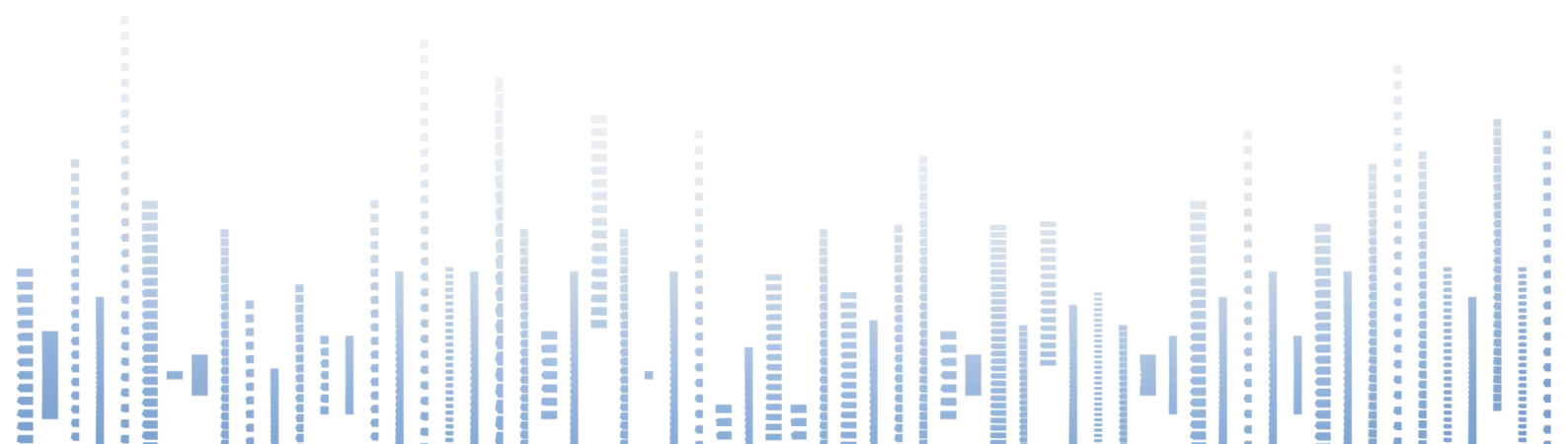
数据安全推进计划
DATA SECURITY INITIATIVE

大数据技术标准推进委员会
Big Data Technology and Standard Committee

数据安全风险评估实务：问题剖析与解决思路

数据安全推进计划
CCSA TC601 大数据技术标准推进委员会

2023年12月



版 权 声 明

报告愿景及目标

全球数字经济持续发展，我国数字化转型加速推进，数据要素市场化进度加快。然而，数据泄露、数据破坏、数据滥用等安全事件频繁发生，这严重危害了国家、社会公众安全，数据安全风险防范的重要性日益凸显。

随着网络安全、数据安全领域的法律法规相继颁布，强调数据处理者应依法依规开展数据处理活动，建立健全数据安全管理制度，加强数据安全风险监测与防范，定期开展数据安全风险评估，数据安全风险的评估与治理已成为业内各方最为关切的话题。然而，尽管大量的法规、标准提供了丰富的理论指引，数据安全风险评估工作实务中仍然存在诸多问题。这些问题分布在整个评估过程的各个阶段，成因错综复杂，严重影响了组织的数据安全风险评估工作落地，长期来看不利于组织数据安全风险治理能力的持续提升。

在此背景下，数据安全推进计划（DSI）联合中国通信标准化协会大数据技术标准推进委员会（CCSA TC601），携手业内众多专家撰写了本报告。本报告旨在解决数据安全风险评估实务中的诸多问题，介绍了当前我国数据安全风险评估的监管要求、标准编制现状以及评估实施方法，提炼了数据安全风险评估工作的具体实施流程，并以评估实施流程为主线，系统性梳理了组织在评估准备、评估实施、评估总结三大阶段面临的具体实务问题，并提出问题解决思路，为数据处理者、评估机构的数据安全风险评估实务提供参考，为相关数据处理者、服务机构纾难解惑，增强产业界信心。

由于编制时间仓促、水平有限，报告难免存在疏漏，欢迎大家批评指正。

联系方式：gongshiran@caict.ac.cn

编制单位

中国信息通信研究院云计算与大数据研究所、中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中国联合网络通信有限公司研究院、中国移动通信集团江苏有限公司、中国人寿保险（集团）公司、中国平安人寿保险股份有限公司、华泰证券股份有限公司、天翼电子商务有限公司、西部证券股份有限公司、中国航天科工集团航天情报与信息研究所、国家电网有限公司、重庆长安汽车股份有限公司、赛力斯集团股份有限公司、北京银行股份有限公司、北京五八信息技术有限公司、杭州美创科技股份有限公司、奇安信科技集团股份有限公司、北京天融信网络安全技术有限公司、联通数字科技有限公司、杭州比智科技有限公司、全知科技（杭州）有限责任公司、腾讯科技（深圳）有限公司、北京亿赛通科技发展有限责任公司、北京塔斯数据技术有限公司、天道金科股份有限公司、杭州数猫科技有限公司、深圳市联软科技股份有限公司、北京数字认证股份有限公司、杭州数梦工场科技有限公司、安徽辰图大数据科技有限公司、北京数安行科技有限公司、北京炼石网络技术有限公司、南京聚铭网络科技有限公司、杭州安恒信息技术股份有限公司、阿里云计算有限公司、厦门服云信息科技有限公司、深圳市华傲数据技术有限公司、杭州极盾数字科技有限公司。

编制工作组

龚诗然、张亚兰、李雪妮、李天阳、张越、郝志婧、刘雪花

编制专家

龚诗然、张亚兰、温暖、王勇、李冰、王志宇、周莹、李文琦、刘飞龙、钱江洪、陈豪、曹咪、陶冶、吴璟、姬长鹏、刘洋、张啸雷、马宁、张扬、柯淑馨、江旺、张炎、周思佳、谢云鹏、洪雪莲、许琛超、邢骁、姜娜、全晓东、李超、张立鹏、张强强、刘斌、苏辉、李鹏、王会宴、杨力、王思涵、朱梦瑶、李娜（北京银行）、王基安、刘蕾、柳遵梁、应以峰、叶桦、朱朔漫、楚赟、苏文亭、梁伟、王玮、艾龙、谢雄、马明、赵宁、周莉、王笑晨、任兴、崔玲龙、何徐麒、曾云、崔壤丹、李滨、姬生利、乐元、张林成、刘灿、张艺伟、梁步庭、李楷、胡国华、卓柳俊、王振东、张红露、王同新、张赣、毛靖文、傅娅兰、陈洪运、宫小茜、郭丽颖、胡嘉伟、甘长华、翟培康、关中华、项宇欣、刘玉红、赵倩、唐开达、陈虎、高柱、徐道晨、李娜（阿里云）、杨智垄、何旭珩、查浩奇。

CONTENTS
目　录

四、数据安全风险评估工作建议

图目录

表目录

一.数据安全风险评估工作背景

全球数据泄露、数据破坏、数据窃取、数据滥用等安全事件频繁发生，严重危害了国家、社会公众安全。针对各国政府机构、关键信息基础设施的网络攻击、数据窃取等违法活动明显增多，数据安全事件涉及的数据以及用户体量也在持续加大。如何有效防范数据安全风险与事件，是全球数字经济发展下的重点问题。

本章节将总结国际、国内数据安全风险形势，分析广大组织面临的各类数据安全风险以及日趋严格的监管合规要求，阐述了组织加强数据安全风险防范的必要性。

(一)数据安全风险形势日益严峻

1.数据泄露：持续呈现高发态势

全球数据泄露事件持续高发。统计数据显示，仅2021年全球范围内公开披露的数据泄露事件已超过四千起，涉及超过200亿条数据。进入2023年，数据泄露的趋势似乎并未得到缓解：2023年4月，威胁猎人发布的《2023年Q1数据资产泄露分析报告》显示，仅2023年第一季度就已发生近千余起数据泄露事件，这些事件涉及上千家组织、近四十个行业。例如，Twitter在2023年1月遭遇了数据泄露事件，包括用户电子邮件地址、姓名等2亿条个人信息被泄露。2023年2月，全美最大的综合医疗服务网络Heritage Provider Network遭遇勒索软件攻击，导致多个医疗机构大量敏感信息泄露。2023年2月，Telegram各大频道突然大面积转发某隐私查询机器人链接，该机器人泄露了大量来自我国各快递、电商平台的个人信息，包含了用户的真实姓名、电话与住址等，数据量高达45亿条。

组织数据安全保障压力倍增。2020年，某电商的客户数据泄露导致不法分子冒充客服对全国二十多个城市的受害者进行了电话诈骗，受害者的被骗金额为几千到十几万元不等。2023年8月，公安部公布了打击侵犯公民个人信息犯罪的十大典型案例，其中黑灰产组织窃取、利用组织掌握的用户个人信息实施犯罪的案例高居榜首。随着个人信息成为黑灰产组织逐利的“重灾区”，组织面对无孔不入的黑灰产组织，在数据安全风险应对上压力倍增。

数据泄露事件为组织带来的损失也在逐年走高。组织数字化转型加快，对数据依赖程度随之加深，数据一旦泄露给组织带来的损失也更加严重。根据IBM《2023年数据泄露成本报告》显示，组织数据泄露事件平均成本达到445万美元，较2022年的435万美元增长2.3%，而较2020年的386万美元则足足增长了15.3%，现已创下历史新高。

2.数据破坏：勒索攻击危害显著

有针对性的数据勒索与破坏事件愈演愈烈。随着全球各行业领域的组织数字化转型程度加深，其系统及承载的数据重要程度也随之提升，其中的关键数据更是组织业务运行命脉，一旦这些关键数据遭到破坏，将面临业务中断、信息系统或网络服务瘫痪，严重的后果可能是长期业务受损，客户信息、商业机密等重要数据泄露，给组织带来重大的经济损失和声誉损失。而近年来，针对政府机构、知名组织的数据勒索、破坏事件也持续增加：2022年，哥斯达黎加政府遭遇Conti勒索软件团伙攻击，国家财政部数个TB的数据以及800多台服务器受到此次攻击影响，国内数字税务服务、海关控制IT系统以及医疗保健系统在多轮攻击下接连瘫痪、被迫下线，导致国内医疗保健系统陷入混乱。同年，法国巴黎的一家医院Center Hospitalier Sud Francilien（以下简称CHSF）遭遇网络攻击并被勒索1000万美元作为解密密钥的赎金。此次攻击直接导致了CHSF多个业务软件、医学影像存储系统无法访问，大量医疗数据被加密迫使医院推迟多台手术计划，大量患者被临时转诊至其他机构，这严重威胁了当地的急、重病患者生命安全。

3.数据窃取：组织“内鬼”作案猖獗

来自“内鬼”的数据窃取也令组织防不胜防。2023年6月6日，Verizon发布了《2023年度数据泄露调查报告》（2023 Data Breach Investigations Report，简称DBIR），分析了从2017年以来的16312起安全事件和5199起数据泄露事件，指出74%的泄露事件由人为因素造成的，约五分之一的数据泄露事件来自于组织的内部。组织收集、存储了大量用户的个人信息数据，一旦组织内部出现了特权账号滥用、数据权限分配不清、人员利用越权访问漏洞等问题，将直接导致拥有内部人员对其获取的数据进行不正当的使用或者窃取。2023年5月，特斯拉两名员工违规挪用、泄露了包括员工个人信息、客户银行信息、生产信息在内的100GB数据，影响超过7.5万人。无独有偶，2023年7月，日本通信运营商NTT DOCOMO的承包商员工盗取了包括用户个人信息在内的596万条商业信息，这些案件均有力证明了组织“内鬼”窃取数据的危害。

(二)组织风险防范面临监管考验

面对日益严峻的网络数据安全风险，各国政府倡导国际、国内或地区内的公私部门开展网络数据安全风险防范合作。例如，2023年《联合国打击网络犯罪公约》结合新型网络犯罪情况，要求缔约国将黑客攻击、非法数据获取等犯罪行为纳入本国刑法执法范围，倡导加强网络数据安全风险的跨国协作与应对。再例如，欧盟《数据治理法案》（2022）提出欧盟境内的公共和私营组织在共享数据时，应遵守的安全与可靠性要求，要求及时报告数据泄露事件，防范全球数据流通带来的数据共享风险。美国《网络安全信息分享法案（CISA）》（2015）也曾鼓励国内的私营组织与政府进行网络威胁情报共享，增强其网络数据安全风险防御能力。

数据安全与隐私保护法规的发展对广大数据处理者的风险防范能力提出了新要求。除了网络数据安全风险的跨国协作与应对，各国的法律法规也明确规定了国内数据处理者的数据安全义务、责任，要求其开展数据保护影响评估等活动，加强对用户个人信息的保护。

中国方面。2021年，中国《中华人民共和国数据安全法》（以下简称《数据安全法》）、《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）相继颁布、实施。作为数据安全领域的基础性法律，《数据安全法》指出数据处理者开展数据处理活动应依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。其中，重要数据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。《个人信息保护法》则进一步强调了个人信息处理者的责任与义务，提出个人信息处理者应对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。在处理敏感个人信息等情形下，个人信息处理者还应当事前进行个人信息保护影响评估，并对处理情况进行记录。

欧盟方面。2018年，欧盟《通用数据保护条例》（General Data Protection Regulation，以下简称"GDPR"）正式生效。GDPR基于其域外效力及严厉的行政处罚措施，提出了个人同意、隐私权影响评估等多项数据处理合规要求，并警示其适用范围内的数据处理主体严格履行合规义务。针对可能会为自然人权利与自由带来高度风险的数据处理方式，GDPR提出数据处理主体应事先进行影响评估，加强对个人敏感信息的保护，限制对个人信息的非授权使用。

美国方面。2023年1月，美国《加州隐私权法案》（California Privacy Rights Act，以下简称CPRA）正式生效。CPRA在《加州消费者隐私法案》（California Consumer Privacy Act，简称CCPA）的基础上进行了修订，要求组织开展数据处理活动风险评估，并定期向当地隐私局提交评估报告。此外，美国的《弗吉尼亚州消费者保护法》与《科罗拉多州隐私法》也要求，针对可能对消费者带来重大风险的行为，信息处理者应开展数据保护影响评估（Data Protection Impact Assessment，简称DPIA），并在评估期间对消费者的信息进行去标识处置。

新加坡、俄罗斯、印度、巴西、韩国等多个国家也通过立法明确了数据处理者的数据保护、风险防范以及数据保护影响评估活动等方面的要求，加强了数据处理者的监督和处罚，极大地推动了以上国家、地区的数据处理者提升数据安全风险防范能力，切实保护数据安全。

(三)新技术应用暗藏新型风险

新技术应用衍生新型安全风险。5G、人工智能、云计算、移动互联网、大数据分析等新兴技术应用极大地推动了各行业领域的组织发展与创新，为广大用户提供了更为智能、便利的服务，但同时也带来了大量的安全漏洞、风险。**以云计算为例。**云计算通过互联网为组织提供了更加灵活、可扩展的计算和存储服务，实现了资源池化、按需扩缩容的能力，但云平台的复杂性以及多租户环境也存在数据隔离失效的问题，存在内部人员越权访问的可能，增加了组织数据泄露的风险。**再例如，5G技术的典型应用场景eMBB（增强移动带宽）**，由于在增强现实（AR）、虚拟现实（VR）、高清视频直播、频等对带宽有

极高要求的业务场景下衍生的海量数据往往涉及个人隐私数据，而传统的安全基础设施难以适应超大流量的5G网络防护以及海量用户隐私数据保护的安全需求。

新兴技术的监管措施与规范的不完善也可能导致数据安全风险。部分处于萌芽期的新兴技术可能因其配套的监管措施与技术规范尚未完善，在实际应用过程中为组织、个人带来尚未被公众充分认识的数据安全风险，导致安全事件一旦发生，出现责任主体判定难、治理成本高等问题。**以生成式AI为例。**其在文本、图片或视频生成等领域中得到了广泛的应用，但如果在学习训练阶段缺乏监管，该技术可能会因其对个人信息进行深度加工、价值挖掘，导致个人信息被违规利用或个人信息主体的权益遭到侵害，带来个人信息泄露的安全风险。针对这一问题，2023年7月我国国家互联网信息办公室（以下简称“国家网信办”）发布了《生成式人工智能服务管理暂行办法》，明确了数据训练的要求，强调涉及个人信息的训练数据处理活动须遵守法律和监管要求——这一定程度上推动了生成式AI技术的安全、合规应用，但对于如何防范其可能引发的数据安全风险问题，仍需产业界的持续探索。

二.数据安全风险评估工作现状

随着我国数字经济的快速发展、传统业务的数字化转型以及数据价值化加速推进，结合全球数据安全风险的整体形势，数据安全风险的识别、评估与应对已成为我国广大组织面临的最紧迫、最根本的问题，受到了国家、行业主管部门以及产业多方的高度重视。

本章节将总结国内数据安全风险评估工作落地情况，介绍数据安全风险评估的相关标准与实施方法，为相关数据处理者、服务机构初步建立数据安全风险评估实施的整体认知。

(一)风险评估已成业界焦点

国家层面，推进数据安全风险评估工作势在必行。国家法规鼓励开展数据安全风险评估，《数据安全法》提出了国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制，数据处理者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，强调了对风险信息的监测与评估是把控数据安全风险的首要途径。

多部门提出数据安全风险评估工作要求。为了规范数据处理活动，防范重大数据安全风险，中华人民共和国国务院（以下简称“国务院”）、国家网信办、工业和信息化部（以下简称“工信部”）、中国人民银行、国家医疗保障局等监管部门、行业主管部门相继发布了数据安全保护工作要求，提出数据处理者应建立健全数据安全风险评估机制，开展风险评估工作，及时消除风险隐患。包括《关键信息基础设施安全保护条例》《汽车数据安全管理若干规定（试行）》《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）》《中国人民银行业务领域数据安全管理办法（征求意见稿）》等多项文件也进一步明确了关键信息基础设施的运营者、重要数据处理者以及特定情形下的个人信息处理者等重点主体应按照有关规定，定期开展风险评估，报送评估报告的具体工作要求。

关键信息基础设施运营者每年开展风险评估。国务院令第745号《关键信息基础设施安全保护条例》要求关键信息基础设施运营者每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

重要数据处理者定期开展数据安全评估。《数据安全法》在第三十条明确了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。2022年，国家网信办发布了《网络数据安全管理条例（征求意见稿）》，要求组织的数据安全管理机构定期开展数据安全宣传教育培训、风险评估、应急演练等活动。涉及处理重要数据或者赴境外上市的，数据处理者应每年开展一次数据安全评估。

主管部门应定期组织开展本行业、本领域的数据安全风险评估，对数据处理者履行数据安全保护义务情况进行监督检查，指导督促数据处理者及时对存在的风险隐患进行整改。工信部发布的《工业和信息化领域数据安全管理办法（试行）》也提出，工信领域的重要数据和核心数据处理者应每年对其数据处理活动至少开展一次风险评估，及时整改风险问题，并向本地区行业监管部门报送风险评估报告。

个人信息处理者应结合具体情形开展安全评估或者个人信息保护影响评估。《个人信息保护法》明确了个人信息处理者在特定的情形下需要通过国家网信部门组织的安全评估或者开展个人信息保护影响评估的要求：例如，第四十条提出了关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，在确需将在中华人民共和国境内收集和产生的个人信息向境外提供的情形下，应通过国家网信部门组织的安全评估。而第五十五条则明确了在处理敏感个人信息、利用个人信息进行自动化决策等五种具体情形下，个人信息处理者应事前进行个人信息保护影响评估，并对处理情况进行记录，并进一步规定了个人信息保护影响评估的内容、报告和处理记录留存等具体要求。

如涉及向境外提供境内收集和产生的重要数据和个人信息的数据处理者开展数据出境风险自评估。此类数据处理者需要按照国家网信办《数据出境安全评估办法》，开展数据出境风险自评估开展数据出境风险自评估，并向国家网信部门申报数据出境安全评估。数据处理者需要在风险自评估环节，重点评估其出境数据的规模、范围、种类、敏感程度、数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险以及数据出境中和出境后遭到篡改、破坏、泄露等风险等方面内容。

地方层面，多地积极响应数据安全风险评估工作。北京、贵州、天津、海南、山西、吉林、安徽、山东、深圳、上海等省市地区纷纷颁布相关数据条例、管理办法等文件，积极落实国家法律法规要求，推动当地数据处理者开展风险评估工作。2019年天津市互联网信息办公室印发的《天津市数据安全管理办法（暂行）》在第七条提出数据运营者应当开展数据安全风险评估的要求，并在第十七条强调数据运营者如向境外提供个人信息和重要数据，应按照相关法律法规的规定开展安全评估。2021年11月，上海市第十五届人民代表大会通过了《上海市数据条例》。其中，第八十一条提出重要数据处理者应按照规定，定期对其数据处理活动开展风险评估，并依法向有关主管部门报送风险评估报告的要求。其他的省市地区（例如：辽宁、安徽、山东、苏州、深圳、厦门等）也均在其数据条例等文件中强调了开展数据处理活动的组织定期进行数据安全风险评估，提高风险识别与处置能力，严格落实个人信息合法使用、数据安全使用承诺和重要数据出境安全管理等相关要求。

由此可见，数据安全风险评估在国家建立健全数据安全治理体系中起到了关键作用：数据安全风险评估推动了各行业、领域的广大数据处理者合法、正当地开展数据处理活动，在提高数据处理者的数据安全保障能力，防范重大数据安全风险等方面具有重要的意义。

(二)评估标准编制进程加快

为更好地响应广大数据处理者的需求、落实数据安全风险评估的法定要求，国家、地方数据安全监管机构以及相关行业组织也相继发布了具体的数据安全风险评估实施指引、标准以及实践指南等文件，积极推动数据安全风险评估标准与指南的研究与制定工作。

国家标准编制进程持续加速。2022年3月，全国信息安全标准化技术委员会（以下简称"全国信安标委"）启动了国家标准《信息安全技术 数据安全风险评估方法》（以下简称《数据安全风险评估方法（征求意见稿）》）的编制工作，并于2023年8月面向社会公众公开征求意见。

《数据安全风险评估方法（征求意见稿）》基于国家标准GB/T 20984-2022《信息安全技术 信息安全风险评估方法》（以下简称《信息安全风险评估方法》）的框架、流程与实施方法，考虑了数据和数据处理活动的特点，借鉴了GB/T37988-2019《信息安全技术 数据安全能力成熟度模型》、GB/T35273-2020《信息安全技术 个人信息安全规范》、JR/T 0223-2021《金融数据安全 数据生命周期安全规范》等国家、行业标准，最终从管理、数据处理活动、技术等维度入手，结合核心数据、重要数据、个人信息、一般数据的安全特点与保护要求，提出了数据安全风险评估的基本概念、要素关系、分析原理、实施流程、评估内容、分析与评价方法等方面的内容。

此外，2023年5月，全国信安标委还编制、发布了《TC260-PG-20231A网络数据安全实践指南——网络数据安全风险评估实施指引》（以下简称《网络数据安全风险评估实施指引》），为广大组织与专业服务机构提供了风险评估的实施流程、实施方法、评估内容等具体指导。

多个行业的数据安全风险评估标准持续完善。数据安全风险与行业领域数据的应用场景息息相关。为了更好地指导业内的广大数据处理者有效识别、评估数据安全风险，因地制宜地加强自身的风险防范能力，一些行业主管部门也在持续推进行业数据安全风险评估方法的编制工作。

以电信网和互联网行业为例。2020年，工信部发布了YD/T 3801-2020《电信网和互联网数据安全风险评估实施方法》标准。该标准同样参考了《信息安全风险评估方法》，将数据作为核心保护对象，面向电信网和互联网的典型数据应用场景，提炼了电信网和互联网数据安全风险的基本要素及要素间的关系，提供了电信网和互联网组织实施数据安全风险评估的具体流程、操作方法与风险分析思路。此外，YD/T 3956-2021《电信网和互联网数据安全评估规范》、YD/T 4241-2023《电信网和互联网数据安全评估技术实施指南》等行业标准也提供了对电信网和互联网网络单元以及业务系统进行安全评估的方法，为业内组织开展数据安全风险评估、现有安全措施评估等工作提供了参考依据。

再例如金融行业。近年，中国人民银行陆续发布了JR/T 0223-2021《金融数据安全 数据生命周期安全规范》《金融数据安全 数据安全评估规范（征求意见稿）》等标准，充分结合金融业机构的组织特点、数据及其处理活动的特征，提供了金融业机构开展数据安全风险评估相关工作的实施流程、重点评估事项，在有效指导金融业机构及时识别数据安全风险，防范数据安全事件的同时，也推动金融业机构充分落实金融业数据安全管理要求，提升数据安全保护工作水平，为各机构实施数据安全风险评估相关的工作提供了重要的参考。上述风险评估标准的发展与演进见表1。

表1 数据安全风险评估标准发展、演进一览

标准名称	发布时间	标准价值
GB/T 20984-2022《信息安全技术 信息安全风险评估方法》	2007年 首次发布 2022年 更新、实施	**• 明确了风险评估实施方法** 说明：提出了信息安全风险评估的基本概念、风险要素关系、风险分析原理、风险评估实施流程和方法，以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式。 **• 构建了风险评估整体框架** 说明：从风险要素关系、风险分析原理、风险评估流程三方面构建了风险评估框架。 **• 制定了风险评估实施流程** 说明：实施流程包括评估准备、风险识别、风险分析、风险评价四个阶段。沟通与协商、文档记录作为必要的手段，贯穿整个评估实施流程。
YD/T 3801-2020《电信网和互联网 数据安全风险评估实施方法》	2020年 发布	**• 明确了电信网和互联网数据安全风险评估实施要点** 说明：基于《信息安全风险评估方法》，总结了电信网和互联网的数据威胁、脆弱性、已有安全措施等要素识别内容、风险要素关系。 **• 提出了对电信网和互联网数据应用场景的识别要求** 说明：提出风险评估依赖数据所涉及的各应用场景，认为针对已识别的待评估数据资产，需要对数据应用场景中的业务流程或使用流程、数据活动、参与主体进行识别，进而识别、分析场景内的数据威胁、脆弱性等风险要素。 **• 细化了电信网和互联网数据安全风险评估实施流程** 说明：将风险评估实施作为一个单独阶段，与风险处置、残余风险评估共同构成整个实施流程三个阶段，在评估实施阶段明确了评估准备、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、已有安全措施识别、风险分析与评价等多个环节的工作内容，制定了电信网和互联网数据安全风险评估实施的整体流程。

标准名称	发布时间	标准价值
DB3212/T1117-2022《政务数据安全风险评估规范》	2022年 发布	• 明确了政务数据安全风险评估实施要点 说明：基于《信息安全风险评估方法》《电信网和互联网数据安全风险评估实施方法》，参考GB/T37973-2019《信息安全技术 大数据安全管理指南》等标准，结合政务数据分级要求，分析政务数据在全生命周期内面临的安全威胁、安全脆弱性、安全措施等要素识别内容、风险要素关系。 • 提出了政务系统资产的识别要求 说明：基于《信息安全风险评估方法》的风险要素与评估实施流程，提出了在评估实施阶段根据政务数据安全管理的目标与原则，进行政务数据分类与分级，并将系统资产价值与安全威胁、安全脆弱性等其他风险要素一并进行识别、赋值。 • 细化了政务数据安全风险评估实施流程 说明：基于评估准备、评估实施、风险分析与评价、编制报告四个阶段，分别明确了评估准备、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、已有安全措施识别、风险分析与评价等多个环节的工作内容，制定了政务数据安全风险评估实施的整体流程。
TC260-PG-20231A《网络安全标准实践指南——网络数据安全风险评估实施指引》	2023年 发布	**• 扩展了风险评估的目标** 说明：结合当前国家法律法规的最新要求，在《信息安全风险评估方法》对组织的业务以及系统、平台等资产的安全风险进行评估、分析这一目标的基础上，提出数据安全风险评估的目标还包括落实法律法规义务，保护关键信息基础设施或个人信息主体权益等方面的内容。 **• 提供了更加清晰的检查项作为风险评估实施要点** 说明：提供了数据安全管理、数据处理活动、数据安全技术、个人信息保护相关的检查项，与《信息安全风险评估方法》《电信网和互联网数据安全风险评估实施方法》以及GB/T39335-2020《信息安全技术个人信息安全影响评估指南》等侧重于方法论构建的评估标准文件形成互补、衔接。 **• 提供了自评估与检查评估两套实施流程** 说明：明确了在自评估与检查评估两种情况下的评估目标确立、评估方案策划、风险分析评价等具体环节的实施差异。

标准名称	发布时间	标准价值
YD/T 3801-2020《电信网和互联网 数据安全风险评估实施方法》	2023年 公开征求意见	• **进一步扩展了风险要素的范围**：结合数据以及数据处理活动的特点，提出了数据安全风险评估涉及的风险要素包括数据处理者、业务、信息系统、数据、数据处理活动、风险源、安全措施。 • **提出了"风险源"的概念**：结合数据以及数据处理活动的特点，提出了风险源（又称"风险隐患"）可能引发数据安全风险。此外，结合《网络数据安全风险评估实施指引》提出的"合规+安全"的风险评估目标，进一步指出风险隐患既包括安全威胁利用脆弱性可能导致数据安全事件的风险隐患，也包括数据处理活动不合理操作可能造成违法违规处理事件的风险隐患。 • **突出了信息调研的重要性**：与《网络数据安全风险评估实施指引》保持了一致，将信息调研作为一个单独的阶段，旨在全面识别风险要素，为后续风险源识别、风险问题分析等工作提供输入。

来源：数据安全推进计划

(三)评估实施方法逐渐成熟

业内相继发布了多项信息安全风险、数据安全风险的评估标准，这些标准相互补充、持续完善，已成为广大数据处理者开展风险评估的重要参考资料。

评估思路方面，各标准均强调了全面识别风险基本要素的重要性。大量的数据流转使数据与其访问主体、传输链路、承载环境、安全策略等因素共同构成了"牵一发而动全身"的数据安全风险。

这一点在国际、国内的多项标准中均有体现：美国国家标准技术研究院（NIST）《隐私工程和风险管理》（NIST 8062）曾提出"问题操作"这一概念，并指出被识别的问题操作可用于评估风险发生的可能性、风险产生的影响。国内的《信息安全风险评估方法》则提出信息安全风险评估需要识别包括资产、威胁、脆弱性、安全措施在内的"基本要素"，通过建立、分析基本要素之间的关系（即：资产存在脆弱性，威胁通过利用脆弱性导致风险，而安全措施的实施是通过降低脆弱性被利用难易程度，以防范威胁、保护资产）进行风险分析。2020年的《电信网和互联网数据安全风险评估实施方法》结合电信网和互联网行业数据以及数据处理活动的特征，进一步提出了该行业的数据安全风险评估需要识别包括数据资产、应用场景、数据威胁、数据脆弱性、安全措施在内的基本要素及其属性，同样通过建立基本要素之间的关系，分析各应用场景下的数据安全事件发生的可能性与影响，最终得出数据资产在多个应用场景下面临的总体风险值。

相较于《信息安全风险评估方法》《电信网和互联网数据安全风险评估实施方法》，2023年《网络数据安全风险评估实施指引》和《数据安全风险评估方法（征求意见稿）》则基于前述的基本要素，提出了数据安全风险的"风险源"这一概念（即：风险源是可能导