企业数据安全风险管理指南

CSA GCR cloud security alliance
GREATER CHINA REGION ®

联盟简介

云安全联盟(Cloud Security Alliance,CSA)是中立、权威的全球性非营利产业组织,于2009年正式成立,致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识,推动数字安全产业全面发展。

云安全联盟大中华区(Cloud Security Alliance Greater China Region, CSA GCR)作为CSA全球四大区之一,2016年在香港独立注册,于2021年在中国登记注册,是网络安全领域首家在中国境内注册备案的国际NGO,旨在立足中国,连接全球,推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《企业数据安全风险管理指南》由 CSA 大中华区数据安全工作组内企业数据安全风险管理项目组专家撰写，感谢以下专家的贡献：

项目组组长：艾龙

原创作者：

陈吴栋	董雁超	方伟	付宗玉	郭海骏
贺志生	黄瑞	雷钰婷	刘楚楚	鹿淑煜
潘万鹏	王皓然	王辉	王良河	谢琴
薛恺	杨天识	杨岁立	杨学治	俞华辰
袁荣婷	张涛	赵宇	周泽元	

审核专家：

董雁超	乐元	刘楚楚	潘万鹏	谢江
谢琴	杨天识	吕鹂啸	郭鹏程	姚凯

研究协调员：卜宋博

贡献单位：

北京江南天安科技有限公司	北京启明星辰信息安全技术有限公司
北京天融信网络安全技术有限公司	北京神州数码云计算有限公司
北森云计算有限公司	格尔软件股份有限公司
广州赛宝认证中心服务有限公司	广州熠数信息技术有限公司
贵州电网有限责任公司信息中心	杭州虎符网络有限公司
杭州美创科技股份有限公司	任子行网络技术股份有限公司
三六零数字安全科技集团有限公司	三未信安科技股份有限公司
上海观安信息技术股份有限公司	上海众人智能科技有限公司
深信服科技股份有限公司	深圳国家金融科技测评中心有限公司

深圳市联软科技股份有限公司　　深圳市智安网络有限公司

苏州云至深技术有限公司　　腾讯云计算（北京）有限责任公司

浙江大华技术股份有限公司　　中兴通讯股份有限公司

（以上排名不分先后）

关于研究工作组的更多介绍，请在 CSA 大中华区官网（https://c-csa.cn/research/） 上查看。

在此感谢以上专家。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱 research@c-csa.cn；国际云安全联盟 CSA 公众号。

序言

数字经济已经成为当今社会快速发展的主流经济，越来越多的国家和企业加速谋划和布局数字经济，抢占发展制高点。我国“十四五”规划中明确提出“加快数字化发展、建设数字中国”的目标，《数字中国建设整体布局规划》发布，在此背景下，我国正处于数字化转型的关键时期，数字技术成为核心引擎，数据成为新的生产要素。云计算、大数据、物联网、人工智能、区块链等新技术正在不断地应用和创新，对数据的开发利用和风险管控已成为当今甚至将来很长一段时间内的热点话题。数据从资源形态通过价值释放转变为资产，通过不断地应用和流通进阶为新的生产要素。数据要素驱动产业数字化转型已经成为全球共识。随着数字技术与实体产业、实体经济的不断融合，各类数字化技术对数据充分地开发和利用，数字空间正在不断的影响和改变着我们生产和生活的方方面面。一方面是物理世界对数字空间的依存度增加了，另一方面是数字空间对物理世界产生的影响、带来的安全风险也将会更大。所以在数字空间视角下，我们认为数据安全的内涵与外延正在不断的扩展。

新事物的发展必然带来变化和不确定性，随着数字化转型的不断深化，数据在不同的主体、不同的场景下以不同的形态在不断地流转与应用，随之带来的数据泄露、数据破坏、数据违法违规使用等等各类数据安全事件也是层出不穷。传统的信息安全风险管理方法已不再适用当今高速发展和不断变化的数字化业务，也无法实现数据全生命周期过程的风险管控。

我国《数据安全法》第二章第十八条中明确提及“国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在**数据安全风险评估、防范、处置**等方面开展协作。”

综上，以合规遵循、业务发展、风险防控等多方面需求驱动，本文构建了以数据为中心的风险管理框架，在充分分析各类数据处理活动场景所面临的数据安全风险的基础上，从数据安全风险管理规划、数据处理活动管理、数据安全风险评估、数据安全风险处置、数据安全风险监督改进、数据安全风险沟通与评审等六大方面给出了切实可行的管理方法，以及通过 20 套附录工具提供了详尽的实践思路，期望能够为各企业数据安全从业者提供参考和帮助。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

1 数据安全政策和背景

1.1 数字经济发展现状

1.1.1数字经济的概念界定和分类范围

进入数字经济时代，世界各国对数据的依赖快速上升，数据已成为国家基础性战略资源，对社会生活方式、经济运行机制、国家治理能力等产生重要影响。

数字经济，是指以数据资源作为关键生产要素、以现代信息网络作为重要载体、以信息通信技术的有效使用作为效率提升和经济结构优化的重要推动力的一系列经济活动。

中国信通院发布的《中国数字经济发展报告（2022）》显示，2021 年我国数字经济规模达到 45.5 万亿元，同比名义增长 16.2%，高于同期 GDP 名义增速 3.4%，占 GDP 比重达到 39.8%。

“十三五”期间，我国数字经济增长主要体现在网上购物、移动支付、在线教育、短视频等领域。

“十四五”规划纲要中明确指出，进一步发展云计算、大数据、物联网、工业互联网、区块链、人工智能、VR 与 AR、数字社会建设等七大数字经济重点产业，意味着数字经济正在成为国家的重点发展对象。

根据国家统计局发布的《数字经济及其核心产业统计分类（2021）》，数字经济产业范围被确定为：1 数字产品制造业、2 数字产品服务业、3 数字技术应用业、4 数字要素驱动业、5 数字化效率提升业等 5 个大类。

数字经济核心产业是指为产业数字化发展提供数字技术、产品、服务、基础设施和解决方案，以及完全依赖于数字技术、数据要素的各类经济活动。分类中 1-4 大类为数字经济核心产业：主要包括计算机通信和其他电子设备制造业、电信广播电视和卫星传输服务、互联网和相关服务、软件和信息技术服务业等，是数字经济发展的基础；第 5 大类为产业数字化部分，指应用数字技术和数据资源为传统产业带来的产出增加和效率提升，是数字技术与实体经济的融合。如图 1 所示：

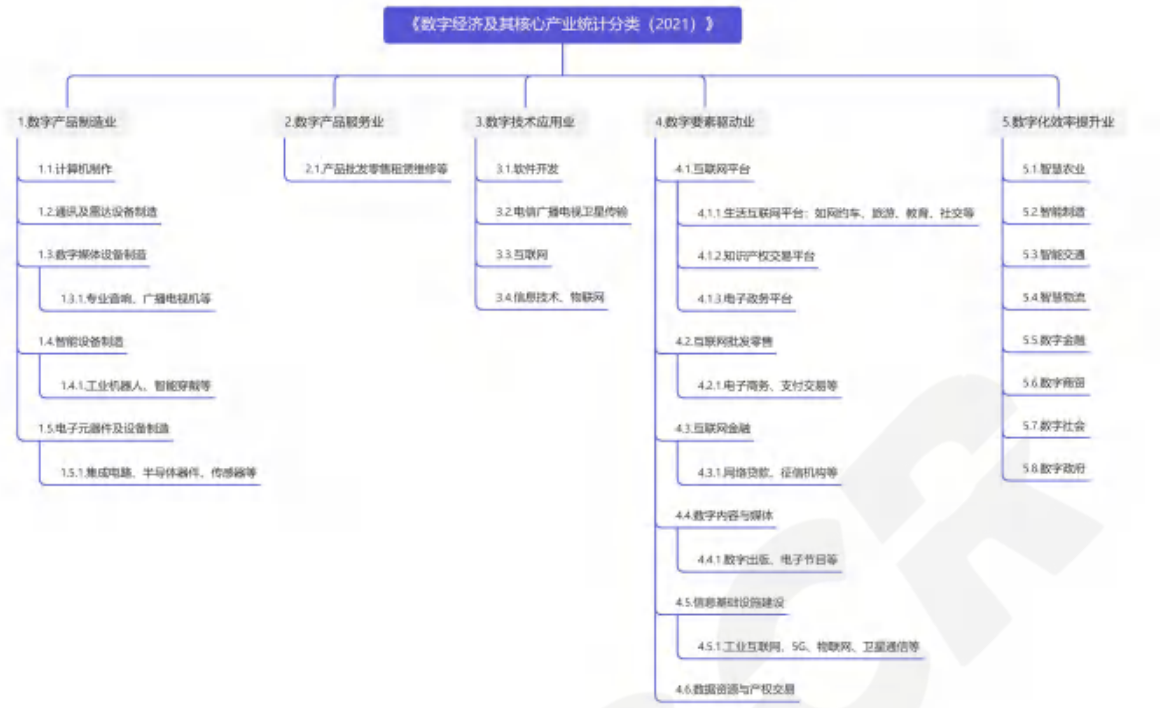

图 1 数字经济及其核心产业统计分类图

1.1.2我国主要区域相关政策和发展目标

目前，我国各省市已陆续出台数字经济相关规划、行动计划、指导意见等，涵盖数字经济、制造业与互联网融合、智慧城市、数字政府等领域，持续推动数字经济战略政策落地实施。

2021 年我国各省市共出台 216 个数字经济相关政策，其中，32 个顶层设计政策、6 个数据价值化政策、35 个数字产业化政策、54 个产业数字化政策、89 个数字化治理政策。

我国数字经济发展具有区域聚集特征，京津冀、长三角、珠三角、川渝等区域成为我国数字经济发展的核心区域，这些区域的数字经济发展目标在相关政策文件中基本明确，如表 1 所示：

表 1 各区域数字经济发展目标表

省（市）	所属区域	政策文件	发展目标
北京	京津冀	《北京市促进数字经济创新发展行动纲要（2020-2022 年）》	打造成为全国数字经济发展的先导区和示范区；到 2022 年，数字经济增加值占地区 GDP 比重达到 55%。
天津		《天津市促进数字经济发展行动方案（2019-2023 年）》	到 2023 年，数字经济占 GDP 比重全国领先，力争把滨海新区打造成为国家数字经济示范区。
河北		《河北省数字经济发展规划（2020-2025 年）》	到 2022 年，基本形成以大数据产业、制造业数字化、服务业数字化、电子信息产业为支撑的数字经济发展格局；到 2025 年，全省电子信息产业主营业务收入突破 5000 亿元。
上海	长三角	《关于全面推进上海城市数字化转型的意见》	到 2025 年，上海全面推进城市数字化转型取得显著成效，国际数字之都建设形成基本框架；到 2035 年，成为具有世界影响力的国际数字之都。
浙江		《浙江省国家数字经济创新发展试验区建设工作方案》	到 2022 年，浙江数字经济增加值要达到 4 万亿元以上，占全省国民经济生产总值比重超过 55%,基本建成全国领先的数字政府先行区、数字经济体制机制创新先导区、数字社会发展样 板区、数字产业化发展引领区和产业数字化转型标杆区。

江苏		《关于深入推进数字经济发展的意见》	以建设数字经济强省为总目标，全力打造具有世界影响力的数字技术创新、国际竞争力的数字产业发展、未来引领力的数字社会建设和全球吸引力的数字开放合作“4”大高地。
广东	珠三角	《广东省培育数字经济产业集群行动计划（2019-2025年）》	建成“国家数字经济发展先导区”，力争2022年数字经济规模达7万亿元，占GDP比重接近55%。
深圳		《深圳市数字经济产业创新发展实施方案（征求意见稿）》	到2022年，全市数字经济产业增加值突破2400亿元，年均增速15%左右；努力建成全国领先、全球一流的数字经济产业创新发展引领城市。
佛山		《佛山市推动数字经济发展实施方案》	2035年全市数字经济总体规模达2万亿元，努力将佛山打造成全国数字经济发展标杆城市之一。
重庆	川渝	《重庆建设国家数字经济创新发展试验区工作方案》	力争到2022年，数字经济总量达到万亿级规模，占GDP比重达到40%以上。
四川		《国家数字经济创新发展试验区（四川）建设工作方案》	力争到2022年，全省数字经济规模超过2万亿元，占GDP比重达到40%。
成都		《成都市推进数字经济发展实施方案》	到2022年，基本形成较为完善的数字经济生态体系，数字经济重点领域产业规模超过3000亿元。

1.1.3数字经济时代的数据安全治理

数据已经成为数字经济时代发展的核心生产要素，数据的安全保护和合法共享也被视为数字经济发展的重大挑战。

从产业发展规律来看，数据安全作为新兴产业，仍面临制度体系、技术和管理体系、产品体系、标准体系、人才体系、评价体系、生态体系等不完备的问题，对产业及企业发展形成诸多制约。

现阶段，国家、行业主管部门的法律法规不断出台，产业、行业的标准规范也在加紧编制、发布，以数据安全合规和数据安全治理为主题发布的白皮书层出不穷，为各行业落实数据安全法律法规要求和初步试行数据安全治理提供了有效的参考和依据。但是，由于数据确权、敏感数据识别、数据流转保护等法律、技术难题的客观存在，从具体行业应用场景来讲，有效、可靠、方便、可负担的解决方案还是不够。

本白皮书以企业数据处理者视角切入，从企业的合规遵循需求、业务发展需求、风险防控需求出发，尝试给出数据生命周期的风险管理方法和运营方案，以保障企业数字化转型的顺利开展，促进数字经济的进一步发展。

1.2 数据安全政策现状

国家竞争焦点正从土地、人口、资本、资源的争夺转向对数据的争夺。未来国家层面的竞争力将部分体现为一国拥有数据的规模、开发利用以及掌控的能力，“数据主权”将成为继边防、海防、空防之后另一个大国博弈的空间。

发达国家和领先的发展中国家都在快速布局和完善数据安全政策和法规，以避免在数字经济发展中落后、受困。

1.2.1国内数据安全政策现状和趋势

1.2.1.1 法律法规

近年来，我国《网络安全法》《数据安全法》《个人信息保护法》等数据安全相关法律法规的相继颁布，为数据安全建设提供了制度支撑和法律保障。

2015 年 7 月 1 日，我国公布并施行了《国家安全法》，并提出“维护国家网络空间主权、安全和发展利益”，为后续《数据安全法》等针对性法律的出台，奠定了基础。

2017 年 6 月 1 日，《网络安全法》施行，提出 “采取技术措施和其他必要措施，维护网络数据的完整性、保密性和可用性”。

2020 年 1 月 1 日，《密码法》施行，为规范密码应用和管理、促进密码事业发展、保障网络与信息安全，提供有效法律支撑。

2021 年，《民法典》《数据安全法》《个人信息保护法》相继施行，标志着我国以数据安全保障数据开发利用和产业发展全面进入法治化轨道，重要数据及个人信息保护成为时代需求。

从“五法一典”的发布进程来看，我国数据安全政策体系经历了从草创到完善的过程，数据安全领域的基础法规架构已初步构建完成，数据安全产业从此进入新的发展快车道，迎来发展的黄金期。

1.2.1.2 地方政策

从地方维度看，广东省在数据安全立法方面，出台相关政策最多，高达 7 项；浙江省紧随其后，出台相关政策 5 项；其次是贵州省、山东省、江苏省、山西省等地区。

此外，北京、上海、天津等数据要素市场化进程较深入的直辖市，均有出台相关政策。而地方性政策的发布时间，主要集中在 2019 年、2020 年和 2021 年。

近几年作为我国工业经济向数字经济迈进的关键时期，地方致力于促进数据依法有序自由流动，保障数据安全，加快数据要素市场培育，推动数字经济更好融入新发展格局，并以“数据”为中心，积极出台针对性政策条例。

目前比较有代表性的地方性数据安全政策有《深圳经济特区数据条例》和《上海市数据条例》等，这些地方性安全政策的不断出台，将为地方推动数字经济更好服务和融入新发展格局，奠定基础。

中国各省份、直辖市，乃至主要城市，在未来几年内，将会陆续出台更多地方性数据安全相关政策，以保障地方在数据要素市场化以及数字化转型过程中数据的安全。

1.2.1.3 行业政策

从行业维度看，适用全行业的数据安全政策数量较多，为整体上落实数据安全措施提供多场景规范性指导作用。

此外，从行业属性出发，政府领域因其行业特性，数据价值度高、敏感性强，针对数据安全的相关要求更高，成为出台数据安全政策数量最多的领域；互联网因为涉及大量用户个人信息，对数据安全也有较高要求，其次是金融、工业、医疗、教育、交通、电信等行业，其相关政策数量分别为 74 项、36 项、25 项、17 项、15 项、9 项、8 项、7 项、6 项。

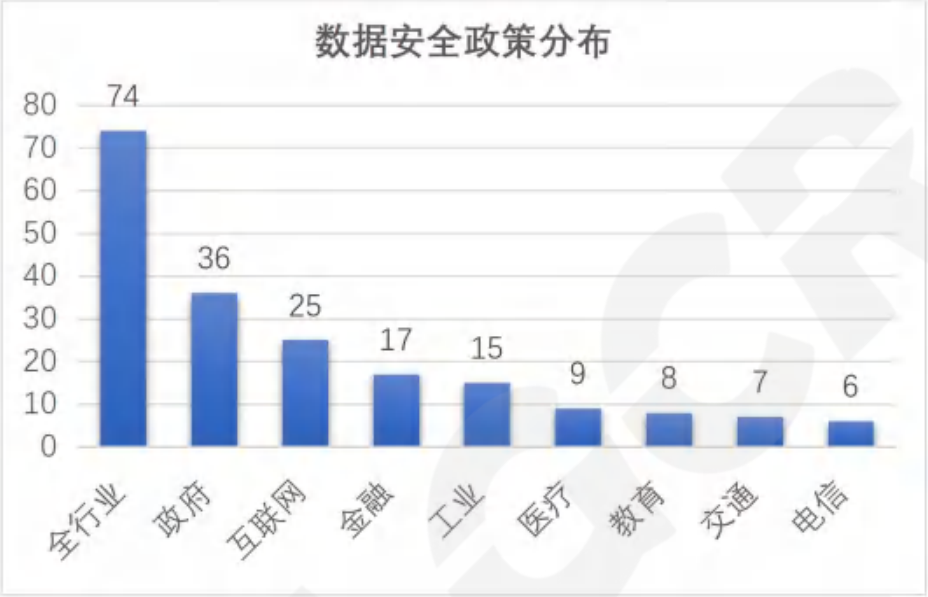

图 2 数据安全行业政策分布

从政策数量分布来看，数据安全政策的覆盖范围并不仅仅是政府、互联网等行业，而是全行业、全场景、全方位的。

但由于数据安全治理和企业的业务运营高度相关，数据流转应用的场景和问题又纷繁复杂，如何更好地既符合法规、政策要求，又满足企业业务发展，仍需要进一步细化的业务场景化的示范指南、标准规范来进一步支撑。

1.2.1.4 发展趋势

中央关于“十四五”规划和二〇三五年远景目标建议明确提出建设网络强国、数字中国，发展数字经济，建立数据安全保护基础制度和标准规范，保障国家数据安全。

一是数据安全产业政策环境进一步完善。《“十四五”大数据产业发展规划》对推动数据安全产业发展做出明确部署。《数据安全法》出台后，《网络数据安全管理条例（征求意见稿）》《工业和信息化领域数据安全管理办法（试行）》等数据安全相关行政法规、部门规章也陆续公开征求意见，催生数据安全产品和服务市场需求不断攀升，

助推数据安全产业繁荣发展。

二是数据安全标准体系进一步健全。安全发展，标准先行，标准化工作是保障数据安全的重要基础。2020 年，工业和信息化部印发《电信和互联网行业数据安全标准体系建设指南》后，满足行业监管需要、符合行业发展需求的数据安全标准体系逐步健全完善。

三是数据安全人才培养持续稳步推进。2022 年 4 月，在工业和信息化部网络安全管理局指导下，中国信通院、中国互联网协会发起“电信和互联网行业数据安全人才强基计划”，分阶段、分重点有序推进数据安全人才培养核心能力建设，面向紧缺岗位开展数据安全人才培养与能力认定，建设素质优良的行业数据安全人才库。

四是数据安全产业生态协同机制逐渐形成。近日，在工业和信息化部网络安全管理局的指导下，中国互联网协会成立数据安全与治理工作委员会，积极发挥平台作用，助力技术创新和产业发展。

1.2.2国外数据安全政策总体情况

各国数据保护法律法规主要围绕数据提供者、数据基础设施提供者、数据服务提供者、数据消费者、数据监管者等参与方，目的是将数据保护范围、各参与方对应的权利和义务、相关行为准则等要点界定清晰。

表 2 列举了美国、欧盟、澳大利亚、俄罗斯、新加坡等国已制定或发布的数据保护相关法律法规，这些国家的数据安全法律法规分为两类：

一是制定专门的数据保护法律法规，并明确相应的数据安全管理部门，如欧盟、俄罗斯、新加坡等。其中，俄罗斯有关数据安全的主要法律是《个人数据保护法案》，涉及到的主要监管部门是俄罗斯电信/信息技术和大众传媒联邦监管局。新加坡有关数据保护的主要法律是《个人数指保护法令》(PDPA)。同时，为了执行《个人数据保护法令》，新加坡专门成立了个人数据保护委员会（PDPC）来承担 PDPA 的制定和实施工作。

二是数据保护的相关要求分散地体现各国各项法律法规及部门规章的相关条款中，但尚未颁布数据保护的专门法律法规，也未设置相应的管理部门，如美国、澳大利亚等。

表 2 国外数据保护相关法律规范

国家/地区	法律法规名称	条款内容	生效时间
美国	《隐私法案》	针对联邦行政部门收集、利用和保护个人数据等方面做出规定，适用于美国公民和在美国取得永久居留权的外国人。 侧重四个政策目标： 1) 限制披露各机构保存的个人信息记录； 2) 限制披露各机构保存的个人信息记录； 3) 授予个人修改信息记录的权利； 4) 要求政府机构遵守收集、维护和公开记录的法定规范。	1974 年 12 月美国国会通过
	《电子通信隐私法》	详细规定了执法机关访问电子通信和相关数据的标准，不仅针对动态传输的有线、口头与电子通信保护作出具体规定，还规范了对静态存储的电子通信的安全保障要求，协调国家安全与个人隐私、通信秘密保障之间的冲突。 包括“笔式记录器法”“窃听法”“存储通讯法”三个主要章节。 1) “笔式记录器法”针对执法机关利用笔式记录器或类似的追踪记录设备，记录或解码由传输有线或电子通信的仪器或设施传输的拨号、路由、寻址或信令信息的设备或过程，但该等信息不包括任何通信的内容； 2) “窃听法”管理实时性拦截通过线路进行传输的通讯，并将范围扩大到电子通信； 3) “存储通讯法”涉及对存储的有线和电子通信或账户记录的访问和披露，特别的是这部分首次界定了“电子储存”的概念。	1986 年美国国会制定
	《计算机欺诈和滥用法》	鼓励研究者出于公共利益去根除漏洞，为善意的安全研究人员提供明确的规定以促进网络安全的发展。 列举了获取国家安全信息、泄露机密、侵入政府电脑、获取欺诈和获取价值、损坏计算机或信息、贩卖密码、威胁要损坏计算机七类犯罪活动，以及“侵入计算机的局外人”“超出其授权范围的入侵者”两种违法情形。	1986 年 10 月 16 日美国总统 R. 里根签署
	《澄清海外合法使	该法案提出，无论服务提供者的通信、记录	2018 年 3 月

	用数据法案》	或其他信息是否存储在美国境内，只要相关通信内容、记录或其他信息为该服务提供者拥有、控制或者监管，均应当按照法令要求，保存、备份、披露。 该法案打破了以往跨国数据类证据调取过程中遵循的数据属地管辖模式，构建了一套全新的以数据控制者实际数据控制权限为衡量依据的标准框架。 该法案单方面赋予美国政府对全球绝大多数互联网数据的“长臂管辖权”,有关人士指出，这是美国政府对他国数据主权的挑衅，不仅侵犯个人隐私，而且与多国立法存在冲突，威胁到跨国企业的互利合作。 该法案主要规定包括： 1) 美国政府证据调取范围、 2) 明确服务提供者域外司法协助义务、服务提供者域外司法协助义务的例外、外国政府向美国企业请求获取数据的司法协助等。	23 日美国国会通过
	《消费者隐私法案》	2018 年 6 月，美国加利福尼亚州州长签署公布《消费者隐私法案》（California Consumer Protection Act，CCPA），并于 2020 年 1 月 1 日生效。 CCPA 为消费者控制个人信息提供了合法途径，被认为是全美当前最严格的隐私立法。 尽管，CCPA 是一部专门针对加州消费者的隐私保护法律，但加州的经济体量与科技创新实力居于世界领先，因此该部立法的意义深远超出其原本的立法层级，对其他州的立法进程起到重要标杆作用。 CCPA 的主要内容包括法案出台的背景、消费者的权利、企业的义务以及法案中用语的详细解释四个部分。《消费者隐私法案》规定，一旦企业违反隐私保护要求，将面临支付给每位消费者最高 750 美元的赔偿金以及最高 7500 美元的罚款。	2018 年 6 月美国加州州长签署 2020 年 1 月 1 日生效
	《关于加强国家网络安全的行政命令》	《行政命令》旨在采用大胆举措提升美国政府网络安全现代化、软件供应链安全、事件检测和响应以及对威胁的整体抵御能力，是美国政府对 SolarWinds 供应链攻击、微软 Exchange 漏洞攻击，以及 Colonial Pipeline 输油管道等一连串备受瞩目的重大网络安全事件的响应。	2021 年 5 月 12 日美国总统拜登签署

		《行政命令》包括九个部分的内容：政策、移除威胁信息共享的障碍、联邦政府网络安全现代化、增强软件供应链的安全、成立网络安全审查委员会、联邦政府网络安全漏洞和事件应急响应标准化、加强联邦政府网络中网络安全漏洞的检测能力、加强联邦政府网络安全事件的调查、修复能力、国家安全系统。	
	《消费者数据保护法》	2021 年 3 月 2 日，美国弗吉尼亚州州长拉尔夫-诺森（Ralph Northam）签署了《消费者数据保护法》，于 2023 年 1 月 1 日生效。这一法案的出台，使得弗吉尼亚州成为美国第二个具备数据隐私立法的州。 CDPA 参考借鉴了加州 CCPA 以及欧盟 GDPR 的成果，在推进企业保护消费者数据隐私、赋予消费者相关权利等方面更为完善。 CDPA 除了赋予消费者访问、更正、删除和获取个人数据副本的权利外，还明确消费者享有自由选择出售自身个人数据以及允许自身个人数据用于定向广告或分析决策的权利。	2021 年 3 月 2 日美国弗吉尼亚州州长签署 2023 年 1 月 1 日生效
	《统一个人数据保护法》	2021 年 8 月，美国统一法律委员会投票通过了 UPDPA，这是一项旨在统一各州隐私立法的示范法案，于颁布之日起 180 日生效。 UPDPA 基于数据实践有利于或不利于数据主体的可能性，对“兼容”“不兼容”和“禁止”的数据实践做出区分；对假名数据提供宽泛的豁免。 UPDPA 主要内容包括： 适用范围，个人数据主体所持有的个人数据，个人数据主体的访问权和更正权，假名数据，兼容、不兼容和禁止的数据实践，收集控制者、第三方控制者和实践者的责任，自愿共识标准，执行和规则制定。 该法适用于在该州范围内的由数据控制者或者数据处理者开展的活动，包括商务、生产产品或者是为本州居民提供服务。	2021 年 8 月美国统一法律委员会投票通过 颁布后 180 日生效

欧盟	《个人数据自动化处理中的个人保护公约》	《108 号公约》是世界上第一部关于数据保护的国际公约。旨在确保在每个缔约方在其管辖范围内的公民，不管其国籍或居住地，在对其个人数据进行自动化处理过程中得到保护，尊重其权利和基本自由，特别是对于隐私权方面的尊重。 《108 号公约》（2018 年版）由一般规则、数据保护基本原则、个人数据跨境流通、监管机构、相互协作、公约委员会、公约修正案、最后条款等八章节、32 条款构成。建立了有关个人数据保护的基本原则以及各缔约国之间的基本义务，并将对个人基本自由与权利的保护作为缔约国履行条约规定的国家义务的出发点。此外，公约委员会的建立，在一定程度上建立起了针对个人数据保护的多国合作框架。	1981 年欧洲委员会通过
	《关于涉及个人数据处理的个人保护以及此类数据自由流通的第 95/46/EC/ 号指令》	《95 指令》直接以指令而非条约的形式要求各成员国完善数据保护立法，致力于协调各国对自然人在数据处理领域的基本权利和自由的保护，消除个人数据在共同体内部自由流通的障碍。首次提出知情同意原则，将“数据主体已明确表示同意”作为数据处理的合法条件之一；采用统一立法模式，规定建立独立的数据保护机构，是个人信息保护法中主张域外效力的典型代表。 《95 指令》包括 72 条序言和 34 条条款，旨在提高欧洲个人信息保护法律的统一程度，弥补 1980 年出台的《第 108 号公约》，虽对成员国具有约束力，但真正执行国家并不多，实施效果也存在差异的现实情况，进而应对高速发展的信息技术时代带来的保护个人数据权利、消除法规不一所造成的数据流通障碍的双重挑战。	1995 年 10 月 24 日通过
	《通用数据保护条例》	2016 年 4 月 14 日，欧洲议会和欧盟理事会通过了《通用数据保护条例》，简称 GDPR，于 2018 年 5 月 25 日正式生效。 GDPR 被称为“史上最严隐私法案”。一方面，GDPR 赋予了个体用户对于自身数据更多的自主权和选择权；另一方面，GDPR 针对用户数据的控制主体和处理主体制定了十分严格的限制性规则，有力地推进欧盟数字单一市场的建立。 GDPR 具有域外效力管辖权设计，全球企业都可能受到 GDPR 的管制，GDPR 同时设	2016 年 4 月 14 日通过 2018 年 5 月 25 日生效

		立数据保护官等制度辅助企业义务的履行以及监督机构的监管。 GDPR 在《95 指令》的基础上重新制定，共计 11 章 99 条，相较于仅 34 条的《95 指令》来说，做出了多达 3500 处具体修改，GDPR 生效的两年后《95 指令》被废止。同时，GDPR 整合了之前的隐私保护指令、电子通信隐私保护指令以及欧盟公民权利指令等，通过统一欧盟法规来协调整个欧洲的数据隐私法律，保护所有欧洲公民免受隐私侵犯和数据泄露的侵害，并简化国际业务中对于数据隐私的监管方式。	
	《非个人数据自由流动条例》	《条例》旨在统一有关非个人数据的自由流动规则，与已经实施生效的 GDPR 形成数据治理的统一框架，以此平衡个人数据保护、数据安全，推进欧盟在单一数字市场战略下打造富有竞争力的数字经济。 《条例》包括 39 条序言和 9 条条款，从禁止数据本地化与推动发展新技术两方面，规范非个人数据流动。 《条例》界定了非个人数据的范畴，即为 GDPR 中界定的个人数据（任何已识别或可识别的自然人相关的信息）以外的数据；明确非个人数据在欧盟境内跨境流动的规则，为整个欧洲的数据存储和处理设定了框架，禁止数据本地化限制；允许有权机关为根据欧盟法或国家法履行其职责要求获取数据访问的权力，有权机关对数据的访问不得以数据在另一成员国处理为由受到拒绝；鼓励和促进欧盟层面自律性行为守则的制定，其以透明性和交互性原则为基础，合理考虑开放标准，保障数据转移和数据服务商自由转换。	2018 年 11 月 14 日颁布 2019 年 5 月 28 日生效
	《数据治理法案》	《法案》的出台，被视为落实《欧洲数据战略》所采取的重要立法举措，一定程度上强化了欧盟对于公共数据的赋能，为欧洲新的数据治理方式奠定了基础。 《法案》构建了三项适于各个行业的数据共享机制： 1) 公共部门数据再利用机制； 2) 数据中介机构及通知制度； 3) 数据利他主义制度。 《法案》共九章 38 条，包括一般规定、重复使用公共部门机构持有的某些类别的受	2021 年 11 月 25 日欧盟委员会发布 2022 年 4 月 6 日批准生效

		保护数据、适用于数据中介服务的要求、数据利他主义、主管当局和程序规定、欧洲数据创新委员会、国际访问和转移、授权和委员会程序、最终和过渡条款。《法案》明确了公共部门数据再利用条件。允许自然人或法人在公共部门所提供的安全处理环境中访问并再利用公共数据。《法案》针对可以被再利用的数据进行敏感性方面的限制，要求开展数据再利用的公共部门具有技术设备上的相关保障，各成员国必须设立一个单一联络点，支持研究人员和创新企业使用数据，以及必须建立能够通过技术手段和法律援助对公共部门进行支撑的数据再利用体系。公共部门机构应施加条件，以保持所使用的安全处理环境的技术系统功能的完整性。《法案》倡议建立非营利性质的“数据中介机构”，为公共数据空间提供基础设施。数据中介机构需要在指定的主管当局进行备案。	
德国	《联邦数据保护法》	《联邦数据保护法》旨在通过数据保护实现一般人格权的保护，同时强化个人信息自决权理论，这意味着德国将个人数据保护的法律站位上升到落实宪法（即《德国基本法》）的高度而不是简单的政府执法工作。 该法使德国数据保护法律制度与欧盟 2016 年颁布的《通用数据保护条例》（GDPR）和《关于有权机构在预防、调查、侦察或批捕犯罪嫌疑人或执行刑事处罚中自然人保护和有关数据自由流通的指令》相互衔接。 《联邦数据保护法》的主要内容为： 1) 法律主旨优先处理欧洲法而非国内宪法； 2) 保护的直接客体并非一般意义上的数据，而是与个人具有关联性的个人数据； 3) 立法目标和保护客体决定了该法保护权益的特殊性； 4) 明确侵犯公民个人信息自决权行为的犯罪构成要件和罚则。	1977 年德国联邦议会出台 最新修订于 2019 年 11 月
	《IT 安全法》	2021 年 5 月 28 日，德国联邦议院颁布《IT 安全法》2.0 版本，旨在保护重要基础设施数据安全，通过弥补法律漏洞并扩大监管框架，以提高德国 IT 系统的安全性，并加强国家安全。	2021 年 5 月 28 日颁布

		《IT 安全法》的主要内容为： 1) 扩大联邦信息安全办公室（BSI）的权限； 2) 加强对数字消费者的保护； 3) 新增制造商、供应商和关键基础设施部门的义务； 4) 对跨国传输要求设置官方查询联络点； 5) 对有关罚款的规定进行修订。	
澳大利亚	《隐私法》	《隐私法》于 1988 年颁布，是个人信息保护的一项法律，其三个特点为： 1) APP 实体必须采取合理措施保护个人信息免遭滥用、侵犯和丢失，以及未经授权的访问、修改或披露，并在收集个人信息的目的不再需要时销毁或取消其身份。 2) 制定了有关收集、管理、处理、使用、披露和以其他方式处理个人信息的要求。 3) 向境外传输个人信息之前，APP 实体必须采取合理措施，确保海外接收方不会违反与该个人信息有关的 APP。 《隐私法》的原则是对于有关个人信息的操作管理设定概括性的标准，它所适用的情形包括：个人信息的收集(例如，填写表格)；个人信息的使用和透露；个人信息的准确性；个人信息持有的安全性；个人取阅个人信息的权利等等。	1988 年颁布
	《电信法》	《电信法》于 1997 年颁布，确立了执法和情报部门要求私营部门提供针对加密技术的自愿性和强制性技术协助的法律框架。 被纳入国家关键基础设施范围内的电信运营商按照电信安全改革框架，采取措施全面提高网络安全水平。 《电信法》共计包括四个附表，附表一为标准运营商许可条件包括十个章节 88 条，附表二为标准服务提供商规则包括六个章节 20 条，附表三为承运人的权利与豁免包括三个章节 63 条，附表四 ACMA 可审查决定包括两个章节。	1997 年颁布
俄罗斯	《俄罗斯联邦个人数据法》	《俄罗斯联邦个人数据法》颁布于 2006 年 7 月 27 日，是个人信息保护领域重要法律，也是数据与信息安全法律制度体系中主要法律准则。其两个特点为：	2006 年 7 月颁布 最新修订于

		1) 个人信息匿名化处理条件。个人信息的匿名化只能在获得个人同意的情况下进行，或者在俄罗斯联邦法律在个人数据领域中规定的其他情况下才能进行。 2) 强化数据安全，保护数据主权。在跨境数据流动方面，实行严格管控制度，推行数据本地化制度其中包括隐私保护、维护网络安全、便利执法等具体监管目标，并且要求开始跨境传输个人数据之前，处理者有义务确保在个人数据传输到的外国国家对个人数据主体的权利提供充分的保护。 2020 年 12 月 10 日，俄罗斯联邦会议国家杜马发布《俄罗斯联邦个人数据法》修正案，进一步明确公共个人数据处理规则，旨在建立保护个人数据主体权利和自由的机制。	2020 年 12 月 10 日
新加坡	《个人数据保护法》	新加坡的数据保护法律体系以 2012 年通过的 PDPA 为主。 PDPA 承认个人有权保护其个人数据，而各组织则需要为一个合理的人在这种情况下认为适当的目的而收集、使用和披露个人数据。 为了更好地执行 PDPA，新加坡个人数据保护委员会 (PDPC)出台了一系列条例及指引，包括： 2021 年《2021 个人数据保护条例》、2021 年《个人数据保护（数据泄露通知）条例》、2021 年《个人数据保护（违法构成）条例》、2021 年《个人数据保护（执行）条例》、2013 年《个人数据保护（请勿致电登记处）条例》等。 此外，PDPC 还发布了咨询指南，用以解释 PDPA 以供企业合规参考。 PDPA 适用的主体包括个人、公司、协会、社会团体等法人或非法人团体，无论该等自然人或实体是否依据新加坡法律设立，是否为新加坡居民或居民企业，或是否在新加坡具有办事处或营业地，只要以上自然人或实体具备以下数据处理行为，均适用于 PDPA。	2012 年通过

韩国	《个人信息保护法》	PIPA 颁布时间为 2011 年 3 月 29 日，作为韩国管辖权范围内具有统一性、一般性、专门性的个人数据保护法律。对个人信息保护的基本原则、个人信息保护的基准、信息主体的权利保障、个人信息自决权的救济等问题作出了全面的规定。具有以下 4 个特点： 1) 明确数据跨境流动的多种渠道； 2) 建立隐私政策审查机制； 3) 引入数据可携权； 4) 对于自动化决策的拒绝权和解释权。 PIPA 主要包括十章节 76 条，主要包括个人信息保护原则、数据主体权利、国家责任和与其他法律关系、隐私策略制定、个人信息处理和安全管理、数据主体权利保障、信息通信服务提供者等处理个人信息的特殊情况、个人信息纠纷调解委员会、个人信息集体诉讼等，规定了个人信息的管理、个人信息的安全措施、信息主体的权利保障、个人信息的团体诉讼等制度，旨在保护所有公民的个人信息权益，以防信息收集、泄露、不当使用与滥用。法律的适用范围涵盖公共与私人部门管理的一切个人信息，通过规定与个人信息的处理和保护有关的事项，保护个人的自由和权利，实现个人的尊严和价值。	2011 年 3 月 29 日颁布 最新修订于 2020 年

2 数据安全风险管理概述

2.1 数据生命周期处理活动概述

2.1.1数据生命周期定义的思考

在 GB/T 35274-2017《信息安全技术 大数据服务安全能力要求》中对“数据生命周期（data lifecycle）”定义为：数据从产生，经过数据采集、数据传输、数据存储、数据处理（如计算、分析、可视化等）、数据交换，直至数据销毁等各种生存形态的演变过程。该标准中的“数据生命周期（data lifecycle）”概念与 GB/T 35295-2017《信息技术 大数据术语》中“数据生存周期（data lifecycle）”概念是一致的。GB/T 35295-2017 将“数据生存周期（data lifecycle）”定义为“将原始数据转化为可用于行动的知识的一组过程”，但是并没有给出具体的过程描述。

在 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》中沿用了“数据生存周期”的概念，并定义了 6 个阶段，其命名与 GB/T 35274-2017 完全一致。GB/T 37988-2019 对数据生存周期 6 个阶段的具体说明如下：

- 数据采集：组织内部系统中新产生数据,以及从外部系统收集数据的阶段；
- 数据传输：数据从一个实体传输到另一个实体的阶段；
- 数据存储：数据以任何数字格式进行存储的阶段；
- 数据处理：组织在内部对数据进行计算、分析、可视化等操作的阶段；
- 数据交换：组织与组织或个人进行数据交换的阶段；
- 数据销毁：对数据及数据存储媒体通过相应的操作手段,使数据彻底删除且无法通过任何手段恢复的过程。

特定的数据所经历的生存周期由实际的业务所决定,可为完整的 6 个阶段或是其中的几个阶段。

在其他一些标准中对“数据生命周期”的提法虽略有差异，但总体来说基本与 GB/T 37988-2019 的定义比较接近。例如：

- GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

数据全生命周期包括并不限于数据采集、存储、处理、应用、流动、销毁等过程。

- JR/T 0223-2021《金融数据安全 数据生命周期安全规范》

金融数据生命周期是指金融业机构在开展业务和进行经营管理的过程中，对金融数据进行采集、传输、存储、使用、删除、销毁的整个过程。

- YD/T 3802-2020《电信网和互联网数据安全通用要求》与 YD/T 3956-2021《电信网和互联网数据安全评估规范》

数据全生命周期各阶段（数据采集、数据传输、数据存储、数据使用、数据开放共享、数据销毁）。

此外，以下标准则直接采纳了 GB/T 35274-2017 中“数据生命周期（data lifecycle）”的定义：

- GB/T 39725-2020《信息安全技术 健康医疗数据安全指南》

数据生命周期内的各项活动，包括数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等。

- 联盟团标 T/ISEAA 002-2021《信息安全技术 网络安全等级保护大数据基本要求》

同 GB/T 35274-2017。

为了方便拉齐认知，本文将统一采用“数据生命周期”的概念，并以“采集、传输、存储、处理、交换、销毁”作为通用的 6 个阶段描述。针对不同业务场景，如无特殊说明，将统一采用上述说法。

2.1.2数据处理活动与数据生命周期的关系

在《数据安全法》中并没有“数据生命周期”的提法，但是其对“数据处理”的定义“包括数据的收集、存储、使用、加工、传输、提供、公开等。”实际上与“数据生命周期”有非常紧密的关联。为方便理解，我们将数据处理的 7 个活动与数据生命周期的 6 个阶段做了一个简单的对照，如下表所示。

表 3 数据安全生存周期与数据处理活动对比

GB/T 37988-2019 数据生存周期 6 个阶段		《数据安全法》 数据处理 7 个活动
数据采集	组织内部系统中新产生数据，以及从外部系统收集数据的阶段；	数据收集
数据传输	数据从一个实体传输到另一个实体的阶段；	数据传输
数据存储	数据以任何数字格式进行存储的阶段；	数据存储
数据处理	组织在内部对数据进行计算、分析、可视化等操作的阶段；	数据使用、加工
数据交换	组织与组织或个人进行数据交换的阶段	数据提供、公开
数据销毁	对数据及数据存储媒体通过相应的操作手段，使数据彻底删除且无法通过任何手段恢复的过程。	未定义

从以上对比可知，二者主要差异在于《数据安全法》未提及“数据销毁”活动。我们认为，数据处理活动强调的是关键活动场景，而数据生命周期强调的是全过程闭环，二者并没有本质的矛盾。为便于在不同过程或者活动中全面识别数据安全风险，本文充分参考了现行各行业的标准和相关实践，进一步丰富了数据处理活动场景，并将不同数据处理活动场景与数据生命周期阶段进行划分，以便在识别关键活动场景的同时，能够做到数据安全风险的闭环管理。

2.2 数据安全风险概述

2.2.1数据安全风险的概念

我国自 2021 年 9 月 1 日起施行的《数据安全法》是为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益而制定。其所称数据，是指任何以电子或者其他方式对信息的记录。而本文所指数据，遵照《网络安全法》的定义，为网络数据，即通过网络收集、存储、传输、处理和产生的各种电子数据，属于《数据安全法》中所定义数据的子集。

《数据安全法》中对数据安全的定义为“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”，并着重对数据处理活动中的风险防范、处置、评估提出要求，包括：

- 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；
- 发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向

有关主管部门报告；

- 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

虽然《数据安全法》并没有明确指出何为数据安全风险，但是有提及数据“一旦遭到篡改、破坏、泄露或者非法获取、非法利用”，会“对国家安全、公共利益或者个人、组织合法权益”造成不同程度的危害。结合《网络安全法》中所提到的“维护网络数据的完整性、保密性、可用性”与“防止网络数据泄露或者被窃取、篡改”，并综合参考GB/T 31722-2015《信息技术 安全技术 信息安全风险管理》和GB/T 20984-2022《信息安全技术 信息安全风险评估方法》中对“信息安全风险”的定义——特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害。

综上，我们可以了解到企业数据安全风险可以理解是企业数据的保密性、完整性、可用性、可控性受到影响后，可能引发的数据泄露、篡改、破坏、丢失、滥用或者非法获取、非法利用等等一系列会给国家安全、公共利益或组织、个人合法权益、企业自身利益造成影响的安全事件。

2.2.2数据安全风险的类型

图 3 数据安全风险分类示例

如上图，数据的安全风险可根据其来源整体上分为两大类，一是企业数据因越权访

问、非法爬取、脱库、撞库、非法拷贝、拒绝服务攻击、中间人攻击、嵌入恶意代码、数据污染、数据过载、人员有意或无意操作、设备故障、自然灾害等等安全威胁，利用管理制度流程及安全保障能力的脆弱性，影响数据的保密性、完整性、可用性、可控性而造成的数据泄露、数据篡改、数据破坏、数据丢失、数据伪造、数据滥用等等安全风险。二是因企业数据处理活动违反法律、行政法规等有关规定，因违法违规开展收集数据、存储数据、使用数据、加工数据、传输数据、提供数据、公开数据、交易数据等处理活动，引起的违法违规风险。以及其他可能对国家安全、公共利益或组织、个人合法权益造成影响的数据安全风险。

2.3 数据安全风险影响分析

2.3.1数据安全风险对国家的影响

随着信息科技的迅猛发展，数据包含丰富的商业价值，也作为国家的基础性战略资源与国家的安全和利益息息相关。数据监控、网络攻击、数据跨境等均会对国家的数据主权产生威胁，进而危及国家安全。

- **境外数据监控危及国家安全**

在棱镜门事件中，美国国家安全局对 Facebook、谷歌、微软等互联网公司的数据进行了监控和获取，这一举动严重侵害了各国用户的合法利益。美国出台的爱国者法案，也纵容其可以对存储在美国互联网公司云服务器中的任何数据进行随意地调查，这项规定为美国实施数据监控进行了铺垫，也给我国国家安全带来重大隐患。

- **关键信息基础设施网络攻击威胁国家安全**

关键信息基础设施往往包含大量的重要数据，是不法分子进行网络攻击的重点目标。《中华人民共和国网络安全法》第三十一条提到，关键信息基础设施是指提供公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域运行的信息系统，因此关键信息基础设施与国家安全、国计民生以及公共利益紧密相连，如果其遭到网络攻击，势必会影响国家安全。

- **数据跨境侵害国家数据主权**

数据跨境在推动经济发展的同时，可能也会侵害国家数据主权。由于各国数据发展

实力不尽相同，必然会存在发展强国和发展弱国。那么对于数据发展弱国来说，若不加入数据跨境的行列，则会限制自身的发展；若加入数据跨境的行列，但跨境又不予限制，将会有大量的数据流向数据发展强国，势必会侵害数据主权，进而影响国家安全。故而，平衡和合理限制数据发展强国与弱国之间的数据跨境，对于国家安全更有保障。

2.3.2数据安全风险对社会的影响

当前，数据已成为社会经济发展的关键生产要素和核心引擎，而数据掌握多寡成为世界各国软实力和竞争力的重要标志。为此，党中央、国务院高度重视数据安全工作，作出一系列重要部署，近两年连续将“数据安全”写入政府工作报告，纳入年度重点工作任务。

- **数据冲突挑战当前社会主流价值观**

互联网带给我们的是一个具有开放性、可存储性和可再现性的数字空间，面对获得数据的自由权利与数据安全的冲突、保护个人隐私与数据公开的冲突以及人类知识开放共享与知识产权保护的冲突等问题，必然带来了对当前社会主流价值观念的质疑和思考，在种种冲突与矛盾中该如何界定和划分是不能回避的问题。在解决这类问题时，人们会依靠道德和法律，这时道德和法律同技术一样重要。因此，必须完善法律制度，规范人们的行为，以形成新的价值观念。

- **国际化数据斗争制约社会经济发展**

大量的信息系统和应用业务要与国际接轨，诸如电信、电子商务、电子支付等使信息空间跨越国境，使得国际上围绕数据的获取、使用和控制的斗争愈演愈烈。国家的“数据边疆”在不断延伸和交错，“控制数据权”成为综合国力、竞争能力的重要体现。没有一个良好的数据安全体系，国家就会处于高度经济金融风险和信息战的威胁之中。

2.3.3数据安全风险对组织自身的影响

数字化时代，企业办公信息化程度越来越高，伴随而来的是数据泄露等数据安全事件发生的频率也越来越高。企业除了要面对来自外部的恶意攻击，还要应对内部的威胁行为。

- **数据意外泄露**

人们的潜意识里，通常会把数据泄露事件归结于黑客攻击，但其实他们两者之间并没有绝对的关联，很多数据泄露事件源于人员疏忽等导致的意外事件。大多数高级管理人员和小企业主表示，疏忽和意外损失是他们最近一次安全事件的根本原因。如员工由于操作失误将本不该共享的文件共享出去。这种数据泄露意外事件，对组织自身在商业竞争、合法利益、声誉信誉等方面的影响是极其恶劣的。

- **员工有意泄露**

前雇员或在职人员，可能是造成数据泄露最大的出口。内部员工尤其是肩负重要职位的涉密人员，通常是企业机构的最先得到及获得最多数据的，他们会在各种可能下出卖或带走数据。2017 年 1 月 17 日，华为公司就曾内部通报了已离职的 6 名员工涉嫌侵犯知识产权，将公司商业机密泄露给竞争关系公司，涉嫌构成侵权的专利估值高达 300 万元。来自内部员工的数据泄露，往往让组织疲于应对，造成的经济损失更是无法估量。

- **黑客攻击**

黑客往往会对有价值的对象发起攻击。黑客组织可以利用各种意想不到的方式来攻击网络，窃取数据，利用出售数据或勒索受害方支付赎金的方式肆意敛财。据美国网络安全公司 RiskIQ 发布的年度报告(Evil Internet Minute)显示，全球每分钟就有 1.5 家组织遭受勒索软件攻击，企业平均损失 15221 美元。这种来自黑客的攻击，会让组织在一定程度上遭受财产损失。

- **数据安全意识**

数据安全管理者通常会更注重数据安全技术，而忽视数据安全管理。对于大多数管理者而言，数据安全技术的采取，会更加迅速并且很直观地产生安全效应。然而，只有做好了数据安全管理，才能够将这种安全的状态持续下去，尤其是相关责任人的安全意识。

2.3.4数据安全风险对个体的影响

日常生活中，人们对于个人信息的保护意识相对淡薄，导致个人信息在收集、传输、使用、销毁等方面面临安全威胁。

- **个人信息收集过程中的威胁**

当前，数据成为了平台企业发展和盈利的核心引擎，大量的企业为了自身的商业利益，引发了个人信息过度收集、非法收集等安全事件。例如，应用强制获取系统权限，窃取用户个人信息，或者强制用户输入大量非业务必需的个人信息；恶意人员通过技术手段在没有取得用户同意的情况下，窃取访问记录、操作记录等个人信息。

- **个人信息传输中的威胁**

数据时代，信息的在线传输变得稀松平常，由此也引发了个人信息安全威胁。一方面，可能由于个人采取了不安全的传输方式，导致个人信息泄露；另一方面，可能由于不法分子将窃取的个人信息进行恶意传播或者售卖，导致个人信息泄露。这两种情况，均会对个体的名誉、隐私等合法权益产生影响。

- **个人信息使用过程中的威胁**

出于商业利益的诱惑，不法商家在过度收集和非法收集个人信息之后，会进行非法使用。一是个人信息倒卖黑市猖獗，姓名、身份证号、手机号等个人信息的贩卖产业链活跃程度进一步加深，个人隐私安全面临严重危机。二是所谓的“人肉搜索”。搜索者利用被搜索者在网络上散布的个人信息对其个人隐私不断挖掘，并且将其公布诱导更多的人参与，对被搜索者的正常生活造成极大的干扰，甚至有被搜索者无法承受选择结束自己的生命。三是算法推荐等大数据技术的不正当使用，从而带来的“信息茧房”“大数据杀熟”“网络沉迷”等社会隐患，也严重侵害了广大公民的个人权益。

- **个人信息销毁过程中的威胁**

数据时代，数字化存储极大地方便了人们的生活，但由于其容易复制的属性，引发出一系列数据销毁的安全问题。用户在互联网上进行的操作，会被网站记录下来，其中包含个人验证信息、操作记录、浏览次数等。即使有相关法律法规进行约束，要求在保存一定时间之后进行销毁，但数据销毁行为不易监管，无法确认是否彻底销毁了数据而未保留任何副本。同时，也可能由于数据销毁不彻底导致个人信息泄露。

2.4 数据安全风险管理的必要性

数据安全是网络空间安全的基础，是国家安全的重要组成部分，其重要性已经引起政府部门和企事业单位的重视，也是科研工作者更加需要关注的研究领域。为了控制数据安全风险造成的不同程度的影响，数据生命周期中的每个处理活动场景都需要针对性

的数据安全风险控制措施作为支撑，我们认为做好数据安全管理可从三个方面推进数据安全治理体系的落实。

一是有助于奠定数据安全治理基础，构建数据安全底座。通过数据资产发现、识别与梳理，进行资产盘点，开展数据分类分级，基于数据分类分级结果、重要数据的流转及使用情况，构建数据风险管理体系，为后续场景化的数据安全能力落地提供坚实支撑。

二是可以为数据全生命周期安全策略的制定提供依据。数据安全风险管理输出了数据安全风险评估分析和处置结果，因此可以在此基础上，以业务场景下的数据全生命周期视角，梳理数据安全策略架构；基于数据处理活动，识别具体业务场景，将数据、动作和特定人员或组织进行关联，有针对性地设计安全防护措施。

三是为有序建设，分步落实数据安全能力奠定基础。在数据安全风险管理基础上，围绕威胁路径，梳理数据安全关键能力，明确数据安全能力建设的优先级、依赖关系、所需资源，确保可执行性，实现数据安全痛点问题的精准管控。

3 数据安全风险管理

3.1 数据安全风险管理框架

图 4 企业数据安全风险管理框架

本文借鉴 GB/T 31722-2015《信息技术 安全技术 信息安全风险管理》中的风险管

理思路，以数据识别和场景识别为基础，充分考虑各类数据所处的活动场景，形成了企业数据安全风险管理框架，帮助企业应对各类数据安全风险，如上图 3 所示。风险管理框架主要包括数据安全风险管理规划、数据处理活动管理、数据安全风险评估、数据安全风险处置、数据安全风险沟通与评审、数据安全风险监督改进六个环节，其中数据安全风险沟通与评审和数据安全风险监督改进贯穿数据安全风险管理流程始终。

企业数据安全风险管理不仅是一套工具组合而成的产品级解决方案，而是从决策层到技术层，从管理制度到工具支撑，自上而下、贯穿整个组织架构的完整链条。企业数据安全风险管理框架的各个环节相辅相成、互相支撑。数据安全风险管理规划将从组织层面、政策层面、数据资产梳理角度做好准备工作，它是数据风险管理的基础，首先要“摸清家底”，且数据安全风险管理组织内的各个层级需要对数据安全风险管理的目标和宗旨达成共识；数据处理活动管理对“家底”怎样进行管理、分类分级、典型场景建立相应的方法论，为后续的数据安全风险评估提供方法论支持；数据安全风险评估阶段将根据数据处理的方法论，借助技术手段进行风险评估；数据安全风险处置阶段将根据风险评估结果触发相应的处置策略；数据安全风险沟通与评审和数据安全风险监督改进环节也是框架中必不可少的环节，它为最终的管理目标实现提供了实时的“风向标”。

数据安全风险管理规划：此阶段工作主要是做好数据安全风险管理的顶层设计，包括明确管理目标、明确管理对象和范围，建立管理组织架构，明确人员责任和权利。在进行正式的风险管理之前，先做组织和政策保障的工作，成立专门的数据风险管理小组，制定相应的管理目标和管理策略，并梳理企业自身的数据资源情况，为后续的工作打下基础。

数据处理活动管理：此阶段工作首先要明确数据资源管理的目标、方法，明确数据资产识别、数据分类分级工作开展的思路、方法、过程，然后梳理清楚企业数据处理活动的典型场景。为企业数据安全风险管理提供方法论支持，避免过程中出现分散管理、多方向、多模式的乱象。

数据安全风险评估：此阶段主要采用安全产品和技术手段对数据安全风险进行评估（可借鉴传统的信息系统风险评估工作模式），如进行数据识别、场景识别、威胁识别、现有控制措施识别、脆弱性识别，进而进行风险分析、风险计算和风险评价，最终得出风险清单。此阶段是风险管理的核心环节，能够准确并全面地评估出企业数据的风险将

对风险处置和风险屏蔽的完成率起着决定性作用。

数据安全风险处置：此阶段是对上一阶段发现的数据安全风险制定具体的风险处置措施，根据不同的风险等级采用不同的风险处置策略，也可以通过平衡成本和风险容忍度，采取控制风险、转嫁风险、避免风险、接受风险等手段进行风险处置。此环节是整个数据风险管理框架的最后一环，是风险管理的最终目的。

数据安全风险沟通与评审：此阶段贯穿数据安全风险管理始终，主要活动包括获得管理层对数据安全风险管理的支持、明确数据安全风险管理的内在需求和外在合规要求，对风险处置结果进行确认。它对整个风险管理的朝着既定目标发展保驾护航。

数据安全风险监督改进：此阶段贯穿于数据安全风险管理始终，此阶段可以采取一定技术手段、管理手段、运营手段，对数据安全风险进行安全监督和监测，监测数据安全风险的状况，并可以通过进行外部第三方认证的形式，来获得对数据安全风险管理工作的认可。保证风险识别和风险处置的准确性和有效性。

3.2 数据安全风险管理规划

3.2.1数据安全风险管理目标

数据安全风险管理要以最小成本获得最大安全保障，或者以最小的成本将数据安全风险控制到最低水平。数据安全风险管理的目标是让数据处理更安全，保障数据保密性、完整性、可用性，以及数据处理的安全合规性，本质上也是保障数据资产的价值。数据安全风险管理的最终目的是支撑组织机构的业务，要能切实落实如下关键任务：

- 对数据处理者的数据和数据处理活动进行全面安全评估和管理，了解处理的数据及开展数据处理活动的情况，发现存在的数据安全风险和违法违规问题，及时防范数据安全风险；
- 对重要数据和个人信息处理活动定期开展风险评估，了解处理的重要数据的种类、数量及开展数据处理活动的情况，对面临的数据安全风险及其应对措施进行处置和管理。
- 对开展共享、交易、委托处理等活动进行数据安全风险评估，发现对外提供重要数据可能存在的数据安全风险和问题；

- 在开展可能直接影响国家安全、公共利益或者大量个人、组织合法权益的数据处理活动前开展数据安全风险管理，发现可能存在的数据安全风险和违法违规问题。
- 根据数据安全事件和监管需求，由国家、行业或地方主管监管部门组织开展数据安全评估检查，发现数据安全风险和问题。

企业数据安全风险管理从战略和战术层面支撑数据安全治理工作的开展，通过制定数据安全策略和流程来保护企业数据，通过实施安全访问、分类分级、合规使用的数据安全策略，实现业务的目标，数据安全风险管理涉及数据、业务、安全、技术、管理、运营等多个方面。企业数据安全风险管理是企业风险管理的一个子集，数据安全风险管理既可在企业风险管理框架下进行，也可独立实施。

3.2.2数据安全风险管理的对象和范围

企业数据安全风险管理是企业落实数据安全治理体系的核心，也是企业数字化转型的基础，是企业的一个顶层策略，包括从企业战略、企业文化、组织建设、方法策略、制度体系、流程建设、技术和工具等多个方面提升数据安全风险应对能力的过程，控制数据安全风险或将风险带来的影响降至最低。

数据安全风险管理是基于风险的数据安全管理，也就是，始终以风险为主线进行数据安全的管理。从概念上讲，数据安全风险管理应该涉及角色、数据、数据操作、数据载体和数据环境中的各类对象。因此根据实际业务目标的不同，数据安全风险管理的侧重点，即风险管理选择的范围和对象重点应有所不同。

3.2.3数据安全风险管理组织

企业开展数据安全风险管理工作，应与数据安全管理以及其他管理工作紧密结合，把风险管理的各项工作要求融入数据安全管理、业务管理和业务工作流程中。建设如下数据安全风险的组织架构。

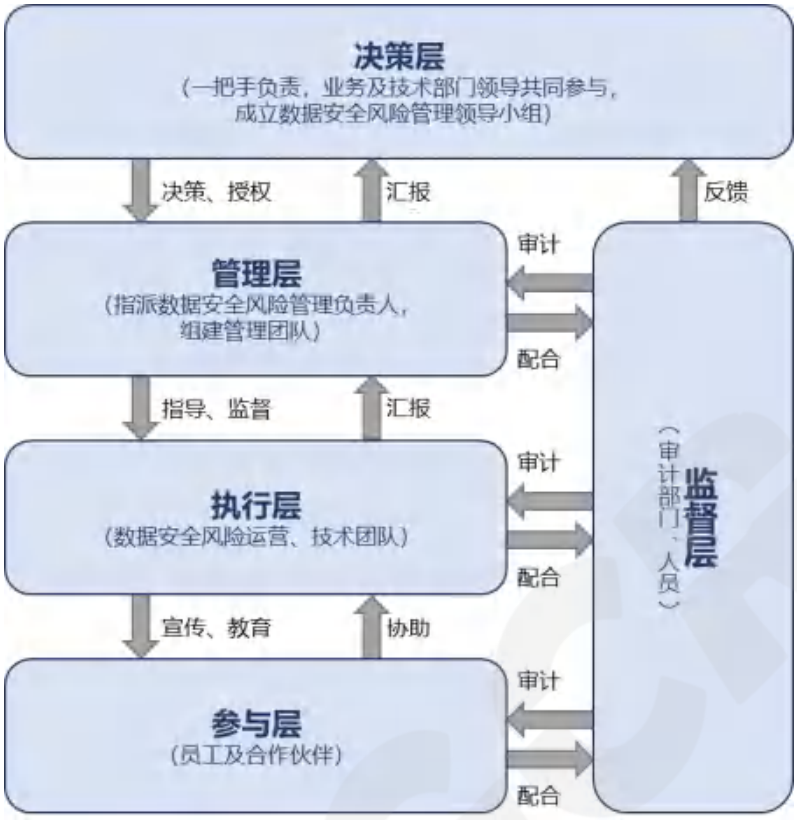

图 5 企业数据安全风险管理组织架构

1、 决策层是企业数据安全风险管理领导小组，由企业一把手负责，业务及技术部门领导共同参与，总体负责数据安全风险管理工作的统筹组织、指导推进和协调落实。

2、 管理层负责企业数据安全风险管理工作，成员包含主要部门的主要负责人，负责数据安全风险相关工作的实施、相关政策和制度的制定评审工作，对企业数据安全风险进行组合管理，度量风险和评估风险，确定数据安全风险的关键指标，建立数据安全风险预警机制，保障数据安全风险管理工作所需资源，并设立数据安全风险管理专职部门或岗位，负责日常数据安全风险管理工作。

3、 执行层负责落实数据安全风险管理，根据公司的数据安全风险管理策略和规程，落实本部门的数据安全风险防控和管理。识别数据安全风险的类别，对相关风险进行评估，决定转移、避免或降低风险的策略，对本部门有关的数据安全事件进行防控和处置。

4、 参与层是全部业务的参与者，包括内部员工及外部合作伙伴，应定期开展数据安全风险意识宣传教育工作。对专业的技术人员开展数据安全风险管控技术培训，并要求其通过权威的认证，以保证其有能力完成其所承担的工作。

5、 监督层对管理层、执行层、参与层的工作进行定期审核监督。由安全审计和稽核部门组成，提供独立、客观的数据安全风险管理审查，监督数据安全风险管理政策的执行。通过系统的方法进行审计和分析，发现的问题及时反馈给决策层，对违规行为予以纠正，并对后续的整改情况进行监督。

3.3 数据处理活动管理

DIKW（Data-to-Information-to-Knowledge-to-Wisdom Model）模型中提到：通过某种方式组织和处理数据，分析数据间的关系，就得到了信息，从而使得数据在企业各类业务活动中具备了上下文和含义，从而在不断应用和流动中产生价值。

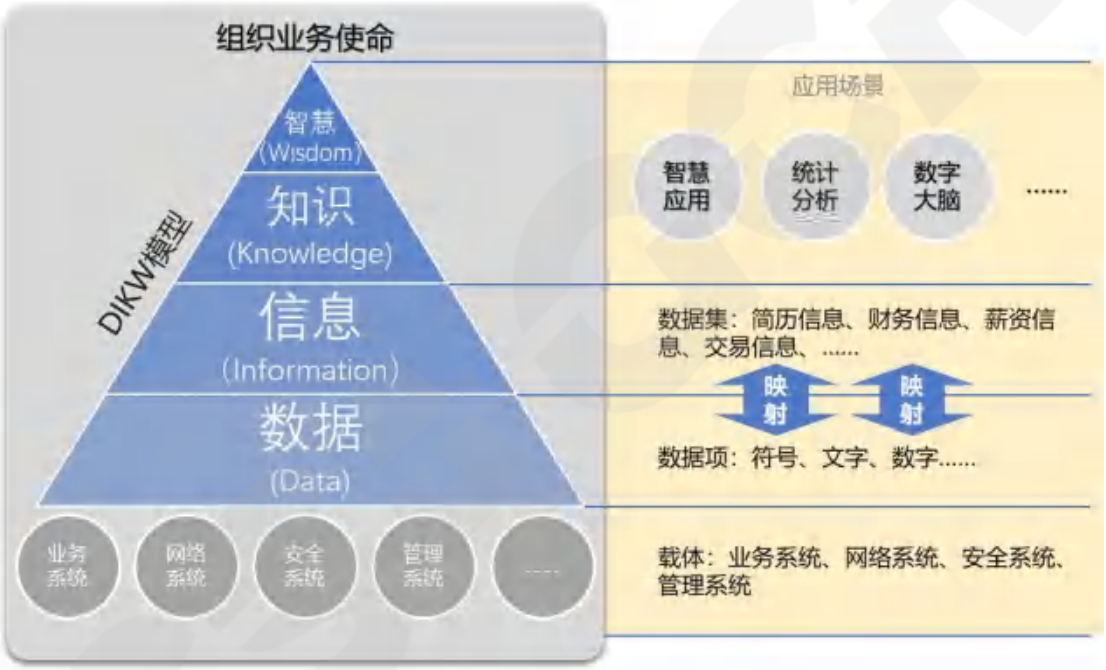

图 6 建立数据与信息的映射关系

在数据安全风险管理的视角下，数据处理活动管理的目标是在业务活动与系统数据存储间建立起数据处理活动场景与业务信息、数据集、数据项的映射关系，从而将静态存储的数据和动态流转与使用的数据关联起来，实现数据处理活动的管理。

3.3.1数据识别与标记

数据成为资源是发现和利用数据价值的一个过程，数据管理是数据资产管理和数据安全保护的必要过程，一方面可为数据资产管理提供数据模型、数据标准、数据质量等基础支撑，另一方面可为数据安全保护明晰对象和范围，为数据安全建设筑牢根基。

在企业中，并非所有的数据都构成数据资产，数据资产是能够为组织产生价值的数据资源1，数据资产的形成需要对数据资源进行主动管理并形成有效控制。数据安全保护不能仅限于价值保护层面，需要以合规遵循、风险控制、业务战略等多维视角驱动，应当聚焦在企业业务活动中的各类数据，通过数据资产管理对数据进行价值转化的过程中，同步关注各类数据的安全风险和保护措施。

以数据安全风险管理为目标，为有效识别各类数据在不同场景下面临的威胁和存在的脆弱性，我们认为需要做好数据识别、业务信息识别、数据分类分级等相关工作。

3.3.1.1 数据识别

数据识别过程应当围绕业务场景充分识别其业务活动中涉及终端、应用系统、数据存储节点下的各类数据。

- **结构化数据识别**

结构化数据识别，应当以应用系统为单位，充分识别各系统，以及所关联数据库中存储的库、表、列等基本结构化数据信息和数据相关方，形成结构化数据清单。《结构化数据清单》应包含库、表、列的原始名称及其对应的中文含义和说明信息、数据量级、数据相关方信息等基本内容，可参考【附录 **B.1 数据清单 表 12**】。

- **非结构化数据识别**

非结构化数据识别，应当以业务为单位，充分识别业务活动所涉及终端、移动介质、应用系统、数据存储服务器中与业务相关的数据文件资源。《非结构化数据清单》应包含数据文件存储路径、数据文件名称、数据文件内容描述、数据文件格式、数据文件量级、数据文件相关方等基本内容，可参考【附录 **B.1 数据清单 表 13**】。

3.3.1.2 业务信息识别

数据在业务活动中流转和应用时，往往不是固定的结构或者单一的文件，而是根据业务活动需要以数据集的形式呈现在各类应用场景下。这里我们将业务场景下有具体业务含义的数据集称为信息，如果将上述两个步骤理解为静态数据识别，那么此环节则是聚焦业务活动中的动态数据。《业务信息映射清单》应包含：业务分类、业务条线、业

[1] 信通院《数据资产管理实践白皮书（5.0 版）》
数据资产是指由组织（政府机构、企事业单位等）合法拥有或控制的数据资源，以电子或其他方式记录，例如文本、图像、语音、视频、网页、数据库、传感信号等结构化或非结构化数据，可进行计量或交易，能直接或间接带来经济效益和社会效益

务活动名称、业务信息名称、结构化数据集映射描述、非结构化数据集映射描述、数据项描述等相关信息，可参考【附录 **B.1 数据清单 表 14**】。

3.3.1.3 数据分类分级[2]

数据分类分级是明确数据基本属性、应用场景和重要程度的基础环节，也是数据安全风险管理的必要输入。企业开展数据分类分级时，应同时遵守国家和行业数据分类分级要求和规范，若企业所属行业暂无数据分类分级规范时，应当以国家要求和规范为主要遵循。本文参考全国信息安全标准化技术委员会在 2021 年 9 月发布的《网络安全标准实践指南——数据分类分级指引》来针对数据的分类与分级进行阐述。数据分类可以使数据中心化、聚类化，从而使数据能够发挥出更大的价值，为数据管理和使用提供更精准有效的基础样本；数据分级则可以保证不同敏感级别数据的保护措施能够处理得更加合理科学，确保数据的安全、可控、可用，避免“一刀切”问题。整体过程应当遵循“先分类、再分级、审批上报、动态管理”的标准流程。

（1）数据分类

进行数据分类时，按照先行业领域分类、再业务属性分类的思路进行分类。行业领域视角，可将数据分为工业数据、电信数据、金融数据、能源数据、交通运输数据、自然资源数据、卫生健康数据、教育数据、科学数据等行业领域数据。业务属性视角，包括但不限于业务条线、责任部门、描述对象、上下游环节、数据主题、数据用途、涉及数据处理活动、数据来源等维度进行分类。

如涉及法律法规有专门管理要求的数据类别（如个人信息），应按照有关规定或标准对个人信息、敏感个人信息进行识别和分类。

（2）数据分级

进行数据分级时，建议通过定量与定性相结合的方式，首先识别数据分级要素情况，然后开展数据影响分析，确定数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响的对象和影响程度，最终综合确定数据级别。

a) 影响数据分级的要素，包括数据领域、群体、区域、精度、规模、深度、覆盖度、重要性、安全风险等，其中领域、群体、区域、重要性、安全风险通常属于定性要

[2] 《信息安全技术 网络数据分类分级要求》征求意见稿）

素，精度、规模、覆盖度属于定量要素，深度通常作为衍生数据的分级要素。

b) 影响对象是指数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响的对象。影响对象通常包括国家安全、经济运行、社会稳定、公共利益、组织权益、个人权益。

c) 影响程度是指数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能造成的影响程度。影响程度从高到低可分为特别严重危害、严重危害、一般危害。对不同影响对象进行影响程度判断时，采取的基准不同。如果影响对象是组织或个人权益，则以本单位或本人的总体利益作为判断影响程度的基准。如果影响对象是国家安全、经济运行、社会稳定或公共利益，则以国家、社会或行业领域的整体利益作为判断影响程度的基准。

根据上述思路最终形成如下表格，将数据级别划分为一般数据、重要数据、核心数据。

表 4 数据分级确定参考规则

业务分类	影响程度		
	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	重要数据
社会稳定	核心数据	重要数据	一般数据
公共利益	核心数据	重要数据	一般数据
组织权益、个人权益	一般数据	一般数据	一般数据

（3）对数据分类分级结果进行审核和完善，最后批准发布实施，对数据进行分类分级标识，形成数据分类分级清单和重要数据、核心数据目录，按有关程序报送重要数据和核心数据目录等。

（4）数据分类分级完成后，当数据的业务属性、重要程度和可能造成的危害程度发生变化时通常需要进行动态更新。

数据分类分级标识过程中，应针对《结构化数据清单》《非结构化数据清单》《业务信息映射清单》分别标记数据、信息、数据集的类别和级别属性。

3.3.2数据处理活动管理

图 7 数据处理活动的描述

如上图，数据处理活动可以理解为是产生在业务活动中不同主体与客体之间，在不同环境下各类数据操作的组合。为确保全面理清各类数据在静态存储和动态流转、应用过程中的活动场景，数据处理活动场景管理应当从业务活动视角和系统交互视角两个维度切入，充分识别各业务活动中的数据操作和各系统间的数据输入输出，建立业务活动中的数据操作行为基线，为进一步开展风险识别和评估提供全面的场景支撑。

首先识别企业业务场景，并根据企业发展战略和业务发展需要，对业务场景排列优先级。业务场景识别内容包括各条线业务的属性、定位、完整性和关联性识别。业务属性主要识别业务的功能、对象、流程、范围和覆盖地域等。业务的定位主要识别业务在发展规划中的地位。业务的完整性主要识别其为独立业务或非独立业务。业务的关联性识别主要识别与其他业务之间的关系。然后根据业务的重要程度排列优先级，结合各类业务场景识别出相应的数据处理活动行为及其对应数据生命周期阶段。

企业应当按照各类场景的优先级定期开展数据安全风险评估工作。随着企业的业务发展或组织架构的调整，每年定期或变更触发各场景的识别工作。

3.3.2.1 业务数据操作行为识别

此环节应以业务模型为基础，业务条线为单位，充分识别业务活动中主体、客体、环境、应用、系统、数据集等相关核心要素，并能够聚焦到业务活动中的数据对象，厘清各类数据操作，形成《业务数据处理活动清单》，包括但不限于数据收集、数据访问、数据增删改查、数据拷贝、数据导入导出、数据加工、数据分析、数据展示、数据测试、数据提供、数据公开披露、数据删除、数据销毁等数据处理活动，以及相关活动涉及的数据生命周期阶段——采集、传输、存储、处理、交换、销毁，可参考【B.2 数据处理活动场景清单 表 16】。

3.3.2.2 应用系统数据流向识别

此环节应以系统交互模型为基础，以各系统组件为对象，充分识别业务应用开展过程中的各系统组件的数据输入和输出，厘清各系统组件在数据交互过程中业务数据描述，形成《系统数据流向清单》，包括但不限于业务信息、数据集、数据结构、交互协议、交互接口、交互类型等，可参考【B.2 数据处理活动场景清单 表 17】。

3.3.2.3 数据生命周期阶段识别

数据安全风险分析可以从不同维度进行，例如数据生命周期、数据状态、数据处理活动、数据业务场景等等。本文将主要参考 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》中所采用的“数据生存周期安全过程”进行数据全生命周期各个阶段（采集、传输、存储、处理、交换和销毁）的风险分析，同时也充分结合《数据安全法》中所定义的各类数据处理活动（收集、存储、使用、加工、传输、提供、公开）、常见的数据业务场景（重要数据处理、数据跨境流动、个人信息数据处理）等进行更细粒度的风险分析。

3.4 数据安全风险评估

数据安全风险评估包含风险识别、风险分析和风险评价三个过程。此阶段，应充分结合数据管理过程，在数据识别、业务信息识别、数据分类分级、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，充分识别其业务活动场景下的各类数据集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。

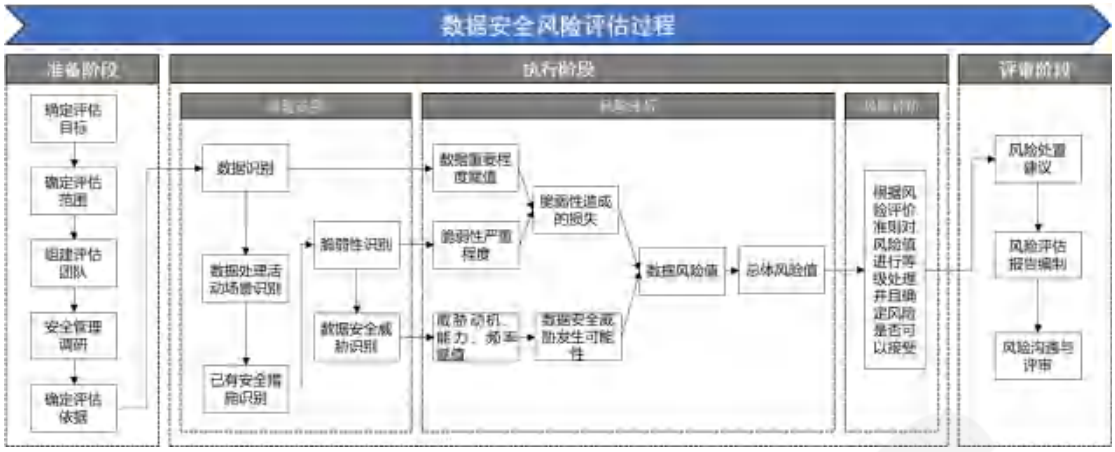

图 8 数据安全风险评估方法

在开展风险评估工作前，应做好评估准备工作，包含确定评估目标、确定评估范围、组建评估团队、安全管理调研和确定评估依据等。

3.4.1风险识别

风险识别的目的是发现、识别和描述可能妨碍组织实现业务目标的风险。相关的、适当的和最新的信息对于识别风险很重要。组织可以使用一系列技术来识别可能影响一个或多个目标的不确定性风险。

为了充分梳理数据在业务场景中的处理活动，我们建议以“业务信息”及其对应的“处理活动”为单位进行风险识别，同时可根据“业务信息”到“数据集”的映射来进行细化的数据生命周期场景映射。

风险识别阶段需要在评估范围内，明确各类数据集在不同数据处理活动场景下的已有安全措施、脆弱性和数据安全威胁。

3.4.1.1 数据重要程度赋值

在【3.3.1 数据识别与标记】完成的基础上确定评估范围，针对评估范围内的各个数据集、数据项进行整理，确定被评估数据所在位置、数据安全等级等内容。

参考【3.3.1.3 数据分类分级】，将数据的安全级别由低到高划分为三个级别：一般数据、重要数据和核心数据。为了将数据风险进行量化分析，参照【A.1 数据重要程度赋值表】对数据的重要程度进行赋值。

本阶段输出成果为《数据赋值清单》，模板见【B.1 数据清单】。

3.4.1.2 数据处理活动场景识别

确定待评估的数据和数据集后，在【3.3.2 数据处理活动管理】的基础上，针对各数据，识别其涉及的各类数据处理活动场景，并进一步识别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。应确保场景识别结果与实际情况保持一致。

本阶段输出成果为《数据处理活动场景清单》，模板见【B.2 数据处理活动场景清单】。

3.4.1.3 已有安全措施识别

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数据安全威胁利用脆弱性导致安全事件发生的可能性，如行为监测系统、入侵检测系统；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，如数据脱敏、数据加密。评估人员应判断已有安全措施得到正确使用、安全策略设置合理、策略得到有效执行。

本阶段输出成果为《已有安全措施清单》，模板见【B.3 已有安全措施清单】。

3.4.1.4 脆弱性识别

（1） 安全脆弱性

安全脆弱性是数据应用场景自身存在的，如无法被数据安全威胁利用，其本身不会对数据安全造成损害。评估时应对全部脆弱性进行识别，并根据脆弱性可利用难度及现有安全措施有效性，综合判断脆弱性的可利用性。

安全脆弱性识别一般从数据生命周期进行，常见的脆弱性示例见**【C.1.1 安全脆弱性】**（随着新场景、新技术的发展，此清单需要定期维护）。识别中发现的不符合项应视为脆弱性，包含脆弱性编号、所在应用场景名称和脆弱性名称。

脆弱性识别所采用的方法主要有：问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。

（2） 合规脆弱性

合规脆弱性是指被评估方未能遵循国家法律、行政法规、规范性文件、地方性法规和行业监管要求，并落实相关规范。**与安全脆弱性不同，合规脆弱性无需被数据安全威**

胁利用，可直接造成违法违规风险。此环节应该作为组织数据安全管理红线，在识别业务场景下的安全脆弱性和威胁前，应当重点评估。在赋值计算时，这类脆弱性可利用性和风险发生可能性应该设置为最大值。

合规脆弱性识别可参考**【C.1.2 合规脆弱性】**（随着各行业最新监管要求的发布，此清单需要定期维护）中罗列的各项国家法律、行政法规、规范性文件、地方性法规和行业监管合规文件，参考合规文件中的合规要求进行识别，若不满足某个文件的合规性要求，即视为存在该项文件的脆弱性，包含脆弱性编号、所在应用场景名称和脆弱性名称（合规文件名称）。

（3） 脆弱性可利用性

应用场景的脆弱性严重程度由脆弱性可利用性分析计算而来。脆弱性可利用性与访问路径、访问复杂性、权限要求、用户交互有关。

- 访问路径。该特征反映了脆弱性被利用的路径，包括：物理访问，本地访问，邻近网络访问，远程网络访问。
- 访问复杂性。该特征反映了攻击者能访问目标系统时利用脆弱性的难易程度，可用高、中、低 3 个值进行度量。
- 权限要求。该特征反映了攻击者为了利用脆弱性需要通过目标系统鉴别的要求，可用无、低、高进行度量。
- 用户交互。该特征从攻击行为利用脆弱性时是否需要用户交互的条件反映了脆弱性利用的难易程度，可用不需要和需要 2 个值进行度量。

通过**【A.2 脆弱性可利用性赋值表】**为各脆弱性进行赋值，汇总到脆弱性清单中。

本阶段输出成果为《脆弱性清单》，模板见**【B.4 脆弱性清单】**。

3.4.1.5 数据安全威胁识别

威胁是一种对数据构成潜在破坏的可能性因素，是客观存在的。对于数据来说，数据安全威胁识别，主要分析数据在应用场景流转过程可能影响数据机密性、完整性、可用性的威胁类型，并进一步分析其属性，包括威胁动机、威胁能力、威胁发生频率。

评估时应根据当前脆弱性识别的情况，依据**【C.2 数据安全威胁与脆弱性的利用关系示例】**（在后期项目实施过程中，随着脆弱性清单的维护，此表格可能需要随之更新），梳理可利用各个脆弱性的威胁，包含威胁编号、威胁名称、影响数据编号和方位。

数据安全威胁要素属性包括威胁动机、能力及发生频率。分析出具体数据安全威胁后，需要进一步分析数据威胁的属性。数据安全威胁发生可能性将由威胁动机赋值、威胁能力赋值及威胁发生频率赋值共同确定。

威胁动机赋值表如**【A.3 威胁动机赋值表】**所示。

威胁能力赋值表如**【A.4 威胁能力赋值表】**所示。

威胁发生频率赋值表如**【A.5 威胁发生频率赋值表】**所示。

本阶段输出成果为《数据安全威胁清单》，模板见**【B.8 数据安全威胁清单】**。

3.4.2风险分析

数据安全风险分析应当聚焦到业务场景，以业务活动下的数据集及其在业务场景下对应的数据生命周期阶段、数据处理活动为分析对象，形成风险清单，包括但不限于数据生命周期、业务数据处理活动、业务信息、映射的数据集、数据项、数据存储环境、风险类型和描述等内容，如**【B.9 风险清单】**所示。其中，风险的类型和描述可参考 2.2.2 数据安全风险的类型。

本文通过定性赋值法开展数据安全风险计算，方法是：通过确定数据安全威胁利用脆弱性来定性“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”，最终得到评估范围内的“总体风险值”。参考 GB/T 20984-2022 的风险计算思路，且由于各风险因子之间的关联性强弱不同，根据实践经验，本文分别采用相乘法或相加法进行关联计算，使得整体过程更加简单明确。

风险计算的主要过程为：

（1） 脆弱性可造成的损失计算

首先，依据脆弱性可利用性，计算应用场景的脆弱性严重程度，即：

$A_i = \frac{\sum_{j=1}^{n} a_j}{n}$，其中，$A_i$为第$i$个应用场景的脆弱性严重程度，$a_j$为第$i$个应用场景存在的脆弱性的可利用性，$n$为第$i$个应用场景存在的脆弱性数量。计算结果见**【B.5 应用场景脆弱性严重程度】**。

然后，依据应用场景的脆弱性严重程度，计算数据的脆弱性严重程度，即：

$V_i = \frac{\sum_{j=1}^{n} b_j}{n}$，其中，$V_i$为第$i$个数据的“脆弱性严重程度”,$b_j$为第$i$个数据所在应用场景的脆弱性严重程度，$n$为第$i$个数据所在应用场景的数量。计算结果见**【B.6 数据脆弱性严重程度】**。

最后，根据“数据重要程度赋值”及数据“脆弱性严重程度”，计算安全事件一旦发生后的“脆弱性可造成的损失”，即：

$F_i = \sqrt{\sigma_i \times V_i}$，其中$F_i$为第$i$个数据的“脆弱性可造成的损失”，$\sigma_i$为第 个数据的重要程度赋值；$V_i$为第$i$个数据的“脆弱性严重程度”。计算结果见**【B.7 数据脆弱性可造成的损失】**。

（2） 威胁发生可能性计算

数据安全威胁发生可能性计算公式为：

$t_i = \sqrt{\frac{x_i + y_i}{2} \times f_i}$，$\{t_i | 1 \le t_i \le 5\}$，其中$t_i$为第$i$个数据威胁发生的可能性，$x_i$为第$i$个数据威胁的动机值，$y_i$为第$i$个数据威胁的能力值，$f_i$为第$i$个数据威胁的发生频率值。

综合计算各个威胁发生可能性之后，汇总在**【B.8数据安全威胁清单】**中。

（3） 数据风险值计算

首先，根据**【B.8 数据安全威胁清单】**，计算出各数据的“数据威胁发生可能性”，即：

$L_i = \frac{\sum_{j=1}^{n} t_j}{n}$，其中，$L_i$为第$i$个数据的“数据威胁发生可能性”，$t_j$为第$i$个数据面临的第$j$个威胁的发生可能性，$n$为第$i$个数据面临的威胁的数量。计算结果见**【B.10 数据风险值计算结果清单】**。

然后，根据计算出的各数据“数据威胁发生可能性”，以及**【B.7 数据脆弱性可造成的损失】**中各数据脆弱性可造成的损失，计算数据的安全风险值，即：

$R_i = \sqrt{L_i \times F_i}$，其中$R_i$为第$i$个数据的安全风险值，$L_i$为第$i$个数据的“数据威胁发生可能性”，$F_i$为第$i$个数据的“脆弱性可造成的损失”。计算结果见**【B.10 数据风险值计算结果清单】**。

（4） 总体风险值计算

采用如下公式对总体数据安全风险值进行计算：

$R=\frac{\sum_{i=1}^{n} R_i*\sigma_i}{\sum_{i=1}^{n} \sigma_i}$，其中$R$为“总体数据安全风险值”，$R_i$为第 个数据的安全风险值，$\sigma_i$为第 个数据的重要程度赋值， 为数据的个数。

3.4.3 风险评价

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。

风险评价的方法是：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。**【C.3 数据安全风险等级划分参考表】**为风险等级划分方法示例，将总体风险级别划分为五级，由高到低分别为：很高、高、中等、低、很低，每个等级代表了相应风险的严重程度，等级越高，风险越高。

完成风险评价后，需要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**【C.4 数据安全风险评估报告参考模板】**。

3.5 数据安全风险处置

数据安全风险处置应结合各企业风险接受情况判定风险是否可以接受，对不可接受风险应采取相应的风险处置措施降低风险级别。风险处置措施应着重对可能被威胁利用的脆弱性来制定，找出引发不可接受风险的脆弱性，提出具体的风险处置措施。数据安全风险处置措施应包括风险级别、风险描述、风险值、风险处置措施、风险处置步骤、相关责任人、预计时间等要素，如**【B.11 风险处置建议清单】**所示。制定数据安全风险处置措施前应综合考虑法律法规要求、业务发展需要、数据安全管理和技术能力、组织人员能力等多方面因素。

常见的风险处置措施如下：

- 控制风险

实施有效控制，降低威胁发生的现实可能性和造成的影响，将风险降低到可以接受的等级，包括减少威胁，即通过有效实施风险控制措施，避免威胁发生，从而保护信息资产；减少脆弱点，即通过有效实施风险控制措施，减少脆弱点。如采取适当的技术措施，对员工实施安全教育培训，强化员工的安全意识和安全操作能力；降低影响，即通过保护性措施降低威胁发生后可能造成的损失。如对重要信息的备份、制定业务连续性计划等。

- 转嫁风险

将风险全部或部分地转移到其他责任方，如通过购买保险或外包等方式将风险转移给其他方。

- 避免风险

远离风险环境或采取与风险环境相隔离的措施。如将有高安全要求的设备或业务活动设置在高安全区中，增加特殊数据防护手段防止设备或业务活动遭受威胁的影响。

- 接受风险

接受风险的决策。

3.6 数据安全风险监督改进

数据安全风险监督改进的目的是保证和提升数据安全风险管理过程的质量和有效性。在规划风险管理流程时，应该将持续监督和优化改进作为其中的一部分内容，明确界定其职责。流程的所有阶段都应该进行监督和改进。监督和改进包括计划、收集和分析信息、记录结果和提供反馈。监督和改进的结果应纳入整个组织绩效的管理、评估和报告等活动中。

3.6.1数据处理活动监督

数据处理活动监督应设置独立的团队来开展工作，成员一般由审计部门担任，不建议由其他部门兼任。监督团队需要定期向决策者汇报当前数据处理活动管理状况，并履行以下工作职责：

- 根据本机构数据处理活动管理实际情况，确定相应审计策略及规范，包括但不限于审计周期、审计方式、审计形式等内容。
- 监督数据安全管理政策、方针的执行，验证安全手段应用的有效性。
- 公布投诉、举报方式等信息，并及时受理数据处理活动管理的相关投诉和举报。
- 开展数据处理活动管理审计和分析，发现并反馈问题和风险，对机构后续相关整改工作进行监督。

- 配合组织聘请的第三方公司或团队开展数据处理活动管理外部审计工作。
- 审查商务智能分析和数据科学研究提出的计划和决策。

3.6.2风险评估监督

即使经过精心的设计和实施，风险应对方案仍然可能达不到预期的效果，而且可能产生预料之外的后果。风险评估监督需要成为风险应对方案实施的一个组成部分，以保证不同形式的应对方案持续有效。

风险评估监督还可能引入需要管理的新风险。如果没有合适的应对方案或应对方案没有充分改变风险，则应记录风险并持续进行评估。决策者和其他利益相关方应了解风险应对后剩余风险的特征和水平，剩余风险应形成记录文件并进行监测、审查，并酌情进一步处理。

风险评估监督应通过适当的机制记录和报告风险管理流程及其成果。记录和报告的目的是：

- 在整个组织内传达评估监督活动和风险管理成果；
- 为改进风险管理活动的决策提供信息；
- 协助与利益相关方的互动，包括对风险管理活动负有责任的相关方。

3.6.3运营监督

运营监督的关键是强调实战的牵引作用。通过监督提升全员主动参与效应，并持续优化改进。

通过对内部审核等各项监测活动结果的分析，采集内外部与数据安全风险管理有关的信息，为体系的持续改进提供输入信息。通过管理评审，识别管理体系改进的需求，识别偏离数据安全风险管理目标的原因或现行体系在适应环境方面的差距，制定改进的具体措施寻找改进的机会，明确具体的改进计划。实施改进措施并验证其结果，保留实施过程和结果的相关记录。

3.6.4技术监测

数据安全风险监测应当以敏感数据识别能力为基础，围绕数据生命周期的流转和

应用、各业务场景下的数据操作行为，以及潜在的数据安全威胁和脆弱性等多个维度对可能发生的数据安全风险进行持续监测，并能够采用可视化技术对告警事件分类展示，并追踪展示风险事件的处理进度及结果。

3.6.4.1 敏感数据监测

敏感数据自动识别能力是数据安全风险监测的基础能力，应当能够在数据识别与标记管理过程的基础上，结合数据标签标记技术和数据特征识别技术，将《结构化数据清单》《非结构化数据清单》《业务信息清单》等相关成果固化到技术工具中，并能够结合各类数据标签标记和内容特征去动态的监测流动中和存储中的敏感数据。

3.6.4.2 数据处理活动监测

数据处理活动监测能力建设是数据安全风险监测机制的核心环节，应当以数据处理活动管理过程为基础，围绕数据处理活动中的主体、客体、环境、操作等环节采集完善的日志信息，以识别全量业务数据操作行为为基础，并能够聚焦到数据存储环境下实现数据流向的重点分析，以及对各操作行为场景下的数据生命周期的识别，以实现数据处理活动监测过程的闭环管理。日志源可来自应用系统、数据存储系统等业务应用类系统，也可以来自数据库审计、网络防泄漏、终端防泄漏、网络审计等监控与审计类系统。

（一） 业务数据操作行为基线监测

业务数据操作行为监测聚焦在业务视角，围绕业务活动中的所有数据操作行为进行建模和解析，并结合所对应的正常业务行为基线进行对比分析，所监测的信息至少包括：访问账号、访问时间、协议、源/目的IP、访问应用、操作数据、操作类型、执行结果、操作次数。

（二） 系统数据流向监测

系统数据流向监测聚焦在系统视角，在业务数据操作行为监测的基础上，围绕业务所涉及的应用系统相关的各类数据存储组件进行全面的数据输入输出监测，所监测的信息至少包括：源/目的IP、访问时间、协议、端口、访问账号、访问接口、输入/输出数据等信息。

（三） 数据生命周期监测

数据生命周期监测可在业务数据操作监测和系统数据流向监测的基础上，提炼各个过程中的关键属性，识别其所属数据生命周期阶段。

3.6.4.3 数据安全风险监测

数据安全所面临的威胁可以包括来自有组织的黑客的恶意攻击、窃取大量的企业数据售卖、员工安全意识不足外发敏感数据等情形。传统的网络安全态势感知过程需要依靠网络边界安全产品，如入侵防御系统、统一威胁管理系统等，去解析流量特征，通过特征库匹配进行威胁识别，此方案与实际业务活动关联度较低，且误报率较高，往往需要大量人工进行二次分析与研判。

本文数据安全风险监测方案建立在业务数据操作行为基线监测、系统数据流向监测、数据生命周期监测的基础上，在全面识别各类业务场景下的数据处理活动后，通过构建数据处理活动行为基线，并对批量下载、违规访问、越权访问、非正常时段访问、批量执行等威胁行为进行识别与分析，结合被操作数据的分类分级标签来判断数据重要程度，然后基于数据重要程度、风险级别以及发生频率，确定威胁行为对应的风险值，最后根据风险值和预设机器学习模型对异常业务活动进行预测，得到对应的数据安全风险预测结果。通过结合业务活动对数据安全风险进行预测，有利于提高预测结果的准确性、降低人工研判的投入以及避免数据泄露事件的发生。下表中，针对可能发生的威胁行为，及其对应的特征判定方法给出了举例。

表 5 常见威胁行为判定示例

序号	威胁类型	特征	所需判定字段
1	采集/处理/存储组件存在漏洞	/	IP、漏洞等级
2	未授权执行修改操作	超出行为基线权限：执行 ALTER 语句	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象（到字段）、操作类型、操作时长、影响行数、执行结果、操作次数、
3	网页被篡改	/	IP、网站篡改告警
4	未授权执行创建操作	超出行为基线权限：执行 CREATE 语句	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象（到字段）、操作类型、操作时长、影响行数、执行结果、操作次数
5	未授权接口接入	/	IP、异常告警类型
6	敏感信息外发	/	源 IP、目的 IP、日期时间、加解密字段（表征传输敏感数据有无加密）、敏感数据操作类型（外发、接收或其他）记录、敏感信息关键字
7	敏感数据未脱敏	/	已完成脱敏信息

8	创建索引，导致敏感数据暴露	超出行为基线权限：执行 CREATE INDEX	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象、操作类型、操作时长、影响行数、执行结果、操作次数
9	非工作时间操作	超出访问时间	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象（到字段）、操作类型、操作时长、影响行数、执行结果、操作次数
10	传输未加密	监测到敏感数据发送	源 IP、目的 IP、日期时间、加解密字段（表征传输敏感数据有无加密）、敏感数据操作类型（外发、接收或其他）记录、敏感信息关键字
11	使用移动存储介质导出敏感数据	监测到敏感数据导入	源 IP、目的 IP、日期时间、敏感数据操作类型（外发、接收或其他）记录、敏感信息关键字、表征使用移动介质接入导出关键字
12	敏感信息外发	监测到敏感信息外发	源 IP、目的 IP、日期时间、加解密字段（表征传输敏感数据有无加密）、敏感数据操作类型（外发、接收或其他）记录、敏感信息关键字
13	高频多次导出数据	超出行为基线中操作次数阈值，导出数据	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象、操作类型、操作时长、影响行数、执行结果、操作次数
14	批量导出数据（运维人员）	超出行为基线中操作行数，阈值导出数据	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象、操作类型、操作时长、影响行数、执行结果、操作次数
15	数据被非恶意删除	超出行为基线权限：执行 DELETE、DROP 语句	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象、操作类型、操作时长、影响行数、执行结果、操作次数、
16	批量删除数据	超出行为基线中操作行数、阈值删除数据	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象、操作类型、操作时长、影响行数、执行结果、操作次数
17	数据未备份	数据未定期备份	备份产品备份成功信息
18	数据未授权访问	超出行为基线中的访问对象	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象（到字段）、操作类型、操作时长、影响行数、执行结果、操作次
19	更改权限，超权限使用数据	超出行为基线：执行 GRANT、REVOKE、DENY 语句	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象、操作类型、操作时长、影响行数、执行结果、操作次数

20	运维人员绕行堡垒机直联	针对防护对象直联	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象、操作类型、操作时长、影响行数、执行结果、操作次数
21	违规使用高危操作	超出行为基线：执行 CREATE TRIGGER、ALTER TRIGGER、DROP TRIGGER	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象（到字段）、操作类型、操作时长、影响行数、执行结果、操作次
22	未定期更新系统分类分级情况	/	各专业部门分类分级完成情况百分比
23	未授权的采集源	/	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象（到字段）、操作类型、操作时长、影响行数、执行结果、操作次数
24	数据污染	数据入库时，攻击者接入采集系统污染待写入的原始数据，破坏数据完整性	源 IP、目的 IP、sql 注入等告警信息
25	数据无效写入	数据入库时，数据不符合规范或无效	不合规
26	敏感数据在传输过程中未加密	/	源 IP、目的 IP、日期时间、加解密字段（表征传输敏感数据有无加密）、敏感数据操作类型（外发、接收或其他）记录、敏感信息关键字
27	敏感数据存储未加密	/	进行加密关键字

28	大数据平台的组件的违规访问控制	/	事件主体（源 IP 和源端口、源 MAC 地址、用户名、客户端工具名）、事件客体（目的 IP 和端口、目的 MAC 地址、数据库名、数据表名、字段名），事件时间、操作类型（数据操作类、结构操作类、事务操作类、用户管理类和其他辅助操作类）、事件描述（操作具体内容，如操作语句）、事件结果（返回代码、执行时长、返回结果集、返回行数）
29	数据未定期备份和恢复	/	备份产品备份成功信息（指定频次）
30	数据批量导出	超出行为基线中操作次数阈值，导出数据	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象、操作类型、操作时长、影响行数、执行结果、操作次数
31	数据批量导入	超出行为基线中操作次数阈值，导入数据	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象、操作类型、操作时长、影响行数、执行结果、操作次数
32	数据脱敏有效性验证	/	脱敏有效性占比值
33	超出数据共享安全防护要求（固定 IP)	/	源 IP、目的 IP、端口、数据库名称、用户名、操作时间、数据对象、操作类型、操作时长、影响行数、执行结果、操作次数
34	违规对外共享接口访问	与第三方机构共享数据时，接口权限混乱，导致第三方能访问其他未开放的数据	源 IP、目的 IP、日期时间、调用参数
35	数据销毁未经审核	/	销毁记录与工单系统核对是否未审批
36	数据到期未销毁	数据失效或业务关闭后，遗留了敏感数据仍然可以被访问，破坏了数据的机密性	数据销毁有效性工作情况

3.7 数据安全风险沟通与评审

数据安全风险沟通为数据安全风险管理主循环的五个步骤（即数据安全风险管理规划、数据处理活动管理、数据安全风险评估、数据安全风险处置、数据安全风险监控改

进）中相关方提供沟通和咨询。沟通是通过相关方之间交换和/或共享关于风险的信息，就如何管理风险达成一致的活动。沟通是为所有参与人员提供交流途径，以保持参与人员之间的协调一致，共同实现安全目标。

数据安全风险评审包括对风险因素和数据安全风险管理循环的五个主体步骤（即数据安全风险管理规划、数据处理活动管理、数据安全风险评估、数据安全风险处置、数据安全风险监控改进）的沟通和评审。评审是对监视的结果定期或不定期对风险管理过程的运行情况与相关方进行交流和获取对风险评估结果的判断，并基于了解风险管理过程的执行情况，进行分析和评价，从而确定风险管理过程的有效性，有效性包括执行情况和执行效果。

3.7.1 沟通与评审的内容

数据安全风险沟通包括以下方面内容：

- 确保组织风险管理的结果；
- 收集风险信息；
- 分享风险评估结果并提出处理计划；
- 避免或减少因相关方之间缺乏相互了解而导致的信息安全漏洞发生和后果；
- 支持决策制定；
- 获取新的信息安全知识；
- 与其他各方协调并计划应对措施，以减少任何事件的后果；
- 让相关方对风险有责任感；
- 提高认识。

风险因素的评审包括背景建立过程中关注的内外部环境以及风险评估过程中识别信息的变化，包括但不限于以下方面和内容：

- 风险管理范围的变化，包括新的资产、新的部门等；
- 评估对象价值的变化，比如业务的变动带来的价值变化；
- 新的或变化的威胁，或之前未评价的威胁信息；
- 新发现的或者是变化的脆弱点；
- 风险发生带来的后果的变化；
- 新发布的相关法律法规、行业监管要求和标准；
- 相关组织架构的变化；

- 管理层的变化；
- 相关方要求的变化。

风险管理的监视和评审包括以下方面和内容：

- 风险管理过程的执行情况；
- 风险因素识别的全面性和合理性；
- 风险管理目标的实现情况；
- 风险处置计划的实施情况
- 风险控制措施的运行有效性；
- 风险控制成本效益的合理性；
- 风险评估原则和风险接受原则的合理性；
- 当前风险评估方法的有效性和产生结果的一致性，以及新的风险评估方法。

3.7.2 沟通与评审的方式

沟通的双方角色不同，所采取的方式有所不同。有关数据安全风险管理相关人员的角色和责任的划分参见下表。下表给出了不同层面人员之间沟通的方式。

表 6 沟通方式

方式		接受方			
		决策层	管理层	执行层	参与层
发出方	决策层	交流	指导和检查	指导和检查	表态
	管理层	汇报	交流	指导和检查	宣传和介绍
	执行层	汇报	汇报	交流	宣传和介绍
	参与层	反馈	反馈	反馈	反馈

沟通的各种方式及应用范围说明如下：

- 指导和检查

指机构上级对下级工作的指导和检查，用以保证工作质量和效率，适用于决策层对管理层、决策层对执行层和管理层对执行层；

- 表态

指机构高层支持数据安全风险管理的对外表态，用以得到外界认同和支持，适用于决策层对参与层；

- 汇报

指机构下级对上级作工作汇报，用以得到上级认可，适用于管理层对决策层、执行层对决策层和执行层对管理层；

- 宣传和介绍

指机构的风险管理对象和数据安全风险管理的对外宣传和介绍，用以得到外界支持和配合，适用于管理层对执行层、管理层对参与层；

- 培训和咨询

指专业人员对数据安全风险管理相关方的培训和咨询，用以提高人员的安全意识、知识和技能，适用于执行层对参与层、执行层对决策层、参与层对管理层和参与层对执行层；

- 反馈

指机构风险管理对象使用者对机构数据安全风险管理的意见反馈，用以了解实施效果和用户需求，适用于参与层对决策层、参与层对管理层、参与层对执行层；

- 交流

指同级或同行之间的对等交流，用以共享信息和协调工作，适用于决策层对决策层、管理层对管理层、执行层对执行层、参与层对参与层。

4 企业数据安全风险管理典型实践

本文以电力行业某企业数据安全风险管理实践为典型案例，介绍企业数字化转型现状、数据安全风险管理组织、数据安全风险管理制度、数据安全风险防护措施等方面的内容。电力安全关系国计民生，是国家安全的重要保障。该企业作为关键信息基础设施运营者，深刻认识到保障网络安全、数据安全就是保障电网安全，特别是在当前全力推进数字化转型和数字电网建设时，必须进一步增强风险意识，筑牢数据安全屏障，为数字电网保驾护航。

4.1 企业数字化建设背景

（一）整体政策背景和数字化转型现状

数字经济时代，数据已成为重要的生产要素和基础的战略资源，其价值日益凸显。特别是在当前，新一轮科技革命突飞猛进，数字经济蓬勃发展，全球疫情持续演变，外部环境日趋复杂，网络安全、数据安全已成为新的战场。

2020 年 9 月，我国提出碳达峰碳中和目标。电力行业是碳减排的关键，电力数字化是推动碳达峰、碳中和目标如期实现的重要一环。传统电力产业“发-输-变配-用”各节点彼此孤立，难以协同，导致电力生产效率低，难以产生高经济效益。5G、AI、大数据、IoT 等数字化技术与日常生产、经营、管理等各环节融合，不仅能有效助力电力企业减少各生产环节的冗余性，构建安全可控、绿色低碳、高效敏捷的综合性能源基础设施，最终实现绿色能源运用；同时也成为能源生产结构、存储形式、分享机制及消费模式变化背景下的破局之道。

随着电力行业数字化建设的推进，数据安全将成为企业整体安全中极其重要的一环，若电力企业发生数据安全事件，不仅会对电力企业自身的业务、信誉和经济利益造成严重损害，甚至可能影响能源供应，导致社会恐慌，威胁国家安全。

（二）电力行业典型应用场景描述

- 配电房监测场景分析

电网企业在配电房监测过程中，需要采集配电房的环境、设备等数据传输给后台来进行分析，保障配电房的安全。

在采集阶段，企业进行安全防护的主要目标是保障数据准确安全地进行采集。这期间，配电房的采集设备容易因木马、病毒、程序后门、非授权访问等，影响到数据的完整性及保密性。待数据采集完成后，采集设备将数据传输至后台分析。在数据传输阶段，容易因明文传输造成数据泄露。

- 配网规划场景分析

配网规划旨在通过分析和研究未来负荷增长情况以及城市配电网现状的基础上，进行系统扩建、改造计划的最优设计。

企业会使用经济、人口、社会用电量的历史数据来进行负荷预测，在这个过程中应

保障历史数据的安全存储。在数据存储阶段，容易因明文存储、非授权访问及管理员泄露等因素引发安全风险，企业应注重对这些数据进行差异化和加密存储。

- 营销数据挖掘场景分析

电网企业为发挥数据价值，会对客户资料、合同等营销数据进行数据挖掘。在数据挖掘的过程中，会有大量的源数据聚集，此时应重点防止源数据发生泄漏。在挖掘分析后的展示过程中，会出现大量敏感个人信息，同时应注重对这些重要信息的脱敏展示。

根据目前电力行业的各数据应用场景进行分析，可以发现在数据应用的各环节存在极大的数据安全风险，一旦发生数据泄露、损毁等事件，将对企业造成不可估量的损失，企业应及时开展数据安全风险管理。

4.2 企业数据安全风险管理实践

（一）综述

为加强企业数据安全风险管理，明确各类数据安全风险类型，降低数据安全风险发生的可能性及其造成的影响，电力行业企业应组建数据安全风险管理组织，进行数据安全风险评估，将数据安全风险纳入管控，并建立数据安全防护措施，将风险控制到可接受范围。

（二）数据安全风险管理组织

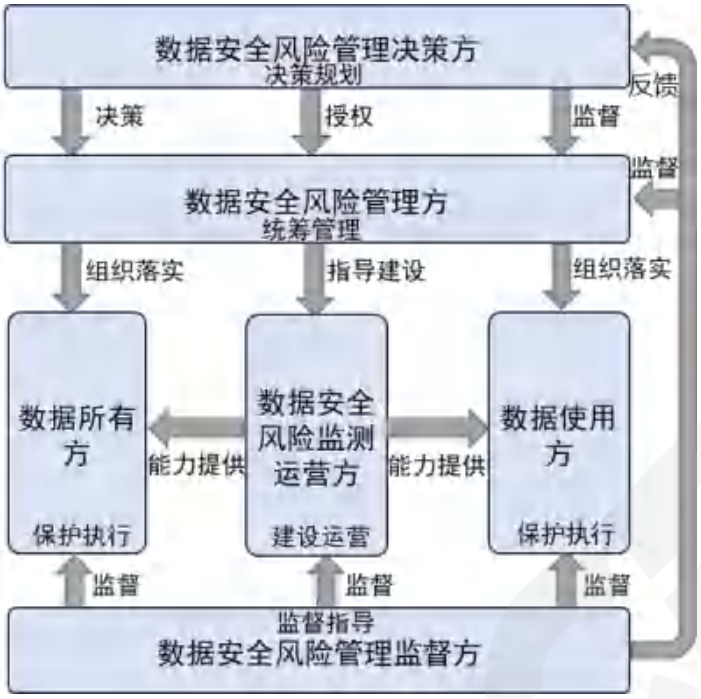

图 9 企业数据安全风险管理组织架构示例

- 数据安全风险管理领导小组

负责确定风险管理的发展思路，协调推动企业风险管理的规划与建设；当安全事件发生后，负责应急处置工作的总体协调和指导。

- 数据安全风险管理方

负责制定企业内部整体的风险管控和隐患排查的规范要求的预防机制，牵头开展风险管理；当安全事件发生后，负责统筹开展安全事件的应急处置和调查工作。

- 数据安全风险监测运营方

负责数据安全风险防控能力建设、数据安全应急预案与演练、数据安全风险监测预警、数据安全应急处置、数据安全灾难恢复等相关工作。

- 数据所有方

负责承接企业风险管理整体要求，在本业务域制定风险管控和隐患排查的机制，并贯彻落实相关要求；当安全事件发生后，负责配合开展本业务域的应急处置和调查工作。

- 数据使用方

企业内外部数据使用方，依据企业数据安全各项管理要求落实各类业务数据处理活动场景下的数据安全风险防护工作。

- 数据安全风险管理监督方

负责监督、指导各级部门数据安全风险管理制度建设、技术保护措施建设。负责检查与监督各级部门数据安全风险管理工作考核指标达成。

（三）数据安全风险管理制度

企业已围绕数据安全风险管理规划、数据安全风险管理要求、数据分类分级管理、数据安全风险评估管理、数据全生命周期风险管控、数据安全风险审计、数据安全应急管理、数据安全教育培训等方面制定了整体的数据安全风险管理制度体系。

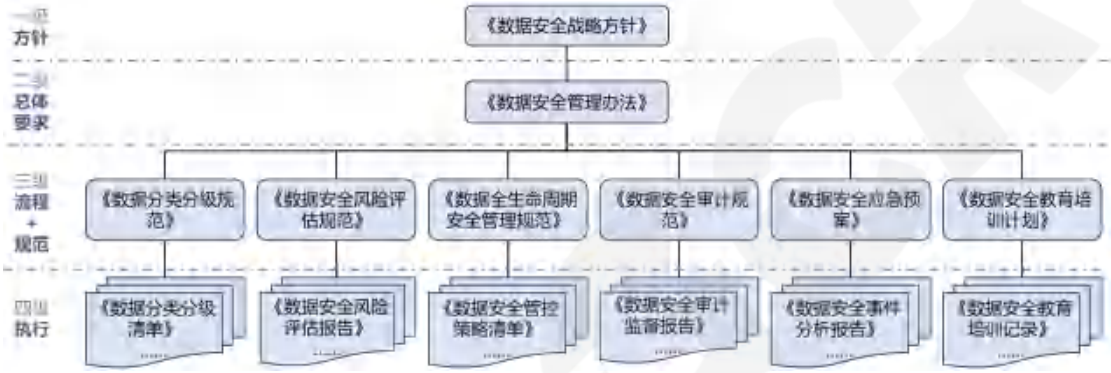

图 10 企业数据安全风险管理制度体系示例

《数据安全战略方针》明确了数据安全风险管理的目标、原则和基本路线。

《数据安全管理办法》明确了数据安全管理机构设置和职责划分，以及数据分类分级管理、数据安全风险管理、数据生命周期安全管理、数据安全审计管理、数据安全应急管理、数据安全教育培训管理等方面的总体要求。

《数据分类分级规范》明确了数据分类分级流程、数据分类分级原则、数据分类分级模型、数据分类方法、数据分级方法等，指导企业有序开展数据分类分级工作，确保企业能够更加科学、客观、准确地开展数据分类分级工作。

《数据安全风险评估规范》包含数据安全风险评估的实施方法和过程，实施方法中具体对数据安全风险评估的要素即数据资产、数据应用场景、脆弱性、安全措施、威胁之间的关联关系进行了描述，实施流程描述了数据安全风险评估开展的整体过程及各部门间的职责，该文件可以指导企业开展规范化的数据安全风险评估。

《数据生命周期管理规范》以数据分类分级为基础，明确了数据处理活动场景、数据安全保护技术、数据生命周期管控要求等内容，充分衔接数据分类分级属性、数据活

动场景和数据安全各类管控措施，为数据全生命周期安全管控实践提供全面的指导，并给出可落地的产品和技术路线。

《数据安全审计规范》明确了数据安全审计的目标及范围、数据资产管理审计、数据生命周期管理审计、数据操作审计等相关审计要求、审计方法、审计流程等。

《数据安全应急管理预案》紧密衔接企业网络安全应急机制，细化数据泄露、数据滥用、数据篡改、数据损毁、数据违规使用等数据安全事件场景，并结合数据分类分级制定数据安全专项应急措施。用于提高企业数据安全风险预警和事件处置能力，有效预防和处置数据安全突发事件，最大限度地预防和减少数据安全事件造成的损害和影响，保障企业数据安全。

目前企业每年至少开展 1 次全面的数据安全风险检查评估专项行动，对重点业务域的数据资产进行梳理，归纳这些数据资产归属的数据处理活动场景，对不同场景下数据资产存在的脆弱性和威胁进行定性定量地分析，同时结合现有的数据安全保护能力对数据安全风险进行计算，以极低、低、中等、高、很高的等级来进行描述，为企业后续建立监测平台和防护能力组件提供了良好的依据。

同时，企业根据个人信息安全评估等相关标准规范开展了个人信息安全影响评估专项行动，对涉及个人信息处理的业务场景进行了安全风险分析，确保个人信息的使用处于可控制的风险范围。

（四）数据安全风险防护措施

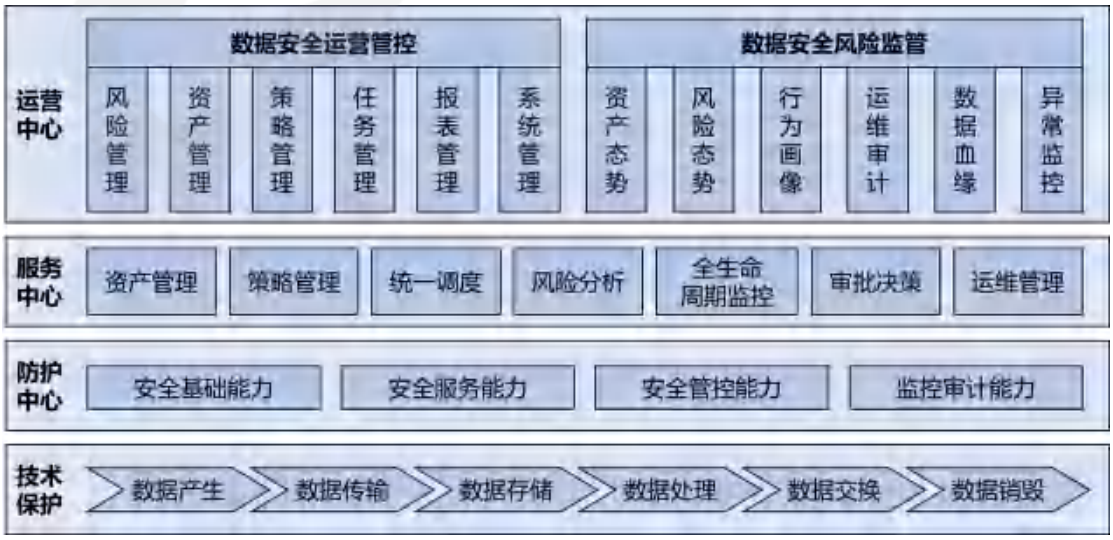

图 11 企业数据安全风险防护技术体系示例

（1） 建立数据安全风险监管平台

通过建设企业统一的安全中台，以“安全即服务”为理念将数据加密、脱敏、审计等安全能力服务化，实现资源的按需提供、灵活调配；根据不同的场景提供不同的安全服务，形成“一场景一策略”的安全控制措施；对重要数据活动进行全链路监测和预警，开展常态化数据安全运营工作，构建了服务中台化、策略场景化、运营常态化的技术防护体系。数据安全风险监管方面主要目标是实现全局的数据风险监测以及管理，包括数据资产态势分析、数据安全风险态势分析、数据处理活动行为画像、数据安全运维审计、数据血缘分析、异常行为监控。根据数据资产事件进行统计，展示各种级别、类别的数据资产事件的对比，针对数据安全事件进行分类统计，形成数据安全风险趋势分析。同时，以数据流向分析为基础，建立账号与数据资产之间的访问关系视图，呈现数据访问路径，当出现异常访问时可给予相应的风险告警。

（2） 融合数据安全防护能力组件

针对已有数据安全风险，企业在数据安全管理平台中融合了数据水印、数据脱敏、数据审计、数据安全网关、数据加密、数据共享交换、数据泄露监测、数据备份容灾等数据安全管控能力，覆盖了实际业务场景下的数据全生命周期安全保护需求，落实了敏感数据“进不来”“拿不走”“看不懂”“改不了”“跑不掉”的防护目标。

附录 A：数据安全风险赋值表

A.1　数据重要程度赋值表

数据重要程度赋值可根据企业数据分类分级实际情况针对不同级别数据进行重要程度量化赋值，此处给出分为 3 个级别时的赋值示例供参考。

表 7 数据重要程度赋值表

赋值	数据安全级别
5	核心数据
3	重要数据
1	一般数据

A.2　脆弱性可利用性赋值表

表 8 脆弱性可利用性赋值表

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

注：此表格中，访问路径、访问复杂性、权限要求、用户交互等关键因素判定等级时采用“或”的关系。

A.3　威胁动机赋值表

表 9 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，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；

A.4 威胁能力赋值表

表 10 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；

A.5 威胁发生频率赋值表

表 11 威胁发生频率赋值表

赋值	标识	定义
5	很高	出现的频率很高（或≥1 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≥ 1 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

赋值	标识	定义
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

附录 B：数据安全风险管理工具模板

B.1 数据清单

表 12 结构化数据清单

应用系统	数据库名称	数据库中文名	数据表名称	数据表中文名	字段名称	字段中文名	字段说明	数据量级	数据所有方	数据使用方	数据管理方

表 13 非结构化数据清单

数据文件存储路径	数据文件名称	数据文件内容描述	数据文件格式	数据文件量级	数据文件所有方	数据文件使用方	数据文件管理方

表 14 业务信息映射清单

业务分类	业务条线	业务活动名称	业务信息名称	结构化数据集映射描述	非结构化数据集映射描述	数据项描述

表 15 数据赋值清单

数据编号	数据名称	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	数据重要程度赋值

B.2 数据处理活动场景清单

表 16 业务数据处理活动清单

场景编号	业务条线	业务活动	主体	环境	数据处理活动	业务操作流程描述	业务信息名称	数据集描述	涉及应用系统	涉及数据生命周期描述

表 17 应用系统数据流向清单

场景编号	业务信息名称	数据集描述	数据来源	数据去向	数据结构	交互协议	交互接口	交互类型

B.3 已有安全措施清单

表 18 已有安全措施清单

安全措施编号	安全措施名称	安全措施描述	关联应用场景	安全措施类型	措施有效性

B.4 脆弱性清单

脆弱性编号	所在应用场景名称	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

表 19 脆弱性清单

B.5 应用场景脆弱性严重程度

表 20 应用场景脆弱性严重程度

应用场景编号	应用场景名称	脆弱性严重程度赋值

B.6 数据脆弱性严重程度

表 21 数据脆弱性严重程度

数据编号	脆弱性严重程度赋值

B.7 数据脆弱性可造成的损失

表 22 数据脆弱性可造成的损失

数据编号	脆弱性可造成的损失

B.8 数据安全威胁清单

威胁编号	威胁名称	影响数据编号	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	可利用的脆弱性

表 23 数据安全威胁清单

B.9 风险清单

表 24 风险清单

数据生命周期	业务数据处理活动	业务信息名称	映射的数据集描述	数据项描述	数据存储环境	风险类型	风险描述

B.10 数据风险值计算结果清单

表 25 数据风险值计算结果清单

数据编号	数据名称	数据威胁发生可能性	脆弱性可造成的损失	安全风险值

B.11 风险处置建议清单

表 26 风险处置建议清单

风险级别	风险描述	风险值	风险处置措施	风险处置步骤	相关责任人	预计时间

附录 C：数据安全风险分析资料清单

C.1 常见脆弱性示例

C.1.1 安全脆弱性

表 27 安全脆弱性

数据生命周期	脆弱性名称
数据采集	采集终端未对用户进行身份鉴别
数据采集	采集终端存在弱口令用户
数据采集	采集终端存在多人共用同一账号的情况
数据采集	采集终端未配置登录失败处理功能
数据采集	采集终端用户的口令未定期更换

数据生命周期	脆弱性名称
数据采集	采集终端未对用户进行访问控制
数据采集	采集终端未及时清理多余、过期的账户
数据采集	采集终端存在超级管理员等特权账户
数据采集	采集终端未对用户进行安全审计
数据采集	采集终端的安全审计未覆盖到所有用户
数据采集	未对采集终端的审计记录进行保护和备份
数据采集	未对采集终端的审计进程进行保护，用户可中断进程
数据采集	采集终端所在的物理环境安全不可控，易受到破坏
数据采集	采集终端所在的物理环境温湿度指标不可调节，存在不符合终端工作要求的情况
数据采集	采集终端未对数据源的真实性（如名称、IP 等）进行鉴别
数据采集	采集终端存在安全漏洞或未及时安装补丁程序
数据采集	采集终端未对采集的数据进行分类分级标识
数据采集	未定期核查用于收集数据的软硬件功能、接口功能、安全基线配置是否正常，并及时处理异常情况
数据采集	未在采集设备的软硬件更新、接口升级、配置变更前，在测试环境中充分验证新版本的可用性，并制定变更失败回退方案
数据采集	采集终端不具备采集失效报警的功能，并能够根据采集日志追溯至失效的采集部件
数据采集	未建立采集设备过载报警机制，应根据预计的采集设备工作负荷设计报警的阈值
数据采集	未计算实际业务的数据采集量，并依据设计文档判断实际的采集量是否大于预期的采集量
数据采集	未使用密码技术或校验技术对采集的数据进行完整性的校验
数据采集	未建立数据分类分级审核机制，对策略进行审核和批准，并对数据的分级分类进行监控纠正，建立分级分类清单保护机制，记录数据分类分级清单的操作
数据采集	未对无效数据建立审查回溯机制
数据采集	大数据采集系统不具备冗余机制
数据采集	未在分类的基础上围绕数据损坏、丢失、泄露等建立数据分级
数据采集	数据分类分级工具不具有敏感数据识别、敏感数据类型发现、自定义分类和分级、数据标记管理、过程记录、过程分析能力
数据采集	未留存数据分类分级清单
数据采集	数据分类分级制度中未映射了业务属性
数据采集	未建立数据清洗、转换操作相关的管理规范
数据采集	未建立数据采集的规范和标准，包括采集的数据格式标准、采集范围最小化原则、数据采集分级分类规范等
数据采集	当业务变更时，未重新评估预计的业务采集量，并根据业务采集量重新设计数据采集设备的承载量

数据生命周期	脆弱性名称
数据采集	未在设计文档中明确数据清洗、转换过程中使用的规则、手段、方法
数据采集	在数据清洗、转换过程中，未保留详细的审计记录，记录内容应至少包括转换/清洗前的数据、转换/清洗后的数据、转换/清洗使用的手段和方法、转换/清洗的时间等
数据采集	未围绕数据脱敏、数据加密、链路加密等建立数据采集过程保护
数据采集	未围绕采集周期、采集频率、采集内容等设置统一数据采集策略
数据采集	未对数据采集范围进行检查、反馈和更新
数据采集	未对数据采集过程进行记录与留存
数据采集	未限制数据采集系统的访问方式（如登录地址限制、终端接入方式等），建立访问权限管控机制，防止未预期的访问者窃取采集的数据
数据采集	未建立数据采集质量管理规范、数据质量管理流程、实施数据质量校验、数据质量监管，强化数据采集质量能力
数据采集	未建立数据源接入的申请和审核机制
数据采集	未对接入数据源实现生命周期管理，建立准入准出机制，并对数据源状态进行监控
数据采集	不具有数据源鉴别、数据源管理、数据源安全认证能力
数据采集	未围绕《网络安全法》《数据安全法》《个人信息保护法》等国家法律法规及行业规范，制定数据采集安全合规管理规范
数据采集	未以数据采集安全合规管理规范为基础，建立数据采集的风险评估流程
数据传输	未借助负载均衡、防入侵攻击等设备建立网络风险防范
数据传输	数据链路中部署的安全设备的性能（如支持的最大网络并发连接量、接口最大带宽量等）不能满足业务高峰期数据传输的需求
数据传输	未建立对加密算法配置、变更、管理等操作过程的审核机制和监管手段
数据传输	数据传输节点的性能（如支持的最大网络并发连接量、接口最大带宽量等）不能满足业务高峰期数据传输的需求
数据传输	未对密钥进行安全管理
数据传输	未对密钥系统管理人员建立审核监督机制
数据传输	数据传输方未梳理需要保证传输完整性的场景
数据传输	数据传输过程中，未采取有效措施保证数据完整性
数据传输	数据传输方未梳理需要保证传输保密性的场景
数据传输	数据传输过程中，未采取有效措施保证数据保密性
数据传输	未根据数据分类分级管理规定制定相应等级的数据传输策略
数据传输	未对数据传输策略进行检查，对不符合规定的传输方式给予警告并整改
数据传输	未对涉及国家重要信息、企业机密信息和个人隐私信息的数据场景进行加密
数据传输	未采用加密等安全方式对大数据平台进行远程管理，防止数据在网络传输过程中被窃听

数据生命周期	脆弱性名称
数据传输	未对不同级别数据建立不同等级的加密传输能力
数据传输	未在数据通信两端采取身份鉴别机制来保证数据传输到预期目标
数据传输	未对通过人机接口输入或通过通信接口输入的内容是否符合系统设定要求进行检查，不具有数据有效性检验功能
数据传输	不具备校验功能有效性审计措施，当发生功能失效的情况时，能够及时向管理员提供警报或提示
数据传输	数据传输方未提供通信线路、传输节点的硬件冗余
数据传输	未对网络设备的负载情况和网络带宽使用情况进行监控，并在不满足业务高峰期需要时进行告警
数据传输	网络总带宽量和各传输链路带宽量不能满足业务高峰期数据传输的需求
数据存储	存储媒体未对用户进行身份鉴别
数据存储	存储媒体存在弱口令用户
数据存储	存储媒体存在多人共用同一账号的情况
数据存储	存储媒体未配置登录失败处理功能
数据存储	存储媒体用户的口令未定期更换
数据存储	存储媒体未对用户进行访问控制
数据存储	存储媒体未及时清理多余、过期的账户
数据存储	存储媒体存在超级管理员等特权账户
数据存储	存储媒体未对用户进行安全审计
数据存储	存储媒体的安全审计未覆盖到所有用户
数据存储	组织未对存储媒体的审计记录进行保护和备份
数据存储	组织未对存储媒体的审计进程进行保护，用户可中断进程
数据存储	关键存储媒体所在的物理环境未进行电磁屏蔽
数据存储	存储媒体所在的物理环境安全不可控，易受到破坏
数据存储	存储媒体所在的物理环境温湿度指标不可调节，存在不符合终端工作要求的情况
数据存储	存储媒体存在安全漏洞或未及时安装补丁程序
数据存储	存储媒体未配置安全的远程连接协议
数据存储	存储媒体未关闭高危端口或非使用的端口
数据存储	存储媒体的网络时钟未进行同步
数据存储	组织未采取技术工具对存储媒体的使用历史、性能指标、错误或损坏情况等性能进行监控
数据存储	未对备份数据定期开展检查
数据存储	未对备份数据建立安全管控能力
数据存储	未定期对数据备份文件进行恢复测试并记录和保存测试结果
数据存储	未建立数据复制、备份与恢复的操作规程
数据存储	未建立数据存储冗余策略和设计指导
数据存储	存储媒体未进行用户-终端一对一绑定或限制远程连接网络地址范围

数据生命周期	脆弱性名称
数据存储	未对数据存储系统重要节点的入侵行为进行检测并对严重事件进行报警
数据存储	未对存储介质进行分类分级
数据存储	未建立存储介质使用审批制度
数据存储	未定期对存储介质开展测试
数据存储	未对存储介质配置安全能力（如：认证鉴权、访问控制、通信举证、文件防病毒等）
数据存储	未定期对数据存储系统进行安全基线配置检查
数据存储	数据存储系统不具备对多副本一致性进行扫描自检并对不一致数据尝试进行修复和告警的机制
数据存储	对委托第三方云平台、数据中心等存储数据的情况，第三方数据存储服务供应商未通过相应等级的网络安全等级保护测评或其他相关测评
数据存储	对委托第三方云平台、数据中心等存储数据的情况，未与第三方数据存储服务供应商签署了正式的数据存储服务协议，并对其责任、义务及违约后果进行明确约定
数据存储	不具备对于如删除数据、更改数据存储系统配置等高危操作进行授权审批的机制和技术手段
数据存储	未采用分布式存储、容灾备份及恢复、业务快照等保证数据可用性的技术手段
数据存储	存储的数据未自动进行分类分级
数据存储	组织未依据安全策略保证重要数据的存储完整性
数据存储	组织未依据安全策略保证重要数据的存储机密性
数据存储	组织未对数据进行本地备份和异地备份
数据存储	未采用对数据存储系统的输入输出接口进行安全管控并对接入设备进行安全扫描的技术手段
数据存储	组织未依据数据的大小、性质（如结构化、非结构化等）等选择合适的逻辑存储方式（如集中存储、分散存储等）
数据存储	未定期对数据存储系统的运维人员进行培训和考核
数据处理	不具备对个人信息去标识化的处理能力
数据处理	个人信息和重要数据在使用前，未进行安全影响评估
数据处理	未建立敏感数据访问控制机制
数据处理	未定期查看数据处理活动操作审计记录
数据处理	未审核数据处理的日常操作行为，对违规行为予以提醒
数据处理	组织未依据脱敏策略对数据进行脱敏
数据处理	未围绕损坏、丢失、窃取等建立数据处理环境保护机制
数据处理	未围绕访问控制、监管审计、职责分离等建立数据处理安全能力

数据生命周期	脆弱性名称
数据处理	未对数据处理过程建立适当的授权审批机制
数据处理	未制定数据处理过程操作规范
数据处理	针对数据处理结果访问与使用，未建立适当的权限管控和审计机制
数据处理	组织未对数据导入导出过程进行监控和审计
数据处理	组织未对数据分析过程进行监控和审计
数据处理	未制定数据分析过程中数据资源操作规范和实施指南
数据处理	未建立对数据分析结果进行审核的机制
数据处理	组织未对数据使用过程进行监控和审计
数据处理	未建立数据使用者安全责任制度
数据处理	使用个人信息，未建立在明示同意的基础上
数据处理	组织未对数据脱敏过程进行监控和审计
数据处理	未制定数据脱敏处理规范和流程
数据处理	未建立适当的数据脱敏效果评估机制
数据处理	未明确需要数据脱敏的业务场景
数据处理	不具备统一数据脱敏工具（包括：静态脱敏、动态脱敏）
数据处理	数据脱敏工具未与数据权限管理平台实现联动
数据处理	未对数据脱敏操作过程进行记录
数据处理	未制定特权账户的使用规范
数据处理	未建立审核违规使用和恶意行为的机制
数据处理	组织未对用户可执行的操作进行时间和网络范围上的限制
数据处理	未定期审计不同账户的使用情况
数据交换	未建立数据导入导出安全保障制度规范
数据交换	未基于数据分类分级要求建立数据导入导出安全策略
数据交换	未对导入导出行为进行记录
数据交换	不具有导入导出权限管理能力
数据交换	不具有导入导出身份认证能力
数据交换	不具有导入导出完整性验证能力
数据交换	组织未明确数据发布公开的内容、范围和规范
数据交换	组织未定期审查发布数据中是否包含非公开信息
数据交换	组织未对数据发布行为进行安全审计
数据交换	不具有数据资源公开应急处置能力
数据交换	组织未明确数据共享的内容范围
数据交换	组织未明确数据共享的管理措施和安全规范
数据交换	组织未明确数据共享涉及的各部门和岗位的职责与权限
数据交换	组织未对数据共享行为进行安全审计
数据交换	数据共享范围，不符合国家、政务行业及区域相关规定
数据交换	数据共享策略，不满足相关法律法规和数据保护要求
数据交换	未制定数据共享流程规范

数据生命周期	脆弱性名称
数据交换	数据共享接口未配置必要的访问权限控制
数据交换	未建立适当的共享数据溯源机制
数据交换	未建立数据共享场景的规范要求
数据交换	未建立数据共享审核流程
数据交换	不具有数据共享审计策略
数据交换	未利用数据加密、安全通道等措施保护共享数据
数据交换	不具有 API 数据接口安全防范能力
数据交换	数据开放平台未建立防数据爬取机制
数据交换	数据开放平台用户在登录时未采用身份鉴别措施
数据交换	数据开放平台用户列表里的用户身份标识不具有唯一性
数据交换	数据开放平台存在空口令用户
数据交换	数据开放平台未根据业务需求和安全要求建立适当的访问控制机制
数据交换	针对数据开放平台未对特权账户、临时账户等特殊用户进行管控
数据交换	未定期对数据开放平台的安全性进行验证
数据销毁	组织未明确存储媒体销毁处理策略、管理制度和机制，以及销毁对象和流程
数据销毁	组织未对存储媒体的销毁行为进行记录
数据销毁	组织未对存储媒体的销毁过程进行监控
数据销毁	组织未依据存储媒体类型的不同，建立软销毁和硬销毁的销毁策略
数据销毁	未设置数据销毁的监督角色
数据销毁	未建立数据销毁审批机制
数据销毁	组织未明确数据销毁场景、销毁对象、销毁方式、销毁要求
数据销毁	组织未依据国家法律法规要求，销毁个人信息、重要数据等敏感数据
数据销毁	未配备必要的数据销毁工具
数据销毁	不具备识别并销毁全部数据副本及备份数据的机制和技术手段
数据销毁	不具备确保被销毁数据及其副本内容不可被恢复的措施和技术手段
数据销毁	未建立针对数据销毁效果的评估机制
数据销毁	关于个人信息的销毁策略及管理制度，不满足国家相关法律和标准的要求
数据销毁	关于重要数据的销毁策略及管理制度，不满足国家相关法律和标准的要求
通用阶段	组织未指定或授权业务部门或人员负责数据安全管理制度的制定
通用阶段	组织未编制和更新数据安全合规清单
通用阶段	组织未及时更新数据处理制度流程以及技术工具
通用阶段	组织未对非授权设备私自连接到内部网络的行为进行检查或限制

数据生命周期	脆弱性名称
通用阶段	组织未对内部用户非授权连接到外部网络的行为进行检查或限制
通用阶段	网络区域边界隔离策略不合理或未设置边界隔离
通用阶段	组织未及时变更或终止数据安全岗位转离岗人员的数据访问权限
通用阶段	组织未定期对数据安全岗位人员进行安全意识和岗位技能培训和考核
通用阶段	组织未对外部访问人员进行安全管控，如访问受控区域管理、数据访问权限控制、涉密时签署保密协议等
通用阶段	组织未建立数据安全领导小组，指定机构最高管理者或授权代表担任小组组长，并明确组长与小组各成员的岗位职责
通用阶段	组织未开展数据安全需求分析
通用阶段	组织未对数据供应商的数据安全能力进行评估
通用阶段	组织未形成数据资产清单并定期更新维护
通用阶段	组织未采取可靠技术措施将重要业务网络区域与其他网络区域进行隔离
通用阶段	无线接入设备未开启接入认证功能
通用阶段	组织未限制无线网络的使用，或无线网络未通过安全网关接入内部网络
通用阶段	业务系统在建设的过程中未遵循数据安全“三同步”原则，设计偏向功能实现，忽视数据安全建设
通用阶段	组织缺乏快速有效的数据安全事件应急响应机制和溯源机制
通用阶段	组织缺乏各部门之间联动的数据安全风险预警和应急响应机制
通用阶段	组织未明确元数据语义的统一格式和管理规则
通用阶段	数据安全管理制度未通过正式、有效的方式进行发布，并进行版本控制
通用阶段	组织未依据实际执行情况对数据安全管理制度的合理性和适用性进行论证和审定

C.1.2 合规脆弱性

合规脆弱性是指被评估方未能遵循国家法律、行政法规、规范性文件、地方性法规和行业监管要求，并落实相关规范。以下列出部分典型合规文件供不同行业不同区域企业参考：

表 28 合规脆弱性

合规文件分类	合规文件名称
国家法律	《中华人民共和国网络安全法》
	《中华人民共和国密码法》
	《中华人民共和国民法典》
	《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》
	《中华人民共和国刑法》

	《中华人民共和国电子商务法》
	《中华人民共和国未成年人保护法》
	《中华人民共和国消费者权益保护法》
	《中华人民共和国广告法》
	《中华人民共和国基本医疗卫生与健康促进法》
	《中华人民共和国测绘法》
	《中华人民共和国电子签名法》
	《中华人民共和国反垄断法》
	其他适用的国家法律
行政法规	《全国人民代表大会常务委员会关于加强网络信息保护的决定》
	《关键信息基础设施安全保护条例》
	《信息网络传播权保护条例》
	《计算机信息网络国际联网安全保护管理办法》
	《中华人民共和国计算机信息网络国际联网管理暂行规定》
	其他适用的行政法规
规范性文件	《个人信息和重要数据出境安全评估办法（征求意见稿）》
	《网络交易监督管理办法》
	《互联网个人信息安全保护指引（征求意见稿）》
	《网络安全审查办法》
	《个人信息出境安全评估办法(征求意见稿)》
	《网络安全等级保护条例(征求意见稿)》
	《移动互联网应用程序个人信息保护管理暂行规定(征求意见稿)》
	《数据出境安全评估办法》
	《网络数据安全管理条例》(征求意见稿)
	《数据安全管理办法(征求意见稿)》
	《未成年人网络保护条例(征求意见稿)》
	其他适用的规范性文件
地方性法规	《北京市数字经济促进条例》
	《上海市数据条例》
	《上海市公共数据开放实施细则(征求意见稿)》
	《上海市数据交易场所管理实施办法(征求意见稿)》
	《天津市促进大数据发展应用条例》
	《天津市数据安全管理办法（暂行）》
	《广东省数字经济促进条例》
	《广东省企业首席数据官建设指南》
	《广州市跨境电商行业合规指引(试行)》
	《深圳经济特区人工智能产业促进条例》
	《深圳经济特区数据条例》
	《四川省数据条例》
	《浙江省数字经济促进条例》
	《海南省大数据开发应用条例》
	《辽宁省大数据发展条例》
	《江苏省数字经济促进条例》

	《江苏省数据出境安全评估申报工作指引(第一版)》	
	《河南省网络安全条例(草案)》	
	《山西省大数据发展应用促进条例》	
	《贵州省大数据安全保障条例》	
	《贵州省大数据发展应用促进条例》	
	《贵阳市健康医疗大数据应用发展条例》	
	其他适用的地方性法规	
行业监管要求	电力	《国家发展和改革委员会令 2014 年第 14 号-电力监控系统安全防护规定》
		《国能安全[2015]36 号-电力监控系统安全防护总体方案等安全防护方案和评估规范》
		《电力行业网络安全管理办法（修订征求意见稿）》
		《2022 年能源工作指导意见》
		《电力可靠性管理办法（暂行）》
		其他适用的电力行业数据安全监管要求
	交通	《汽车数据安全管理若干规定》
		《关于加强车联网网络安全和数据安全工作的通知》
		《关于开展汽车数据安全、网络安全等自查工作的通知》
		《车联网网络安全和数据安全标准体系建设指南》
		《汽车采集数据处理安全指南》
		《车联网网络安全和数据安全标准体系建设指南》
		《关于进一步加强新能源汽车企业安全体系建设的指导意见》
		其他适用的交通行业数据安全监管要求
	卫生	《国家医疗保障局关于加强网络安全和数据保护工作的指导意见》
		《关于印发国家健康医疗大数据标准、安全和服务管理办法（试行）的通知》
		《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》
		《国务院办公厅关于促进“互联网＋医疗健康”发展的意见》
		《药品监管网络安全与信息化建设“十四五”规划》
		《“十四五”生物经济发展规划》
		其他适用的卫生行业数据安全监管要求
	金融	《银行保险机构信息科技外包风险监管办法》
		《银行业金融机构全面风险管理指引》
		《关于银行业保险业数字化转型的指导意见》
		《金融标准化“十四五”发展规划》
		《中国银保监会银行业金融机构监管数据标准化规范（2021 版）》
		《关于 2022 年进一步强化金融支持小微企业发展工作的通知》
		《中国银联金融信息技术应用创新产品能力评估指引(试行)》
		《证券期货业网络安全管理办法（征求意见稿）》
		《银行保险机构消费者权益保护管理办法（征求意见稿）》
		《银行保险监管统计管理办法（征求意见稿）》
		其他适用的金融行业数据安全监管要求

	运营商	《省级基础电信企业网络与信息安全工作考核要点与评分标准》
		《基础电信企业专业公司网络与信息安全工作考核要点与评分标准》
		《电信和互联网行业提升网络数据安全保护能力专项行动》
		《电信和互联网企业网络数据安全合规性评估要点》
		其他适用的运营商行业数据安全监管要求
	工业	《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）
		《关于“十四五”推动石化化工行业高质量发展的指导意见》
		其他适用的工业行业数据安全监管要求
	其他行业	适用于其他行业的数据安全监管要求

C.2 数据安全威胁与脆弱性的利用关系示例

表 29 数据安全威胁与脆弱性的利用关系示例

数据安全威胁类别	数据安全威胁行为	脆弱性描述
越权访问与数据资源滥用	任何用户在任何网络环境下可登录进行任何操作	采集终端未对用户进行身份鉴别
越权访问与数据资源滥用	任何用户在破解授权用户口令后可在任何时间进行越权操作	采集终端存在弱口令用户
身份假冒	授权用户在登录之后，在任何时间可冒充他人进行任何操作，造成追责困难	采集终端存在多人共用同一账号的情况
身份假冒	任何用户可在任何网络环境下对授权用户的口令进行暴力破解，进而登录进行任何操作	采集终端未配置登录失败处理功能
身份假冒	任何用户在破解授权用户口令后可在任何时间进行越权操作	采集终端用户的口令未定期更换
越权访问与数据资源滥用	授权用户在任何网络环境下，可登录进行任何操作	采集终端未对用户进行访问控制
越权访问与数据资源滥用	非授权用户在任何网络环境下，可登录进行任何操作	采集终端未及时清理多余、过期的账户
越权访问与数据资源滥用	授权用户在任何网络环境下，可登录进行任何操作	采集终端存在超级管理员等特权账户
越权访问与数据资源滥用	授权用户可在任何网络环境下，登录进行越权操作	采集终端未对用户进行安全审计
越权访问与数据资源滥用	部分授权用户可在任何网络环境下，登录进行越权操作	采集终端的安全审计未覆盖到所有用户
越权访问与数据资源滥用	任何用户可在任何网络环境下对审计记录进行删除，且无法恢复	未对采集终端的审计记录进行保护和备份

数据安全威胁类别	数据安全威胁行为	脆弱性描述
越权访问与数据资源滥用	授权用户可在任何网络环境下，中断审计进程而进行越权操作	未对采集终端的审计进程进行保护，用户可中断进程
物理破坏	任何用户或虫蚁鼠害等可在任何时间对采集终端进行破坏	采集终端所在的物理环境安全不可控，易受到破坏
物理环境变化	任何时间下，采集终端由于温湿度不符合条件而停止工作	采集终端所在的物理环境温湿度指标不可调节，存在不符合终端工作要求的情况
身份假冒	非授权用户可在任何网络环境下冒充授权采集源提交数据	采集终端未对数据源的真实性（如名称、IP 等）进行鉴别
恶意代码注入	任何用户可在任何网络环境下，对采集终端进行任何攻击行为	采集终端存在安全漏洞或未及时安装补丁程序
分类分级标记	授权用户在配置安全策略时，无任何参考，随意配置或一致性配置	采集终端未对采集的数据进行分类分级标识
业务中断/缓慢	采集终端可能由于异常原因停止工作	未定期核查用于收集数据的软硬件功能、接口功能、安全基线配置是否正常，并及时处理异常情况
业务中断/缓慢	采集终端可能由于升级、更新等操作而停止工作	未在采集设备的软硬件更新、接口升级、配置变更前，在测试环境中充分验证新版本的可用性，并制定变更失败回退方案
业务中断/缓慢	采集终端可能由于某些原因停止工作，而相关人员无法及时发现	采集终端不具备采集失效报警的功能，并能够根据采集日志追溯至失效的采集部件
业务中断/缓慢	数据采集业务可能由于采集系统发生故障而被迫中断	大数据采集系统不具备冗余机制
采集过载	实际采集的数据可能超出预期量，造成数据采集存储设备性能浪费	未计算实际业务的数据采集量，并依据设计文档判断实际的采集量是否大于预期的采集量
采集过载	实际采集的数据可能超出预期量，造成数据采集存储设备性能浪费	当业务变更时，未重新评估预计的业务采集量，并根据业务采集量重新设计数据采集设备的承载量
业务中断/缓慢	采集设备可能由于过载而停止工作	未建立采集设备过载报警机制，应根据预计的采集设备工作负荷设计报警的阈值
清洗转换错误	任何人员可在任何时间，通过任何终端随意地进行数据清洗、转换等操作	未建立数据清洗、转换操作相关的管理规范

数据安全威胁类别	数据安全威胁行为	脆弱性描述
清洗转换错误	任何人员可在任何时间，通过任何终端随意地进行数据清洗、转换等操作	未在设计文档中明确数据清洗、转换过程中使用的规则、手段、方法
清洗转换错误	无法对数据清洗、转换过程进行追溯	在数据清洗、转换过程中，未保留详细的审计记录，记录内容应至少包括转换/清洗前的数据、转换/清洗后的数据、转换/清洗使用的手段和方法、转换/清洗的时间等
数据篡改	采集数据被篡改之后，无法被发现	未使用密码技术或校验技术对采集的数据进行完整性的校验
越权访问与数据资源滥用	任何用户可在任何网络环境下，通过任何终端访问数据采集系统	未限制数据采集系统的访问方式（如登录地址限制、终端接入方式等），建立访问权限管控机制，防止未预期的访问者窃取采集的数据
分类分级标记	无法保证分类分级清单的准确性和完整性	未建立数据分类分级审核机制，对策略进行审核和批准，并对数据的分级分类进行监控纠正，建立分级分类清单保护机制，记录数据分类分级清单的操作
恶意的数据源	任何数据源可在任何网络环境下进行接入	未建立数据源接入的申请和审核机制
业务中断/缓慢	可能由于数据源发生故障造成数据采集业务中断	未对接入数据源实现生命周期管理，建立准入准出机制，并对数据源状态进行监控
无效数据写入	任何人员可在任何时间，通过任何终端随意地进行数据采集操作	未建立数据采集的规范和标准，包括采集的数据格式标准、采集范围最小化原则、数据采集分级分类规范等
无效数据写入	可能由于数据采集范围不合规导致采集业务受到影响	未对数据采集范围进行检查、反馈和更新
无效数据写入	可能由于采集到无效数据导致业务受到影响	未对无效数据建立审查回溯机制
分类分级标记	可能造成数据分类分级策略不合理的情况	未在分类的基础上围绕数据损坏、丢失、泄露等建立数据分级策略
分类分级标记	可能造成数据分类分级策略不合理的情况	数据分类分级制度中未映射业务属性
业务中断/缓慢	技术工具不能满足业务需求	数据分类分级工具不具有敏感数据识别、敏感数据类型发现、自定义分类和分级、数据标记管理、过程记录、过程分析能力

数据安全威胁类别	数据安全威胁行为	脆弱性描述
业务中断/缓慢	无法保证数据分类分级清单的可用性	未留存数据分类分级清单
采集行为不合规	数据采集业务可能面临合规风险	未围绕《网络安全法》《数据安全法》《个人信息保护法》等国家法律法规及行业规范，制定数据采集安全合规管理规范
业务中断/缓慢	数据采集风险评估可能达不到预期的效果	未以数据采集安全合规管理规范为基础，建立数据采集的风险评估流程
数据泄露	数据采集过程中可能发生数据泄露的风险	未围绕数据脱敏、数据加密、链路加密等建立数据采集过程保护
业务中断/缓慢	数据采集结果可能达不到预期的效果	未围绕采集周期、采集频率、采集内容等设置统一数据采集策略
恶意的数据源	可能由于数据源假冒等原因采集到不符合预期的数据	不具有数据源鉴别、数据源管理、数据源安全认证能力
业务中断/缓慢	无法对数据采集过程进行追溯	未对数据采集过程进行记录与留存
无效数据写入	无法保证数据采集的质量符合预期	未建立数据采集质量管理规范、数据质量管理流程、实施数据质量校验、数据质量监管，强化数据采集质量能力
数据窃取	授权用户可在任何网络环境下，随意配置或不配置数据传输保密性措施	数据传输方未梳理需要保证传输保密性的场景
数据窃取	任何用户可在任何网络环境下对传输的数据进行窃取	数据传输过程中，未采取有效措施保证数据保密性
数据篡改	授权用户可在任何网络环境下，随意配置或不配置数据传输完整性措施	数据传输方未梳理需要保证传输完整性的场景
数据篡改	任何用户可在任何网络环境下对传输的数据进行破坏	数据传输过程中，未采取有效措施保证数据完整性
业务中断/缓慢	业务高峰期时，数据传输业务中断或缓慢	数据传输节点的性能（如支持的最大网络并发连接量、接口最大带宽量等）不能满足业务高峰期数据传输的需求
业务中断/缓慢	业务高峰期时，数据传输业务中断或缓慢	数据链路中部署的安全设备的性能（如支持的最大网络并发连接量、接口最大带宽量等）不能满足业务高峰期数据传输的需求
业务中断/缓慢	业务高峰期时，数据传输业务中断或缓慢	网络总带宽量和各传输链路带宽量不能满足业务高峰期数据传输的需求

数据安全威胁类别	数据安全威胁行为	脆弱性描述
业务中断/缓慢	任何时间下，数据传输业务中断	数据传输方未提供通信线路、传输节点的硬件冗余
数据泄露	合法用户可在不安全的网络环境下进行远程管理，造成数据泄露	未采用加密等安全方式对大数据平台进行远程管理，防止数据在网络传输过程中被窃听
业务中断/缓慢	业务高峰期时，数据传输业务中断或缓慢	未对网络设备的负载情况和网络带宽使用情况进行监控，并在不满足业务高峰期需要时进行告警
数据泄露	任何用户可在任何网络环境下假冒数据接受方	未在数据通信两端采取身份鉴别机制来保证数据传输到预期目标
恶意代码注入	恶意用户可将恶意代码注入至业务系统	未对通过人机接口输入或通过通信接口输入的内容是否符合系统设定要求进行检查，不具有数据有效性检验功能
恶意代码注入	恶意用户可将恶意代码注入至业务系统	不具备校验功能有效性审计措施，当发生功能失效的情况时，能够及时向管理员提供警报或提示
数据泄露	数据可能按照不匹配的等级传输策略进行传输	未根据数据分类分级管理规定制定相应等级的数据传输策略
数据泄露	数据传输策略可能不规范	未对数据传输策略进行检查，对不符合规定的传输方式给予警告并整改
数据泄露	任何用户可在任何网络环境下，窃取重要信息	未对涉及国家重要信息、企业机密信息和个人隐私信息的数据场景进行加密传输
数据泄露	数据可能按照不匹配的等级传输策略进行传输	未对不同级别数据建立不同等级的加密传输能力
数据泄露	可能存在加密算法不合理或者失效的情况	未建立对加密算法配置、变更、管理等操作过程的审核机制和监管手段
数据泄露	任何用户可在任何网络环境下，通过任何终端对密钥进行窃取，进而窃取数据	未对密钥进行安全管理
数据泄露	密钥系统管理人员无意或者故意泄露密钥，导致数据泄露	未对密钥系统管理人员建立审核监督机制
业务中断/缓慢	任何用户可在任何网络环境下，对数据传输网络进行攻击破坏	未借助负载均衡、防入侵攻击等设备建立网络风险防范
身份假冒	任何用户可在任何网络环境下，冒充合法终端接入网络节点，窃取、破坏数据	存储媒体未进行用户-终端一对一绑定或限制远程连接网络地址范围

数据安全威胁类别	数据安全威胁行为	脆弱性描述
越权访问与数据资源滥用	任何用户在任何网络环境下可登录进行任何操作	存储媒体未对用户进行身份鉴别
越权访问与数据资源滥用	任何用户在破解授权用户口令后可在任何时间进行越权操作	存储媒体存在弱口令用户
身份假冒	授权用户在登录之后，在任何时间可冒充他人进行任何操作，造成追责困难	存储媒体存在多人共用同一账号的情况
身份假冒	任何用户可在任何网络环境下对授权用户的口令进行暴力破解，进而登录进行任何操作	存储媒体未配置登录失败处理功能
身份假冒	任何用户在破解授权用户口令后可在任何时间进行越权操作	存储媒体用户的口令未定期更换
越权访问与数据资源滥用	授权用户在任何网络环境下，可登录进行任何操作	存储媒体未对用户进行访问控制
越权访问与数据资源滥用	非授权用户在任何网络环境下，可登录进行任何操作	存储媒体未及时清理多余、过期的账户
越权访问与数据资源滥用	授权用户在任何网络环境下，可登录进行任何操作	存储媒体存在超级管理员等特权账户
越权访问与数据资源滥用	授权用户可在任何网络环境下，登录进行越权操作	存储媒体未对用户进行安全审计
越权访问与数据资源滥用	部分授权用户可在任何网络环境下，登录进行越权操作	存储媒体的安全审计未覆盖到所有用户
越权访问与数据资源滥用	任何用户可在任何网络环境下对审计记录进行删除，且无法恢复	组织未对存储媒体的审计记录进行保护和备份
越权访问与数据资源滥用	授权用户可在任何网络环境下，中断审计进程而进行越权操作	组织未对存储媒体的审计进程进行保护，用户可中断进程
数据窃取	任何用户可在任何时间，通过电磁干扰、收集等手段，破坏和窃取关键数据	关键存储媒体所在的物理环境未进行电磁屏蔽
物理破坏	任何用户、虫蚁鼠害等可在任何时间对存储媒体进行破坏	存储媒体所在的物理环境安全不可控，易受到破坏
物理环境变化	任何时间下，存储媒体由于温湿度不符合条件而停止工作	存储媒体所在的物理环境温湿度指标不可调节，存在不符合终端工作

数据安全威胁类别	数据安全威胁行为	脆弱性描述
		要求的情况
恶意代码注入	任何用户可在任何网络环境下，对存储媒体进行任何攻击行为	存储媒体存在安全漏洞或未及时安装补丁程序
数据窃取	任何用户可在任何网络环境下，对数据进行窃取	存储媒体未配置安全的远程连接协议
恶意代码注入	任何用户可在任何网络环境下，通过端口对存储媒体进行攻击	存储媒体未关闭高危端口或非使用的端口
分类分级标记	导致无法针对不同分类分级数据采取差异化的安全策略	存储的数据未自动进行分类分级
数据篡改	任何用户可在任何网络环境下，对重要数据进行篡改、破坏而不被发现	组织未依据安全策略保证重要数据的存储完整性
数据窃取	任何用户可在任何网络环境下，对重要数据进行窃取	组织未依据安全策略保证重要数据的存储机密性
数据损毁	一旦发生人为或者意外事故，导致数据遭受损毁后，无法进行恢复	组织未对数据进行本地备份和异地备份
身份假冒	任何用户可在任何网络环境下，利用中间人攻击等手段，对关键业务数据进行拦截、篡改，进而导致关键业务发生中断、瘫痪等意外错误	存储媒体的网络时钟未进行同步
业务中断/缓慢	导致对数据的检索、遍历、编辑等操作变得缓慢或中断	组织未依据数据的大小、性质（如结构化、非结构化等）等选择合适的逻辑存储方式（如集中存储、分散存储等）
业务中断/缓慢	导致无法对超过安全阈值的存储媒体进行告警	组织未采取技术工具对存储媒体的使用历史、性能指标、错误或损坏情况等性能进行监控
业务中断/缓慢	可能由于存储节点发生故障，导致业务中断	未采用分布式存储、容灾备份及恢复、业务快照等保证数据可用性的技术手段
恶意代码注入	任何用户可在任何网络环境下对数据存储系统进行恶意代码注入	未采用对数据存储系统的输入输出接口进行安全管控并对接入设备进行安全扫描的技术手段
业务中断/缓慢	任何用户可在任何网络环境下对数据存储系统进行攻击	未对数据存储系统重要节点的入侵行为进行检测并对严重事件进行报警

数据安全威胁类别	数据安全威胁行为	脆弱性描述
业务中断/缓慢	可能由于数据存储系统配置错误导致业务中断	未定期对数据存储系统进行安全基线配置检查
业务中断/缓慢	数据备份文件可能无法正常进行恢复	未定期对数据备份文件进行恢复测试并记录和保存测试结果
业务中断/缓慢	可能由于数据存储系统多副本数据不一致导致业务受到影响	数据存储系统不具备对多副本一致性进行扫描自检并对不一致数据尝试进行修复和告警的机制
第三方脆弱性	可能由于合作的第三方单位存在脆弱性，而导致自身受到数据安全威胁	对委托第三方云平台、数据中心等存储数据的情况，第三方数据存储服务供应商未通过相应等级的网络安全等级保护测评或其他相关测评
第三方脆弱性	可能由于合作的第三方单位存在脆弱性，而导致自身受到数据安全威胁	对委托第三方云平台、数据中心等存储数据的情况，未与第三方数据存储服务供应商签署了正式的数据存储服务协议，并对其责任、义务及违约后果进行明确约定
数据损毁	任何用户可在任何网络环境下，通过任何终端对数据存储系统进行高危操作	不具备对于如删除数据、更改数据存储系统配置等高危操作进行授权审批的机制和技术手段
人员意识	可能由于运维人员安全意识不足导致数据安全事件的发生	未定期对数据存储系统的运维人员进行培训和考核
数据安全建设威胁	存储介质可能按照级别不匹配的安全策略进行保护	未对存储介质进行分类分级
越权访问与数据资源滥用	任何用户可在任何使用场景下使用存储介质	未建立存储介质使用审批制度
业务中断/缓慢	可能由于存储介质自身性能的问题导致业务受到影响	未定期对存储介质开展测试
越权访问与数据资源滥用	任何用户可在任何使用场景下使用存储介质	未对存储介质配置安全能力（如：认证鉴权、访问控制、通信举证、文件防病毒等）
业务中断/缓慢	可能由于存储节点发生故障，导致业务中断	未建立数据存储冗余策略和设计指导
数据误操作	任何用户可在任何网络环境下，通过任何终端随意地操作	未建立数据复制、备份与恢复的操作规程
业务中断/缓慢	可能由于备份数据发生故障导致无法进行恢复	未对备份数据定期开展检查
业务中断/缓慢	可能由于备份数据发生故障导致无法进行恢复	未对备份数据建立安全管控能力

数据安全威胁类别	数据安全威胁行为	脆弱性描述
数据篡改	任何用户可在任何时间，通过任何网络环境进行批量数据篡改	组织未对用户可执行的操作进行时间和网络范围上的限制
数据窃取	任何用户可在任何时间，通过任何网络环境进行批量数据下载	组织未对用户可执行的操作进行时间和网络范围上的限制
数据损毁	任何用户可在任何时间，通过任何网络环境进行批量数据删除	组织未对用户可执行的操作进行时间和网络范围上的限制
数据篡改	任何用户可在任何时间，通过任何网络环境进行批量数据写入	组织未对用户可执行的操作进行时间和网络范围上的限制
数据窃取	任何用户可在任何时间，通过任何网络环境进行批量数据查询	组织未对用户可执行的操作进行时间和网络范围上的限制
越权访问与数据资源滥用	任何用户可在任何时间，通过任何网络环境进行批量权限修改	组织未对用户可执行的操作进行时间和网络范围上的限制
数据泄露	任何用户可在任何网络环境下，有意或无意泄露数据	组织未依据脱敏策略对数据进行脱敏
数据泄露	无法对数据脱敏过程进行追溯	组织未对数据脱敏过程进行监控和审计
越权访问与数据资源滥用	无法对数据分析过程进行追溯	组织未对数据分析过程进行监控和审计
越权访问与数据资源滥用	任何用户可在任何网络环境下，有意或无意泄露数据	个人信息和重要数据在使用前，未进行安全影响评估
越权访问与数据资源滥用	无法对数据使用过程进行追溯	组织未对数据使用过程进行监控和审计
越权访问与数据资源滥用	无法对数据导入导出过程进行追溯	组织未对数据导入导出过程进行监控和审计
数据违规处理	可能无法及时发现异常的数据处理活动	未定期查看数据处理活动操作审计记录
越权处理	任何用户均可越权处理数据	未对数据处理过程建立适当的授权审批机制
数据误操作	任何用户可在任何网络环境下，通过任何终端随意地对数据进行处理	未制定数据处理过程操作规范
数据误操作	任何用户可在任何网络环境下，通过任何终端随意地对数据进行脱敏处理	未制定数据脱敏处理规范和流程

数据安全威胁类别	数据安全威胁行为	脆弱性描述
数据泄露	可能造成数据脱敏效果不符合预期	未建立适当的数据脱敏效果评估机制
越权访问与数据资源滥用	任何用户可在任何网络环境下，通过任何终端对数据处理结果进行访问	针对数据处理结果访问与使用，未建立适当的权限管控和审计机制
越权访问与数据资源滥用	任何用户可通过特权账户越权操作	未制定特权账户的使用规范
行为抵赖	无法及时发现多余、过期、僵尸账户等高危账户	未定期审计不同账户的使用情况
违规操作	无法及时发现违规行为	未审核数据处理的日常操作行为，对违规行为予以提醒
数据泄露	可能导致数据脱敏效果与预期不符	未明确需要数据脱敏的业务场景
数据泄露	任何用户可在任何网络环境下，通过任何终端对敏感数据进行访问	未建立敏感数据访问控制机制
数据泄露	可能由于数据脱敏工具不统一导致脱敏效果不符合预期	不具备统一数据脱敏工具（包括：静态脱敏、动态脱敏）
数据泄露	可能导致数据脱敏效果与预期不符	数据脱敏工具未与数据权限管理平台实现联动
行为抵赖	无法对数据脱敏过程进行追溯	未对数据脱敏操作过程进行记录
违规使用	无法及时发现违规使用和恶意行为	未建立审核违规使用和恶意行为的机制
数据误操作	任何用户可在任何网络环境下，通过任何终端随意地对数据进行分析操作	未制定数据分析过程中数据资源操作规范和实施指南
数据泄露	可能造成个人信息泄露	不具备对个人信息去标识化的处理能力
业务中断/缓慢	分析结果可能不符合预期	未建立对数据分析结果进行审核的机制
人员意识	可能由于数据使用者的安全意识不足，导致发生数据安全事件	未建立数据使用者安全责任制度
违规使用	可能引发违背法律法规规定的风险	使用个人信息，未建立在明示同意的基础上
数据损毁	可能由于数据处理环境不安全导致数据遭到损毁	未围绕损坏、丢失、窃取等建立数据处理环境保护机制
数据损毁	可能由于数据处理安全策略不完善导致数据遭到损毁	未围绕访问控制、监管审计、职责分离等建立数据处理安全能力

数据安全威胁类别	数据安全威胁行为	脆弱性描述
数据泄露	任何用户可在任何网络环境下，超范围共享数据	组织未明确数据共享的内容范围
数据泄露	任何用户可在任何网络环境下，超范围共享数据	组织未明确数据共享的管理措施和安全规范
数据泄露	任何用户可在任何网络环境下，超范围共享数据	组织未明确数据共享涉及的各部门和岗位的职责与权限
数据泄露	任何用户可在任何网络环境下，超范围共享数据	组织未对数据共享行为进行安全审计
数据泄露	任何用户可在任何网络环境下，超范围发布数据	组织未明确数据发布公开的内容、范围和规范
数据泄露	任何用户可在任何网络环境下，超范围发布数据	组织未定期审查发布数据中是否包含非公开信息
数据泄露	任何用户可在任何网络环境下，超范围发布数据	组织未对数据发布行为进行安全审计
数据违规共享	可能面临数据共享合规风险	数据共享范围，不符合国家、政务行业及区域相关规定
数据违规共享	可能面临数据共享合规风险	数据共享策略，不满足相关法律法规和数据保护要求
违规操作	任何用户可随意地进行数据共享操作	未制定数据共享流程规范
共享接口滥用	任何用户可在任何网络环境下，通过任何终端访问数据共享接口	数据共享接口未配置必要的访问权限控制
共享越权	无法对共享的数据进行溯源	未建立适当的共享数据溯源机制
数据爬取	任何用户可通过数据爬取等方式越权获取数据	数据开放平台未建立防数据爬取机制
非授权访问	任何用户均可登录数据开放平台	数据开放平台用户在登录时未采用身份鉴别措施
行为抵赖	用户可能抵赖自己的操作行为	数据开放平台用户列表里的用户身份标识不具有唯一性
身份假冒	空口令用户可被恶意人员利用进行操作	数据开放平台存在空口令用户
数据泄露	任何用户可在任何网络环境下，通过任何终端访问数据开放平台	数据开放平台未根据业务需求和安全要求建立适当的访问控制机制
越权操作	恶意人员可能通过特殊账户进行越权访问	针对数据开放平台未对特权账户、临时账户等特殊用户进行管控
非授权访问	可能由于平台自身的安全性导致被非授权访问	未定期对数据开放平台的安全性进行验证
数据误操作	任何用户可随意地进行数据导入导出操作	未建立数据导入导出安全保障制度规范

数据安全威胁类别	数据安全威胁行为	脆弱性描述
数据泄露	无法依据数据安全级别提供差异化的导入导出策略	未基于数据分类分级要求建立数据导入导出安全策略
行为抵赖	无法对数据导入导出操作进行追溯	未对导入导出行为进行记录
越权操作	任何用户均可进行数据导入导出操作	不具有导入导出权限管理能力
越权操作	任何用户均可进行数据导入导出操作	不具有导入导出身份认证能力
数据一致性问题	可能无法发现导入导出过程中数据完整性被破坏的情况	不具有导入导出完整性验证能力
误操作	用户可随意地进行数据共享操作	未建立数据共享场景的规范要求
越权操作	用户可越权进行数据共享操作	未建立数据共享审核流程
行为抵赖	用户可能抵赖自己的操作行为	不具有数据共享审计策略
数据泄露	共享的数据可能发生泄漏的风险	未利用数据加密、安全通道等措施保护共享数据
数据泄露	无法有效应对由于数据公开而发生的数据安全事件	不具有数据资源公开应急处置能力
数据泄露	任何用户可在任何网络环境下，通过任何终端对 API 接口进行访问	不具有 API 数据接口安全防范能力
数据泄露	任何用户可在任何网络环境下，随意地进行销毁操作	组织未明确数据销毁场景、销毁对象、销毁方式、销毁要求
数据泄露	存在敏感数据泄露的风险	组织未依据国家法律法规要求，销毁个人信息、重要数据等敏感数据
数据泄露	任何用户可在任何网络环境下，随意地进行存储媒体销毁操作	组织未明确存储媒体销毁处理策略、管理制度和机制，以及销毁对象和流程
数据泄露	任何用户可在任何网络环境下，随意地进行存储媒体销毁操作	组织未对存储媒体的销毁行为进行记录
数据泄露	任何用户可在任何网络环境下，随意地进行存储媒体销毁操作	组织未对存储媒体的销毁过程进行监控
数据泄露	任何用户可在任何网络环境下，随意地进行存储媒体销毁操作	组织未依据存储媒体类型的不同，建立软销毁和硬销毁的销毁策略
数据损毁	任何用户可随意地进行数据销毁操作	未建立数据销毁审批机制
违规操作	数据销毁工作可能未按照操作规程进行	未设置数据销毁的监督角色

数据安全威胁类别	数据安全威胁行为	脆弱性描述
数据销毁不彻底	数据销毁可能不彻底	不具备识别并销毁全部数据副本及备份数据的机制和技术手段
数据销毁不彻底	数据销毁工作可能无法有效开展	未配备必要的数据销毁工具
违规操作	已销毁数据可能被违规恢复	不具备确保被销毁数据及其副本内容不可被恢复的措施和技术手段
数据泄露	可能面临数据销毁合规风险	关于个人信息的销毁策略及管理制度，不满足国家相关法律和标准的要求
数据泄露	可能面临数据销毁合规风险	关于重要数据的销毁策略及管理制度，不满足国家相关法律和标准的要求
数据销毁不彻底	数据销毁效果可能不符合预期	未建立针对数据销毁效果的评估机制
越权访问与数据资源滥用	任何用户可在任何网络环境下，对重要业务网络进行非授权访问	组织未采取可靠技术措施将重要业务网络区域与其他网络区域进行隔离
越权访问与数据资源滥用	任何用户可在任何网络环境下，对重要业务网络进行非授权访问	网络区域边界隔离策略不合理或未设置边界隔离
越权访问与数据资源滥用	非授权用户可在任何网络环境下连接内部网络	组织未对非授权设备私自连接到内部网络的行为进行检查或限制
越权访问与数据资源滥用	非授权内部网络用户可随意连接外部网络	组织未对内部用户非授权连接到外部网络的行为进行检查或限制
越权访问与数据资源滥用	任何用户可通过无线网络入侵内部网络	组织未限制无线网络的使用，或无线网络未通过安全网关接入内部网络
越权访问与数据资源滥用	任何用户可通过无线网络入侵内部网络	无线接入设备未开启接入认证功能
数据安全建设威胁	导致后期数据安全建设成本高、投入大、效果不明显	业务系统在建设的过程中未遵循数据安全“三同步”原则，设计偏向功能实现，忽视数据安全建设
数据安全建设威胁	导致数据安全制度与实际业务场景脱节，而无法落地	组织未指定或授权业务部门或人员负责数据安全管理制度的制定
数据安全建设威胁	导致无法保证数据安全制度的正常贯彻和落实	数据安全管理制度未通过正式、有效的方式进行发布，并进行版本控制
数据安全建设威胁	导致无法保证数据安全制度的更新迭代，更好地和业务相匹配	组织未依据实际执行情况对数据安全管理制度的合理性和适用性进行论证和审定

数据安全威胁类别	数据安全威胁行为	脆弱性描述
数据安全建设威胁	导致无法从组织层面规范数据安全管理	组织未建立数据安全领导小组，指定机构最高管理者或授权代表担任小组组长，并明确组长与小组各成员的岗位职责
数据安全建设威胁	导致组织在面对智能终端和网络用户数量的增加、数据来源广泛、数据的多样性、数据结构的复杂化等情况时，难以有效地维护数据	组织未及时更新数据处理制度流程以及技术工具
数据安全建设威胁	导致无法有效应对数据安全事件的发生	组织缺乏快速有效的数据安全事件应急响应机制和溯源机制
数据安全建设威胁	导致无法有效应对数据安全事件的发生	组织缺乏各部门之间联动的数据安全风险预警和应急响应机制
越权访问与数据资源滥用	转离岗人员可在任何网络环境下越权访问数据	组织未及时变更或终止数据安全岗位转离岗人员的数据访问权限
数据安全建设威胁	导致数据安全相关人员的责任意识涣散和技术能力羸弱	组织未定期对数据安全岗位人员进行安全意识和岗位技能培训和考核
数据泄露	外部人员可访问受控区域	组织未对外部访问人员进行安全管控，如访问受控区域管理、数据访问权限控制、涉密时签署保密协议等
数据安全建设威胁	导致组织面临数据安全合规风险	组织未编制和更新数据安全合规清单
数据安全建设威胁	导致组织无法有效地掌握自身的数据资产情况	组织未形成数据资产清单并定期更新维护
数据安全建设威胁	可能由于数据供应商存在脆弱性，而对需求方产生威胁	组织未对数据供应商的数据安全能力进行评估
数据安全建设威胁	导致组织元数据管理混乱，数据维护、检索困难	组织未明确元数据语义的统一格式和管理规则
数据安全建设威胁	导致组织无法有效地推进数据安全建设	组织未开展数据安全需求分析

C.3 数据安全风险等级划分参考表

表 30 数据安全风险等级划分参考表

风险值	结论	描 述	是否接受风险（示例）
4.1-5.0	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	否
3.1-4.0	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	否

		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	
2.1-3.0	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	否
1.1-2.0	低	一旦发生造成的影响程度较低，一般仅限于业务、组织内部或数据本身，通过一定手段很快能解决	是
0-1.0	很低	一旦发生造成的影响低微	是

C.4 数据安全风险评估报告参考模板

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 信息搜集方法

三 风险识别

3.1 数据识别

3.2 数据处理活动场景识别

3.3 已有安全措施识别

3.4 脆弱性识别

3.5 数据安全威胁识别

四 风险分析

4.1 数据重要程度赋值

4.2 脆弱性可造成的损失计算

4.3 数据安全威胁发生可能性计算

4.4 数据风险值计算

参考文献

[1] Neil MacDonald, Peter Firstbrook. Designing an Adaptive Security Architecture for Protection From Advanced Attacks. [R/OL]. [2004-2-12]. https://www.gartner.com/en/documents/2665515

[2] 中国信息通信研究院.中国数字经济发展报告（2022）[R/OL].[2022-07-08].http://www.caict.ac.cn/kxyj/qwfb/bps/202207/t20220708_405627.htm

[3] 国家统计局.数字经济及其核心产业统计分类（2021）[R/OL].[2021-06-03].http://www.stats.gov.cn/tjsj./tjbz/202106/t20210603_1818134.html

[4] 中国软件评测中心.电信和互联网行业数据安全治理白皮书（2020）[R/OL].[2020-12-23].https://www.cstc.org.cn/info/1081/231483.htm

[5] 工业和信息化部.“十四五”大数据产业发展规划[R/OL].[2022-07-06].https://www.miit.gov.cn/jgsj/ghs/zlygh/art/2022/art_5051b9be5d4740daad48e3b1ad8f728b.html

[6] 炼石网络.我国 197 项数据安全政策回顾汇总[R/OL].[2022-03-04].http://www.ciphergateway.com/product/40738.html

[7] 炼石网络.六大洲 14 国 87 项数据安全法规汇总分析[R/OL].[2022-07-27].http://www.ciphergateway.com/product/40971.html

[8] GB/T 31722-2015, 信息技术 安全技术.信息安全风险管理[S]

[9] GB/T 20984-2022, 信息安全技术 信息安全风险评估方法[S]

[10] 《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）》[Z]

[11] GB/T 37988-2019, 信息安全技术 数据安全能力成熟度模型[S]

[12] GB/T 35274-2017, 信息安全技术 大数据服务安全能力要求[S]

[13] GB/T 35295-2017, 信息技术 大数据术语[S]

[14] GB/T 22239-2019, 信息安全技术 网络安全等级保护基本要求[S]

[15] JR/T 0223-2021, 金融数据安全 数据生命周期安全规范[S]

[16] YD/T 3802-2020, 电信网和互联网数据安全通用要求[S]

[17] YD/T 3956-2021, 电信网和互联网数据安全评估规范[S]

[18] GB/T 39725-2020, 信息安全技术 健康医疗数据安全指南[S]

[19] 《信息安全技术 网络数据分类分级要求》（征求意见稿）－全国信息安全标准化技术委员会

[20] GB／T 37988-2019, 信息安全技术 数据安全能力成熟度模型[S]

[21] YDT 3801-2020, 电信网和互联网数据安全风险评估实施方法[S]

[22] GB/T 38667-2020, 信息技术 大数据 数据分类指南[S]

[23] GB/T 35273-2020 信息安全技术 个人信息安全规范[S]

[24] JR/T 0171-2020 个人金融信息保护技术规范[S]

CSA GCR cloud security alliance GREATER CHINA REGION

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网:https://c-csa.cn 电话:0755-86548359
地址:上海市浦东新区东育路255弄5号3FB30(前滩国际经济组织集聚区)/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905