ICS 35.020
CCS 点击此处添加 CCS 号

MH

中华人民共和国民用航空行业标准

MH/T XXXXX—XXXX

民航领域数据安全风险评估指南

Guidelines for data security risk assessment of civil aviation

（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

中国民用航空局　　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。

本文件由中国民用航空局人事科教司提出。

本文件由中国民航科学技术研究院归口。

本文件起草单位：中国民航大学、中国民航信息网络股份有限公司、河南省机场集团有限公司、中国民用航空局信息中心、首都机场集团有限公司、上海机场（集团）有限公司、深信服科技股份有限公司、中国国际航空股份有限公司、中国民用航空华东地区空中交通管理局、中国民用航空华北地区空中交通管理局、中国民用航空总局第二研究所、中国民用航空西南地区空中交通管理局等。

本文件主要起草人：周景贤、邢伟、葛京、窦雪峰、史国阳、王岱、李群、郭睿、李长京、张智铭、王崧灏、张益、吴越、宁文冠、贾琦婧、王岩韬等。

民航领域数据安全风险评估指南

1 范围

本文件确立了民航领域数据安全风险评估的原则，提供了数据安全风险评估流程、评估准备、信息调研、风险识别、分析和评价、评估总结等方面的建议。

本文件适用于民航领域数据处理者（以下简称“数据处理者”）和第三方评估机构开展数据安全风险评估，以及国家和民航行业各级管理部门开展数据安全检查。

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 45389—2025 数据安全技术 数据安全评估机构能力要求

GB/T 45574—2025 数据安全技术 敏感个人信息处理安全要求

GB/T 45577—2025 数据安全技术 数据安全风险评估方法

MH/T 3039—2025 民航领域数据分类分级要求

3 术语和定义

GB/T 25069、MH/T 3039界定的以及下列术语和定义适用于本文件。

3.1

民航领域数据 civil aviation data

以电子或者其他方式在行业发展、监督执法、政务管理、生产运行、服务保障等过程中产生的，或通过收集、监测等方式获取的，用于民航业活动的原始及其衍生业务数据。

3.2

重要数据 key data

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

注1：包括但不限于民用航空器事故相关的飞行数据记录器数据、驾驶舱语音记录器数据、航空器健康状况监测数据，以及超过100万人的旅客个人信息。

注2：仅影响组织自身或公民个体的数据一般不作为重要数据。

[来源：MH/T 3039—2025，3.3]

3.3

核心数据 core data

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

注：核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据，以及超过1亿人的旅客个人信息。

[来源：MH/T 3039—2025，3.3]

3.4

一般数据 general data

核心数据、重要数据之外的其他数据。

[来源：GB/T 43697—2024，3.4]

3.5

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。

[来源：GB/T 45577—2025，3.4]

3.6

数据安全风险问题　data security risk issues

可能导致危害数据保密性、完整性、可用性及数据处理合理性的事件发生。

注：数据安全风险问题也称“风险源”，包括相关的威胁、脆弱性和隐患等。在本文件中简称“风险问题”，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问题，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问题。

[来源：GB/T 45577—2025，3.5，有修改]

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。

[来源：GB/T 45577—2025，3.7]

3.8

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，依据国家和民航行业有关法规与标准，对评估对象的数据安全管理进行评估的活动。

[来源：GB/T 45577—2025，3.9，有修改]

3.9

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，依据国家和民航行业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 45577—2025，3.10，有修改]

3.10

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 45577—2025，3.11]

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：应用程序（Application）

SDK：软件开发工具包（Software Development Kit）

VPN：虚拟专用网络（Virtual Private Network）

5　风险评估概述

5.1　评估适用情形

适用于以下条件之一的民航领域数据处理者，宜启动数据安全风险评估工作。

a）　处理重要数据或核心数据，以及处理民航领域100万人以上个人信息的数据处理者，每年度对其数据处理活动开展数据安全风险评估。

b）　提供、委托处理、共同处理重要数据前，数据处理者开展数据安全风险评估。但是属于履行法定职责或者法定义务的除外。

c）　在申报数据出境前，数据处理者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，或发生重大数据安全事件，数据处理者重新开展数据安全风险评估。

e） 可能直接危害国家安全、社会秩序、公共利益，或者危害大量个人、组织合法利益的数据处理活动前开展数据安全风险评估。
f） 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。
g） 按照国家及行业主管部门有关工作要求开展数据安全风险评估。

5.2 评估思路

民航领域数据安全风险评估，主要围绕民航领域数据和对应的数据处理活动，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，发现数据安全问题，提出数据安全管理和技术防护措施建议，提升数据安全风险防控能力。

数据安全风险评估的具体实施主要包括以下三个部分：

a） 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、现有安全措施等相关要素；
b） 识别数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面的风险问题；
c） 梳理风险问题清单，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形式，主要包括自评估、第三方评估和检查评估。三种评估形式可根据工作需要，选择附录A全部或者部分内容开展数据安全风险评估。

5.3 评估原则

民航领域数据安全风险评估工作遵循以下原则。

a） 客观公正原则：在民航领域数据安全风险评估过程中，根据评估对象实际情况作出客观判断和真实的评价。
b） 科学性原则：在评估过程中，根据特定目的，选择适用的评估方法，制定科学的评估方案，评估结果准确合理。坚持主观评价与客观测算、静态分析与动态分析、定性分析与定量分析相结合，科学合理的开展评估工作。
c） 完备性原则：按照被评估对象所涉及的评估范围进行全面的评估。
d） 最小影响原则：从相关管理层面和工具技术层面，将评估工作对数据和承载数据的应用、系统、网络正常运行的可能影响控制在最小程度。
e） 保密性原则：在评估过程中，参与方对风险评估涉及评估对象的商业信息、客户信息、技术文件等进行保密。

5.4 评估手段

开展数据安全风险评估时，可综合采用以下手段进行评估。

a） 人员访谈：对相关人员进行访谈，对数据的处理、保障措施设计和实施情况进行了解、分析和取证。
b） 资料查验：查验数据安全相关文件资料，如数据安全管理制度、安全策略和机制、合同协议、安全配置和设计文档、系统运行记录等相关文件。
c） 配置核验：核查、验证承载数据的应用、系统、网络的配置和策略，包括数据采集界面、数据展示界面、数据存储界面、数据操作日志记录等。如系统存在高度保密性、可用性的要求，评估可通过事后提供日志列表或测试环境等方式进行。
d） 安全测试：使用数据安全评估评测工具或通过技术手段实际测试数据载体，查看、分析被测试响应输出结果。安全测试前充分评估测试过程对数据载体等造成的影响，对于业务不可中断的系统、应用等，可考虑采用模拟系统验证、离线环境验证等方式。

6 风险评估流程

数据安全风险评估流程，主要包括评估准备、信息调研、风险识别、风险分析和评价、评估总结五个阶段，实施流程见图1，具体说明如下。

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

b) 信息调研：调研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表、业务清单、信息系统清单、数据资产清单、数据处理活动清单，绘制数据业务流程图和编制现有安全措施情况表。

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 5.4 节给出的评估手段识别可能存在的数据安全风险隐患，形成评估结果记录表单。评估过程中做好风险评估工作记录，包含文档查阅记录、人员访谈记录、安全核查记录、技术检测记录等。

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，形成数据安全风险问题清单、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，根据处置建议开展残余风险处置。

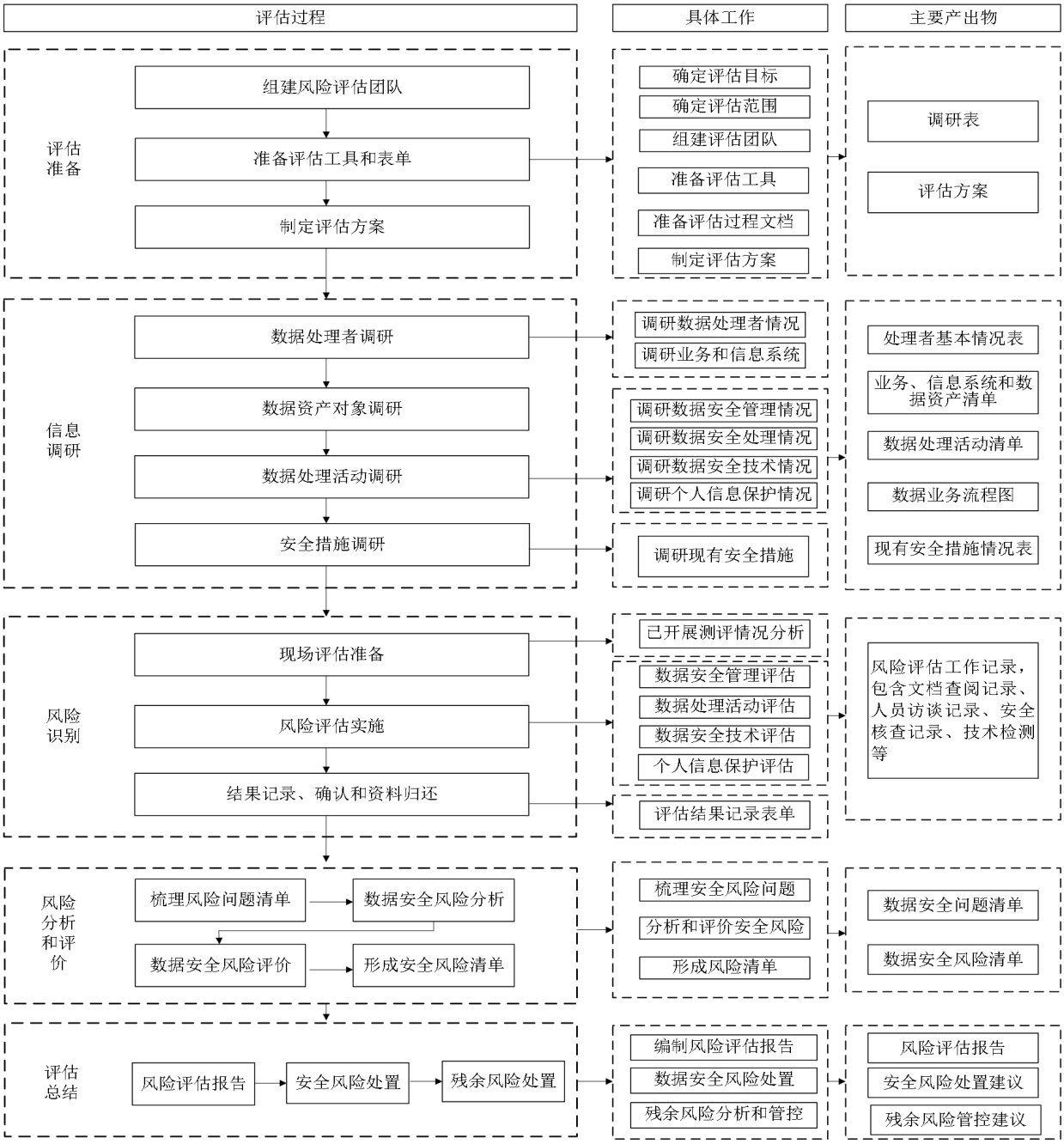

图 1　数据安全风险评估实施流程图

7 评估准备

7.1 确定评估目标

数据处理者根据评估的目的、任务来源等因素来确定评估活动的目标。民航领域数据安全风险评估的目标包括但不限于：

a) 确定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或核心数据等处理活动的数据安全问题和风险；
e) 促进数据处理者完善数据安全保护措施，提升数据安全保护能力；
f) 实现行业主管部门和数据处理者对信息系统数据安全总体态势的掌握。

7.2 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。当选取组织全部数据和数据处理活动作为评估范围时，根据需要采取“全面摸排、重点评估”的原则，宜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、数据处理活动等情况；
b) 依据 MH/T 3039—2025 附录 D 中给出的数据类别与级别，识别和整理安全监管数据、航空安全保卫数据、航空服务数据、机场工程数据、空中交通管理数据等，确定各类数据对应的业务系统与处理流程；
c) 针对已开展数据分类分级的组织，宜将涉及重要数据、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。

注：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。

评估范围信息见表1。填写说明见MH/T 3039-2025附录D，选择“是”的内容宜提供进一步的介绍。

表 1 评估范围信息表

数据名称	数据一级类别	数据二级类别	数据级别	数据载体	数据来源	数据量(GB或条)	数据处理者名称	数据安全责任部门	数据安全负责人	数据处理目的	是否出境	是否开展数据出境安全评估	是否涉及跨主体流动	信息系统名称	网络安全等级保护情况	是否为关键信息基础设施	是否开展过数据安全风险评估

7.3 组建评估团队

数据处理者开展自评估时，组织业务、安全、法务、合规、运维或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。

数据处理者委托第三方评估时，第三方评估机构能力见 GB/T 45389—2025 第 5 章。第三方评估机构在评估中获取的信息只能用于评估目的，不得泄露、出售或者非法向他人提供。

主管部门开展检查评估时，根据评估范围、涉及的民航业务特征、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。被评估方建立

评估专项工作团队，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。评估专项工作团队按照要求做好人员、设备、技术保障等工作，配合开展风险评估。

7.4 准备评估工具和过程文档

开展数据安全风险评估前期准备时，宜根据评估目标和评估范围，准备评估工具、建立评估文档。

a) 准备评估工具。准备数据安全风险评估工具，评估工具宜经安全认证合格或者安全检测合格。自主开发的评估工具及开源评估工具宜实施安全验证后方可使用。
b) 建立评估过程文档。针对评估目标、范围和内容，准备风险评估调研表、安全防护措施调研表等。在评估工作开展过程中，对评估工作相关文件进行统一编号，并规范管理。

7.5 制定评估方案

评估团队编制数据安全风险评估方案，方案内容宜包括但不限于如下方面。

a) 评估概述：包括评估目标、评估依据等内容。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》《中华人民共和国民用航空法》等法律，有关行政法规、司法解释；
   2) 国家网信部门及民航行业主管部门相关数据安全规章、规范性文件，如《民用航空安全管理规定》《民航数据管理办法（试行）》；
   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、民航行业标准等，如 MH/T 3039；
   5) 被评估方数据安全相关管理制度规范宜作为评估依据之一。
b) 评估范围：包括评估对象选择方法、评估对象描述等。
c) 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) 数据处理者从数据安全管理、数据处理活动安全、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，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) 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：包括评估时间进度安排、人员安排等。
f) 工作要求：包括评估工作要求、被评估方保障条件等内容，如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：包括采用的技术工具、测试内容、测试环境、应急措施等。测试方宜向被评估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。

评估团队可邀请民航领域相关数据安全、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。

8 信息调研

8.1 数据处理者调研

评估前宜对数据处理者的基本情况进行调研，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，例如运输机场、航空公司、空中交通管理等。
c) 是否属于特定类型数据处理者，例如民航政务数据处理者、民航安全监管类数据处理者、航空服务类数据处理者、民航关键信息基础设施运营者等。
d) 业务运营地区，开展数据处理活动所在国家和地区等。
e) 主要业务范围和业务规模等。

f） 数据处理相关服务取得行政许可的情况。
g） 被评估单位的资本组成和实际控制人情况。
h） 是否境外上市或计划赴境外上市及境外资本参与情况，或以可变利益实体架构等方式实质性境外上市。

8.2 业务和信息系统调研

业务和信息系统情况的调研内容包括但不限于如下方面。

a） 信息系统基本情况，包括网络规模、拓扑结构等情况和对外连接、运营维护以及是否为关键信息基础设施等情况。
b） 信息系统、APP 和小程序情况，包括系统功能、网络安全检查检测和测评情况、系统连接关系、数据接口、APP 及小程序名称和版本等。
c） 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。
d） 业务涉及个人信息、重要数据或核心数据处理情况。
e） 业务为国家和民航政务部门、第三方实体或境外用户提供服务情况。
f） 接入的外部第三方产品、服务或 SDK 的情况，包括名称、版本、提供方、使用目的、合同协议等。
g） 云平台、大数据、人工智能等新技术的使用情况。

8.3 数据资产对象调研

数据资产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，包括重要数据类别、规模、行业领域（如机场、航空公司、空中交通管理等）、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（如机场、航空公司、空中交通管理等）、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。

注：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。

8.4 数据处理活动调研

数据处理活动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、外部数据源和合同协议等。
b） 数据存储情况，如数据存储方式、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、存储期限和备份冗余策略等。
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、内部数据共享和数据接口等。
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、转换和标注等加工情况，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和共同处理的情况等。
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、敏感程度和保存期限等。
f） 数据公开情况，如数据公开的目的、方式、对象范围、数据种类和数据规模等。

g） 数据删除情况，如删除数据的类别、规模和删除方式等。
h） 数据出境情况，如民航旅客个人信息或重要数据出境，跨境业务、跨境办公、境外上市、使用境外云服务或数据中心和国际交流合作等场景的数据出境，数据出境安全评估实施等情况。

8.5 安全措施调研

已有安全防护措施调研内容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、态势感知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，具体包括：
1） 事件名称、发生原因、事件级别、涉及数据类型和规模、处置措施等；
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民航行业威胁事件、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。

9 风险识别

9.1 风险识别概述

从数据安全管理、数据处理活动安全、数据安全技术和个人信息保护四个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问题。评估实施时宜按照以下步骤开展。
a） 如果被评估方已开展过相关的测评工作，先对已开展的测评工作结论进行分析。
b） 针对评估对象的特点，选择适用的评估内容进行评估，评估内容选择方法如下：
1） 数据处理者识别数据安全管理（见 9.3）、数据处理活动（见 9.4）、数据安全技术（见 9.5）等方面风险问题；
2） 个人信息处理者在 1）的基础上，还宜对个人信息保护风险问题（见 9.6）进行识别，参考 GB/T 45574—2025、GB/T 45577—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） 评估对象涉及数据出境的，按照国家相关法律、法规、规章、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，并结合本文件第 10 章进行风险分析与评价。
c） 针对评估内容，采用评估手段和具体的评估方法，评估各项内容符合情况。
d） 梳理各评估项的风险识别结果，形成风险识别工作记录。

9.2 已开展测评情况分析

被评估方按照法律、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，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、商用密码应用安全性评估、个人

信息保护合规审计时，不再重复对9.4中涉及数据出境的评估内容、9.5中涉及网络安全防护与商用密码应用的内容、9.6中涉及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，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未通过法律、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、商用密码应用安全性评估、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。

9.3 数据安全管理评估

宜从数据安全管理制度、安全组织机构、数据分类分级管理、人员安全管理、数据合作授权管理和数据安全应急管理等方面识别数据安全管理风险。评估项宜符合A.1的规定。

9.4 数据处理活动评估

宜从数据收集安全、数据存储安全、数据传输安全、数据使用和加工安全、数据提供安全、数据公开安全和数据删除安全等方面识别数据处理活动安全风险。评估项宜符合A.2的规定。

9.5 数据安全技术评估

宜从网络安全防护、身份鉴别与访问控制、监测预警、数据加密、数据脱敏、数据防泄露、数据接口安全、数据备份与恢复和安全审计等方面识别数据安全技术风险。评估项宜符合A.3的规定。

9.6 个人信息保护评估

如评估范围涉及个人信息处理，宜从个人信息处理基本原则、个人信息告知、个人信息同意、个人信息处理、敏感个人信息处理、个人信息主体权利、个人信息安全义务、个人信息投诉举报等方面识别个人信息保护风险。评估项宜符合A.4的规定。

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

10 风险分析和评价

10.1 风险分析和评价概述

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问题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10.3.1和10.3.2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。

10.2 梳理风险问题清单

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问题，使用一个或多个风险问题分析其可能引发的数据安全风险，形成数据安全风险问题清单，见表2。

表 2　数据安全风险问题清单

序号	风险问题[a]	风险描述[b]	风险类型[c]	涉及的数据及类型、级别[d]	涉及的数据处理活动[e]

[a] 此项填写风险问题名称，也就是不符合评估项内容，如对于个人信息的标识，没有具体参数类型，如敏感、非敏感、公开、内部等。
[b] 此项参考本文件附录 B 填写实际数据风险情况。
[c] 此项参考本文件附录 B 填写数据安全风险类型。
[d] 此项填写某类风险中一个风险问题涉及的数据情况，参考 MH/T 3039-2025 填写数据类型和级别。
[e] 此项填写某类风险中一个风险问题涉及的数据处理情况，如数据收集、存储、使用和加工，涉及 100 万个人信息向境外提供的情况。

10.3　数据安全风险分析

10.3.1　风险危害程度分析

风险危害程度分析，主要考虑数据价值、风险问题严重程度等因素。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，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 MH/T 3039-2025 确定。个人信息规模和数据敏感程度宜作为数据价值判断的衡量因素。

b)　风险问题严重程度，主要考虑风险问题对数据处理者带来的危害程度。

数据安全风险危害程度的等级和描述见表3。

表 3　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，可能产生如下影响： 1）直接影响国家政治安全； 2）对民航领域生产运行产生特别严重危害； 3）直接影响人民群众航空出行秩序，影响多个地区的人民群众的航空出行，多个地区航空基础设施大面积瘫痪； 4）直接影响民航领域的经济利益安全，如涉及民航营业收入、产业生态、民航基础设施以及重大项目建设等； 5）直接导致特别严重突发卫生事件，造成社会公众健康的传染病疫情等特别严重影响公众健康的事件
高	一旦发生数据安全风险，可能产生如下影响： 1）对国家经济、社会、科技等安全产生危害； 2）直接导致严重突发事件、严重群体性事件、暴力恐怖活动等，对多个地区的航空出行秩序造成严重危害； 3）对民航领域生产运行、宏观调控、交通管理等产生严重危害； 4）对一个或多个省级行政区的民航领域经济运行造成严重危害，如导致民航企业等大范围停工停产、大规模机场基础设施长时间中断运行等； 5）导致民航企事业单位遭受行业监管部门特别严重处罚，或者影响民航领域重要/关键业务无法正常开展，造成经济或技术损失严重破坏机构声誉，企业面临破产； 6）导致严重突发卫生事件，造成社会公众健康的传染病疫情等严重影响公众健康的事件； 7）严重影响行业主管部门履行公共管理、服务、监管等职能

表3　数据安全风险危害程度等级（续）

等级	风险危害程度描述
较高	一旦发生数据安全风险，可能产生如下风险： 1）对民航领域经济运行、行业发展、投资建设等产生一般危害，对民航领域市场经济持续发展产生影响，如民航领域增长速度、市场占有率； 2）对一个或多个省级行政区的民航企业造成影响，如行业发展、技术进步和产业生态等造成危害； 3）直接导致突发事件、群体性事件等，对一个地区的社会秩序造成破坏，如因飞行动态数据异常引发的公共问题； 4）影响一个地区的人民群众的航空出行，多个地区航空基础设施大面积瘫痪； 5）导致民航企事业单位遭受行业监管部门严重处罚，或者影响民航领域部分业务无法正常开展，造成经济或技术损失破坏机构声誉； 6）航空出行过程中对个人造成严重的、不可消除的影响，容易导致自然人的人格尊严受到侵害或人身、财产安全受到危害； 7）直接导致突发卫生事件，造成社会公众健康的传染病疫情等影响公众健康的事件； 8）直接影响行业主管部门履行公共管理、服务、监管等职能
中	一旦发生数据安全风险，可能产生如下风险： 1）对民航领域发展、业务经营、技术进步、产业生态等造成一般危害，如受影响的企业持续时间短、社会负面影响较小； 2）对民航领域或地区经济运行造成一般危害； 3）直接影响人民群众的航空出行秩序，如某机场的公共交通停摆。直接影响民航领域企事业单位、社会团体的生产秩序、经营秩序； 4）对公共利益产生一般危害，影响小范围社会成员使用民航公共设施、获取公共数据资源等； 5）航空出行过程中，对个人造成较大影响，消除影响代价较大
低	一旦发生数据安全风险，可能产生如下风险： 1）对国家安全不造成影响或造成的影响可忽略不计； 2）对民航领域或地区经济运行造成轻微危害； 3）导致个别投诉事件，或在某一时间造成部分民航业务中断，使民航企业事业单位经济利益、声誉、技术等轻微受损； 4）对个人造成困扰，但尚可以克服

10.3.2　风险发生可能性分析

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

a）　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问题的有效性、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；

b）　风险问题发生频率，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，综合分析同类风险问题发生可能性。一般风险问题或安全事件发生频率越高，风险发生可能性越高；

c）　风险问题关联性，主要通过风险问题清单关联分析，发现多个风险问题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。

在综合分析风险问题发生频率、安全措施有效性和完备性、风险问题关联性的基础上，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4。等级越高代表措施完备性、有效性越低，风险越可能发生。如需进行定量分析，可参考C.2。

表 4　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相关风险事件。本单位、国内外民航单位多次高频发生同类安全事件，或容易与其他风险问题结合引发风险，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相关风险事件。本单位、国内外民航单位发生相关风险源，或有一定概率与其他风险问题结合引发风险，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，被评估对象或国内外类似业务的民航单位很少或在较苛刻条件下才会发生相关风险事件，或很难与其他风险问题结合引发风险，风险隐患发生可能性低（例如，几乎不可能发生，或仅可能在罕见和例外的情况下发生）

10.3.3　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、对民航领域生产运行产生特别严重危害的数据安全风险。

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，对民航领域生产运行、宏观调控、交通管理等产生严重危害，或严重影响行业主管部门履行公共管理、服务、监管等职能，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：一般指可能导致民航企事业单位遭受行业监管部门严重处罚，或者影响民航领域部分业务无法正常开展，造成经济或技术损失破坏机构声誉，或直接对自然人的人格尊严造成严重侵害或者人身、财产安全受到严重危害，或直接影响行业主管部门履行公共管理、服务、监管等职能，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：一般指可能对民航领域发展、业务经营、技术进步、产业生态等造成一般危害，或直接对自然人的人格尊严造成侵害或者人身、财产安全受到危害，或者直接影响人民群众的航空出行秩序，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：一般指可能对民航领域或地区经济运行造成轻微危害，或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5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，宜参考C.3进行风险评价。

表 5　数据安全风险评价矩阵

数据安全风险等级		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

10.3.4　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，风险问题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6。

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。

表 6　数据安全风险清单

序号	风险问题[a]	风险类型[a]	风险描述[a]	风险危害程度[b]	风险发生的可能性[c]	风险等级[d]	涉及的数据及类型、级别[a]	涉及的数据处理活动[a]

[a] 序号，风险问题，风险类型，风险描述，涉及的数据及类型、级别，涉及的数据处理活动，按照表 2 填写即可。
[b] 此项按照 10.3.1 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] 此项按照 10.3.2 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] 此项按照 10.3.3 获得的风险等级评价结果，填写风险等级，如高安全风险。

11　评估总结

11.1　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。评估报告准确、清晰地描述评估活动的主要内容（可附必要的证据或记录），提出可操作性的整改措施对策建议。风险评估报告包括以下内容。

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、数据业务流程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问题情况。
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）　数据安全风险问题清单，列出完整的数据安全风险问题清单，并附上关键记录和证据，若证据无法在附录中完整列出，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，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，评估报告由评估组长、审核人签字，并加盖评估机构公章。
k）　有关主管部门规定的其他报告内容。

11.2　数据安全风险处置

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，采取临时安全措施，防止数据安全事件发生。

民航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，按照国家或民航行业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。

11.3　残余风险分析和管控

被评估方按照风险安全整改建议全部或部分实施整改工作后，对仍然存在的安全风险进行识别、控制和管理的活动，包含以下内容。

a）　依据组织的风险评估准则进行残余风险评估，判断是否已经降至可接受水平以及是否产生新的次生风险，为风险管理提供输入。
b）　残余风险仍处于不可接受的风险范围内，则由被评估组织依据风险接受原则考虑是否接受此类风险或增加更多的风险控制措施。
c）　定期开展残余风险再评估，评估结果作为风险管理重要输入。

附 录 A
（资料性）
数据安全风险评估内容

A.1 数据安全管理

A.1.1 数据安全管理制度

A.1.1.1 数据安全制度体系

针对数据安全管理制度体系建设情况，重点评估如下方面：

a) 是否按照国家和民航行业要求，制定数据安全管理办法。管理办法需要包括数据安全总体策略、方针、目标和原则等内容；
b) 是否按照国家和民航行业要求，建立数据分类分级保护制度，制定数据分类和分级方法；
c) 是否按照国家和民航行业要求，建立数据安全应急处置制度；
d) 是否按照国家和民航行业要求，建立数据安全事件上报制度，明确上报流程、内容等要求；
e) 是否结合本单位实际，制定数据安全管理工作规划或工作方案；
f) 是否建立覆盖数据采集、传输、存储、使用、共享以及销毁等数据全生命周期的安全保护机制；
g) 是否建立关键岗位的数据安全管理操作规程。

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，重点评估如下方面：

a) 数据安全制度的制定、评审、发布流程建设情况。制度发布范围是否覆盖全面，发布方式是否正规、有效；
b) 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；
c) 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；
d) 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。对于发生的网络安全和数据安全事件，是否有明确的事件处置记录；
e) 是否按照国家和民航行业要求，制定数据安全风险评估指南或管理办法；
f) 重要数据处理者是否每年度对其重要数据的处理活动开展数据安全风险评估；
g) 重要数据处理者向民航行业主管部门报送的数据安全风险评估报告，是否包括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；
h) 重要数据处理者发生合并、分立、解散、破产等可能影响重要数据安全的，是否采取措施保障数据安全，并向有关部门报告重要数据处置方案。

A.1.2 数据安全组织机构

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，重点评估如下方面：

a) 是否设立由机构最高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；
b) 是否设立数据安全管理部门，成员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岗位，负责日常数据安全管理工作；
c) 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；
d) 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，重点评估如下方面：
a) 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；
b) 数据安全关键岗位设置情况，是否做到职责分离、专人专岗，岗位是否涵盖数据库管理员、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；
c) 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；
d) 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。

A.1.3 数据分类分级管理

A.1.3.1 数据资产管理

针对数据资产管理情况，重点评估如下方面：
a) 是否建立数据资产管理制度，是否开展数据资产识别并形成数据资产清单；
b) 数据资产的梳理范围是否覆盖到所有数据来源；
c) 是否通过数据资产管理工具形成了支持及时更新的数据资产清单；
d) 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；
e) 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；
f) 数据资产管理分为动态资产、静态资产，是否具备不同资产类型的识别能力与技术。

A.1.3.2 数据分类分级制度

针对数据分类分级保护制度建设情况，重点评估如下方面：
a) 是否按照数据分类分级保护制度和标准规范要求，开展数据分类分级工作，识别重要数据、核心数据，形成重要数据、核心数据目录；
b) 是否在相关制度中明确了数据分类管理、分级保护策略；
c) 数据分类分级变更和审核流程情况；
d) 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，重点评估如下方面：
a) 是否对处理的个人信息、重要数据和核心数据进行明确标识；
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) 按照民航数据分类分级标准规范和重要数据目录，评估本单位重要数据识别和重点保护的情况；

d） 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，重点评估如下方面：

a） 重要岗位员工录用前是否进行必要的背景调查，调查记录是否完整；

b） 数据安全关键岗位人员录用，是否对其数据安全意识或专业能力进行考核。

A.1.4.2 保密协议

针对保密协议签订情况，重点评估如下方面：

a） 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；

b） 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，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，重点评估如下方面：

a） 是否制定数据安全培训计划，并定期更新培训计划；

b） 是否对全体人员开展数据安全意识教育培训，并留存记录；

c） 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；

d） 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。

A.1.5 数据合作授权管理

A.1.5.1 合作方管理机制

针对合作方管理机制建设情况，重点评估如下方面：

a） 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；

b） 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。

A.1.5.2 合作协议约束

针对合作协议约束情况，重点评估如下内容：

a） 是否通过合同协议等方式对接收、使用本单位数据的合作方的数据使用行为进行约束；

b) 是否在合作协议中明确了数据处理目的、方式、范围、安全保护责任、保密约定及违约责任和处罚条款等。

A.1.5.3 合作方人员访问权限

针对合作方人员访问权限管理情况，重点评估如下方面：

a) 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；
b) 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；
c) 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；
d) 是否建立合作方人员现场服务安全管理体系，并确认是否按照相应的管理要求开展现场服务人员的身份验证、访问权限控制、现场行为监控等安全管理；
e) 对合作服务商的技术依赖程度是否在可控范围内，是否具备对授权处理数据的控制和管理能力。

A.1.5.4 合作方接入与数据回收

针对合作方接入与数据回收情况，重点评估如下内容：

a) 是否对合作方接入的系统、使用的技术工具进行了技术检测，避免引入木马、后门等；
b) 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) 合作服务到期后，是否进行对账号注销；
d) 是否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，是否按照规定要求，对外部人员远程访问操作系统或数据进行严格管理。

A.1.5.5 民航数据委托处理

涉及民航业务场景或针对法律、法规授权的具有管理公共事务职能的组织委托处理民航数据的情形，重点评估如下方面：

a) 委托他人建设、维护关键信息基础设施、承载重要及以上等级数据的信息系统，存储、加工航班运行、旅客信息、空中流量管理等数据，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) 航班运行、旅客信息、空中流量管理等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重要数据；
c) 支撑航班运行、旅客信息、空中流量管理等数据的相关系统运行的相关服务或系统的安全措施，是否满足数据分级保护的系统管理和相关安全要求。

A.1.6 数据安全应急管理

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，是否进行了处置、记录、整改和上报情况。记录需要包括事件名称、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，重大事件需要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) 近期公布或曝光的民航行业、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，重点评估如下内容：
a) 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；
b) 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；
c) 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；
d) 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；
e) 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；
f) 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民航有关主管部门报告。

A.2 数据处理活动安全评估

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，重点评估如下方面：
a) 是否存在窃取或者以其他非法方式获取数据；
b) 是否在法律法规规定的目的和范围内收集、使用数据；
c) 是否通过合同、协议等合法方式，从外部机构收集数据。

A.2.1.2 通过第三方收集数据

针对通过第三方收集数据情况，重点评估如下方面：
a) 是否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) 是否对从外部数据源获取的数据进行鉴别和记录；
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，重点评估如下方面：
a) 是否制定数据质量管理制度，明确数据质量管理要求；
b) 是否制定数据收集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；
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，重点评估如下方面：

a) 采用自动化工具收集数据时，是否违反相关法律法规或行业政策要求；
b) 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，是否存在收集与提供服务无关数据的情况；
c) 采用人工方式收集数据时，是否对数据收集人员严格管理，是否要求对收集数据直接报送到相关人员或系统，是否在收集任务完成后及时删除收集人员留存的数据；
d) 是否测试自动化工具收集数据对网络服务的影响。

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，重点评估如下方面：

a) 数据收集终端是否存在数据泄露风险；
b) 是否存在收集数据被未授权篡改、污染原始数据风险；
c) 是否制定对异常数据处理的规范文件,是否对收集的异常数据采取更正措施或手段；
d) 是否对数据收集过程进行监控、记录，以及采取相应的安全保护措施；
e) 是否对数据的真实性、准确性、完整性进行检验；
f) 是否对人工收集数据环境进行安全管控；
g) APP、Web 等客户端完成相关数据收集业务后，是否及时对缓存数据进行清理,是否留存敏感个人信息或重要数据。

A.2.2 数据存储安全

A.2.2.1 数据存储适当性

针对数据存储适当性，重点评估如下方面：

a) 是否按照数据分类分级和保护要求,对相应数据采取符合国家要求的密码算法进行加密存储或去标识化存储；
b) 是否制定了数据备份与恢复的策略和操作规程；
c) 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。

A.2.2.2 逻辑存储安全

针对逻辑存储安全情况，重点评估如下内容：

a) 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；
b) 是否采取一定措施确保数据存储的完整性，存储民航领域重要及以上数据时，是否采用密码技术、权限控制等技术措施保证数据完整性；
c) 在我国境内运营收集和产生的个人信息和重要数据是否存储在境内；
d) 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；
e) 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；
f) 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；
g) 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；
h) 永久存储数据类型是否必要，是否明确了永久存储的数据类型及对应的使用场景；

i） 是否对云上数据存放路径、数据量、获取方式以及丢失影响等内容进行梳理，云存储数据备份记录是否完整，是否具有云存储数据恢复相关制度和恢复演练记录；
j） 是否落实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；
k） 是否将脱敏后的数据与可用于恢复数据的信息分开存储；
l） 是否根据安全级别对数据分级差异化存储。

A.2.2.3 存储介质安全

针对存储介质安全情况，重点评估如下内容：
a） 是否制定存储介质的安全管理制度，是否明确对存储介质、存储数据的安全要求；
b） 是否对存储介质进行定期或随机性安全检查,是否对存储介质访问和使用行为进行审计。

A.2.3 数据传输安全

A.2.3.1 数据传输链路安全性

针对数据传输链路安全性，重点评估如下内容：
a） 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；
b） 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；
c） 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；
d） 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；
e） 是否针对数据传输、接收的情况进行记录与审计；
f） 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；
g） 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。

A.2.3.2 数据传输链路可靠性

针对数据传输链路的可靠性，重点评估如下内容：
a） 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；
b） 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。

A.2.4 数据使用和加工安全

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，重点评估如下方面：
a） 是否遵守法律法规，尊重社会公德和伦理，遵守商业道德和职业道德；
b） 是否存在危害或损害国家安全、经济运行、社会秩序、公共利益、组织权益和个人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) 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。

A.2.4.2 数据正当使用

针对数据正当使用情况，重点评估如下内容：

a) 是否有数据使用加工安全策略和操作规程的建设；
b) 数据使用行为是否与承诺或用户协议一致；
c) 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；
d) 数据是否分级，并对重要数据、核心数据、敏感数据采取对应级别保护措施；
e) 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；
f) 是否存在敏感数据未脱敏使用的情况；
g) 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；
h) 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；
i) 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。

A.2.4.3 数据导入导出

针对数据导入导出情况，重点评估如下方面：

a) 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审计措施；
b) 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；
c) 是否定期对个人信息和重要数据导出行为进行安全审计。

A.2.4.4 数据处理环境

针对数据处理环境安全情况，重点评估如下内容：

a) 数据处理环境是否配备安全管控手段，并定期清查风险；
b) 大数据平台等处理组件是否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，重点评估如下内容：

a) 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，至少每半年对访问权限规则和已授权清单进行 1 次复核，及时清理已失效的账号和授权；
b) 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；
c) 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；
d) 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；
e) 是否建设数据防泄露；
f) 是否在数据使用加工过程中采取数据脱敏、水印溯源等安全保护措施；
g) 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；

h) 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进行记录,并定期审计，是否对高风险行为审计及回溯；
i) 委托处理、共同处理网络数据的目的、方式、范围等是否合法、正当、必要；
j) 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，重点评估如下方面：
a) 提供、委托处理、共同处理数据，以及数据处理接收方处理数据的目的、方式、范围是否合法、正当、必要；
b) 是否对数据接收方的诚信、守法等情况进行了调查或了解；
c) 数据提供是否遵守法律法规和行业监管政策要求，是否存在非法买卖、提供他人个人信息或重要数据行为；
d) 对外提供的旅客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，重点评估如下方面：
a) 是否建设数据提供安全策略和操作规程；
b) 是否存在未按要求进行审批的情况；
c) 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；
d) 开展共享、交易、委托处理、共同处理、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；
e) 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；
f) 是否向境外执法机构提供存储于境内的数据和个人信息；
g) 核心数据跨主体流动前是否经国家数据安全工作协调机制评估和批准。

A.2.5.3 数据提供技术措施

针对数据提供技术措施情况，重点评估如下方面：
a) 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；
b) 对外提供的敏感数据是否进行加密及加密有效性；
c) 对共享数据及数据共享过程的监控审计情况；
d) 对外提供数据时是否采取签名、添加水印等安全措施；
e) 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；
f) 数据提供是否存在多方安全计算，联邦学习等技术。

A.2.5.4 数据接收方

针对数据接收方情况，重点评估如下方面：
a) 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，被民航行业各级管理部门处罚等；
b) 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；
c) 是否存在超时、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；

d) 是否对数据接收方的数据安全保护能力进行了审查,验证数据接收方在接收数据后不降低现有数据安全保护水平;
e) 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。

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，重点评估如下方面：

a) 数据进行转移时，是否向民航主管部门报备；
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。

A.2.5.6 数据出境安全

针对数据出境安全情况，重点评估如下方面：

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，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；
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，重点评估如下方面：

a) 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；
b) 是否存在数据公开的安全制度、策略、操作规程和审核留存；
c) 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；
d) 公开的数据是否会存在聚合性风险。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，重点评估如下方面：

a) 是否对数据公开所涉及的安全风险进行评估；
b) 数据公开过程是否开展日志记录；
c) 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；
d) 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民航主管部门批准，涉及个人信息公开是否取得个人单独同意；
e) 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。

A.2.7 数据删除安全

A.2.7.1 数据删除管理

针对数据删除管理情况，重点评估如下内容：

a) 是否依照数据分类分级要求建立数据删除流程和审批机制，明确数据存储期限，并于数据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；
b) 是否建立用户数据删除需求的响应机制；
c) 是否建立用户或业务变更时的数据删除机制；
d) 是否建立数据删除审计机制；
e) 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；
f) 是否按照制定的数据删除策略和管理制度，及时、彻底地进行了数据删除；
g) 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、方式和要求及对应操作规程；
h) 缓存文件是否及时删除。

A.2.7.2 存储介质销毁

针对存储介质销毁情况，重点评估如下方面：
a) 是否存在存储介质销毁管理制度和审批机制；
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；
c) 是否妥善处置销毁的存储介质；
d) 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；
e) 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

对于与民航业务相关的即时通信、快递物流、网上购物、网络支付、音视频、保险、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 数据安全技术评估

A.3.1 访问控制

针对数据访问控制措施情况，重点评估如下方面：
a) 是否建立与数据类别级别相适应的访问控制机制，并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是否存在关联；
d) 是否具有数据访问权限申请、审批机制；
e) 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；
f) 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；
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。

A.3.2 监测预警

针对数据安全监测预警情况，重点评估如下内容：
a) 安全监测预警和信息报告机制的建设落实情况,是否明确对各类数据访问操作的日志记录要求、安全监控要求；

b) 是否建有数据安全监测预警管理信息系统,是否符合民航数据安全监测预警技术要求;
c) 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;
d) 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;
e) 是否具备对数据交换网络流量、API 脆弱性与泄露、违规进行安全监控和分析的能力，是否具备对异常流量和行为进行告警的能力;
f) 是否具备风险信息的获取、分析、研判、通报、处置能力;
g) 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根据泄露的数据进行溯源;
h) 是否具备采用 AI 大模型有效精准识别数据安全缺陷、漏洞等风险的监测预警能力。

A.3.3 数据脱敏

针对数据脱敏情况，重点评估如下方面:
a) 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;
b) 是否对数据脱敏处理的应用场景、处理流程及操作进行记录;
c) 是否具备静态数据脱敏和动态数据脱敏技术能力;
d) 航班信息处理、旅客出行服务、空中流量管理等应用场景的数据脱敏效果是否符合管理要求;
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.3.4 数据防泄露

针对数据防泄露情况，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) 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;
c) 数据防泄露技术措施是否有效。

A.3.5 数据接口安全

A.3.5.1 对外接口安全

针对对外接口安全情况，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) 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,跨系统,跨区域数据流动的安全控制措施满足相关制度要求。

A.3.5.2 接口安全控制

针对数据安全接口控制情况，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) 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；
c) 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；
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) 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；
f) 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；
g) 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.3.6 数据备份与恢复

针对数据备份与恢复情况，重点评估如下方面：
a) 数据备份恢复策略和操作规程是否建设落实；
b) 是否提供本地或异地数据灾备功能；
c) 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；
d) 是否定期开展数据备份恢复工作；
e) 是否定期开展灾难恢复演练。

A.3.7 安全审计

A.3.7.1 审计执行

针对数据安全审计执行情况，重点评估如下方面：
a) 是否具备安全审计能力；
b) 审计的实施情况；
c) 审计策略和要求的合理性，有效性是否符合管理要求；
d) 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；
e) 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。

A.3.7.2 日志留存记录

针对日志留存记录情况，重点评估如下方面：
a) 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安全审计和日志留存，日志留存不少于 6 个月；
b) 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；
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。

A.3.7.3 行为审计

针对数据安全行为审计情况，重点评估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。

A.4 个人信息保护安全评估

A.4.1 个人信息处理合法性评估

A.4.1.1 个人信息处理合法、诚信

针对合法、保护原则遵守情况，重点评估如下方面：

a) 是否存在通过误导、欺诈、胁迫等方式处理个人信息的情况；
b) 是否存在非法收集、使用、加工、传输他人个人信息的情况；
c) 是否存在非法买卖、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《中华人民共和国个人信息保护法》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。

A.4.1.2 个人信息处理正当、必要

针对正当、必要原则遵守情况，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。

A.4.2 个人信息告知

针对个人信息告知情况，重点评估如下方面：

a) 在处理个人信息前，是否按照《中华人民共和国个人信息保护法》的要求，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) 告知事项发生变更的,是否将变更部分告知个人；
e) 个人信息处理规则是否便于查阅和保存。

A.4.3 个人信息同意

针对个人信息同意情况，重点评估如下方面：

a) 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；
b) 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；
c) 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；
d) 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；
e) 因合并、分立、解散、被宣告破产等原因需要转移个人信息的，是否向个人告知接收方的名称或者姓名和联系方式；
f) 因合并、分立、解散、被宣告破产等原因需要转移个人信息的，接收方变更原先的处理目的、处理方式的，需重新取得个人同意。

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，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；
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，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，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，重点评估如下方面：

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,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；
d) 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，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，是否同时提供不针对其个人特征的选项，或者向个人提供拒绝方式；
c) 通过自动化决策方式作出对个人权益有重大影响的决定,是否明确就相应自动化决策方式予以说明,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。

A.4.4.7 个人信息公开

针对个人信息公开情况，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 敏感个人信息处理合法性

针对敏感个人信息处理的合法性，重点评估如下方面：

a) 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；
b) 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；
c) 处理敏感个人信息是否取得个人的单独同意；
d) 法律、行政法规规定处理敏感个人信息取得书面同意的，是否取得个人的书面同意；
e) 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；
f) 是否遵守法律、行政法规对处理敏感个人信息的规定，取得相关行政许可或者作出其他限制。

A.4.5.2 生物特征识别数据安全

针对生物特征识别数据安全情况，重点评估如下方面：

a) 在运输机场等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，及时删除身份鉴别过程中收集、使用的人脸相关数据，通过单独操作注册预留的，仅用于比对的生物特征模板除外；
e) 是否满足生物特征识别有关政策规定；
f) 是否按照规定情形进行删除或者匿名化处理个人的步态、基因、声纹等其他生物特征信息。

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，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，能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，是否能及时个人信息复制；
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，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，重点评估如下方面：

a) 个人信息处理者是否主动删除个人信息；
b) 个人信息处理目的已实现、无法实现或者未实现处理目的，相关个人信息不再必要时是否按要求删除；
c) 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；
d) 在个人撤回同意后，是否按要求删除相关个人信息；
e) 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。

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，重点评估如下方面：

a) 自然人死亡的，其近亲属为了自身的合法、正当利益，是否能就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；
b) 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；
c) 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；
d) 是否及时受理个人提出的注销账号、撤回授权等合理请求。

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，重点评估如下方面：

a) 是否落实个人信息保护内部管理制度和操作规程；
b) 是否实施个人信息分类管理，并产生效果；
c) 是否存在加密、去标识化等安全技术措施应用；
d) 是否合理确定个人信息处理的操作权限；
e) 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；
f) 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，重点评估如下内容：

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，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《中华人民共和国个人信息保护法》第五十六条规定；
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 3 年。

A.4.7.4 个人信息安全应急

针对个人信息应急措施部署情况，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；
d) 是否进行个人信息处理备案以及定期开展个人信息处理合规审查。

A.4.8 个人信息投诉举报

针对个人信息投诉举报情况，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，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

常见数据安全风险类型包括数据泄露风险、数据篡改风险、数据破坏风险、数据丢失风险等，见表B.1。

表 B.1 典型数据安全风险类型示例

序号	风险类型	风险描述
1	数据泄露风险	由于系统存在安全漏洞，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	由于系统存在安全漏洞，或者缺乏有效的安全措施、人员有意或无意操作等，导致数据被未授权修改、删除或插入等，从而影响数据完整性的风险
3	数据破坏风险	由于系统存在漏洞，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、数据主体被仿冒等风险
7	违法违规获取数据	违反法律、行政法规等有关规定，对数据进行不正当获取、收集的风险
8	违法违规出售数据	违反法律、行政法规等有关规定，对数据进行不正当出售、交易的风险
9	违法违规保存数据	违反法律、行政法规等有关规定，对数据进行逾期留存、违规境外存储等风险
10	违法违规利用数据	违反法律、行政法规等有关规定，对数据进行不正当使用、加工、委托处理的风险
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

表B.1　典型数据安全风险类型示例（续）

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	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	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	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	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）
数据安全风险评分方法

C.1 数据安全风险危害程度量化分析方法

结合10.2.1给出的数据安全风险危害程度定性分析方法，表C.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值，得分越高代表风险危害程度越高。

表 C.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%)

C.2 数据安全风险发生可能性量化分析方法

结合10.2.2给出的数据安全风险发生可能性定性分析方法，表C.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值，得分越高代表风险发生可能性越高。

表 C.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%)

C.3 数据安全风险量化评价方法

结合10.3.3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C.1和C.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：

$$R_i = \sqrt{\sigma_i \times V_i} \quad \text{(C.1)}$$

式中：

R_i——第 i 个风险评价分值；

σ_i——第 i 个风险危害程度赋值；

V_i——第 i 个风险发生可能性赋值。

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 37988 信息安全技术 数据安全能力成熟度模型
[5] GB/T 39335 信息安全技术 个人信息安全影响评估指南
[6] GB/T 43697 数据安全技术 数据分类分级规则
[7] JT/T 1547 交通运输数据安全风险评估指南
[8] T/ISC-0011 数据安全治理能力评估方法
[9] 中华人民共和国网络安全法
[10] 中华人民共和国数据安全法
[11] 中华人民共和国个人信息保护法
[12] 中华人民共和国民用航空法
[13] 关键信息基础设施安全保护条例（中华人民共和国国务院令 第745号）
[14] 网络数据安全管理条例（中华人民共和国国务院令 第790号）
[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 中华人民共和国工业和信息化部 中华人民共和国公安部 国家市场监督管理总局令 第9号）
[16] 数据出境安全评估办法（国家互联网信息办公室令 第11号）
[17] 民航数据管理办法（试行）（民航规〔2025〕9号）