广西壮族自治区

数据安全风险评估办法（试行）

1. 总 则

第一条 为强化我区数据安全风险识别与管理，防范化解数据安全风险，推动数据安全和数据应用并重发展，根据《中华人民共和国数据安全法》《广西壮族自治区大数据发展条例》等有关规定，参考《信息安全技术 信息安全风险评估方法》《网络安全标准实践指南-网络数据安全风险评估实施指引》等有关标准，结合我区实际，制定本办法。

第二条 本办法适用于指导广西区域范围内的数据处理者、第三方机构开展数据安全风险评估，同时为有关主管监管部门开展数据安全检查评估提供参考。

第三条 本办法中相关术语的定义：

（一）数据，是指任何以电子或者其他方式对信息的记录，包括公共数据和非公共数据。

（二）数据处理者，是指在数据处理活动中自主决定处理目的和处理方式的个人和组织。

（三）数据处理活动，是指数据收集、存储、使用、加工、传输、共享、开放、销毁等活动。

（四）数据安全，是指通过采取必要措施，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。

（五）数据安全风险评估，是指从风险管理角度，运用科学的方法与手段，根据数据分类分级情况，系统分析数据所面临的安全威胁，以及可能遭受的危害程度，有针对性地提出抵御数据安全威胁的防护对策和措施。

1. 风险评估概述

第四条 数据安全风险评估需坚持预防为主、主动发现、积极防范，对数据处理者数据安全保护和数据处理活动进行风险评估，旨在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。

第五条 数据安全风险评估流程应充分结合数据管理过程，在数据识别、业务信息识别、数据处理活动识别的基础上，结合数据处理活动场景，以业务为核心，以业务条线为范围，以数据和数据处理活动为对象，充分识别业务活动场景下的各类数据及其对应的数据处理活动所面临的威胁和脆弱性，并进行风险分析。评估流程详见【附录C数据安全风险评估流程图】。

第六条 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。

第七条 开展数据安全风险评估时，应综合采取人员访谈、文档查验、安全核查、技术测试等手段进行评估。

1. 风险评估准备

第八条 数据处理者开展数据安全风险评估前，应确定数据安全风险评估的目标，包括但不限于：

（一）摸清数据种类、规模、分布等基本情况；

（二）摸清数据处理活动的情况；

（三）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；

（四）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；

（五）促进完善数据安全保护措施，提升数据安全保护能力。

第九条 应基于业务战略需求及合规需求确定数据安全风险评估范围，评估范围可以是一个或多个场景或系统中的全部数据资产，也可以是特定范围内的数据资产。

第十条 应根据评估范围、涉及的行业特征、专业性质，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。

第十一条 为确保数据安全风险评估结果的有效性，数据安全风险评估队伍应确定被评估单位适用的评估依据，包括但不限于：适用的法律、行政法规、司法解释，需要参照的现行国际标准、国家标准、行业标准等。

第十二条 数据安全风险评估队伍应编制风险评估工作方案，方案内容应包括：评估概述、评估范围、评估内容和方法、评估人员、实施计划、工作要求、测试方案。

第十三条 数据安全风险评估队伍应对被评估单位或被评估的业务部门的管理情况进行充分调研，调研内容包括：单位基本情况、组织管理情况、业务应用情况、网络及数据安全情况等。

本阶段评估人员输出成果为《数据安全风险评估调研清单》，模板见【附录A1数据安全风险评估调研清单】。

1. 风险评估要素识别

第十四条 在确定评估范围基础上，应针对评估范围的数据资产进行整理，确定被评估数据资产的数据类型、数据所在位置、数据量、数据安全等级等内容，数据资产的价值指标直接由数据资产的安全级别决定，可参照【附录B1数据资产赋值表】对数据的重要程度进行赋值。

本阶段评估人员输出成果为《数据资产级别赋值清单》，模板见【附录A2数据资产级别赋值清单】。

第十五条 在确定待评估的数据后，应针对数据进行识别，梳理其涉及的各类数据处理活动场景，包括业务应用场景相关的数据生命周期、参与主体、网络环境及操作流程，确保场景识别结果与实际情况保持一致。

本阶段评估人员输出成果为《数据处理活动场景清单》，模板见【附录A3数据处理活动场景清单】。

第十六条 安全措施可以分为预防性安全措施和保护性安全措施两种，预防性安全措施可以降低利用脆弱性导致安全事件发生的可能性，保护性安全措施可以减少因安全事件发生后对数据、业务造成的影响。评估人员应识别出被评估单位已有安全措施，并判断安全措施是否得到正确使用、安全策略是否设置合理、策略是否得到有效执行。

本阶段评估人员输出成果为《已有安全措施清单表》，模板见【附录A4已有安全措施清单表】。

第十七条 数据安全脆弱性识别应依据国际、国家安全标准或者行业规范、应用流程的安全要求，从管理与技术两个角度进行综合识别，评估人员应参照【附录B2脆弱性识别内容表】采用问卷调查、工具检测、人工核查、文档查阅、渗透性测试等相关方法对被评估单位全部脆弱性进行识别，根据脆弱性可利用难度及已有安全措施有效性，综合判断脆弱性的可利用性，并参照【附录B3脆弱性可能利用赋值表】对各脆弱性的可利用性进行赋值。

本阶段评估人员输出成果为《业务场景脆弱性清单表》，模板见【附录A5业务场景脆弱性清单表】。

第十八条 数据安全威胁是指可能对系统或组织的数据处理活动造成危害的因素，数据威胁要素属性包括数据威胁动机、能力及频率。评估人员应结合当前脆弱性识别情况分析出具体数据威胁后，通过参照【附录B4 数据威胁来源、动机和能力事例】、进一步分析出数据威胁的来源、攻击动机、攻击能力、威胁频率，同时参照【附录B5 数据威胁动机赋值表】、【附录B6 数据威胁能力赋值表】、【附录B7 数据威胁频率赋值表】对数据威胁攻击动机、数据威胁攻击能力、数据威胁频率进行定量判断，并给予赋值，最终数据威胁发生可能性的赋值将由数据威胁攻击动机赋值、攻击能力赋值及威胁频率赋值共同确定。

本阶段评估人员输出成果为《数据安全威胁清单》，模板见【附录A6数据安全威胁清单】。

1. 风险分析与评价

第十九条 本办法通过定量赋值法开展数据安全风险计算，通过数据资产识别、数据应用场景识别、数据威胁识别、脆弱性识别，核对已有安全措施后，由数据价值、脆弱性严重程度和数据威胁属性来定量“脆弱性可造成的损失”以及“数据威胁发生可能性”，计算得到“数据风险值”，最终确定评估范围内的“总体风险值”。

第二十条 风险评价的目的是支持决策，风险评价涉及将风险分析的结果与既定的风险准则进行比较，以确定需要采取何种应对措施。应根据风险评价准则对风险分析中计算的总体风险值进行等级处理，可参照【附录B8 数据安全风险等级划分表】将总体风险划分为5个级别，每个风险等级采用分值计算表示，分值越大，风险越高。

本阶段评估人员输出成果为《数据安全风险清单》，模板见【附录A7数据安全风险清单】。

第二十一条 完成风险分析与评价后，应编制风险处置建议和风险评估报告，并依据风险处置措施预判措施有效性和残余风险。评估报告模板参考【附录D 数据安全风险评估报告模板】。

第二十二条 被评估单位应根据本行业、单位的风险管理策略，确认数据安全风险接受程度，对于不可接受的数据安全风险，应尽快采取风险管控措施进行控制。

1. 附则

第二十三条 涉及国家秘密的数据，按照国家保密法律、法规和制度执行。对于统计、档案工作开展数据安全风险评估活动，还应遵守有关法律、法规的规定。

第二十四条 行业主管部门针对数据安全风险评估另有规定的，从其规定。

第二十五条 本办法由自治区大数据发展局负责解释。

第二十六条 本办法自印发之日起施行。

# 附录A：数据安全风险评估输出成果参考模板

A1：数据安全风险评估调研清单

1、单位基本信息

1.1单位概况

|  |  |
| --- | --- |
| 单位名称 |  |
| 单位性质 |  | 成立时间 |  |
| 人员规模 |  | 办公地点 |  |
| 单位简介 |  |
| 主要业务 |  |

2、组织管理情况

2.1组织架构

请详细描述当前网络安全及数据安全管理的组织架构。

2.2当前数据安全的职责分工

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 分类 | 部门 | 负责人及职务 | 主要职责 | 是否专职 |
| 本单位最高数据安全决策部门/组织 |  |  |  |  |
| 本单位数据安全管理部门/组织 |  |  |  |  |
| 本单位数据安全的具体执行部门/组织 |  |  |  |  |
| 本单位有哪些部门会参与到数据安全工作中 |  |  |  |  |
| 其他 |  |  |  |  |

2.3数据安全的制度流程

|  |  |  |
| --- | --- | --- |
| 编号 | 管理制度名称 | 正式执行时间 |
| 1 |  |  |
|  |  |  |

3、业务应用情况

3.1当前网络拓扑

请详细描述网络拓扑情况。

3.2运行环境信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 节点类型 | 型号  | 版本 | 数量 | 描述 |
| 物理服务器 |  |  |  |  |
| 虚拟服务器 |  |  |  |  |
| 数据库管理系统 |  |  |  |  |
| 云、虚拟化及大数据运行环境 |  |  |  |  |
| 网络设备 |  |  |  |  |
| 安全设备 |  |  |  |  |
| 终端 |  |  |  |  |

3.3系统/平台清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 系统/平台名称 | 系统/平台描述 | 所使用数据库 | 数据规模（万条） | 运维部门 | 当前安全措施 |
| 1 |  |  |  |  |  |  |

3.4系统/平台交互关系

请详细描述业务应用、系统、平台各主要组成部分及其关联关系。

3.5数据存储环境清单

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 厂商、型号及版本 | 类型 | 关联业务系统 | 用途描述 | 数据规模 | 重要程度 |
| 1 |  |  |  |  |  |  |  |

4、网络及数据安全情况

4.1当前网络及数据安全保护措施清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 分类 | 安全措施 | 保护范围 | 措施描述 |
| 1 | 网络安全措施 |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 2 | 数据安全措施 |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |  |

4.2面临的主要问题及风险

| 序号 | 状态 | 问题及影响描述 | 处置情况 | 容忍度 |
| --- | --- | --- | --- | --- |
| 1 |  |  |  | 须处理 |
| 2 |  |  |  | 可接受 |
|  |  |  |  |  |

A2：数据资产级别赋值清单

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 数据资产编号 | 数据资产名称 | 数据所有方 | 所在位置 | 数据规模（数量） | 数据规模（容量） | 数据安全等级 | 数据资产价值赋值 |
|  |  |  |  |  |  |  |  |

A3：数据处理活动场景清单

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 业务场景编号 | 相关数据资产名称 | 业务场景名称 | 业务场景描述 | 生存周期 | 网络环境 | 参与主体 | 操作流程 |
|  |  |  |  |  |  |  |  |

A4：已有安全措施清单表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全措施编号 | 安全措施名称 | 安全措施描述 | 关联业务场景 | 措施有效性 |
|  |  |  |  |  |

A5：业务场景脆弱性清单表

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 脆弱性编号 | 所在业务场景名称 | 脆弱性名称 | 访问路径 | 访问复杂性 | 权限要求 | 用户交互 | 可利用性 | 可利用性赋值 | 已有安全措施 | 防护后可利用性赋值 |
|  |  |  |  |  |  |  |  |  |  |  |

A6： 数据安全威胁清单

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 威胁编号 | 可利用的脆弱性 | 威胁名称 | 威胁来源 | 影响资产编号 | 方位 | 动机 | 能力 | 频率 | 动机赋值 | 能力赋值 | 频率赋值 | 发生可能性 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

A7： 数据安全风险清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 数据资产编号 | 威胁发生可能性 | 脆弱性严重程度 | 风险值 | 价值赋值 | 加权风险值 |
|  |  |  |  |  |  |

# 附录B：数据安全风险评估赋值表参考模板

B1：数据资产赋值表

|  |  |
| --- | --- |
| 赋值 | 数据资产安全级别 |
| 5 | 敏感数据 |
| 3 | 内部数据 |
| 1 | 公开数据 |

B2：脆弱性识别内容表

| 类型 | 识别对象 | 识别内容 |
| --- | --- | --- |
| 技术脆弱性 | 物理环境 | 从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别。 |
| 网络结构 | 从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面进行识别。 |
| 系统软件 | 从补丁安装、物理保护、用户账号、口令策略、资源共享、事件审计、访问控制、新系统配置、注册表加固、网络安全、系统管理等方面进行识别。 |
| 应用中间件 | 从协议安全、交易完整性、数据完整性等方面进行识别。 |
| 应用系统 | 从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别。 |
| 日志留存 | 从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，是否定期对日志进行备份，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，日志保存期限是否符合法律法规要求等方面进行识别。 |
| 数据资产 | 从数据脱敏规则、脱敏方法和脱敏数据的使用限制情况进行识别；从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进行识别；从数据备份恢复策略和操作规程的建设落实情况进行识别。 |
| 管理脆弱性 | 技术管理 | 从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别 |
| 组织管理 | 从安全策略、组织安全、资产分类与控制、人员安全、符合性等方面进行识别 |
| 数据安全管理 | 从数据安全管理制度体系建设、数据安全组织机构建设、数据分类分级管理、人员安全管理、合作外包管理、安全威胁和应急管理等方面进行识别。 |

B3：脆弱性可能利用赋值表

| 赋值 | 脆弱性可利用性 | 访问路径 | 访问复杂性 | 权限要求 | 用户交互 |
| --- | --- | --- | --- | --- | --- |
| 5 | 很高 | 远程网络访问 | 访问复杂性低 | 无权限要求 | 不需要用户交互 |
| 4 | 高 | 邻近网络访问 | 访问复杂性中等 | 权限要求中等 | 不需要用户交互 |
| 3 | 中 | 本地访问 | 访问复杂性中等 | 权限要求中等 | 不需要用户交互 |
| 2 | 低 | 本地访问 | 权限要求高 | 权限要求高 | 需要用户交互 |
| 1 | 很低 | 物理访问 | 访问复杂性高 | 权限要求高 | 需要用户交互 |

B4 数据威胁来源、动机和能力示例

| 分类 | 威胁来源 | 描述 | 主要动机 | 能力 |
| --- | --- | --- | --- | --- |
| 非人为 | 自然灾难 | 非人为不可抗拒的自然灾害，比如水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等 | 具有一定预测性 | 自然灾难的威胁程度不等，可能会对信息系统造成毁灭性的破坏 |
| 环境因素 | 断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、意外事故等环境危害 | 无动机，具有一定预测性 | 威胁程度不等 |
| 人为 | 非恶意行为 | 粗心或未受到良好培训的管理员和用户 | 无动机无预测性，或能力不足 | 掌握内部情况，具有数据访问权限，或掌握可利用的账户信息，由于特殊原因而导致的无意行为或误操作，可以从内部破坏信息系统及数据 |
| 内部恶意员工 | 主要指对机构不满或具有某种恶意目的的内部员工 | 由于对机构不满而有意破坏数据，被收买或威胁窃取或破坏数据，或出于某种目的窃取数据或破坏数据 | 掌握内部情况，具有数据合法访问权限，或掌握可利用的账户信息，可以从内部获取数据 |
| 独立黑客 | 主要指个体黑客 | 企图寻找并利用系统的脆弱性，以达到满足好奇心、检验技术能力以及获取、恶意破坏数据等目的，动机复杂，目的性不强 | 占有少量资源，一般从外部侦察并攻击网络和系统；攻击者水平高低差异很大 |
| 有组织的攻击者 | 国内外竞争者 | 主要指具有竞争关系的国内外工业和商业机构 | 获取商业情报，窃取数据资源，破坏竞争对手的业务和数据，目的性较强 | 具有一定的资金、人力和技术资源，通过多种渠道搜集情报，包括利用竞争对手内部员工、独立黑客以至犯罪团伙 |
| 犯罪团伙 | 主要指黑灰产犯罪团伙。对犯罪行为可能进行长期的策划和投入 | 偷窃、诈骗钱财，窃取机密信息，贩卖个人信息 | 具有一家的资金、人力和技术资源，实施网络犯罪，对犯罪有精密计划和准备 |
| 恐怖组织 | 主要指国内外恐怖组织 | 恐怖组织通过强迫或恐吓政府或社会，以满足其需要为目的，采用暴力或暴力威胁方式制造恐慌 | 具有丰富的资金、人力和技术资源，对攻击行为可能进行长期策划和投入，可能获得敌对国家的支持 |
| 外国政府 | 主要指其他国家或地区设立的从事军事、情报等窃取的机构 | 从其他国家搜集政治、经济、军事情报或机密信息，或获取大量其他国家个人信息进行舆论诱导，目的性极强 | 组织严密、具有充足的资金、人力和技术资源，通过多种渠道，包括技术能力、威逼利诱内部员工窃取信息，将窃取信息、攻击信息系统作为战争手段 |

B5 数据威胁动机赋值表

|  |  |  |
| --- | --- | --- |
| 赋值 | 威胁动机 | 定义 |
| 5 | 很高 | 从其他国家搜集政治、经济、军事情报或机密信息，或获取大量其他国家个人信息进行舆论诱导，目的性极强；恐怖组织通过强迫或恐吓政府或社会，以满足其需要为目的，采用暴力或暴力威胁方式制造恐慌； |
| 4 | 高 | 偷窃、诈骗钱财，窃取机密信息，贩卖个人信息；获取商业情报，窃取数据资源，破坏竞争对手的业务和数据，目的性较强； |
| 3 | 中等 | 企图寻找并利用系统的脆弱性，以达到满足好奇心、检验技术能力以及获取、恶意破坏数据等目的，动机复杂，目的性不强；由于对机构不满而有意破坏数据，被收买或威胁窃取或破坏数据，或出于某种目的窃取数据或破坏数据； |
| 2 | 低 | 无动机无预测性，或威胁能力不足； |
| 1 | 很低 | 无动机，具有一定预测性； |

B6 数据威胁能力赋值表

|  |  |  |
| --- | --- | --- |
| 赋值 | 威胁能力 | 定义 |
| 5 | 很高 | 自然灾害，可能会对信息系统造成毁灭性的破坏； |
| 4 | 高 | 外国政府，组织严密、具有充足的资金、人力和技术资源，通过多种渠道，包括技术能力、威逼利诱内部员工窃取信息，将窃取信息、攻击信息系统作为战争手段 |
| 3 | 中等 | 有组织的攻击，利用竞争对手内部员工、独立黑客以至犯罪团伙；实施网络犯罪，对犯罪有精密计划和准备；对攻击行为可能进行长期策划和投入，可能获得敌对国家的支持。 |
| 2 | 低 | 占有少量资源，一般从外部侦察并攻击网络和系统； |
| 1 | 很低 | 由于特殊原因而导致的无意行为或误操作，可以从内部破坏信息系统及数据； |

B7 数据威胁频率赋值表

|  |  |  |
| --- | --- | --- |
| 赋值 | 标识 | 定义 |
| 5 | 很高 | 出现的频率很高（或≥现的次/周）；或在大多数情况下几乎不可避免；或可以证实经常发生过 |
| 4 | 高 | 出现的频率较高（或≥现的频次/月）；或在大多数情况下很有可能会发生；或可以证实多次发生过 |
| 3 | 中等 | 出现的频率中等（或> 1 次/半年）；或在某种情况下可能会发生；或被证实曾经发生过 |
| 2 | 低 | 出现的频率较小；或一般不太可能发生；或没有被证实发生过 |
| 1 | 很低 | 威胁几乎不可能发生；仅可能在罕见和例外的情况下发生 |

B8 数据安全风险等级划分表

|  |  |  |
| --- | --- | --- |
| 等级 | 标 识 | 描 述 |
| 5 | 很高 | 一旦发生将对业务或组织产生非常严重而深远的影响，对组织信誉严重破坏，严重影响业务或组织的正常运行，产生非常严重的经济损失或社会影响 |
| 4 | 高 | 一旦发生将对业务、其他业务或组织产生较大的影响，在一定范围内给业务或组织的经营、组织信誉造成损害，产生较大的经济损失或社会影响 |
| 3 | 中等 | 一旦发生将对业务或组织运行、组织信誉造成一定的影响，但对经济或社会的影响不大，不影响其他业务或对其他业务影响程度不大 |
| 2 | 低 | 一旦发生造成的影响程度较低，一般仅限于业务、组织内部或数据资产本身，通过一定手段很快能解决 |
| 1 | 很低 | 一旦发生造成的影响低微 |

# 附录C：数据安全风险评估流程图



图：数据安全风险评估流程

数据安全风险评估流程包含准备阶段、执行阶段和评审阶段三个过程。首先在开展风险评估前，需做好评估准备工作，包含确定评估目标、确定评估范围、确定评估依据和方案，以及安全管理调研等，然后通过对数据资产、数据处理活动、已有安全措施、脆弱性、数据安全威胁等相关要素识别风险隐患，梳理问题清单，定量分析和评价数据安全风险，并给出处置建议，最后做风险评估报告的编制和沟通评审。

# 附录D：数据安全风险评估报告模板

一、风险评估概述

1.1评估目的

1.2评估范围

1.3评估依据

1.4评估流程

二、风险评估方法

2.1评估方法

2.2项目组成员

2.3信息收集方法

三、风险评估调研

3.1单位基本信息

3.2组织管理情况

3.3业务应用情况

3.4网络及数据安全情况

四、风险识别

4.1数据识别

4.2数据处理活动场景识别

4.3已有安全措施识别

4.4脆弱性识别

4.5数据安全威胁识别

五、风险分析

5.1数据重要程度赋值

5.2脆弱性可造成的损失计算

5.3数据安全威胁发生可能性计算

5.4数据风险值计算

5.5总体数据安全风险值计算

六、风险分析

6.1风险评估结论

6.2风险处置建议

各附录材料

# 附录E：数据安全风险评估范例

依据实践经验，本文列举一个数据安全风险评估范例。此次范例工作步骤流程如下：

 

具体步骤：

1、对评估范围内的数据进行数据的重要程度赋值和针对各数据识别其涉及的各类数据处理活动场景，并输出《数据资产级别赋值清单》《数据处理活动场景清单》；

2、列出在《数据资产级别赋值清单》中的某个数据i在应用场景i下的所有脆弱性，并结合《已有安全措施清单表》对该应用场景i下的所有脆弱性可利用性进行人工赋值，并输出《业务场景脆弱性清单表》；

3、计算出在应用场景i下的所有脆弱性的严重程度的平均值Ai；

4、计算出数据i在所有应用场景下的所有脆弱性的严重程度的平均值Vi；

5、计算出数据i的脆弱性可造成的损失Fi，并填入《数据脆弱性严重程度赋值表》中，公式为：



6、参照【附录B5 数据威胁动机赋值表】、【附录B6 数据威胁能力赋值表】、【附录B7 数据威胁频率赋值表】对数据i的安全威胁i的动机、能力、频率进行赋值，并计算数据i发生威胁i的可能性，公式为：



并输出《数据安全威胁清单》。

7、参照步骤6列出数据i存在的所有威胁，并计算所有威胁发生的可能性，计算数据i所有威胁发生的可能性的平均值Li；

8、最后根据步骤5计算出的数据i的脆弱性可造成的损失Fi以及步骤7计算出的数据i所有威胁发生的可能性的平均值Li计算出数据i的数据安全风险值，计算公式为：



9、根据以上步骤计算出所有数据的安全风险值并汇总至《数据安全风险清单》中，最后计算出数据安全的总体风险值，计算公式为：

