱雪峰、晏慧、李敏、赵冉、刘曦泽、李晔、陈静、徐峰、王晖、王得福、都婧、马英、张妍、苏艳芳、李媛、程瑜琦、左晓栋、张立武、宋璟、孙勇、王昕、白晓媛、邵萌、苏丹、李海东、张明天、高晨涛。

数据安全技术　数据安全风险评估方法

1　范围

本文件描述了数据安全风险评估的基本概念、要素关系、分析原理，给出了数据安全风险评估的实施流程、评估内容、分析评价方法等。

本文件适用于指导数据处理者、第三方评估机构开展数据安全风险评估，也可供有关主管监管部门实施数据安全检查评估时参考。

2　规范性引用文件

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

GB/T 25069—2022　信息安全技术　术语

GB/T 43697—2024　数据安全技术　数据分类分级规则

3　术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

数据　data

任何以电子或者其他方式对信息的记录。

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

数据处理活动　data processing activities

数据收集、存储、使用、加工、传输、提供、公开、删除等活动。

3.4

合理性　rationality

数据处理活动遵守法律、行政法规要求，符合网络安全和数据安全常识道理，不得损害国家安全、公共利益和个人、组织的合法权益。

3.5

数据安全风险源　data security risk source

可能导致危害数据的保密性、完整性、可用性和数据处理合理性等事件的威胁、脆弱性、问题、隐患等。

注：在本文件中简称“风险源”，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。

3.6

数据安全风险　data security risk

数据安全事件的发生可能性及其对国家安全、公共利益或者组织、个人合法权益造成的损害。

3.7

数据安全风险评估　data security risk assessment

对数据和数据处理活动安全进行风险识别、风险分析和风险评价的整个过程。

3.8

业务　business

组织为实现某项发展规划而开展的运营活动。

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]

3.9

自评估　self-assessment

由评估对象所有者自身发起，组成机构内部的评估小组，依据国家有关法规与标准，对评估对象安全管理进行评估的活动。

[来源：GB/T 20984—2022，3.1.8]

3.10

第三方评估　third party assessment

由数据处理者委托符合相关安全要求的第三方评估机构，依据有关政策法规与标准，对评估对象的数据安全风险进行的评估活动。

3.11

检查评估　inspection and assessment

由数据处理者的上级主管部门、业务主管部门或国家有关主管（监管）部门发起的，依据有关政策法规与标准，对评估对象的数据安全风险进行的评估活动。

[来源：GB/T 20984—2022，3.1.9，有修改]

3.12

移动互联网应用程序　mobile internet application：App

运行在移动智能终端上的应用程序。

注：包括移动智能终端预置、下载安装的应用程序和小程序。

[来源：GB/T 41391—2022，3.1]

4　缩略语

下列缩略语适用于本文件。

GDP：国内生产总值（Gross Domestic Product）

SDK：软件开发工具包（Software Development Kit）

VPN：虚拟专用网络（Virtual Private Network）

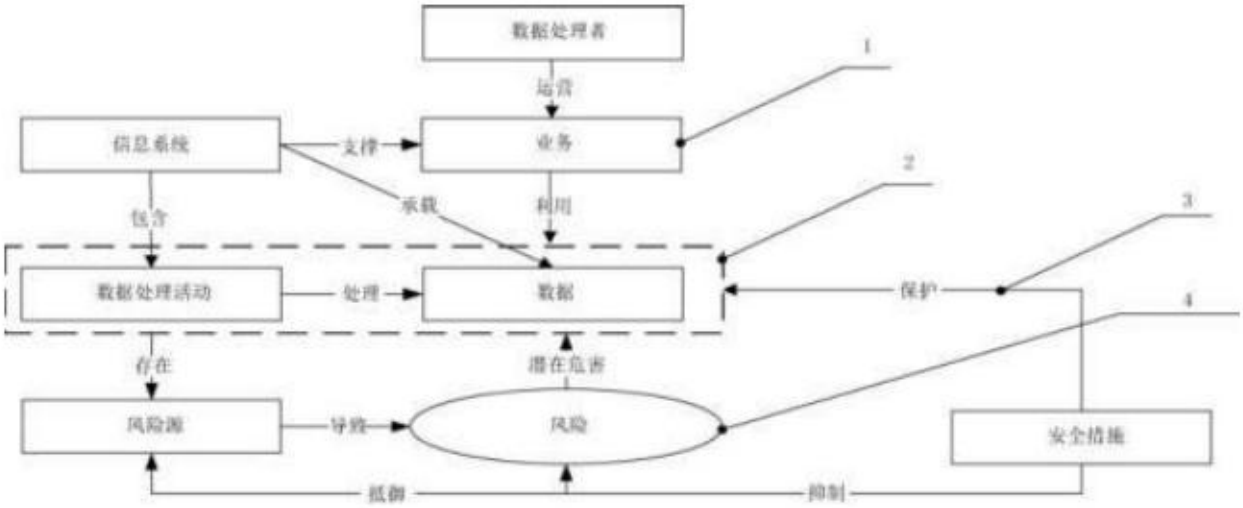
5 通则

5.1 概述

数据安全风险评估，主要围绕数据和数据处理活动，聚焦可能影响数据的保密性、完整性、可用性和数据处理活动合理性的安全风险，掌握数据安全总体状况，发现数据安全隐患，提出数据安全管理和技术防护措施建议，提升数据安全防攻击、防破坏、防窃取、防泄露、防滥用能力。首先通过信息调研识别数据处理者、业务和信息系统、数据、数据处理活动、安全措施等相关要素，然后从数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面识别风险，最后梳理风险源清单，分析数据安全风险、视情评价数据安全风险，并给出整改建议。数据安全风险评估的方式，主要包括自评估、委托第三方评估和检查评估。

5.2 数据安全风险评估要素关系

数据安全风险评估涉及数据、数据处理活动、业务、信息系统、安全措施、风险源等基本要素，要素间关系见图 1。



标引序号说明：

1——风险要素；

2——评估对象；

3——要素关系；

4——风险。

图 1 数据安全风险要素关系

开展数据安全风险评估应充分考虑要素间关系。各要素关系说明如下。

a) 数据和数据处理活动是核心要素，是数据安全风险评估的对象，数据在流转过程中涉及一个或多个数据处理活动，数据处理活动可能涉及不同数据。

b) 数据处理者运营业务，业务利用数据和数据处理活动实现。

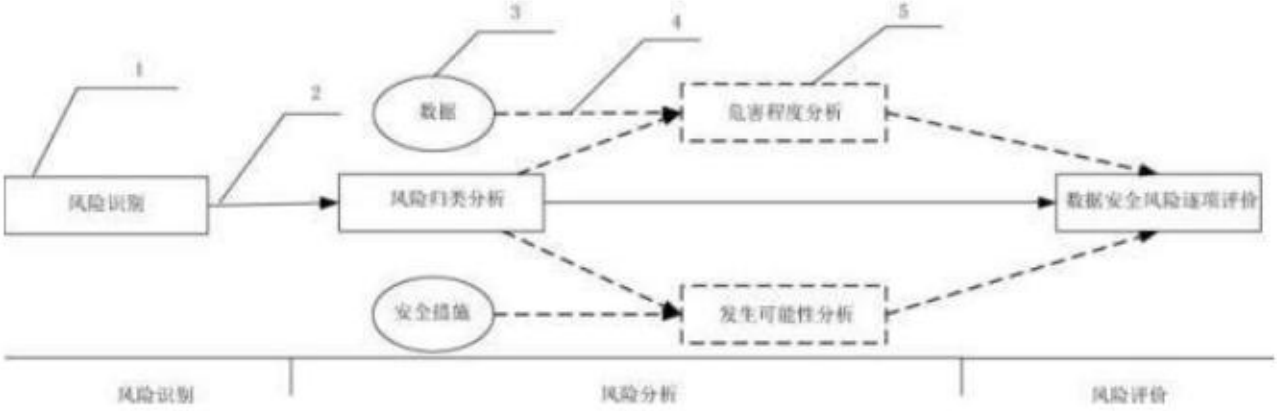
c) 信息系统是业务的支撑，也是数据的载体，信息系统涉及一个或多个数据处理活动。

d) 风险源在数据或数据处理活动中客观存在，由风险源产生的数据安全风险，对数据和数据处理活动有潜在危害。

e) 安全措施用于保护数据和数据处理活动，抵御数据安全风险源，抑制数据安全风险发生。

5.3 数据安全风险评估原理

数据安全风险评估，主要围绕数据处理者的数据和数据处理活动，对可能影响数据保密性、完整性、可用性和数据处理合理性的安全风险进行分析和评价。数据安全风险评估原理见图 2。



标引序号说明：

1——必选分析过程；

2——必需关系；

3——风险分析要素；

4——可选关系；

5——可选分析结果。

图 2 数据安全风险评估原理图

数据安全风险评估主要内容如下。

a) 风险识别：基于信息调研情况，从数据安全管理、数据处理活动安全、数据安全技术、个人信息保护等方面进行数据安全风险识别，识别评估对象现有安全措施完备性并对其有效性进行验证，形成数据安全风险识别工作记录（也称为“评估底稿”）。

b) 风险分析：基于风险识别情况，通过对数据安全风险归类分析（见 9.2.1），梳理数据安全风险源清单，并开展数据安全风险危害程度（见 9.2.2）、数据安全风险发生可能性（见 9.2.3）分析。

   1) 结合数据安全识别工作记录，分析梳理风险源清单，进行数据安全风险归类分析。归类分析时，可基于一项风险源，也可综合多项风险源分析可能引发的数据安全风险。

   2) 结合数据价值和风险源严重程度，分析数据安全风险危害程度。分析风险可能对国家、社会公共利益、组织或个人合法权益造成的危害。

   3) 结合风险源发生频率、安全措施有效性和完备性，分析数据安全风险发生可能性。

c) 风险评价：针对风险源清单，结合风险危害程度和风险发生可能性，逐项评价数据安全风险级别，梳理形成数据安全风险清单。

开展数据安全风险分析和评价时，数据安全风险危害程度分析、风险发生可能性分析等步骤可依据下列情形选择。如不开展数据安全风险危害程度分析、风险发生可能性分析，可基于数据安全风险归类分析结果得到数据安全风险清单。

a) 数据处理者为满足自身数据安全风险防控需要开展评估时，数据安全风险分析和评价等步骤可选。

b) 为落实相关法律法规关于开展数据安全风险评估工作、报送数据安全风险评估报告等要求，履

行重要数据、超 1 000 万个人信息等类型处理者责任义务，以及第三方评估机构开展数据安全风险评估等情形，数据安全风险分析和评价等步骤为必选。

c) 有关主管监管部门实施数据安全检查评估时，可参考本文件自行选取数据安全风险分析和评价等步骤。

d) 其他情形下，可按照实际工作需要自行确认是否选取数据安全风险分析和评价等步骤。

5.4 数据安全风险评估适用情形

适用于以下情形之一的数据处理者，应开展数据安全风险评估。

a) 重要数据处理者、核心数据处理者、处理 1 000 万人以上个人信息的数据处理者，每年度对其网络数据处理活动开展数据安全风险评估。

b) 处理重要数据的大型网络平台服务提供者除依据本文件开展数据安全风险评估外，还应当充分说明关键业务和供应链网络数据安全等情况。

c) 重要数据的处理者提供、委托处理、共同处理重要数据前，开展数据安全风险评估。

d) 当数据范围、数据处理活动、环境、相关方等发生重大变更，被评估对象的政策环境、外部威胁环境、业务目标、安全目标等发生重大变化，超出数据安全风险评估时效等情形的，应重新开展数据安全风险评估。

e) 法律、行政法规、部门规章、强制性国家标准等文件要求开展数据安全风险评估的情形。

适用于以下情形之一的数据处理者，宜结合实际情况开展数据安全风险评估。

a) 重要数据处理者合并、分立、解散、被宣告破产、进行数据转移等情形。

b) 大型网络平台运营者、赴境外上市的数据处理者、党政机关，按照有关规定定期开展数据安全风险评估。

c) 有下列情形之一的，宜在事前开展数据安全风险评估：

1) 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；

2) 重要系统上线前，可根据实际需要开展数据安全风险评估；

3) 新技术应用可能带来数据安全风险的，可根据实际需要开展数据安全风险评估；

4) 其他可能直接危害国家安全、公共利益或者大量个人、组织合法权益的数据处理活动。

5.5 数据安全风险评估实施流程

数据安全风险评估流程，主要包括评估准备、信息调研、风险识别、风险分析与评价、评估总结五个阶段，见图 3。

注：参考 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》3.3 进行数据安全风险自评估、第三方评估及检查评估。

a) 评估准备：是数据安全风险评估的初始预备阶段，在评估实施前应完成评估准备工作。形成调研表、数据安全风险评估方案等。

b) 信息调研：主要用于识别数据处理者的基本情况，厘清其与业务和信息系统的关系，处理的数据和开展的数据处理活动情况，采取的数据安全防护措施。形成数据处理者基本情况、业务清单、信息系统清单、数据资产清单、数据处理活动清单、安全措施情况等，具备条件的，可绘制数据流图。

c) 风险识别：针对各个评估对象，从数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面，通过多种评估手段识别可能存在的数据安全风险隐患。形成数据安全风险识别工作记录。

d) 风险分析与评价：在风险识别基础上开展风险分析、评价，最后提出整改建议。形成数据安全

风险源清单、数据安全风险清单、整改建议等。

e) 评估总结：编制数据安全风险评估报告，开展风险处置。

图 3 数据安全风险评估实施流程图

5.6 数据安全风险评估内容框架

数据安全风险评估，在信息调研基础上，围绕数据安全管理、数据处理活动安全、数据安全技术、个人信息保护等方面开展评估。评估内容框架见图 4，具体评估项见第 8 章，包括以下方面。

a) 数据安全管理包括，数据安全管理制度、安全组织机构、分类分级管理、合作外包管理、安全威胁和应急管理、开发运维管理、云数据安全等。

b) 数据处理活动安全包括，数据收集、存储、传输、使用和加工、提供、公开、删除等。

c) 数据安全技术包括，网络安全防护、身份鉴别与访问控制、监测预警、数据脱敏、数据防泄露、数据接口安全、数据备份与恢复、安全审计等。

d) 个人信息保护包括，个人信息处理基本原则、个人信息告知同意、个人信息处理、敏感个人信息处理、个人信息主体权利、个人信息保护义务、个人信息投诉举报、大型网络平台个人信息保护等。

图 4　数据安全风险评估内容框架图

5.7　数据安全风险评估手段

开展数据安全风险评估时，综合采取下列手段进行评估。

a）　人员访谈：对相关人员进行访谈，核查制度规章、防护措施、安全责任落实情况。

b）　文档查验：查验安全管理制度、合同协议、应急演练报告、事件处置报告及数据安全风险评估报告、网络安全等级保护测评报告等有关材料及制度落实情况的证明材料。

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

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

6　数据安全风险评估准备

6.1　确定评估目标

数据安全风险评估的目标包括但不限于：

a）　明确数据处理者所涉及的数据种类、规模、分布等基本情况。

b）　明确数据处理者数据处理活动的基本情况。

c）　发现可能影响国家安全、公共利益或者个人、组织合法权益的数据安全问题和风险。

d）　发现共享、交易、委托处理、向境外提供重要数据等处理活动的数据安全问题和风险。

e）　促进完善数据安全保护措施，提升数据安全保护能力。

6.2 确定评估范围

根据工作需要和评估目标，确定数据安全风险评估的对象、范围和边界，明确评估涉及的数据、数据处理活动、业务和信息系统、人员和内外部组织等。数据安全风险评估聚焦数据和数据处理活动，评估范围可以是某个单独的业务、信息系统、部门涉及的数据和数据处理活动，可以是组织全部数据和数据处理活动。当选取组织全部数据和数据处理活动作为评估范围时，可根据需要采取“全面摸排、重点评估”的原则，按如下步骤确定评估范围：

a) 全面摸排被评估方的数据安全整体情况，摸清其数据、数据处理活动、数据分类分级等情况；

b) 结合数据分类分级选择重点评估对象，将涉及个人信息、重要数据、核心数据的所有数据处理活动，以及抽样选择的其他典型一般数据的处理活动作为重点评估对象开展评估。如果组织未开展数据分类分级工作，也可结合业务、信息系统的重要性和敏感性，选择核心业务或重要信息系统的数据和数据处理活动作为重点评估对象开展评估。

当选取某个单独的业务、信息系统、部门涉及的数据和数据处理活动进行评估时，可参考上述方法确定评估范围。可选择重点评估对象，也可将涉及的全部数据和数据处理活动纳入评估范围。

6.3 组建评估团队

数据处理者开展数据安全风险评估时，可组织业务、安全、法务、合规、运维、研发等相关部门参与实施，评估组长由数据安全负责人或授权代表担任。数据处理者可委托第三方专业技术机构实施，第三方专业技术机构在评估中获取的信息只能用于评估目的，未经授权不应泄露、出售或者非法向他人提供。

主管监管部门开展检查评估时，可根据评估范围、涉及的行业特征、专业需求，选择具备相关专业能力的评估人员组成评估队伍。评估队伍应提前完成风险评估文档、检测工具等各项准备工作，并签署保密协议。评估队伍在检查评估中获取的信息，只能用于检查任务目的和实施数据安全保护。被评估方应建立专项工作团队，成员一般包括数据安全负责人和安全、法务、合规、运维、研发、业务、数据、风险等部门，或数据处理者内部负责相关事项的其他部门相关人员。专项工作团队应按照要求做好人员、设备、技术保障等工作，配合开展风险评估。

6.4 开展前期准备

开展数据安全风险评估前期准备时，应根据评估目标、评估范围和调研情况，制订工作计划、确定评估依据、确定评估内容、建立评估文档。

a) 制定工作计划。评估工作计划内容一般包括工作目的、工作要求、工作内容、工作流程、调研安排、评估总体进度安排等。开展检查评估时，主管监管部门指导评估团队按照工作要求制定评估工作计划。

b) 确定评估依据。针对评估目标和范围确定评估依据，常见评估依据包括但不限于：

1) 《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律，有关行政法规、司法解释；

2) 网信部门及主(监)管部门相关数据安全规章、规范性文件；

3) 地方数据安全政策规定和监管要求；

4) 数据安全相关国家标准、行业标准等；

5) 开展自评估时，本单位数据安全制度规范可作为评估依据之一。

c) 确定评估内容。结合评估目标、范围、依据，针对被评估方的实际情况，确定被评估方每个评估对象适用的评估内容：

1） 数据处理者应从数据处理活动安全、数据安全管理、数据安全技术等方面进行风险评估；
2） 涉及处理个人信息的，应在1）的基础上，对个人信息保护开展风险评估；
3） 开展评估工作过程中，可根据任务要求、评估重点、监管需要、评估依据等，进一步完善评估内容。

d） 建立评估文档。针对评估目标、范围、依据和内容，准备风险评估调研表、技术测试工具等。在评估工作开展过程中，应对评估工作相关文件进行统一编号，并规范管理。

6.5 制定评估方案

评估团队编制数据安全风险评估工作方案并获得评估管理方的支持、认可，方案内容包括但不限于如下各方面。

a） 评估概述：包括评估目标、评估依据等内容。
b） 评估范围：包括评估对象选择方法、评估对象描述、评估范围等。
c） 评估内容和方法：包括评估内容、评估准则、评估方法等内容。
d） 评估人员：包括评估团队的组织结构、负责人、成员、职责分工等内容。
e） 实施计划：包括时间进度安排、人员安排等内容。
f） 工作要求：包括评估工作要求、被评估方保障条件等内容，工作要求如严格依照评估内容及标准规范，规范评估行为，按照尽量不影响被评估方正常工作的原则，制定评估工作应急保障和风险规避措施，明确告知被评估方评估可能产生的风险，严守工作纪律和保密要求等。
g） 测试方案：开展技术测试前应明确测试方案，包括采用的技术工具、测试内容、测试环境、应急措施等，测试方应向被测方明示测试可能涉及的安全风险，双方就测试方案达成共识。检查评估时应提前向有关部门报备。

评估团队可邀请行业领域相关数据安全、网络安全专家对评估方案进行评议，重点审核方案内容、风险管控、保护措施、可操作性、技术可行性等，进一步修改完善评估方案后，组织实施风险评估工作。

7 信息调研

7.1 数据处理者调研

数据处理者的基本情况的调研内容包括但不限于如下方面。

a） 单位名称、法人和其他组织统一社会信用代码、办公地址、法定代表人信息、人员规模、经营范围、数据安全负责人及其职务、联系方式等基本信息。
b） 单位性质，例如党政机关、事业单位、企业、社会团体等。
c） 是否属于特定类型数据处理者，例如政务数据处理者、大型网络平台运营者、关键信息基础设施运营者等。
d） 所属行业领域。
e） 业务运营地区，开展数据处理活动所在国家和地区等。
f） 主要业务范围、业务规模等。
g） 数据处理相关服务取得行政许可的情况。
h） 被评估单位的资本组成和实际控制人情况。
i） 是否境外上市或计划赴境外上市及境外资本参与情况，或以可变利益实体（VIE）架构等方式实质性境外上市。

7.2 业务和信息系统调研

业务和信息系统情况包括但不限于如下方面。

a) 网络和信息系统基本情况，包括网络规模、拓扑结构、信息系统等情况和对外连接、运营维护等情况以及是否为关键信息基础设施等情况。
b) 业务基本信息，包括业务描述、业务类型、服务对象、业务流程、用户规模、覆盖地域、相关部门等基本信息。
c) 业务涉及个人信息、重要数据或核心数据处理情况。
d) 业务为政务部门或境外用户提供服务情况。
e) 信息系统、App 和小程序情况，包括系统功能、网络安全等级保护备案和测评结论、入口地址、系统连接关系、数据接口、App 及小程序名称和版本等。
f) 数据中心和使用云平台情况。
g) 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。

7.3 数据资产调研

梳理结构化数据（如数据库表等）和非结构化数据（如图表文件等），输出数据资产清单。涉及范围包括但不限于生产环境、测试环境、备份存储环境、云存储环境、个人工作终端、数据采集设备终端等收集和产生的数据。调研内容包括但不限于如下方面。

a) 数据资产情况，包括数据资产类型、数据范围、数据规模、数据形态、数据存储分布、元数据等。
b) 数据分类分级情况，包括数据分类分级规则、数据类别、数据级别、重要数据和核心数据目录情况等。
c) 个人信息情况，包括个人信息类别、规模、敏感程度、数据来源、业务流转及与信息系统的对应关系等。
d) 重要数据情况，包括重要数据种类别、规模、行业领域、数据来源、业务流转及与信息系统的对应关系等。
e) 核心数据情况，包括核心数据类别、规模、行业领域、数据来源、业务流转及与信息系统的对应关系等。
f) 其他一般数据情况。

7.4 数据处理活动调研

针对评估对象和范围，列出数据处理活动清单，描述数据流转关系，绘制数据流图。数据流图应描述数据流转各环节经过的相关方、信息系统，以及每个流动环节涉及的数据类型等。调研内容包括但不限于如下方面。

a) 数据收集情况，如数据收集渠道、收集方式、数据范围、收集目的、收集频率、外部数据源、合同协议、相关系统，以及在被评估方公共场所安装图像采集、个人身份识别设备的情况等。
b) 数据存储情况，如数据存储方式、数据中心、存储系统（如数据库、大数据平台、云存储、网盘、存储介质等）、外部存储机构、存储地点、存储期限、备份冗余策略等。
c) 数据传输情况，如数据传输途径和方式（如互联网、VPN、物理专线等在线通道情况，采用介质等离线传输情况）、传输协议、内部数据共享、数据接口等。
d) 数据使用和加工情况，如数据使用目的、方式、范围、场景、算法规则、相关系统和部门，数据清洗、转换、标注等加工情况，应用算法推荐技术提供互联网信息服务的情况，核心数据、重要数

据或个人信息委托处理、共同处理的情况等。

e) 数据提供情况，如数据提供（数据共享、数据交易，因合并、分立、解散、被宣告破产等原因需要转移数据等）的目的、方式、范围、数据接收方、合同协议，对外提供的个人信息和重要数据的种类、数量、范围、敏感程度、保存期限等。

f) 数据公开情况，如数据公开的目的、方式、对象范围、数据种类、数据规模等。

g) 数据删除情况，如数据删除情形、删除方式、数据归档、介质销毁等。

h) 数据出境情况，是否存在个人信息或重要数据出境，如跨境业务、跨境办公、境外上市、使用境外云服务或数据中心、国际交流合作等场景的数据出境情况。

7.5 安全防护措施调研

调研已有安全措施情况，包括但不限于如下方面。

a) 已开展的等级保护测评、商用密码应用安全性评估、安全检测、风险评估、安全认证、合规审计情况，及发现问题的整改情况。

b) 数据安全管理组织、人员及制度情况。

c) 防火墙、入侵检测、入侵防御等网络安全设备及策略情况。

d) 身份鉴别与访问控制情况。

e) 网络安全漏洞管理及修复情况。

f) VPN 等远程管理软件的用户及管理情况。

g) 设备、系统及用户的账号口令管理情况。

h) 加密、脱敏、去标识化等安全技术应用情况。

i) 3 年内发生的网络和数据安全事件、攻击威胁情况：

1) 3 年内发生的网络和数据安全事件、攻击威胁情况，包括事件名称、数据类型和数量、发生原因、级别、处置措施、整改措施等，重大事件需提供事件调查评估报告；

2) 实际环境中通过检测工具、监测系统、日志审计等发现的威胁；

3) 近期公开发布的社会或特定行业威胁事件、威胁预警；

4) 其他可能面临的数据泄露、窃取、篡改、破坏/损毁、丢失、滥用、非法获取、非法利用、非法提供等安全威胁。

8 风险识别

8.1 通则

从数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面进行数据安全风险识别，发现可能存在的数据安全风险源。具体实施时可按照以下步骤开展。

a) 如果被评估方已开展过相关的测评工作，应先对已开展的测评工作结论进行分析。

b) 针对被评估对象的特点，选择适用的评估内容进行评估，评估内容选择方法如下：

1) 数据处理者均应识别数据安全管理（见 8.3）、数据处理活动（见 8.4）、数据安全技术（见 8.5）等风险情况；

2) 个人信息处理者还应在 1）的基础上，识别个人信息保护风险情况（见 8.6），参考 GB/T 45574—2025 及本文件提出的数据安全风险评估方法，识别敏感个人信息安全风险；

3) 被评估对象涉及数据出境的，应按照国家相关法规、国家标准要求进行数据出境安全保护

工作，若存在未按要求开展相关工作的，直接判定存在安全风险，并结合第 9 章进行风险分析与评价；

4） 梳理各评估项的风险识别结果，形成数据安全风险识别工作记录。

8.2 已开展测评情况分析

被评估方应按照法律、行政法规、部门规章、强制性国家标准等文件要求，通过有关检测评估。在开展风险评估时，应记录被评估方已开展的检测评估工作情况，主要包括：

a） 数据处理活动涉及应开展检测评估工作名称、要求来源等基本情况。

b） 已开展检测评估工作有效性（指是否由有资质机构，按照正常程序开展）。

c） 检测评估内容和结果，及检测评估工作开展情况。

已开展检测评估工作情况应由被评估方提供证明材料，评估人员可在分析评估结果真实性、有效性的基础上视情采纳。

被评估方已开展重要数据出境安全评估、网络安全等级保护测评、个人信息保护合规审计时，不再重复对 8.4 涉及数据出境的评估内容、8.5 中涉及网络安全防护的内容、8.6 中与个人信息保护合规审计内容一致的评估内容开展数据安全风险评估，应采纳已有的有效评估结论，避免重复评估。

若评估对象未实施或通过法律、行政法规、部门规章、强制性国家标准等文件要求的检测评估工作，如网络安全等级保护测评、云计算服务安全评估、互联网信息服务算法推荐安全评估、数据出境安全评估等，则判定存在未按要求开展检测评估工作的安全风险。

8.3 数据安全管理

应从以下方面识别数据安全管理风险。评估项应符合附录 A 的 A.1 的规定。

a） 数据安全管理制度：主要包括数据安全制度体系、数据安全制度落实等，评估项应符合 A.1.1 的规定。

b） 安全组织机构：主要包括数据安全组织架构、数据安全岗位设置等，评估项应符合 A.1.2 的规定。

c） 分类分级管理：主要包括数据资产管理、数据分类分级制度、数据分类分级保护等，评估项应符合 A.1.3 的规定。

d） 人员安全管理：主要包括人员录用、保密协议、转岗离岗、数据安全培训等，评估项应符合A.1.4 的规定。

e） 合作外包管理：主要包括合作方管理机制、合作协议约束、外包人员访问权限、第三方接入与数据回收、政务数据委托处理等，评估项应符合 A.1.5 的规定。

f） 安全威胁和应急管理：主要包括安全威胁和事件、安全应急管理等，评估项应符合 A.1.6 的规定。

g） 开发运维管理：主要包括新应用开发审核，对开发代码、测试数据的安全管理等。评估项应符合 A.1.7 的规定。

h） 云数据安全：主要包括被评估对象使用云计算服务、被评估对象是云计算服务提供者两类，评估项应符合 A.1.8 的规定。

8.4 数据处理活动安全

应从以下方面识别数据处理活动安全风险。评估项应符合 A.2 的规定。

a） 数据收集安全：主要包括数据收集合法正当性、通过第三方收集数据安全、数据质量控制、数据收集方式、数据收集设备及环境安全等。评估项应符合 A.2.1 的规定。

b） 数据存储安全：主要包括数据存储适当性、逻辑存储安全、存储介质安全等评估项应符合A.2.2 的规定。

c) 数据传输安全：主要包括传输链路安全性、传输链路可靠性等。评估项应符合 A.2.3 的规定。

d) 数据使用和加工安全：主要包括数据使用和加工合法性、数据正当使用、数据导入导出、数据处理环境、数据使用和加工安全措施等。评估项应符合 A.2.4 的规定。

e) 数据提供安全：主要包括数据提供合法正当必要性、数据提供管理、数据提供技术措施、数据接收方、数据转移安全、数据出境安全等。评估项应符合 A.2.5 的规定。

f) 数据公开安全：主要包括数据公开适当性、数据公开管理等。评估项应符合 A.2.6 的规定。

g) 数据删除安全：主要包括数据删除管理、存储介质销毁等。评估项应符合 A.2.7 的规定。

h) 其他数据处理活动安全：主要针对即时通信、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进行风险识别。评估项应符合 A.2.8 的规定。

8.5 数据安全技术

应从以下方面识别数据安全技术风险。评估项应符合 A.3 的规定。

a) 网络安全防护：主要包括网络资源管理、网络隔离、边界防护等。评估项应符合 A.3.1 的规定。

b) 身份鉴别与访问控制：主要包括身份鉴别、访问控制、授权管理等。评估项应符合 A.3.2 的规定。

c) 监测预警：主要包括安全监测预警和信息报告机制的建设落实、异常行为监测指标建设等。评估项应符合 A.3.3 的规定。

d) 数据脱敏：主要包括数据脱敏规则、脱敏方法和脱敏数据的使用限制等。评估项应符合A.3.4 的规定。

e) 数据防泄露：主要包括数据防泄露技术手段部署、数据防泄露技术措施有效性等。评估项应符合 A.3.5 的规定。

f) 数据接口安全：主要包括对外接口安全、接口安全控制等。评估项应符合 A.3.6 的规定。

g) 数据备份恢复：主要包括数据备份恢复策略和操作规程的建设落实情况、数据灾备、数据备份恢复等。评估项应符合 A.3.7 的规定。

h) 安全审计：主要包括审计执行、日志留存记、行为审计等。评估项应符合 A.3.8 的规定。

8.6 个人信息保护

如被评估范围涉及个人信息处理，应从以下方面识别个人信息保护风险，评估项应符合 A.4 的规定。

注：个人信息处理者能参考 GB/T 39335—2020 识别个人信息保护风险。视情采纳(部分)个人信息保护影响评估工作结论。

a) 个人信息处理基本原则：主要包括合法、诚信原则，正当、必要原则等。评估项应符合 A.4.1 的规定。

b) 个人信息告知：主要包括处理个人信息告知规则等。评估项应符合 A.4.2 的规定。

c) 个人信息同意：主要包括个人信息前取得个人同意、撤回同意等。评估项应符合 A.4.3 的规定。

d) 个人信息处理：主要包括个人信息保存、个人信息共同处理、个人信息委托处理、个人信息转移、向他人提供个人信息、自动化决策、个人信息公开等。评估项应符合 A.4.4 的规定。

e) 敏感个人信息处理：主要包括敏感个人信息处理通用规则、生物特征识别信息安全等。评估项应符合 A.4.5 的规定。

f) 个人信息主体权利：主要包括个人信息的查阅、复制、可携带、更正、补充、删除及其他个人信息主体权利保障等。评估项应符合 A.4.6 的规定。

g) 个人信息安全义务：主要包括个人信息保护措施、个人信息保护负责人、个人信息保护影响评估、个人信息安全应急等。评估项应符合 A.4.7 的规定。

h) 个人信息投诉举报：主要包括投诉举报渠道建设情况，接受投诉、举报的联系方式公布情况等。

评估项应符合 A.4.8 的规定。

i) 大型网络平台个人信息保护：主要包括个人信息保护合规制度体系建设、处理个人信息的规范和保护个人信息的义务等。评估项应符合 A.4.9 的规定。

9 风险分析与评价

9.1 通则

在信息调研、风险识别基础上，按照 9.2 和 9.3 进行风险分析和评价，形成数据安全风险清单。其中，所有数据安全风险评估过程均应按照 9.2.1 进行风险归类分析，梳理形成数据安全风险源清单。可结合实际需要，视情开展风险危害程度分析、风险发生可能性分析、风险评价。不进行风险评价时，风险归类分析形成的数据安全风险源清单可作为数据安全风险清单。

数据安全风险分析，主要从影响数据保密性、完整性、可用性和数据处理合理性角度分析各项风险源可能引发的数据安全风险，及风险危害程度和发生的可能性。可基于实际情况，视情对数据安全风险进行评价。风险评价一般结合评估对象实际情况，基于 9.2.2 和 9.2.3 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。

9.2 数据安全风险分析

9.2.1 风险归类分析

结合信息调研情况和数据安全风险识别工作记录，梳理发现的数据安全风险源，使用一个或多个风险源分析其可能引发的数据安全风险，形成数据安全风险源清单。可参考附录 B 所列典型数据安全风险类型进行风险分析。数据安全风险源清单见表 1，表中各字段填写要求如下。

a) 序号：填写风险编号，如 1 或 R1 等。

b) 风险类型：填写数据安全风险归类分析的结果，如数据泄露风险。

c) 风险描述：填写实际数据风险情况，如某项、某几项或某类数据存在数据泄露风险。

d) 风险源描述：填写风险源名称，如访问某数据时，某部门某业务或信息系统身份鉴别信息不健全，在某种情形下可能被攻击者或内部员工访问、下载，可能导致一定量级某类数据泄露。

e) 涉及的数据及类型、级别：填写某类风险中一个风险源涉及的数据情况，如涉及 1 000 万银行卡号，属于个人信息，重要数据。

f) 涉及的数据处理活动：填写某类风险中一个风险源涉及的数据处理情况，如数据收集、存储、使用和加工，涉及 1 000 万个人信息向境外提供的情况。

表 1 数据安全风险源清单

序号	风险类型	风险描述	风险源描述	涉及的数据及类型、级别	涉及的数据处理活动

9.2.2 风险危害程度分析

风险危害程度分析，主要考虑数据价值、风险源严重程度等因素。将结合数据级别、规模、种类、处理目的、方式、范围等情况，综合分析数据安全风险一旦发生，对国家安全、公共利益、组织或者个人合法权益造成的危害程度。风险危害程度分析遵循就高从严、整体分析原则，如果该风险涉及多项数据，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。分析方法如下。

a) 数据价值主要从数据分级、经济效益、业务效益、投入成本计量等方面分析。数据级别、经济效

益、业务效益等越高代表数据价值越高。其中，数据安全级别按照 GB/T 43697—2024 确定。个人信息规模和数据敏感程度可作为数据价值判断的衡量因素。

b) 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见表 2，风险危害程度从低到高可分为低、中、较高、高、很高5 个级别。附录 C 的 C.1 给出各类数据安全风险危害程度等级参考。如需进行定量分析，见附录 D 的 D.1。

表 2 数据安全风险危害程度等级

等级	风险危害程度描述
很高	一旦发生数据安全风险，对国家安全、经济运行造成严重危害或特别严重危害，对社会稳定、公共利益造成特别严重危害
高	一旦发生数据安全风险，对国家安全和经济运行产生危害，对社会秩序和公共利益产生严重危害。对组织权益产生特别严重危害、对组织自身运营造成特别严重危害或对个人信息主体产生特别严重危害
较高	对国家安全和经济运行产生有限危害，对社会秩序和公共利益产生危害，对组织权益、组织自身运营产生严重危害，对个人信息主体合法权益产生严重危害
中	对国家安全和经济运行不产生危害，对社会秩序和公共利益产生一般危害，对组织权益、组织自身运营产生危害，对个人权益产生危害
低	对国家安全和经济运行、社会秩序和公共利益几乎不产生危害，对组织权益、组织自身运营、个人权益造成一般危害
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、个人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	

9.2.3 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的数据安全风险，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，如表 3 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。C.2 给出各类数据安全风险发生可能性等级参考。如需进行定量分析，可参考 D.2。

表 3　风险发生可能性等级

等级	风险发生可能性描述
高	涉及违法违规行为、数据安全措施明显不足或安全措施有效性较弱，被评估方已经发生或在通常条件下会发生。本单位、国内相同或相似业务模式的单位多次高频发生同类安全事件，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	数据安全风险事件发生的可能性一般。或有一定数据安全措施，但有效性不足，被评估对象在一定条件下会发生，本单位、国内相同或相似业务模式的单位发生相关风险源，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	数据安全措施完备、有效，被评估对象或同类组织很少或在较苛刻条件下才会发生相关风险事件，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）

9.3　数据安全风险评价

使用风险危害程度和可能性进行数据安全风险评价，评价结果包括如下方面。

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，如需获得风险定量评价结果，可参考 D.3 进行风险评价。

表 4　数据安全风险评价矩阵

数据安全安全风险等级		风险危害程度				
		很高	高	较高	中	低
风险发生可能性	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

9.4 形成数据安全风险清单

针对各项数据安全风险完成风险评价后，整理各项风险评估结果，风险源清单基础上形成数据安全风险清单，列出各项风险的风险等级、危害程度、发生可能性等。数据安全风险清单见表5。表5各字段填写要求如下。

注：若不开展风险危害程度和发生可能性分析，将表1直接作为数据安全风险清单。

a) 序号，风险类型，风险描述，风险源描述，涉及的数据及类型、级别，涉及的数据处理活动，按照表1填写即可。

b) 风险危害程度：按照9.2.3获得的风险危害程度分析结果，填写风险危害程度等级，如高。

c) 风险发生的可能性：按照9.2.3获得的风险发生可能性分析结果，填写风险发生可能性等级，如高。

d) 风险等级：按照9.3获得的风险等级评价结果，填写风险等级，如高安全风险。

表5 数据安全风险清单

序号	风险类型	风险描述	风险危害程度	风险发生的可能性	风险源描述	风险等级	涉及的数据及类型、级别	涉及的数据处理活动

10 评估总结

10.1 编制评估报告

根据评估情况，评估团队编制数据安全风险评估报告(报告模板见附录E)。评估报告应准确、清晰地描述评估活动的主要内容(并附必要的证据或记录)，提出可操作性的整改措施对策建议。风险评估报告的内容包括：

a) 数据处理者基本信息、数据安全管理机构信息、数据安全负责人姓名和联系方式等；

b) 评估概述，包括评估目的及依据，评估对象和范围，评估结论等；

c) 评估工作情况，包括评估人员、评估时间安排、评估工具和环境情况等；

d) 信息调研情况，包括数据处理者、业务和信息系统、数据、数据处理活动、安全措施等情况，形成的数据资产清单、数据处理活动清单、数据流图等文件可视情放在报告正文或附件中；

e) 数据安全风险识别，包括数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面识别的风险源情况；

f) 风险分析与评价，对数据安全问题可能带来的安全风险进行综合分析，视情对风险进行评价；

g) 整改建议，针对发现的数据安全问题或风险，提出整改措施或风险处置建议；

h) 数据安全风险源清单，列出完整的数据安全风险源清单，并附上关键记录和证据，若证据无法在附录中完整列出，应列出证据关键信息和序号，在提交评估报告时作为附件提交；

i) 涉及重要数据、个人信息、核心数据的，应详细列出处理的数据种类、数量(不包括数据内容本身)，开展数据处理活动的情况，面临的数据安全风险及其应对措施等；

j) 委托第三方机构开展评估或检查评估的，评估报告应由评估组长、审核人签字，并加盖评估机构公章。

重要数据的处理者应当每年度向省级以上有关主管部门报送风险评估报告内容除上述内容外，还

应当包括下列内容。

a) 在信息调研情况中，增加处理重要数据的目的、种类、数量、方式、范围、存储期限、存储地点等，开展数据处理活动的情况，不包括数据内容本身。

b) 在信息调研情况中，增加数据安全管理制度及实施情况，加密、备份、标签标识、访问控制、安全认证等技术措施和其他必要措施及其有效性。

c) 在信息调研情况中，增加发现的网络数据安全风险，发生的网络数据安全事件及处置情况。

d) 在信息调研情况中，提供、委托处理、共同处理重要数据情况。

e) 在数据安全风险识别中，单独列出提供、委托处理、共同处理重要数据的风险评估情况、网络数据出境情况。

f) 处理重要数据的大型网络平台服务提供者报送的风险评估报告，除包括前款规定的内容外，还应当充分说明关键业务和供应链网络数据安全等情况。

g) 有关主管部门规定的其他报告内容。

10.2 风险处置建议

评估人员结合实际情况，对发现的数据安全风险提出处置建议，酌情指导数据处理者整改。被评估方应制定数据安全风险处置方案，限期完成整改，无法及时完成整改的，应采取临时安全措施，防止数据安全事件发生。

重要数据的处理者存在可能危害国家安全的重要数据处理活动的，应当按照省级以上有关主管部门责令整改或者停止处理重要数据等要求，立即采取有效措施处置风险。

常见数据安全风险处置措施包括但不限于以下选项。

a) 停止收集某些类型的数据。

b) 预处理阶段对某些类型数据进行销毁。

c) 缩小处理范围。

d) 缩短存储期限。

e) 加强对应数据处理活动岗位人员培训。

f) 匿名化、去标识化。

g) 完善管理制度。

h) 补充签署协议(针对数据转移)。

i) 修订隐私条款。

10.3 残余风险分析

评估人员根据数据处理者决定的风险处置措施，结合风险识别和评估方法，预判措施有效性和残余风险，形成记录。被评估方完成整改后，评估方可视情开展数据安全风险复评工作，复评时可重点分析风险处置后的残余风险，以及采取额外控制措施可能导致的次生风险等。

附 录 A
（规范性）
数据安全风险识别内容

A.1 数据安全管理

A.1.1 安全管理制度

A.1.1.1 数据安全制度体系

针对数据安全制度体系建设情况，应重点评估如下方面：

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。

A.1.1.2 数据安全制度落实

针对被评估方数据安全制度落实情况，应重点评估如下方面。

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

A.1.2.1 数据安全组织架构

针对被评估方数据安全组织架构建设情况，应重点评估如下方面：

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。

A.1.2.2 数据安全岗位设置

针对被评估方数据安全岗位设置情况，应重点评估如下方面：

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

A.1.3.1 数据资产管理

针对数据资产管理情况，应重点评估如下方面：

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。

A.1.3.2 数据分类分级制度

针对数据分类分级制度建设情况，应重点评估如下方面：

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。

A.1.3.3 数据分类分级保护

针对数据分类分级保护情况，应重点评估如下方面：

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

A.1.4.1 人员录用

针对人员录用情况，应重点评估如下方面：

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。

A.1.4.2 保密协议

针对保密协议签订情况，应重点评估如下方面：

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。

A.1.4.3 转岗离岗

针对人员转岗离岗管理情况，应重点评估如下方面：

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。

A.1.4.4 数据安全培训

针对人员数据安全培训情况，应重点评估如下方面：

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

A.1.5.1 合作方管理机制

针对合作方管理机制建设情况，应重点评估如下方面：

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。

A.1.5.2 合作协议约束

针对合作协议约束情况，应重点评估如下方面：

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。

A.1.5.3 外包人员访问权限

针对外包人员访问权限管理情况，应重点评估如下方面：

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。

A.1.5.4 第三方接入与数据回收

针对第三方接入与数据回收情况，应重点评估如下方面：

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。

A.1.5.5 政务数据委托处理

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

a) 委托他人建设、维护电子政务系统，存储、加工政务数据，是否经过严格的批准程序，是否以合同等手段监督受托方履行相应的数据安全保护义务；
b) 政务数据受托方依照法律、法规的规定和合同约定履行数据安全保护义务的情况，是否擅自留存、使用、泄露或者向他人提供政务数据；
c) 支撑电子政务相关系统运行的相关服务或系统的安全措施，是否满足电子政务系统管理和相关安全要求。

A.1.6 安全威胁和应急管理

A.1.6.1 安全威胁和事件

识别安全威胁和安全事件情况，包括但不限于：

a) 近3年发生的网络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。

A.1.6.2 安全应急管理

针对数据安全应急管理情况，重点评估：

a) 数据安全事件应急预案制定和修订情况，是否定义数据安全事件类型，明确不同类别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；
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

针对开发运维管理情况，应重点评估如下方面：

a) 新应用开发审核流程建设情况，进行数据处理需求安全合规审核情况；
b) 开发程序的修改、更新、发布的批准授权和版本控制流程；
c) 工程实施、验收、交付的安全管理情况；
d) 对开发代码、测试数据的安全管理情况；
e) 产品或业务上线前进行安全评估的情况；
f) 开发测试环境和实际运行环境的隔离情况、测试数据和测试结果的控制情况；
g) 开发测试中使用真实个人信息、核心数据、重要数据情况，开发测试前对相关数据进行去标识化、脱敏处理(测试确需信息除外)情况；
h) 对开发和运维人员行为的监督和审计情况；
i) 远程运维的审批、管理和安全防护措施；
j) 第三方 SDK 或开源软件的运行维护、二次开发等技术资料完备性。

A.1.8 云数据安全

被评估对象使用云计算服务时，应重点评估如下方面：

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。

被评估对象是云计算服务提供者时，应重点评估如下方面：

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、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

A.2.1.1 数据收集合法正当性

针对数据收集合法正当性情况，应重点评估如下方面：

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。

A.2.1.2 通过第三方收集数据

重点评估从外部机构收集数据的安全情况：

a) 通过合同协议等合法方式，约定从外部机构收集的数据范围、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。

A.2.1.3 数据质量控制

针对数据质量控制情况，应重点评估如下方面：

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；
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。

A.2.1.4 数据收集方式

针对数据收集方式，应重点评估如下方面：
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。

A.2.1.5 数据收集设备及环境安全

针对数据收集设备及环境安全情况，应重点评估如下方面：
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

A.2.2.1 数据存储适当性

针对数据存储适当性，应重点评估如下方面：
a) 数据存储安全策略和操作规程的建设落实情况；
b) 存储位置、期限、方式的适当性；
c) 永久存储数据类型的必要性。

A.2.2.2 逻辑存储安全

针对逻辑存储安全情况，应重点评估如下方面：
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。

A.2.2.3 存储介质安全

针对存储介质安全情况，应重点评估如下方面：

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

A.2.3 数据传输

A.2.3.1 传输链路安全性

针对数据传输链路安全性，应重点评估如下方面：

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。

A.2.3.2 传输链路可靠性

针对数据传输链路的可靠性，应重点评估如下方面：

a) 网络传输链路的可用情况，包括对关键网络传输链路、网络设备节点实行冗余建设，建立容灾方案和宕机替代方案等情况；
b) 点对点传输中是否存在传输经过第三方、被第三方缓存情况。

A.2.4 数据使用和加工

A.2.4.1 数据使用和加工合法性

针对数据使用和加工合法性，应重点评估如下方面：

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。

A.2.4.2 数据正当使用

针对数据正当使用情况，应重点评估如下方面：

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。

A.2.4.3 数据导入导出

针对数据导入导出情况，应重点评估如下方面：
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。

A.2.4.4 数据处理环境

针对数据处理环境安全情况，应重点评估如下方面：
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。

A.2.4.5 数据使用和加工安全措施

针对数据使用和加工安全措施情况，应重点评估如下方面：
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；
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

A.2.5.1 数据提供合法正当必要性

针对数据提供合法正当必要性，应重点评估如下方面：

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。

A.2.5.2 数据提供管理

针对数据提供管理情况，应重点评估如下方面：
a) 数据提供安全策略和操作规程的建设落实情况；
b) 数据对外提供的审批情况；
c) 对外提供数据前，数据安全风险评估情况和个人信息保护影响评估情况；
d) 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。

A.2.5.3 数据提供技术措施

针对数据提供技术措施情况，应重点评估如下方面：
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。

A.2.5.4 数据接收方

针对数据接收方情况，应重点评估如下方面：
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。

A.2.5.5 数据转移安全

针对因合并、分立、解散、被宣告破产等原因向外转移数据，或承接其他数据处理者转移数据等场

景，重点评估：

a） 是否向有关主管部门报告；

b） 是否制定数据转移方案；

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

d） 没有接收方的，对相关数据删除处理情况。

A.2.5.6 数据出境安全

针对数据出境安全情况，重点评估：

a） 数据出境场景梳理是否合理、完整，是否覆盖全部业务场景和产品类别；

b） 出境线路梳理是否合理、完整，是否覆盖公网出境、专线出境等情形；

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

d） 针对公网出境场景，监测核查实际出境数据是否与申报内容一致。

A.2.6 数据公开

A.2.6.1 数据公开适当性

针对数据公开适当性，应重点评估如下方面。

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。

A.2.6.2 数据公开管理

针对数据公开管理情况，应重点评估如下方面：

a） 数据公开的安全制度、策略、操作规程和审核流程的建设落实情况；

b） 数据公开的条件、批准程序，涉及重大基础设施的信息公开是否经过主管部门批准，涉及个人信息公开是否取得个人单独同意；

c） 数据公开前的安全评估情况，是否事前评估数据公开条件、环境、权限、内容等风险；

d） 因法律法规、监管政策的更新，对不宜公开的已公开数据的处置情况；

e） 对公开数据的脱敏处理、防爬取、数字水印等控制措施。

A.2.7 数据删除

A.2.7.1 数据删除管理

针对数据删除管理情况，应重点评估如下方面：

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。

A.2.7.2 存储介质销毁

针对存储介质销毁情况，应重点评估如下方面：
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

针对网络安全防护情况，应重点评估如下方面。
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。
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

A.3.2.1 身份鉴别

针对身份鉴别措施情况，应重点评估如下方面：

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。

A.3.2.2 访问控制

针对数据访问控制措施情况，应重点评估如下方面：

a) 建立与数据类别级别相适应的访问控制机制情况，是否限定用户可访问数据范围；
b) 是否在数据访问前设置身份认证等措施，防止数据的非授权访问；
c) 数据访问权限与访问者的身份关联情况；
d) 数据访问权限申请、审批机制的建设落实情况；
e) 是否以满足业务实际需要的最小化权限原则进行授权。

A.3.2.3 授权管理

针对数据权限管理情况，应重点评估如下方面：

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

针对数据安全风险监测预警情况，应重点评估如下方面：

a) 安全监测预警和信息报告机制的建设落实情况，是否明确对组织内部各类数据访问操作的日志记录要求、安全监控要求；
b) 异常行为监测指标建设情况，包括 IP 地址、账号、数据、使用场景等，对异常行为事件进行识别、发现、跟踪和监控等；
c) 对批量传输、下载、导出等敏感数据操作的安全监控和分析的情况，是否实现对数据异常访问

和操作进行告警；

d) 对数据交换网络流量进行安全监控和分析的情况，是否具备对异常流量和行为进行告警的能力；

e) 风险信息的获取、分析、研判、通报、处置工作开展情况；

f) 数据安全缺陷、漏洞等风险的监测预警能力建设情况。

A.3.4 数据脱敏

针对数据脱敏情况，应重点评估如下方面：

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

针对数据防泄露情况，应重点评估如下方面：

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

A.3.6.1 对外接口安全

针对对外接口安全情况，应重点评估如下方面：

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。

A.3.6.2 接口安全控制

针对数据接口安全控制情况，应重点评估如下方面：

a) 接口安全控制策略设置情况，是否规定使用数据接口的安全限制和安全控制措施，明确包括接口名称、接口参数等内容的数据接口安全要求；

b) 是否对涉及个人信息和重要数据的传输接口实施调用审批；

c) 是否定期对接口（特别是对外数据接口）进行清查，清查不符合要求的接口是否立即关停；

d) 涉及敏感数据的接口调用是否具备安全通道、加密传输、时间戳等安全措施；

e) 数据接口部署身份鉴别、访问控制、授权策略、接口签名、安全传输协议等防护措施情况；

f) 对接口类型、名称、参数等安全要求规范情况；

g) 与接口调用方是否明确数据的使用目的、供应方式、保密约定及数据安全责任等情况；

h) 是否对接口访问做日志记录，同时对接口异常事件进行告警通知的情况。

A.3.7 数据备份恢复

针对数据备份恢复情况，应重点评估如下方面：

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

A.3.8.1 审计执行

针对数据安全审计执行情况，应重点评估如下方面：

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。

A.3.8.2 日志留存记录

针对日志留存记录情况，应重点评估如下方面：

a) 对数据授权访问、收集、批量复制、提供、公开、销毁、数据接口调用、下载、导出等重点环节进行日志留存管理情况；

b) 日志记录内容，是否包括执行时间、操作账号、处理方式、授权情况、IP 地址、登录信息等；

c) 日志记录是否能够对识别和追溯数据操作和访问行为提供支撑；

d) 是否定期对日志进行备份，防止数据安全事件导致日志被删除；

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。

A.3.8.3 行为审计

针对数据安全行为审计情况，应重点评估如下方面：

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

A.4.1.1 合法、诚信原则

针对合法、诚信原则遵守情况，应重点评估如下方面：

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。

A.4.1.2 正当、必要原则

针对正当、必要原则遵守情况，应重点评估如下方面。

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

针对个人信息告知情况，应重点评估如下方面：

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

针对个人信息同意情况，应重点评估如下方面：

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

A.4.4.1 个人信息保存

针对个人信息保存情况，应重点评估如下方面：

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。

A.4.4.2 个人信息共同处理

对于两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，重点评估：是否约定各自的权利和义务，约定是否不影响个人向任一个人信息处理者行使权利。

A.4.4.3 个人信息委托处理

针对个人信息委托处理情况，应重点评估如下方面：

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。

A.4.4.4 个人信息转移

因合并、分立、解散、被宣告破产等原因需要转移个人信息的，重点评估：

a) 是否向个人告知接收方的名称或者姓名和联系方式；

b) 接收方是否继续履行个人信息处理者的义务；

c) 接收方变更原先的处理目的、处理方式的，是否重新取得个人同意。

A.4.4.5 向他人提供个人信息

向他人提供个人信息的，应重点评估如下方面。

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

b) 是否取得个人的单独同意。

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

A.4.4.6 自动化决策

针对自动化决策情况，应重点评估如下方面：

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。

A.4.4.7 个人信息公开

针对个人信息公开情况，应重点评估如下方面：

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

A.4.5.1 通用规则

针对敏感个人信息处理规则，应重点评估如下方面：

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。

A.4.5.2 生物特征识别信息安全

针对人脸识别数据安全情况，应重点评估如下方面：

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

A.4.6.1 个人信息的查阅、复制、可携带

针对个人信息的查阅、复制、可携带等主体权利保障情况，应重点评估如下方面：

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。

A.4.6.2 个人信息的更正、补充

针对个人信息的更正、补充等主体权利保障情况，应重点评估如下方面：
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。

A.4.6.3 个人信息的删除

针对个人信息的删除等主体权利保障情况，应重点评估有以下情形的，个人信息处理者是否主动删除个人信息：
a) 个人信息处理目的已实现、无法实现或者为实现处理目的不再必要时；
b) 个人信息处理者停止提供产品或者服务，或者保存期限已届满；
c) 个人撤回同意；
d) 个人信息处理者违反法律、行政法规或者违反约定处理个人信息。

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

A.4.6.4 其他个人信息权利

针对个人信息主体权利保障情况，还应重点评估如下方面：
a) 个人信息处理者是否为个人提供对其个人信息处理规则进行解释说明的途径；
b) 通过自动化决策方式作出对个人权益有重大影响的决定，是否为个人提供解释说明的途径，个人是否有权拒绝个人信息处理者仅通过自动化决策的方式作出决定；
c) 自然人死亡的，其近亲属为了自身的合法、正当利益，是否可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

A.4.7.1 个人信息保护措施

针对个人信息保护措施部署情况，应重点评估如下方面：
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。

A.4.7.2 个人信息保护负责人

针对个人信息保护负责人设置情况，应重点评估如下方面：

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。

A.4.7.3 个人信息保护影响评估

针对个人信息保护影响评估开展情况，应重点评估如下方面：

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。

A.4.7.4 个人信息安全应急

针对个人信息安全应急措施部署情况，应重点评估如下方面：

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

针对个人信息投诉举报情况，应重点评估如下方面：

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

针对大型网络平台个人信息保护情况，应重点评估如下方面：

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
（资料性）
典型数据安全风险类型

本附录给出了常见数据安全风险类型，如数据泄露风险、数据篡改风险、数据破坏风险、数据丢失风险等，如表 B.1 所示。

表 B.1 典型数据安全风险类型示例

序号	风险类型	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
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

表 B.1　典型数据安全风险类型示例（续）

序号	风险类型	描述
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

附 录 C
（资料性）
数据安全风险分析参考

C.1 数据安全风险危害程度分析参考

针对 9.2.2 给出的数据安全风险危害程度，表 C.1 给出各类数据安全风险危害程度等级参考。

表 C.1 数据安全风险危害程度等级参考

危害程度等级	影响对象	风险危害程度示例
很高	国家	1）直接影响国家政治安全。 2）直接影响涉及国家安全的行业、提供重要公共产品的行业、国家重大基础设施（如能源、电力）等关系国家经济命脉的行业的正常运行和发展，如大面积业务中断、大规模基础设施瘫痪等。 3）可能导致我国重要设施暴露在高度威胁中或严重影响我国领土、主权完整。例如我国核心网络设施和信息系统的高精度位置信息，带精确坐标的实景影像数据泄露。 4）可能直接导致我国重大经济决策泄露，造成货币汇率、银行利率、物价水平、劳动就业总水平、失业率、进出口贸易总规模等发生巨大波动、GDP 显著下降等重大金融风险。例如引起全国整体 GDP 下降超 1%
	公共利益	1）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，引起大范围社会恐慌，比如造成重大人员伤亡、财产损失或环境污染等。 2）直接导致一个或多个省（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 1 000 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。 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。 4）可能直接影响人民群众重要民生保障的事项、物资、工程和项目等。可能导致发生特别重大突发事件、特别重大群体性事件、暴力恐怖活动等；可能引发社会性恐慌，对社会稳定、公共利益造成特别严重危害。例如发生影响全国范围内的重大舆情，引起全国范围内的群众恐慌、社会动荡
高	国家	1）关系国家安全重点领域，或者对国土、经济、科技、文化、社会、生态、军事、网络、人工智能、核、生物、太空、深海、极地、海外利益等任一领域国家安全造成严重威胁。 2）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。 3）直接影响多个行业内多个企业、大规模用户，对行业发展、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、关键产业链、核心供应链等。 4）可能导致我国重要设施受到较高威胁或影响我国领土、主权完整。例如我国重要网络设施和信息系统的高精度位置信息，带精确坐标的实景影像数据被外方掌握。 5）可能直接影响宏观经济运行，造成社会总供给和总需求、国民生产总值、货币汇率、银行利率、物价水平、劳动就业总水平、失业率、进出口贸易总规模等发生较大变动。例如引起 1 个及以上省、自治区、直辖市的 GDP 或某行业整体 GDP 下降超 1%

表 C.1　数据安全风险危害程度等级参考（续）

危害程度等级	影响对象	风险危害程度示例
高	公共利益	1）直接导致重大突发事件、重大群体性事件等，引起社会矛盾激化，对社会稳定造成严重危害，比如造成人员伤亡、财产损失或环境污染等。 2）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。 3）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。 4）可能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。 5）可能导致发生重大突发事件、重大群体性事件等。可能严重影响人民群众的日常生活秩序；可能严重影响各级党政机关履行公共管理和服务职能。可能严重影响法制和社会伦理道德。例如发生影响多个省、自治区、直辖市范围内的重大舆情，引起多个省、自治区、直辖市范围内的群众恐慌、社会动荡
	组织	1）可能导致组织受到刑事处罚，可能对组织造成重大经济或技术损失，企业全面停业整顿，企业面临破产。 2）可能导致组织受到来自主管部门的行政处罚，对机构构成严重影响（如某业务板块终止运行、吊销营业执照或吊销相关业务许可证等），或重大经济损失，直接或者间接损失合计在营业额 10%（含）以上的
	个人	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，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
较高	国家	1）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。 2）对单个行业领域发展、业务经营、技术进步、产业生态等造成危害。 3）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
	公共利益	1）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。 2）直接影响公共场所的活动秩序、公共交通秩序，如影响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	1）可能导致组织受到来自主管部门或行政机关的行政处罚或整改要求，对机构构成较大影响（如某业务板块的临时关停处罚或定期整改处罚），直接或者间接经济损失合计在营业额[10%，5‰）以内的，或造成较严重的声誉损失。 2）组织业务数据和经营管理数据处理存在特别严重数据安全风险隐患，存在超过 10 万个人信息违法违规收集使用行为等，可能导致组织遭到监管部门处罚、安全事件或法律诉讼等，企业面临破产等。或自然人遭受特别严重影响，如：失去工作、导致长期心理疾病，导致死亡等
	个人	个人信息主体可能会遭受较大影响，如遭受诈骗且诈骗金额在个人财产的 10%以上、资金被盗用且被盗用金额在个人财产的 10%以上、被解雇、名誉严重受损、健康状况恶化等。 个人信息处理存在特别严重数据安全风险隐患，存在超过 10 万个人信息违法违规收集使用行为等，可能导致自然人遭受特别严重影响，如：失去工作、导致长期心理疾病，导致死亡等

表 C.1　数据安全风险危害程度等级参考（续）

危害程度等级	影响对象	风险危害程度示例
中	公共利益	1)可能影响企事业单位、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。 2)可能影响公共场所的活动秩序、公共交通秩序，如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	1)对组织造成轻微经济损失，如直接或间接经济损失合计在营业额 5‰以内，或造成一定声誉损失。 2)组织业务数据和经营管理数据处理存在严重数据安全风险隐患。可能影响组织的业务生产经营，破坏组织声誉、公信力等，企业遭受经济损失
	个人	1)个人信息主体可能会遭受影响，如信用评分受损、名誉受损、被法院传唤、导致较小疾病等。 2)个人信息处理存在严重数据安全风险隐患、存在超过 1 万个人信息违法违规收集使用行为等。可能导致自然人遭受严重影响，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
低	组织	1)对组织造成潜在经济与声誉损失。 2)组织业务数据和经营管理数据处理存在一般数据安全风险隐患，可能导致组织的经济利益、声誉等轻微受损
	个人	1)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等。 2)个人信息处理存在一般数据安全风险隐患、存在少部分个人信息违法违规收集使用行为等。可能导致自然人遭受一般影响，如：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

C.2　数据安全风险发生可能性分析参考

针对 9.2.3 给出的数据安全风险发生可能性，表 C.2 给出各类数据安全风险可能性等级参考。

表 C.2　数据安全风险可能性等级参考

可能性等级	风险发生可能性示例
高	风险源发生频率：在该行业领域的数据安全防护中，在多数情况下会发生的风险，发生频率高（或≥1 次/月）或可证实多次发生过。 安全措施有效性和完备性：缺少数据安全防护措施或具有少量的数据安全防护措施，无法或难以抵御大部分数据安全破坏行为。 风险源关联性：通过风险源清单关联分析，易与其他风险源进行关联或能够关联的风险源超过已识别风险源清单的 60%，导致数据安全事件或引发新的数据安全风险
中等	风险源发生频率：在该行业领域的数据安全防护中，在特定条件下可能会发生的威胁，发生频率中等（或≥1 次/半年）或被证实曾经发生过。 安全措施有效性和完备性：具有相应的数据安全防护措施，能抵御初级数据安全破坏行为，但无法抵御有组织的数据安全破坏行为。 风险源关联性：通过风险源清单关联分析，会与其他风险源进行关联或能关联的风险源超过已识别风险源清单的 20%，导致数据安全事件或引发新的数据安全风险

表 C.2　数据安全风险可能性等级参考（续）

可能性等级	风险发生可能性示例
低	风险源发生频率：在该行业领域的数据安全防护中，一般不太容易发生的或在很罕见和例外的情况下发生的威胁，发生频率低、没有被证实发生过或几乎不可能发生。 安全措施有效性和完备性：具有较为完善的数据安全防护措施，能抵御数据安全破坏行为。 风险源关联性：通过风险源清单关联分析，几乎不可能与其他风险源进行关联，导致数据安全事件或引发新的数据安全风险

附 录 D
（资料性）
数据安全风险量化分析与评价方法

D.1 数据安全风险危害程度量化分析方法

结合 9.2.2 给出的数据安全风险危害程度定性分析方法，表 D.1 按照百分制给出数据安全风险危害程度量化分析方法，结合实际情况，根据得分区间给出风险危害程度得分，得分越高代表风险危害程度越高。

表 D.1 数据安全风险危害程度等级参考

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

D.2 数据安全风险发生可能性量化分析方法

结合 9.2.3 给出的数据安全风险发生可能性定性分析方法，表 D.2 按照百分比给出数据安全风险发生可能性量化分析方法，结合实际情况，根据得分区间给出风险发生可能性得分，得分越高代表风险发生可能性越高。

表 D.2 数据安全风险发生可能性等级参考

等级	得分
高	[75%，100%]
中	[30%，75%)
低	[0%，30%)

D.3 数据安全风险量化评价方法

结合 9.3 给出的数据安全风险评价方法，本条提出数据安全风险量化评价方法，结合实际情况，根据 D.1 和 D.2 给出的量化结果计算风险分值，得分越高代表风险等级越高。计算公式如下：

$R_i=\sqrt{\sigma_i \times V_i}$，其中 R_i 为第 i 个风险评价分值，σ_i 为第 i 个风险危害程度赋值；V_i 为第 i 个风险发生可能性赋值。

附 录 E
（资料性）
数据安全风险评估报告模板

E.1 数据安全风险评估报告封面样式见图 E.1。

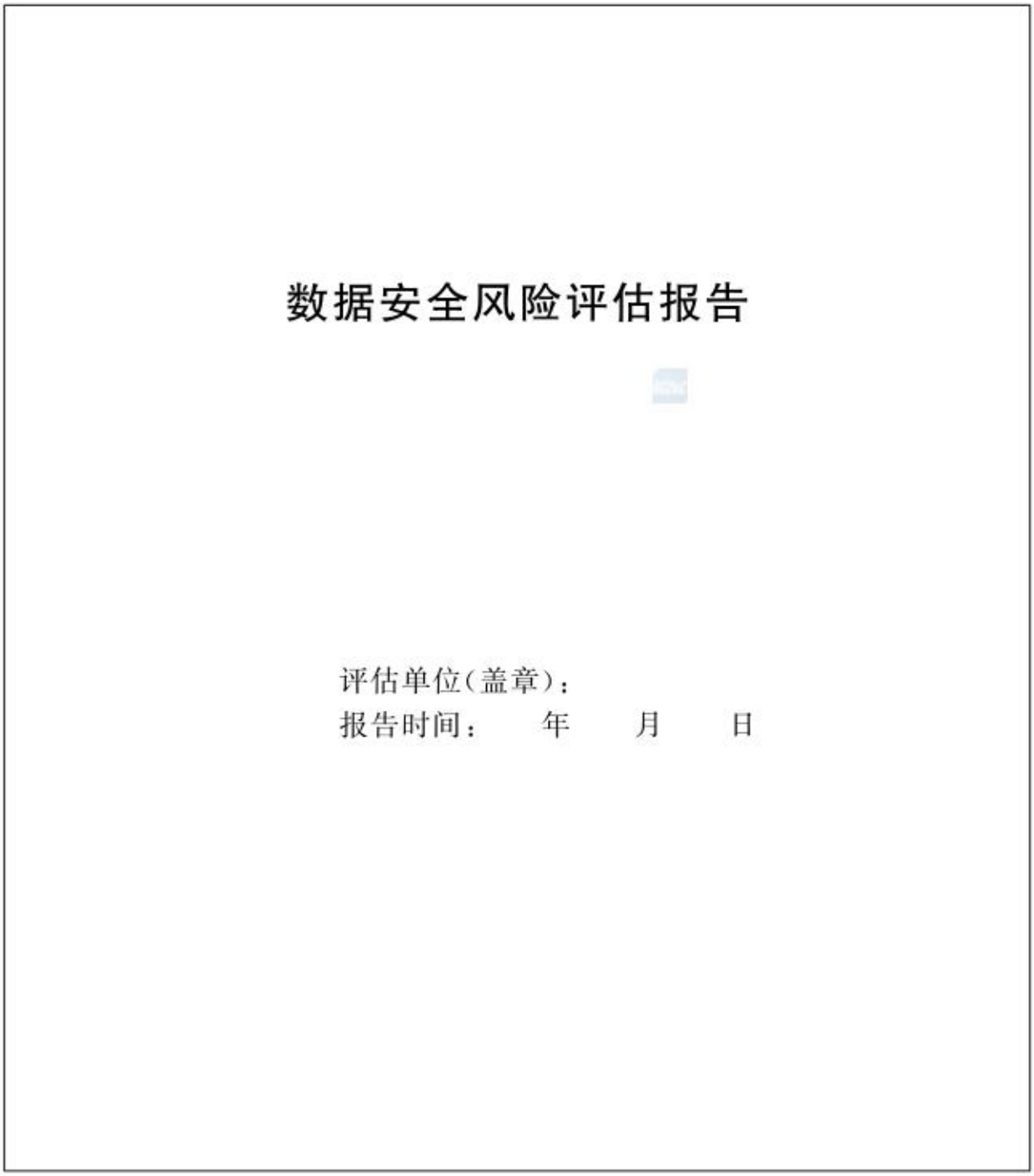


图 E.1 数据安全风险评估报告封面

E.2　数据安全风险评估报告基本信息表样式见图 E.2。

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		联系方式	
审核批准	评估组长		日期	
	审核人		日期	

图 E.2　数据安全风险评估报告基本信息

E.3　数据安全风险评估报告主要内容样式见图 E.3。

一、评估概述

1.1　评估目的

1.2　评估依据

1.3　评估对象和范围

说明评估对象的选择原则，描述评估对象和评估范围。

1.4　评估结论概要

说明数据和数据处理活动的概要情况，评估结果概要。

二、评估工作开展情况

2.1　评估人员情况

说明评估工作组织和评估团队人员情况，被评估方参与人员情况。

2.2　评估时间安排情况

说明本次评估工作的时间进度安排，描述各阶段完成的任务、工作成果和时间节点等内容。

2.3　评估工具和环境情况

说明使用的评估工具，接入的网络或系统环境、技术测试内容等情况。

三、信息调研情况

按照 GB/T 45577—2025 第 7 章内容说明信息调研情况。

3.1　数据处理者基本情况

说明数据处理者的机构实体基本情况。

图 E.3　数据安全风险评估报告主要内容

3.2 业务和信息系统情况

说明主营业务、信息系统、App 和网络拓扑等情况。

3.3 数据资产情况

说明数据资产、数据分类分级，涉及个人信息、重要数据、核心数据目录等情况。

3.4 数据处理活动情况

说明数据收集、数据存储、数据使用、数据加工、数据传输、数据提供、数据公开、数据删除、数据出境情况。

针对评估对象结合实际情况画出数据流转图。

3.5 安全措施情况

说明已开展的安全测评认证和核实情况，数据安全管理机构、人员及制度情况，网络和数据安全主要措施。

四、数据安全风险识别

按照 GB/T 45577—2025 第 8 章，从数据安全管理、处理活动、技术、个人信息处理等方面，说明各评估对象的风险隐患或安全问题，如有必要可附上关键证据材料。

4.1 数据安全管理风险识别

4.2 数据处理活动风险识别

4.3 数据安全技术风险识别

4.4 个人信息处理风险识别

五、风险分析与评价

按照 GB/T 45577—2025 第 9 章，针对本报告第 4 章发现的问题隐患，分析数据安全风险，视情进行风险评价，提出整改建议。

5.1 风险分析

5.2 风险评价（可选）

5.3 整改建议

附录 XXXX

附录可给出完整的数据安全风险源清单，根据实际需要提供评估底稿，或者补充相应的证据材料等。

图 E.3 数据安全风险评估报告主要内容（续）

E.4 数据安全风险评估报告声明模板样式见图 E.4。

声 明

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

本报告是[被评估方名称]的网络数据安全风险评估报告。

本报告评估结论的有效性建立在被评估方提供相关证据的真实性基础之上。

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

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

单位名称（加盖单位公章）

年 月 日

图 E.4 数据安全风险评估报告声明模板

参 考 文 献

[1] GB/T 20984—2022 信息安全技术 信息安全风险评估方法

[2] GB/T 35273—2020 信息安全技术 个人信息安全规范

[3] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

[4] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

[5] GB/T 41391—2022 信息安全技术 移动互联网应用程序(App)收集个人信息基本要求

[6] GB/T 45574—2025 数据安全技术 敏感个人信息处理安全要求

[7] JR/T 0223—2021 金融数据安全 数据生命周期安全规范

[8] YD/T 3801—2020 电信网和互联网数据安全风险评估实施方法

[9] 中华人民共和国个人信息保护法(2021 年 8 月 20 日中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议通过)

[10] 中华人民共和国数据安全法(2021 年 6 月 10 日中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过)

[11] 中华人民共和国网络安全法(2016 年 11 月 7 日中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过)

[12] 《互联网信息服务深度合成管理规定》(2022 年 11 月 3 日国家互联网信息办公室、工业和信息化部、公安部联合印发)

[13] 《互联网信息服务算法推荐管理规定》(2022 年 11 月 16 日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联合印发)

[14] 《常见类型移动互联网应用程序必要个人信息范围规定》(2021 年 3 月 12 日国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、市场监管总局办公厅联合印发)

[15] 《App 违法违规收集使用个人信息认定方法》(2019 年 11 月 28 日国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、市场监管总局办公厅联合印发)