电信领域数据安全风险评估规范

（标准号：YD/T 3956—2024）

1 范围

本文件规定了电信领域数据安全风险评估的原则、流程、方法及工具等。

本文件适用于电信领域重要数据和核心数据处理者、处理1000万人以上个人信息的数据处理者在中华人民共和国境内开展数据处理活动的数据安全风险评估。电信领域一般数据处理者对其数据处理活动的数据安全风险评估，也可参照本文件。

2 规范性引用文件

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

GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1 数据 data

任何以电子或者其他方式对信息的记录。

3.2 风险评估 risk assessment

风险识别、风险分析和风险评价的全过程。

[来源：GB/T 29246-2017，2.71，有修改]

3.3 **合规性评估** compliance assessment

评估数据处理活动是否符合法律法规、政策文件、标准规范等相关要求的过程。

3.4 **电信数据处理者** telecommunication data processor

取得电信业务经营许可证，且在电信数据处理活动中自主决定处理目的、处理方式的电信业务经营者。

注：本文件中的“电信数据处理者”简称为“数据处理者”。

3.5 **电信领域重要数据** key data in telecommunication field

特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的电信数据（包括原始数据和汇聚、整合、分析等处理中以及处理后的衍生数据）。仅影响电信数据处理者自身的电信数据一般不作为重要数据。

3.6 **电信领域核心数据** core data in telecommunication field

关系国家安全、国民经济命脉、重要民生、重大公共利益的电信数据（包括原始数据和汇聚、整合、分析等处理中以及处理后的衍生数据）。

3.7 **电信领域一般数据** general data in telecommunication field

其他未纳入重要数据、核心数据目录的电信数据。

3.8 **数据载体** data carrier

数据处理活动中使用的系统、平台、设备、媒介等。

3.9 **评估报告** evaluation report

评估机构根据评估规范的要求，在履行必要的评估程序后，对被评估对象出具的书面工作报告。

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
IP	网际互连协议	Internet Protocol
MAC	网络设备物理地址	Media Access Control
APP	移动应用程序	Mobile Application

5 概述

5.1 评估原则

电信领域数据安全风险评估工作遵循以下原则：

a) 规范性原则：指遵循电信领域行业相关要求开展数据安全评估工作；

b) 客观公正原则：指评估人员在评估活动中应充分收集证据，对评估对象实施的安全措施的有效性和可靠性做出客观公正的判断；

c) 可复现原则：指在相同的环境下，对同一评估对象，不同的评估人员依照同样的要求，使用同样的方法，对每个评估实施过程的重复执行都应得到同样的评估结果；

d) 可控性原则：在评估过程中，应保障参与评估的人员、使用的技术和工具、评估过程都是可控的;

e) 完备性原则:严格按照被评估对象所涉及的评估范围进行全面的评估;

f) 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降低到最低限度，不会对被评估对象涉及的应用、系统、网络运行产生显著影响;

g) 保密性原则：在实施评估过程中，应保护数据处理者的商业秘密不被泄露。

5.2 评估内容

电信领域数据安全风险评估包括合规性评估和安全风险分析两部分内容。合规性评估由正当必要性评估、基础性安全评估、数据全生命周期安全评估三部分组成,重点分析数据处理的目的、方式、范围以及保障能力等是否符合法律、行政法规要求；安全风险分析由风险源识别、安全影响分析、综合风险研判三部分组成，通过综合分析数据处理活动面临的威胁、所采取的保障措施情况以及发生数据泄露、损毁、丢失等安全事件后产生的影响范围、程度等因素，综合研判数据处理活动安全风险等级。电信领域数据安全风险评估可数据处理者自行组织,也可委托第三方评估机构开展。

6 风险评估流程

6.1 评估整体流程

电信领域数据安全风险评估的实施过程一般包括组建评估团队、确定评估范围、制定评估方案、实施风险评估、形成评估报告等内容。实施风险评估包括数据处理活动分析、合规性评估及安全风险分析三部分，具体流程见图1所示。

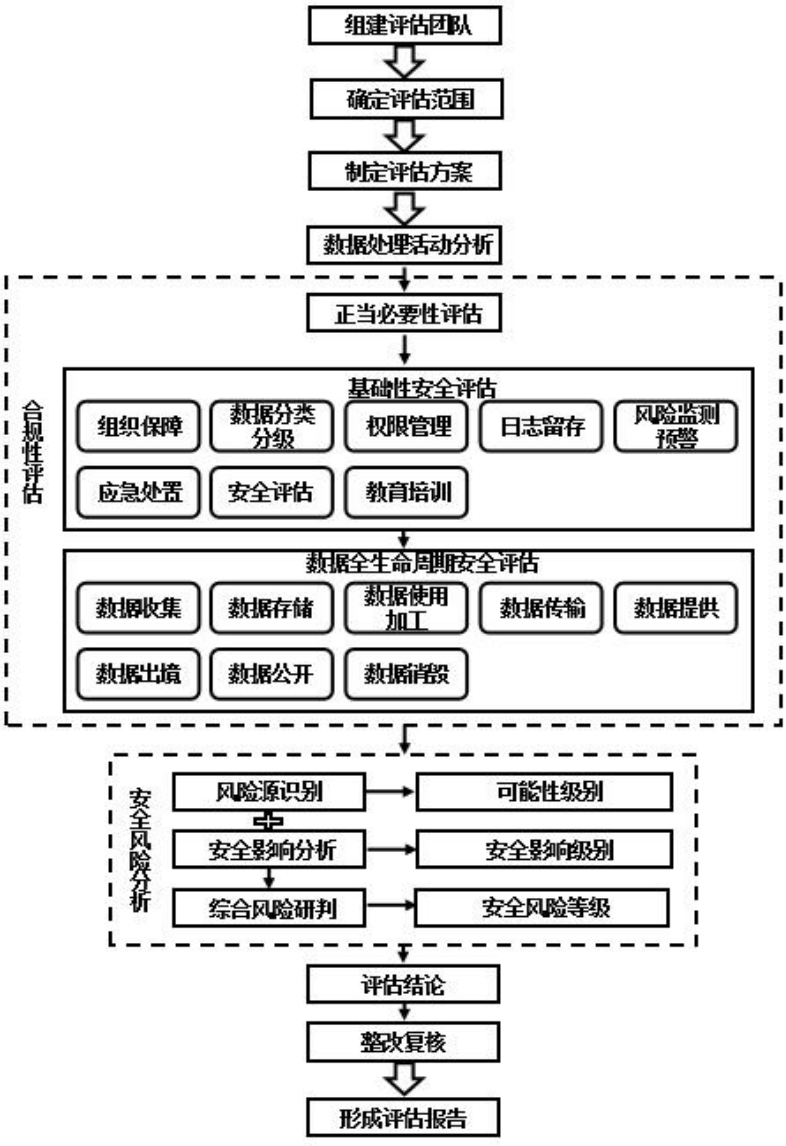

图 1 电信领域数据安全风险评估流程

6.2 组建评估团队

风险评估工作开展前，数据处理者应综合考虑组织规模、业务种类、数据数量、种类、涉及系统的复杂程度等因素，组建至少包括组织管理、业务运营、技术保障、安全合规等人员组成的评估团队，必要时可聘请相关专业的技术专家和技术负责人组成专家小组。评估团队原则上应具备不少于5名专业评估人员，包括1名评估团队组长、4名评估团队成员，其中至少4人应熟悉数据安全风险评估的方法和流程，掌握依据数据安全风险评估相关标准规范开展风险评估的能力，并取得工业和信息化领域数据安全风险评估相关技能评价证书。评估团队组长负责统筹安排评估工作分工，推进评估工作开展，组织完成评估结论、编写评估报告等。

委托第三方评估机构开展评估工作时，数据处理者应与被委托机构共同组建评估团队，确定评估团队组长和团队成员。同时，数据处理者还应指定本单位至少1名数据安全专业人员为评估工作对接人，负责协调本单位相应资源、对第三方评估机构相应工作进行管理和监督。此外，在评估工作开展前，数据处理者还应及时与被委托机构沟通，签订书面评估委托协议或评估合同，规范开展评估工作，保障数据处理者的安全生产运行和数据安全。

6.3 确定评估范围

评估团队应首先制定数据安全风险评估调研表并提供给数据处理者，通过发放调查表格、电话沟通等远程方式，或现场调研、会议等线下方式指导数据处理者完整、准确填写，实现对数

据处理者全部数据处理活动的充分调研，了解掌握数据种类、范围、处理方式以及相关信息系统的基本情况，确定评估范围。数据安全风险评估范围应覆盖数据处理者全部重要数据和核心数据，以及一定比例的一般数据。一般数据以抽样方式选取，抽样应尽量保证评估数据范围覆盖全部数据类别（二级子类）（可参考附录A），且数据载体避免重复。调研了解的信息内容包括：

a) 数据的种类、数量；

b) 处理数据的目的、方式、范围以及业务场景；

c) 支撑数据处理活动的信息系统描述，包括系统功能、系统架构、数据库、数据表、字段等，可对外传输数据的接口清单、按组件和接口划分的数据流示意图、数据处理涉及的数据流示意图；

d) 数据安全保障措施情况，包括管理制度建设及落实情况、技术手段建设及应用情况、数据安全管理机构人员设置及履职情况等；

e) 数据处理实施情况，包括数据操作方式（现场运行、外部托管、云外包等）、可接触到数据的人员范围及权限分配情况、数据存储位置、备份与恢复、留存时限、销毁计划与方式等；

f) 如涉及委托处理或共享、转让数据的，在合同或相关协议中应包括共享、转让的目的、方式、范围以及获取方身份、获取方数据安全保障情况、获取方接入信息系统

描述、安全责任划分情况等;

g) 其他评估过程中需要了解的内容。

6.4 制定评估方案

评估团队可根据实际需要制定风险评估工作方案。工作方案制定过程中，需与涉及数据处理活动的业务部门积极沟通，保障评估的可行性。评估方案包括：评估范围、评估依据、评估团队基本信息、工作计划、使用的评估工具情况、保障条件等。

6.5 实施风险评估

评估团队首先进行数据处理活动分析，识别数据处理者所有数据处理活动及各处理活动所对应的数据类型、名称、数量，处理数据的目的、方式、频率、涉及的获取方及信息系统情况等。然后开展合规性评估，包括正当必要性评估、基础性安全评估和数据全生命周期安全评估，研判合规性评估结果。之后进一步开展安全风险分析，通过风险源识别判断安全事件发生的可能性级别，结合安全影响分析结果，研判数据处理活动安全风险等级（分为极高、高、中、低四个等级）。在形成评估结论后，数据处理者应依据评估结论开展风险整改与复核。

6.6 形成评估报告

评估团队在完成实施风险评估后，经与数据处理者协商一致，根据评估结论形成评估报告，评估报告应包含数据处理者基本情况、评估团队基本情况、数据处理活动分析、合规性评估、安全风险分析、评估结论及应对措施等。

7 风险评估方法

7.1 人员访谈

评估人员通过与被评估数据处理者相关人员进行交流、讨论、询问等活动，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，以评估数据安全保障措施有效性。数据处理者需要安排熟悉数据流转过程，以及承载数据的应用、系统、网络情况的人员参加访谈。

7.2 资料查验

评估人员查阅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，用以评估数据安全管理相关制度文件是否符合标准要求。数据处理者需要事先完整准备上述文档以供评估人员查阅。

7.3 人工核验

数据处理者相关人员展示、演示，评估人员核查、验证承载数据的应用、系统、网络，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，以评估数据安全保障措施有效性。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。

7.4 工具测试

评估人员通过使用适当的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，以

评估数据安全保障措施有效性。数据处理者需要提前准备相关测试环境以保障工具的顺利接入与使用。工具检测前充分评估检测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。

8 实施风险评估

8.1 数据处理活动分析

不同业务、活动、场景下数据处理目的、方式、范围以及数据种类、数量等均不相同，为全面、科学地评估数据处理活动的综合安全风险，评估团队在正式开展风险评估前，应进行数据处理活动分析，识别数据处理者所有数据处理活动及各处理活动所对应的数据类型、名称、数量，处理数据的目的、方式、频率、涉及的获取方及信息系统情况等。为方便后续风险评估的实施，评估团队在开展数据处理活动分析时，可根据处理活动所涉及数据的级别分为一般数据处理活动分析、重要数据和核心数据处理活动分析，分别形成数据处理活动分析表。

8.2 合规性评估

8.2.1 概述

合规性评估包括正当必要性评估、基础性安全评估和数据全生命周期安全评估三部分，若正当必要性未满足，则合规性评估不通过。基础性安全评估和数据全生命周期安全评估每项评估结果可分为符合、部分符合、不符合、不适用，分别对应1分、0.5分、0分，以及不计算得分。针对基础性安全评估和数据全生命

周期安全评估指标项，若X为符合项数量，Y为部分符合项数量、Z为不符合项数量，则平均归一化算数分值=(X+0.5Y)/(X+Y+Z)。平均归一化算数分值小于0.7，则判定合规性评估不通过；平均归一化算数分值大于等于0.7且满足正当必要性，则判定合规性评估通过。合规性评估不通过的，可以直接判定安全风险分析中的风险源识别环节结果（可能性级别）为高。

8.2.2 正当必要性评估

评估团队应查验数据处理活动所涉及的业务说明、需求分析、合同协议、监管文件等能反映数据处理目的的相关文件，评估分析数据处理目的是否合理、正当，所涉及的数据数量、类型、频率是否为实现该目的下的最小范围。其中合理、正当的目的包括：

a) 合法开展业务所必需的；

b) 配合政府机构工作所必需的；

c) 开展合法科学研究所必需的；

d) 开展合法新闻报道所必需的；

e) 履行合同义务所必需的；

f) 保障公民合法权益、生命健康、财产安全等所必需的；

g) 履行法律法规所规定的义务所必需的。

8.2.3 基础性安全评估

8.2.3.1 组织保障

8.2.3.1.1 一般数据处理活动

评估团队应重点评估的内容包括：

a) 查验数据处理者数据安全岗位人员名单，是否根据需要配备一定数量的数据安全管理人员，岗位人员名单是否包括部门名称、姓名、联系方式和工作职责等;

b) 查验数据处理者数据安全管理制度文档，是否明确数据安全基础性管理和数据全生命周期各环节安全保护要求和操作规程；能覆盖数据分类分级、权限管理、日志留存、风险监测预警、应急响应、安全评估、教育培训等方面，并针对不同级别数据，明确数据生命周期各环节具体分级保护要求和操作规程；是否建立数据安全管理制度执行落实情况监督检查和考核问责制度，对数据处理活动进行安全监督管理，并协助电信主管部门开展工作。

8.2.3.1.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上,进一步开展以下评估工作:

a) 查验数据处理者数据安全管理体系与制度文档是否完备:

1) 是否建立完整的数据处理者数据安全工作体系,工作体系是否能覆盖涉及数据安全保护和数据处理活动的相关部门，联合各相关部门开展数据安全保护工作，明确各相关部门的责任与分工;

2) 是否明确数据安全管理机构,负责提出数据安全重大决策建议，定期组织召开数据安全相关工作会议，建立数据安全管理机构与相关部门的协作机制;

3) 是否在数据安全管理责任部门至少配备一名数据安全专职人员，相关执行部门至少配备一名数据安全责任人，负责组织开展部门内数据安全相关工作。

b) 查验数据处理者数据处理关键岗位职责说明文件或人员任命书内容是否完备:

1) 是否指定数据处理者法定代表人或者主要负责人为数据安全第一责任人，领导团队中分管数据安全的成员为直接责任人；相关岗位人员情况是否登记入册;

2) 相关岗位人员是否签署数据安全责任书或保密协议，内容包括岗位职责、相关义务、处罚措施、注意事项等。

8.2.3.2 数据分类分级

8.2.3.2.1 一般数据处理活动

评估团队应重点评估的内容包括:

a) 查验数据处理者数据分类分级管理制度，是否明确数据分类分级管理范围、数据分类分级原则、标准及变更流程等内容；是否综合考虑业务需求、数据来源和用途等因素，划分本单位数据类别；是否在数据分类的基础上，按照电信主管部门要求以及相关标准规范制定数据分级标准识别重要数据和核心数据，明确各级数据界限，包括具体类别、子类、范围、对应的数据等，是否针对不同级别的数据制定差异化的保护策略;

b) 查验数据处理者数据资产梳理相关制度文件，是否明确数据资产的安全管理目标和原则，是否明确数据资产的维护和使用责任，是否明确数据资产梳理手段方式，是否明确定期系统梳理电子化数据与其它方式记录的数据要求，是否明确数据存储情况梳理原则和梳理周期;

c) 查验数据处理者数据资产梳理记录、数据资产清单等有关文件是否完备:

1) 是否使用人工核对、自动化识别等方式，定期梳理本单位电子化数据与其它方式记录的数据，并留存梳理记录;

2) 是否覆盖数据处理者全范围，涵盖电子化数据与其它方式记录的数据，全面掌握数据处理者数据资产分布、迁移、资产异常等情况;

3) 是否按照电子化数据与其它方式记录的数据两类分别形成数据资产清单，并根据规范要求对已形成的数据资产清单进行定期更新，形成资产变更记录;

4) 是否针对数据规模大、挖掘价值高的一般数据实施动态管理，及时调整数据分级结果。

8.2.3.2.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上，进一步开展以下评估工作:

a) 查验数据处理者数据安全管理相关制度文件，是否明确重要数据和核心数据目录和目录备案管理要求;

b) 查验数据处理者是否按照相关法律法规、标准规范要求形成重要数据和核心数据目录;

c) 查验数据处理者备案登记记录，是否按照有关规定开展目录备案和备案变更工作，是否在备案内容发生重大变化时，在发生变化的三个月内履行备案变更手续。

8.2.3.3 权限管理

8.2.3.3.1 一般数据处理活动

评估团队应重点评估的内容包括:

a) 查验数据处理者数据访问权限管理制度，是否明确各部门和相关人员权限管理要求，是否建立数据内部登记、审批等工作机制，包括账号权限分配、开通、使用、变更、注销等审批流程和操作要求，重点关注账号权限变更、沉默账号、离职人员账号回收等情况;

b) 通过数据处理者演示账号生命周期管理流程，验证针对开发、测试、运维及运营人员等在创建和注销系统账号时，是否严格遵循系统账号创建和注销申请审批流程，并记录审批过程和结果；查验数据处理者涉及授权特定人员超权限处理数据的，是否采取多人审批授权或操作监督，是否留存审批并记录;

c) 查验数据处理者是否建立并定期更新数据处理相关系统权限分配表，是否对能够处理相关数据的业务系统账号进行定期梳理；按照业务需求、安全策略、权责明确原则和

最小授权原则等，合理界定本数据处理者的数据访问和处理权限，按照角色或用户组进行授权；是否对数据处理、数据安全管理、日志审计等岗位角色进行分离设置，是否严格控制超级管理员角色账号数量；

d) 查验数据处理活动有关平台系统，是否对涉及数据高风险操作的（如批量复制、批量传输、批量销毁等操作），采取多人审批授权或操作监督；

e) 通过技术验证数据处理活动有关平台系统是否配备账号安全管理措施，避免非授权账号访问处理数据：

1) 是否配置口令复杂度策略，如：口令长度不少于8位，使用大写字母、小写字母、数字及特殊字符中至少三种的组合，且与用户名-无相关性；

2) 是否配置账号锁定策略，对系统账号口令输入尝试次数进行限制；

3) 是否对口令遗忘的申请和重置流程实施严格管理。

8.2.3.3.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上，进一步开展以下评估工作：

a) 查验数据处理者数据访问权限管理制度、规程、记录，是否明确重要数据和核心数据处理权限审批和记录管理要求，是否严格控制权限范围；针对其它方式记录的数据，

是否实施单次授权，对数据处理、携带方式和区域范围等进行限定;

b) 演示权限管理系统配置策略，是否精细化配置数据访问处理权限，访问主体精确到用户、访问对象精确到文件或数据库表；是否设置账号最大使用期限;

c) 技术验证重要数据和核心数据处理活动有关平台系统权限管理技术措施是否完备:

1) 是否通过基于IP、MAC地址、服务路径等方式对所有接入重要数据和核心数据处理活动平台系统的用户或业务进行身份认证和权限控制;

2) 是否限制非正常登录次数，非正常登录场景包括异常时间登录行为、短时间内在不同IP地址段登录行为、非正常工作区域登录等;

3) 是否配置会话失效策略，在登录后长时间无操作状态下可自动退出;

4) 是否对登录的验证信息（例如口令鉴别信息）采取保护措施（如口令加密、时间戳等方式），防止重放性攻击，防止非授权的数据访问;

5) 是否存在可绕过账号登录的安全漏洞（例如远程代码执行漏洞）或者越权漏洞。

8.2.3.4 日志留存

8.2.3.4.1 一般数据处理活动

评估团队应重点评估的内容包括:

a) 查验数据处理者日志管理相关制度文件，是否明确日志管理要求，包括日志记录范围、留存时间、日志备份要求、日志审计职责划分、人员配备与审计频度等内容;

b) 查验数据处理者数据处理日志及系统运行日志记录，是否包括执行时间、操作账号、处理方式、授权情况、操作对象等，日志记录保存时间是否不少于6个月;

c) 查验数据处理者日志审计相关制度，是否结合数据处理场景明确审计策略，包括审计目的、审计对象、审计内容、审计操作规程、审计频度、审计结果、审计问题整改跟踪等;

d) 查验数据处理者日志审计报告，是否定期开展日志审计，形成审计报告，报告是否包含操作时间、操作主体、操作类型、操作对象、操作结果、审计问题、改进方案、异常情况处置记录等内容; 是否对审计发现问题进行整改跟踪。

8.2.3.4.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上,进一步开展以下评估工作:

a) 演示日志审计平台主要功能、配置策略等，是否具备日志审计技术能力，是否将本数据处理者重要数据和核心数据处理活动全量纳入审计范围;

b) 查验日志留存操作规范、日志记录等，是否对高风险操作的（如批量复制、批量传输、批量销毁等操作)日志进行备份，日志记录是否包含操作时间、操作账号、处理方式、授权情况、操作对象、数据量级具体操作语句等内容。是否对日志的备份文件定期进行完整性校验，以保证日志备份文件的可用性和真实性;

c) 查验日志审计制度规范、审计报告等，是否每半年对重要数据处理活动进行审计并形成审计报告，每季度对核心数据处理操作进行审计并形成审计报告。

8.2.3.5 风险监测预警

评估团队应重点评估的内容包括:

a) 查验数据处理者数据安全风险监测预警相关制度文件，是否明确数据安全风险监测预警工作负责部门，是否明确风险监测预警目的、方式、内容、操作规程、频度等内容，是否定期开展风险监测预警工作;

b) 查验数据处理者数据安全风险监测预警方案，是否明确风险监测预警工作职责分工、实施流程、处置措施及总结通报等内容。其中，实施流程是否对数据资产、数据处理活动、网络与系统设备、数据处理账号、内外部数据流动等实施监测巡查，对异常流动等行为进行排查预警与处置，形成处置记录;

c) 查验数据安全风险上报记录，是否按照有关要求对可能造成较大及以上安全事件的风险向本地区行业监管部门报告。

8.2.3.6 应急处置

8.2.3.6.1 一般数据处理活动

评估团队应重点评估的内容包括:

a） 查验数据处理者数据安全事件应急预案，是否充分考虑数据处理者涉及的各类数据安全事件业务场景，包括数据泄露（丢失）、数据被篡改、数据被损毁、数据违规使用等，是否根据事件等级明确应急响应责任分工、工作流程、处置措施等;

b） 查验数据处理者数据安全应急演练工作记录，是否制定数据安全事件应急演练计划；是否针对数据泄露（丢失）、数据被篡改、数据被损毁、数据违规使用等典型场景，至少每年开展一次演练，并做好演练记录；是否根据演练结果视情况优化本数据处理者数据安全保护措施，形成演练报告;

c） 查验数据处理者数据安全应急响应处置记录是否完备:

1) 是否在发生数据安全事件后，按照应急预案及时开展应急处置，采取数据恢复、关闭违规人员账号、下线相关系统接口等处置手段或补救措施;

2) 发生可能损害用户合法权益的数据安全事件，是否及时告知用户，并提供减轻危害措施；

3) 是否在事件处置完成后立即开展事件调查、问题整改、责任追究，在规定时限内形成报告，每年向本地区行业监管部门报告数据安全事件处置情况（未发生数据安全事件的无需上报）。

8.2.3.6.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上，进一步开展以下评估工作：

查验数据处理者数据安全应急响应处置记录，是否在发生重要数据和核心数据安全事件时，立即向本地区行业监管部门报告（未发生数据安全事件的无需上报）。

8.2.3.7 安全评估

8.2.3.7.1 一般数据处理活动

评估团队应重点评估的内容包括：

a) 查验数据处理者数据安全风险评估报告或自查记录，内容是否完善：

1) 是否包括数据处理者基本情况、评估团队基本情况、数据处理活动分析、合规性评估、安全风险分析、评估结论及应对措施等内容；

2) 是否对评估工作中发现的问题进行分析并明确对应问题所关联的风险，是否具有明确的风险或问题处理处置计划及对应的改进措施。

b) 查验数据处理者数据安全风险或问题跟踪记录，是否对评估或自查中发现的安全风险或问题进行实际整改或改进，是否对整改措施的有效性进行复核。

8.2.3.7.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上，进一步开展以下评估工作：

a) 查验数据处理者数据安全风险评估工作相关管理制度、操作规程、评估报告等，是否明确至少每年开展一次数据安全风险评估，评估范围是否覆盖全部重要数据和核心数据，以及一定比例的一般数据；

b) 查验数据处理者数据安全风险评估报送记录，是否在规定期限内向本地区行业监管部门报送风险评估报告。

8.2.3.8 教育培训

8.2.3.8.1 一般数据处理活动

评估团队应重点评估的内容包括：

a) 查验数据处理者数据安全岗位人员教育和培训计划，培训内容是否涵盖数据安全法律、行政法规、标准规范、数据处理者数据安全管理制度和工作要求、数据安全领域知识技能、数据安全保护意识等；

b) 查验数据处理者数据安全岗位人员教育培训工作记录（如培训计划、通知、议程、课件、签到表、考核记录等），培训对象是否覆盖数据处理者数据安全岗位人员，年度培训时长是否不少于10学时，培训后是否组织对培训内容进行考核评定，并留存考核评定记录。

8.2.3.8.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上，进一步开展以下评估工作：

查验数据处理者重要数据和核心数据处理岗位人员教育和培训计划，是否针对重要数据和核心数据处理岗位定期开展全员教育和培训，培训内容是否额外包括重要数据和核心数据安全管理要求、安全操作规程等，年度培训时长是否不少于20学时。

8.2.4 数据全生命周期安全评估

8.2.4.1 数据收集

8.2.4.1.1 一般数据处理活动

评估团队应重点评估的内容包括：

a) 查验数据处理者数据收集相关制度文件，管理要求是否完备：

1) 是否明确应遵循合法、正当原则，结合本数据处理者产品或服务业务功能需要开展数据收集活动；

2) 是否明确数据收集渠道、数据格式、收集流程和收集方式、存储期限，不得窃取或者以其他方式非法收集数据。

b) 查验数据处理者具体业务用户协议或隐私政策文件，是否明确个人信息收集的目的、用途和范围，是否按照公开透明原则，将收集规则以通俗易懂、简单明了的文字向用户明示并获得授权。

8.2.4.1.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上,进一步开展以下评估工作:

a) 查验数据获取协议、承诺书等，是否针对间接途径获取的重要数据和核心数据的活动，是否与数据提供方签署协议、承诺书等，明确数据合作范围、目的、方式，以及双方应承担的安全责任等;

b) 查验数据处理者数据收集相关系统配置策略，是否根据数据安全级别采取相应的安全措施（如防火墙、入侵检测系统、入侵防御系统、白名单接入控制等）防止数据收集设备遭受网络攻击，保障采集过程中数据不被泄露;

c) 技术验证数据收集设备安全技术措施的有效性，技术能力是否完备:

1) 是否采用口令鉴别、生物鉴别、图片验证码、短信验证码、证书鉴别等至少两种以上的方法对接入用户进行身份认证和访问控制;

2) 是否配置口令复杂度策略，如口令长度不少于8位，使用大写字母、小写字母、数字及特殊字符中至少三种的组合，且与用户名、字符顺序无相关性;

3) 是否配置账号锁定策略，对系统账号口令输入尝试次数进行限制;

4) 是否对口令遗忘的申请和重置流程实施严格管理，口令重置流程是否存在业务逻辑设计缺陷，是否留存申请和重置记录。

d) 查验数据收集记录，是否记录数据收集来源、时间、类型、数量、频度、流向等内容。

8.2.4.2 数据存储

8.2.4.2.1 一般数据处理活动

评估团队应重点评估的内容包括:

a) 查验数据处理者数据存储环节相关制度文件，内容是否完备:

1) 是否结合数据分类分级策略和管理要求明确数据存储安全策略和操作规程，包括各类数据存储平台系统差异化的安全存储措施（如加密、访问控制等）、数据存储介质安全策略和管理规定等;

2) 是否明确对数据存储系统账号权限管理、访问控制、日志留存等方面的安全要求。

b) 查验数据处理者与数据存储系统管理和运维人员签订的保密协议或数据安全责任承诺书，是否明确数据使用范围、操作权限、违约责任等，有效约束相关人员行为；

c) 查验数据存储系统核心功能、安全配置策略等，是否落实差异化的安全存储要求，是否配备对用户或业务（应用程序）的访问控制措施，避免非授权访问。

8.2.4.2.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上，进一步开展以下评估工作：

a) 查验数据处理者重要数据和核心数据备份恢复相关管理制度，是否制定重要数据和核心数据容灾备份的规范和操作规程，明确规定数据容灾备份的周期、备份方式、备份地点等；

b) 查验数据存储系统安全配置策略，是否配备校验技术、密码技术等安全防护措施进行安全存储，是否提供重要数据和核心数据容灾备份的安全防护能力，是否定期开展数据恢复性测试，对备份数据的有效性和可用性进行检查和恢复验证；

c) 查验数据处理者数据存储介质（含云存储形态与终端存储形态）管理制度，是否明确数据存储介质的获取、使用、维护、升级、标记和销毁等流程和审批记录要求，是否明

确数据存储介质获取渠道、格式化规程、资产标识规程等要求。

8.2.4.3 数据使用加工

8.2.4.3.1 一般数据处理活动

评估团队应重点评估的内容包括:

a) 查验数据处理者数据使用加工管理制度，相关要求是否完善:
   1) 是否符合国家相关法律法规对数据使用和分析处理的目的和范围的要求;
   2) 是否结合数据分级保护原则,明确数据使用安全策略和操作规程;
   3) 是否制定数据使用审批流程、数据使用结果发布、安全保护规则，以及相关人员岗位职责等。
b) 查验数据处理者数据导出规程、工作记录等，是否明确导出场景、导出范围，以及相应的审批规则，是否明确要求导出的数据类型及数量为当前处理活动场景所必需的最小数据集。

8.2.4.3.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上,进一步开展以下评估工作:

a) 查验数据处理者使用加工制度文件、操作规程、工作记录等，是否从账号身份管理原则、身份凭证保护、最小授权

原则、数据权限默认设置、权限申请和审批等方面提出数据使用安全管控要求:

1) 是否对数据安全管理人员、数据使用人员、日志审计人员的角色进行分离设置,为内部人员分配完成职责所需的最小数据使用权限;
2) 涉及授权特定人员超权限处理数据的,是否由数据安全责任人进行审批并记录;
3) 是否及时清除数据处理活动相关平台系统中测试账号、默认账号，杜绝多人共用同一系统账号的情况。

b) 查验数据脱敏处理管理规范或制度文件，是否明确数据脱敏应用场景，以及相应的脱敏规则、方法、流程等:

1) 是否明确在数据权限和资源申请阶段,针对不同的数据脱敏需求，明确数据脱敏规则及方法;
2) 是否建立数据脱敏处理技术应用安全评估机制,对脱敏后的数据可恢复性进行安全评估,是否对于可恢复形成原始数据的脱敏方法（含算法）进行安全加固;
3) 是否使用脱敏的数据开展业务系统的开发测试。

8.2.4.4 数据传输

8.2.4.4.1 一般数据处理活动

评估团队应重点评估的内容包括:

a) 查验数据处理者数据传输相关制度文件、操作规程，相关要求是否完善:

1) 是否根据法律法规、业务需求、业务系统可用性、建设成本等要求，明确网络安全域划分策略，以及相应的数据安全防护策略;
2) 是否结合数据分类分级策略和管理要求明确制定不同网络区域间数据传输安全保护规则，如访问控制、加密等。

b) 查验数据处理者数据传输的安全防护技术措施的落实情况，是否针对不同网络安全域之间的数据传输采取如校验等安全防护技术措施。

8.2.4.4.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上,进一步开展以下评估工作:

a) 查验数据处理者数据传输审批工作机制，是否对跨主体或使用互联网传输重要数据和核心数据的情形进行前置审批;
b) 技术验证数据处理者在安全边界部署的安全管控技术措施，是否配备数据访问控制、身份认证措施，实现数据传输过程的审批管理:
1) 是否有审批限制，审批通过后数据可传输，审批未通过不可传输;
2) 是否留存审批的日志。

a) 查验数据处理者数据加密相关制度文件或内部标准、技术措施等，是否依据传输数据级别，明确提出相匹配的数据加密要求（数据加密、数据签名、散列等）;

b) 技术验证数据传输安全措施的有效性，是否在传输重要数据时，采取校验技术、密码技术、安全传输通道或者安全传输协议等安全措施保证传输数据的安全性;

c) 查验数据处理者数据接口安全规范、操作规程等，相关要求是否完善:

1) 是否明确规定使用数据接口的安全限制和安全控制措施等;

2) 是否采取访问控制、签名等措施；针对跨安全域的数据接口，是否采用安全通道、传输加密、时间戳等措施。

d) 查验数据处理者的安全接口清单，是否定期更新，包括接口名称、接口参数、对端业务系统、接口方式等相关内容;

e) 查验数据处理者接口认证鉴权技术能力核心功能、配置策略等，是否能够通过MAC地址、IP地址或端口号绑定等方式限制非授权或违规设备接入，是否具备接口安全监测能力，能够发现非授权或违规设备、系统接入，并及时进行告警和处置。

8.2.4.5 数据提供

8.2.4.5.1 一般数据处理活动

评估团队应重点评估的内容包括:

a) 查验数据处理者数据提供相关制度文件，是否区分数据提供场景，对应不同的数据提供场景建立相应的数据提供安全策略和操作规程，明确数据提供范围、类别、条件和程序；

b) 查验数据处理者数据提供清单，是否包含获取方数据处理者名称、联系人信息，以及提供形式、期限、涉及的业务或系统、数据安全保护措施等内容，是否定期对清单进行更新；

c) 查验数据处理者数据提供服务合同或协议，是否按照最小必要的原则规定数据获取方可接触到的数据范围、使用权限、用途等，是否明确数据获取方的数据安全保护责任。

8.2.4.5.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上，进一步开展以下评估工作：

a) 查验数据处理者数据提供相关制度文件，是否明确对重要数据和核心数据获取方安全能力进行核验，并签署数据安全协议；

b) 查验数据处理者针对数据获取方的安全管理记录，是否对数据获取方的资质和数据安全保护能力进行核验，是否签署数据安全协议，明确双方数据安全保护责任；

c) 查验重要数据和核心数据提供相关记录、操作规程等，是否对提供的重要数据和核心数据进行脱敏处理；对于无法

脱敏的，是否采取校验技术、密码技术、安全传输通道、安全传输协议等安全保障措施；跨主体提供核心数据时，是否已评估安全风险，采取必要的安全保护措施，是否由本地区行业监管部门审查后报工业和信息化部。

8.2.4.6 数据出境

评估团队应重点评估的内容包括:

a) 查验数据处理者数据出境活动清单、数据出境安全评估报告等。是否按要求开展数据出境风险评估，评估结果是否在有效期内，评估内容是否包括数据出境的规模、范围、种类、敏感程度，以及数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险等；是否向国家网信部门申报数据出境安全评估，并获得批准;

b) 查验数据处理者与境外获取方订立的合同或者其他具有法律效力的文件，是否充分约定了数据安全保护责任义务、境外获取方承诺承担的责任义务、以及履行责任义务的管理和技术措施、能力等；是否建立通畅的个人信息权益维护渠道；是否采取加密等技术措施保障数据出境安全。

8.2.4.7 数据公开

8.2.4.7.1 一般数据处理活动

评估团队应重点评估的内容包括:

a) 查验数据处理者数据公开相关制度文件，是否明确数据公开范围、类别、条件和流程，明确可能对国家安全、公共

利益产生影响的数据，不得公开，是否区分数据公开场景，对应不同的数据公开场景建立相应的数据公开安全策略和操作规程；

b) 查验数据处理者数据公开相关业务系统的审批记录，是否具有数据公开的审批流程，明确审批重点内容、审批记录留存要求，公开数据的具体内容是否仅满足业务场景需求且未超出授权范围；

c) 查验数据处理者数据公开记录、风险评估报告等，是否在数据公开前开展数据安全风险评估。

8.2.4.7.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上，进一步开展以下评估工作：

a) 查验数据处理者重要数据公开相关制度文件，是否区分重要数据公开场景，对应不同的数据公开场景建立相应的数据公开安全策略和操作规程，明确重要数据公开范围、内容与有效控制机制；

b) 查验数据处理者重要数据公开相关制度文件，是否建立重要数据公开脱敏机制，明确对于法律、行政法规要求公开的数据场景（如网站、APP、业务登记单、显示屏幕等展示场景），应采用静态脱敏等措施防止发生敏感数据泄露和滥用。

8.2.4.8 数据销毁

8.2.4.8.1 一般数据处理活动

评估团队应重点评估的内容包括:

a) 查验数据处理者数据销毁相关制度文件，是否结合数据分类分级管理制度和安全需求，建立数据销毁安全策略和操作规程，明确销毁对象、销毁原因（如在数据业务下线、用户退出服务、节点失效、过多备份、数据试用结束、数据超出保存期限等情况）和销毁流程、数据销毁技术处理策略等;

b) 查验数据销毁工具，是否对不同类型的存储介质（闪存、移动硬盘、固态硬盘、硬盘、磁带、光盘等），提供不同的销毁措施。如针对用户注销服务、存储介质维护需要带出机房等场景可采用多遍覆盖、删除密钥、执行固件擦除命令等安全数据删除方式，针对介质报废等场景，可采取高压击穿、消磁、粉碎等物理损毁手段;

c) 查验数据处理者数据销毁工作记录，是否对销毁后所涉及的资源进行回收，包括账号、物理资源、云资源、系统存储空间、数据共享途径等，并对销毁过程进行记录。

8.2.4.8.2 重要数据和核心数据处理活动

在上述一般数据处理活动安全评估的基础上,进一步开展以下评估工作:

a) 查验数据处理者数据销毁相关制度文件是否设置销毁相关监督角色，监督操作过程;

b) 查验数据处理者数据销毁相关工作记录是否针对数据销毁建立完善的操作审批机制，采用多人操作模式，限制单人拥有完整操作权限;

c) 查验数据处理者数据销毁相关制度文件否明确重要数据和核心数据销毁后，不得以任何理由、任何方式进行恢复;引起备案内容发生变化的，是否履行备案变更手续。

8.3 安全风险分析

在完成合规性评估后，应进一步对其数据处理活动的安全风险进行分析研判，并及时开展风险处置，保障安全风险可控。安全风险分析主要包括风险源识别、安全影响分析以及综合风险研判三部分，具体实施流程见图2所示。

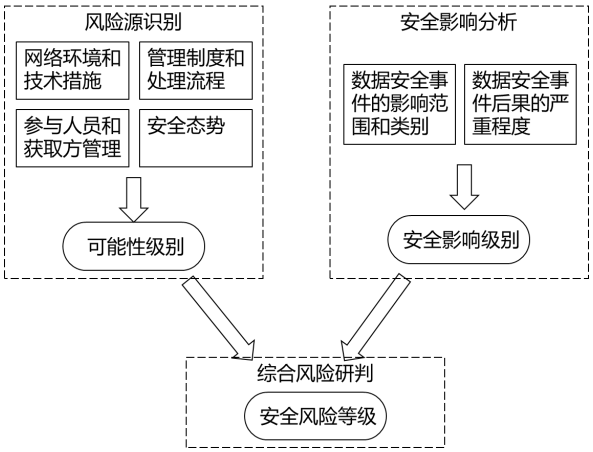

图 2 电信领域数据安全风险分析实施流程

8.3.1 风险源识别

8.3.1.1 识别范围概述

风险源识别是根据数据处理活动面临的威胁、系统的脆弱性、采取的安全措施等因素，研判数据安全事件发生的可能性级别。

与数据安全事件发生可能性相关的要素可归纳为网络环境和技术措施、管理制度和处理流程、参与人员和获取方管理、安全态势等四个方面。网络环境和技术措施包括处理数据的网络环境、信息系统部署位置、安全防护策略及设备、运行状态监测记录、数据泄露监测预警与拦截处置、检查评估及渗透测试、数据识别、数据加密、介质管理、数据备份与恢复、销毁管理、日志审计等情况；管理制度和处理流程包括数据安全管理制度建设、重点环节日志留存、数据安全风险监测报送、数据安全事件应急响应、内部审批登记机制建立等情况；参与人员和获取方管理包括数据安全管理机构设立、人员培训和考核、人员职责明确、人员权限管理、数据获取方管理等情况；安全态势包括曾经发生过数据安全事件情况、受到数据安全监管处罚情况、收到数据安全风险预警信息情况等。

8.3.1.2 网络环境和技术措施

评估团队可参考以下因素开展评估：

a) 处理数据的网络环境是否为内部网络；

b) 处理数据的信息系统是否与其他系统隔离，是否与其他系统存在数据交互，交互方式是否为网络接口，是否存在未鉴权、未认证接口，是否配备接口安全保障措施，如身份验证、流量监控、数据加密等；

c) 数据处理过程中是否实施严格的访问控制、权限管理等；

d) 处理数据的信息系统边界是否部署安全防护设备，配置严格的安全防护策略，实现对网络攻击、入侵、木马病毒等的拦截防护;

e) 是否监测和记录网络运行状态，是否标记、分析数据流转状态，及时发现数据异常流量和违规使用等情况;

f) 是否配备数据防泄露技术能力，全面覆盖处理数据的系统和终端，实现对网络、蓝牙、USB、邮件等多渠道的数据泄露监测预警与拦截处置;

g) 是否定期对处理数据的信息系统进行安全检查、评估、渗透测试等，并及时进行补丁更新和安全加固，是否有效防范信息系统漏洞;

h) 处理重要数据、核心数据的信息系统是否具备重要数据、核心数据识别能力，能够对重要数据、核心数据进行有效、准确的识别发现;

i) 是否采用加密传输、加密存储等方式保障重要数据、核心数据安全，加密方式是否安全有效;

j) 是否对存储数据的介质进行加强管理，根据数据级别设置相应的审批管理机制，针对重要数据和核心数据实施多级权限审批管理，禁止非相关人员接触，并严格留存使用记录;

k) 是否对数据进行定期备份与恢复，备份方式是否安全可靠，是否实现重要数据和核心数据容灾备份，保障数据可用性;

l) 是否配备数据销毁技术手段，保障重要数据、核心数据销毁后的不可恢复;

m) 是否制定数据日志审计策略，明确审计方法、内容、流程等要求，实现对重要数据、核心数据收集、存储、传输、使用、提供、公开、销毁等环节的实时审计，并对异常操作进行预警。

8.3.1.3 管理制度和处理流程

评估团队可参考以下因素开展评估:

a) 是否根据数据级别建立完备的数据管理制度，覆盖数据全生命周期，明确重要数据、核心数据目录备案，以及数据安全风险评估、权限管理、日志留存、风险监测预警、获取方管理、应急响应、教育培训等相关管理要求;

b) 是否对数据授权访问、批量复制、使用加工、出境、销毁等重点环节进行日志留存，留存时间是否不少于6个月，涉及出境环节日志记录是否按照国家有关规定留存;

c) 是否建立数据安全风险监测报送机制，及时发现、识别和报送数据安全风险;

d) 是否建立数据安全事件应急响应机制，制定应急预案和处置流程，定期开展应急演练;

e) 是否建立内部审批和登记等工作机制，对重要数据和核心数据处理活动进行严格管理并留存记录。

8.3.1.4 参与人员和获取方管理

评估团队可参考以下因素开展评估：

a) 是否配备数据安全管理人员，统筹负责数据处理活动的安全监督管理；

b) 是否建立数据获取方管理制度，形成获取方管理台账，加强对获取方数据使用情况的监督管理；

c) 重要数据、核心数据处理者是否设立数据安全管理机构，明确内部数据处理关键岗位、职责以及任职要求，负责履行数据安全管理义务；

d) 重要数据、核心数据处理者是否对数据处理关键岗位从业人员进行数据安全相关培训和考核，保障其有相应的数据安全保护专业知识和技能，能够全面了解掌握数据安全政策法规有关要求；能够合理正确使用、配置组织配备的重要数据安全防护技术工具；

e) 重要数据、核心数据处理者是否与数据处理关键岗位从业人员签订署数据安全责任书，责任书内容包括数据安全岗位职责、义务、处罚措施、注意事项等内容；

f) 重要数据、核心数据处理者数据处理关键岗位人员权限是否进行区分，是否通过有效手段限制不同身份数据处理者权限；

g) 重要数据、核心数据处理者是否与涉及处理重要数据、核心数据的获取方签署数据安全保护合同或协议，明确获取处理使用重要数据的目的、方式、范围、留存期限、超期

处理的方式、再转移限制、安全保障措施以及相应的责任义务;

h) 重要数据、核心数据处理者是否对重要数据、核心数据获取方数据安全保护能力进行核验，保障其采取有效的安全措施保障重要数据、核心数据安全。

8.3.1.5 安全态势

评估团队可参考以下因素开展评估:

a) 是否曾发生过数据安全事件;

b) 是否受到数据安全监管处罚;

c) 是否收到数据安全风险预警信息。

评估团队对以上因素进行充分了解后，通过人员访谈、资料查验、技术测试等方式，识别已采取的措施与当前的状态，综合评价数据安全事件发生的可能性级别。具体识别标准见表1所示，其中可能性级别的识别应采取就高原则，根据网络环境和技术措施、管理制度和处理流程、参与人员和获取方管理、安全态势4个方面识别出最高可能性级别作为数据处理活动可能引发数据安全事件的可能性级别。

表 1 可能性级别判定表

判断因素	可能性描述（对照可能性级别对应的可能性描述，从高至低进行梳理，满足一条即可判定）	可能性级别	备注
网络环境和技术措施	1、处理数据的信息系统存在数据脱敏、备份还原、防病毒、防攻击、防泄露、日志审计、数据销毁、接口安全防护、系统安全加固、网络运行状态监测、存储介质安全保护等技术保护措施缺失或功能和性能严重不足的。合规性评估中技术措施相关评估项评估结果存在 3 个及以上不符合的或 5 个及以上部分符合的，或技术检测发现高危风险或 5 个及以	高	满足一条即可判定

判断因素	可能性描述（对照可能性级别对应的可能性描述，从高至低进行梳理，满足一条即可判定）	可能性级别	备注
	上中危风险的，可视为相关技术保护措施缺失或功能和性能严重不足。 2、无法有效、准确识别出重要数据、核心数据的。 3、存在重要数据、核心数据未加密存储、传输的，因专用设备限制，经验证无法完成数据加密的除外。 4、重要数据、核心数据处理过程中未实施访问控制、权限管理等的。 5、重要数据和核心数据未开展容灾备份和存储介质安全管理的。 6、重要数据、核心数据销毁后仍可恢复的。		
	1、处理重要数据、核心数据的信息系统处于互联网环境中，或处于内网环境中、但与5个及以上信息系统存在交互，且不存在数据安全技术保护措施缺失，相关接口均进行充分的安全防护，各项技术能力充分。 2、处理重要数据、核心数据的信息系统处于内网环境中，仅与5个以内信息系统存在交互，且不存在数据安全技术保护措施缺失，相关接口均进行充分的安全防护，仅存在数据脱敏、日志审计、数据销毁、网络运行状态监测等小部分技术手段能力不充分的问题的。合规性评估中技术措施相关评估项评估结果存在3个以下不符合的或3个及以上，5个以内部分符合的，或技术检测发现1个及以上，5个以内中危风险的，可视为小部分技术手段能力不充分。 3、处理一般数据的信息系统处于互联网环境中，或处于内网环境中、但与5个及以上信息系统存在交互，且不存在数据安全技术保护措施缺失，相关接口均进行充分的安全防护，仅存在数据脱敏、日志审计、数据销毁、网络运行状态监测等小部分技术手段能力不充分的问题的。合规性评估中技术措施相关评估项评估结果存在3个以下不符合的或3个及以上，5个以内部分符合的，或技术检测发现5个以内中危风险的，可视为小部分技术手段能力不充分。	中	满足一条即可判定
	1、处理重要数据、核心数据的信息系统处于内网环境中，仅与5个以内信息系统存在交互，且不存在数据安全技术保护措施缺失，相关接口均进行充分的安全防护，各项技术能力充分。 2、处理一般数据的信息系统不存在数据安全技术保护措施缺失，相关接口均进行充分的安全防护，各项技术能力充分。 3、处理一般数据的信息系统处于内网环境中，仅与5个以内信息系统存在交互，且不存在数据安全技术保护措施缺失，相关接口均进行充分的安全防护，仅存在数据脱敏、日志审计、数据销毁、网络运行状态监测等小部分技术手段能力不充分的问题的。合规性评估中技术措施相关评估项评估结果存在3个以下不符合的或3个及以上，5个以内部分符合的，或技术检测发现5个以内中危风险的，可视为小部分技术手段能力不充分。	低	满足一条即可判定
管理制度和处理流程	1、数据安全管理制度缺失，基本未对数据处理流程进行管理，或数据安全管理制度不够全面，存在1个及以上重点环节、重点场景数据安全管理制度要求缺失的情况，无法有效对数据处理活动进行全生命周期管理。合规性评估中管理措施相关评估项评估结果存在3个及以上不符合的或5个及以上部分符合的，可视为重点环节、重点场景数据安全管理	高	满足一条即可判定

判断因素	可能性描述（对照可能性级别对应的可能性描述，从高至低进行梳理，满足一条即可判定）	可能性级别	备注
	制度要求缺失。 2、未对数据授权访问、批量复制、使用加工、出境、销毁等重点环节进行日志留存。 3、未建立数据安全风险报送监测、数据安全事件应急响应机制，未按要求定期开展数据安全应急演练，无法有效对数据安全风险进行监测处置。 4、未建立内部审批和登记工作机制，未对重要数据和核心数据处理活动实施严格管理并留存记录。		
	1、数据安全管理制度基本全面，管理制度可以覆盖数据处理活动全生命周期所有环节、所有场景，仅部分管理要求尚不完善。合规性评估中管理措施相关评估项评估结果存在3个以内不符合的，或2个以上5个以内部分符合的可视为部分管理要求尚不完善。 2、对数据授权访问、批量复制、使用加工、出境、销毁等重点环节进行日志留存，但存在留存内容、留存时限等不满足法律规范要求等问题。 3、建立数据安全风险报送监测、数据安全事件应急响应机制，按照要求制定应急预案，并定期组织应急演练，可以基本实现对数据安全风险的监测发现和数据安全事件的应急处置，但存在应急演练对象范围覆盖不全，留存记录不完整，数据安全风险识别准确率不足70%等问题。 4、建立内部审批和登记工作机制，对重要数据和核心数据处理活动实施严格管理并留存记录，但存在留存内容不完整，无法全面、准确反映重要数据和核心数据处理活动基本情况，包括数据数量、类型、处理目的、方式、涉及的信息系统以及安全保障措施情况等。	中	满足一条即可判定
	1、数据安全管理制度完备，实现对重要数据、核心数据处理活动进行全生命周期管理，管理要求明确、全面。合规性评估中管理措施相关评估项评估结果仅存在2个及以内部分符合的可视为管理制度完备。 2、对数据授权访问、批量复制、使用加工、出境、销毁等重点环节进行日志留存，留存内容、留存时限满足法律规范要求。 3、建立数据安全风险报送监测、数据安全事件应急响应机制，按照要求制定应急预案，并定期组织应急演练，应急演练对象范围覆盖全面，留存记录完整、可以准确识别数据安全风险并及时开展应急处置。 4、建立内部审批和登记工作机制，对重要数据和核心数据处理活动实施严格管理并留存记录，留存内容完整、准确。	低	需全部满足
参与人员和获取方管理	1、未建立数据获取方管理制度，未形成获取方管理台账。 2、未配备数据安全管理人员，统筹负责数据处理活动的安全监督管理。 3、重要数据、核心数据处理者未设立数据安全管理机构，未明确内部数据处理关键岗位、职责、任职要求以及负责履行数据安全管理的义务。 4、重要数据、核心数据处理者未对数据处理关键岗位人员进行数据安全相关培训和考核。 5、重要数据、核心数据处理者未与数据处理关键岗位人员签订数据安全责任书。 6、重要数据、核心数据处理者未对处理关键岗位人员权限进行区分，	高	满足一条即可判定

判断因素	可能性描述（对照可能性级别对应的可能性描述，从高至低进行梳理，满足一条即可判定）	可能性级别	备注
	未通过有效手段限制不同身份数据处理者权限。 7、重要数据、核心数据处理者未对获取方处理重要数据、核心数据的行为进行任何约束，或已出现获取方滥用数据的情形。		
	1、初步建立数据获取方管理制度，但存在管理环节缺失，管理要求设置严重不合理等问题；初步形成获取方管理台账，但台账内容不完整、不准确，存在获取方未记录在台账内的情形。 2、配备数据安全管理人员，但存在数据安全管理人员数量不充足、职责不合理清晰、能力不匹配等问题，无法全面统筹负责数据处理活动的安全监督管理。 3、重要数据、核心数据处理者设立数据安全管理机构，但内部数据处理关键岗位、职责、任职要求以及负责履行数据安全管理的义务等不清晰明确。 4、重要数据、核心数据处理者对数据处理关键岗位从业人员进行数据安全相关培训和考核，但考核周期、考核内容设置不合理，未对考核不通过人员进行有效约束。 5、重要数据、核心数据处理者与数据处理关键岗位人员签订数据安全责任书，但存在内容不全面、不充分的问题，例如未明确约定数据安全岗位职责、义务、处罚措施、注意事项等内容。 6、重要数据、核心数据处理者对数据处理关键岗位人员权限进行区分，通过有效手段限制不同身份数据处理者权限，但存在权限划分不合理等问题。 7、重要数据、核心数据处理者与重要数据、核心数据的获取方签订数据安全相关合同/协议，但相关协议/合同条款设置不合理、全面，无法充分、有效地约束获取方处理重要数据、核心数据的行为，且未对获取方协议/合同履行情况进行检查、审计或评估，无法真实有效掌握获取方协议/合同履行情况。	中	满足一条即可判定
	1、建立数据获取方管理制度，管理环节全面、管理要求科学、合理；建立获取方管理台账，记录内容全面、详尽、清晰、准确。 2、配备数据安全管理人员，数据安全管理人员数量充足、职责清晰合理，且相关人员能力与岗位职责互相匹配，可以全面统筹负责数据处理活动的安全监督管理。 3、重要数据、核心数据处理者设立数据安全管理机构，内部数据处理关键岗位、职责、任职要求以及负责履行数据安全管理的义务等清晰明确，不存在管理职责不清等问题。 4、重要数据、核心数据处理者对数据处理关键岗位人员培训充分、调查全面、约束有效。 5、重要数据、核心数据处理者对数据处理关键岗位人员权限进行区分，通过有效手段限制不同身份数据处理者权限，且权限划分合理、准确等。 6、重要数据、核心数据处理者与重要数据、核心数据的获取方签订的相关协议/合同条款设置合理、全面，可以对获取方处理重要数据、核心数据的行为进行约束，且定期对获取方协议/合同履行情况进行检查、	低	需全部满足

判断因素	可能性描述（对照可能性级别对应的可能性描述，从高至低进行梳理，满足一条即可判定）	可能性级别	备注
	审计或评估，可以真实有效掌握获取方协议/合同履行情况。		
安全态势	1、2 年内发生 3 次及以上较大数据安全事件，或发生过 1 次及以上重大及以上数据安全事件。 2、1 年内受到过电信主管部门发出的数据安全监管处罚。	高	满足一条即可判定
	1、2 年内发生过不超过 2 次较大数据安全事件。 2、1 年内收到过电信主管部门发出的重要数据、核心数据相关风险预警信息。	中	满足一条即可判定
	1、2 年内未发生过较大及以上数据安全事件。	低	需全部满足

8.3.2 安全影响分析

评估团队应综合分析数据处理活动存在安全风险时，数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对国家安全、公共利益产生何种影响及影响程度，包括以下维度：

a) 影响国土安全，是否会导致其他国家掌握我国国防建设、军事部署、关键设施等情况，进而影响我领土安全和主权完整；

b) 影响经济安全，是否会导致我国重要经济数据外泄，致使我国经济利益遭受巨大损失，引发经济风险；

c) 影响网络安全，是否会导致我国电信和互联网等公共服务中断运行或主要功能故障、重要数据和核心数据泄露，对我国网络稳定运行造成巨大危害和损失；

d) 影响社会安全，是否会导致人民群众公共利益遭受危害、引发公共安全事件、影响人民群众日常生活秩序，对我国社会稳定产生重大影响;

e) 影响科技安全，是否会导致我国先进技术数据外泄，影响我国在该领域的国际领先地位。

评估团队在进行安全影响分析时候，可按照以下两方面开展:

a) 综合考虑重要数据和核心数据的种类、数量、级别等基本属性，初步分析发生数据安全事件后可能影响的范围和类别;

b) 根据数据安全事件发生后可能导致的后果严重程度，研判安全影响级别，具体判定标准见表2所示。

对于涉及多个安全影响类别的，选取各安全影响类别下级别最高的，作为重要数据和核心数据处理活动安全影响级别。

注：一般数据因其数据敏感程度较低，在发生泄露、损毁、丢失等安全事件后不会对国家安全、公共利益产生较大影响，因此针对一般数据处理活动，可直接判定其安全影响级别为一般。

表 2 安全影响级别判定表

安全影响类别	安全影响描述	安全影响级别
国土安全	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。	特别严重
	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。	严重
	可能导致我国重要设施受到一般威胁或可能间接影响我国领土、主	一般

安全影响类别	安全影响描述	安全影响级别
	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泄露，但尚未被外方掌握。	
经济安全	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%。	特别严重
	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、直辖市、自治区的 GDP 或电信领域整体 GDP 下降超 1%。	严重
	可能严重影响市场经济运行秩序，如市场行为、市场结构、商品销售、交换关系、生产经营秩序、涉外经济关系等。例如引起 1 个及以上省、直辖市、自治区的 GDP 或电信领域整体 GDP 下降不足 1%。	一般
网络安全	可能导致我国发生全国范围内电信和互联网大面积瘫痪、顶级域名系统解析功能故障、大型互联网平台访问严重异常、大规模重要数据和核心数据泄露、应急通信中断等安全事件。例如全国范围内大量互联网用户无法正常上网，1 亿以上个人信息泄露等。	特别严重
	可能导致我国发生多个省份电信和互联网大面积瘫痪、大型域名系统解析功能故障、大型互联网平台访问异常、重要数据和核心数据泄露、应急通信中断等安全事件。例如 1 个以上省、直辖市、自治区大量互联网用户无法正常上网，1 千万以上个人信息泄露等。	严重
	可能导致我国一个省份电信和互联网大面积瘫痪、省内具有影响力的网站和平台访问异常、重要数据和核心数据泄露、应急通信中断等安全事件。例如 1 个省、直辖市、自治区大量互联网用户无法正常上网，1 百万以上个人信息泄露等。	一般
社会安全	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。	特别严重
	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、直辖市、自治区范围内的重大舆情，引起多个省、直辖市、自治区范围内的群众恐慌、社会动荡。	严重
	可能对人民群众的日常生活秩序造成一定影响；可能影响一定范围的企事业单位、社会团体的生产秩序、经营秩序、教学科研秩序、医疗卫生秩序等；可能影响公共场所的活动秩序、公共交通秩序。例如发生影响 1 个省、直辖市、自治区范围内的重大舆情，引起 1	一般

安全影响类别	安全影响描述	安全影响级别
	个省、直辖市、自治区范围内的群众恐慌、社会动荡。	
科技安全	可能导致我国尖端技术数据外泄；对我国先进科学技术研发进程等产生严重影响。例如我国在国际上领先的科学技术成果数据被外泄。	特别严重
	可能导致我国先进技术数据外泄；对我国先进科学技术研发进程等产生较大影响。例如我国出口管制物项相关技术数据被外方掌握。	严重
	可能影响我国重要科学技术的研发进程，影响我国重要技术的相关性能指标。例如我国出口管制物项相关技术数据外泄但尚未被外方掌握。	一般

8.3.3 综合风险研判

评估团队应综合分析数据安全事件发生的可能性级别以及安全影响级别两方面因素，研判数据处理活动安全风险等级，安全风险等级可分为极高、高、中、低四个等级。安全风险等级判定方法见表3所示。

表 3　安全风险等级判定表

安全风险等级		可能性级别		
		低	中	高
安全影响级别	特别严重	中	高	极高
	严重	低	中	极高
	一般	低	低	高

注：某项数据涉及多项处理活动时，按照风险就高原则，选取数据处理活动安全风险等级最高的，作为该项数据的最终安全风险等级。

8.3.4 评估结果与风险控制

评估团队应根据风险评估情况编制形成电信领域数据安全风险评估报告，并对风险评估结果负责，保障评估结果真实、准确。对于评估中发现的安全风险隐患，数据处理者应及时采取有

效的应对措施消除风险隐患。

9 评估工具

9.1 评估工具的安全要求

评估团队应使用来源可靠、安全稳定的评估工具，要求相关人员严格遵守操作流程，防止引入新的风险。评估工具应保障来源安全可靠，保障不对数据处理者生产运营造成影响。未通过检测和校验的评估工具不得应用于评估工作。

9.2 评估工具的使用要求

评估团队应保障评估人员可熟练使用相关数据安全检测评估工具，并在现场评估过程中安全、规范、合理的使用评估工具。使用评估工具对承载数据的系统、设备等进行测试时应慎重实施，尽量避免在数据处理者的业务高峰期进行技术测试。

9.3 常用数据安全风险评估工具

常用数据安全风险评估工具包括：数据资产扫描工具、数据流量分析工具、系统脆弱性扫描工具、系统主机安全检查工具、数据安全检测评估工具等。

附录 A

（资料性）

电信领域数据分类参考

序号	一级类别	二级类别
1	网络规划运维数据域	网络规划建设
2		网络运行维护
3		其他
4	安全保障数据域	网络与数据安全保障
5		物理安全保障
6		应急通信保障
7		其他
8	经济运行与业务发展数据域	行业发展
9		业务发展战略规划与重大决策
10		其他
11	关键技术成果数据域	重大科技成果
12		国家科技计划
13		其他
14	业务运营数据域	产品数据
15		营销数据
16		渠道数据
17		客户服务数据

18		公开业务运营服务数据
19		其他
20	管理数据域	基础管理数据
21		综合管理数据
22		其他
23	用户数据域	用户身份相关数据
24		用户服务使用数据
25		用户设备信息
26		用户统计分析类数据
27		其他
28	其他数据域	其他