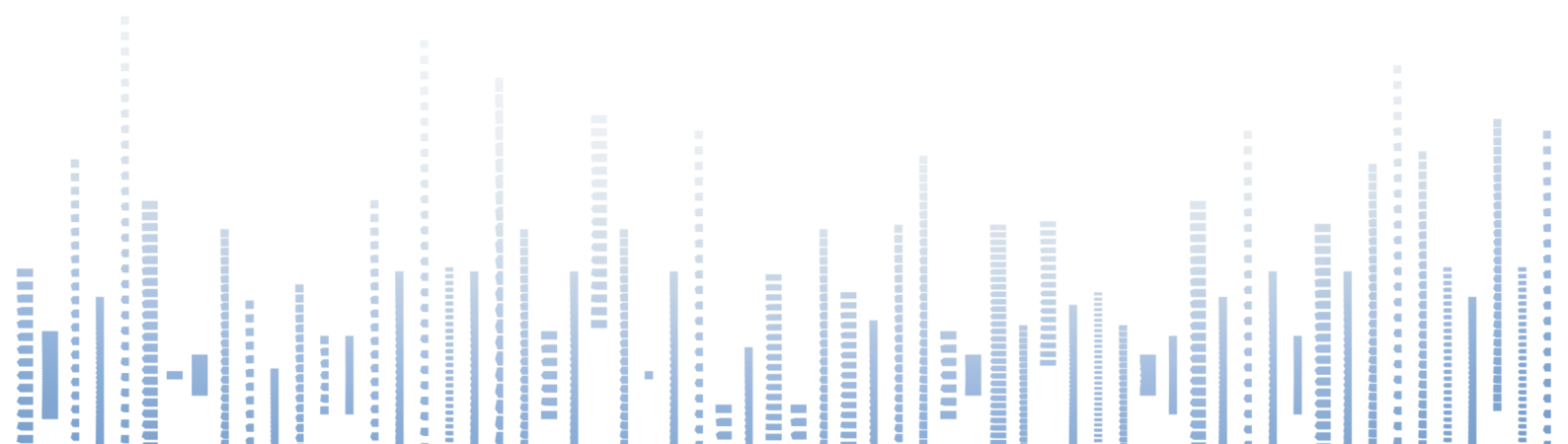
数据安全推进计划
DATA SECURITY INITIATIVE

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

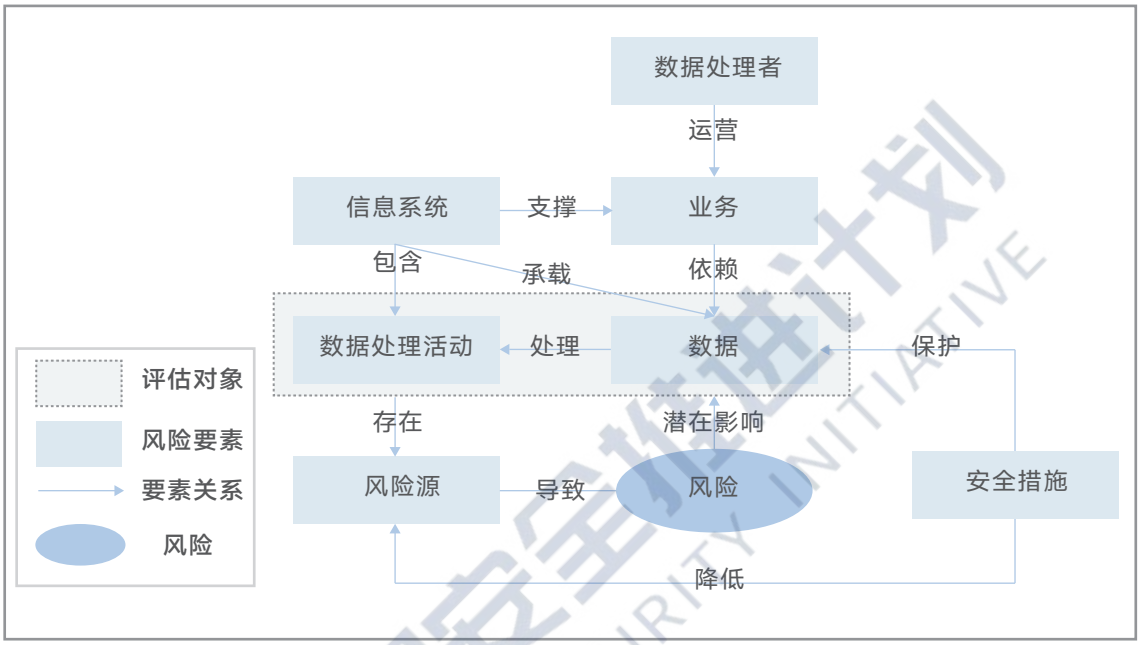
业内相继发布了多项信息安全风险、数据安全风险的评估标准，这些标准相互补充、持续完善，已成为广大数据处理者开展风险评估的重要参考资料。

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

致危害数据的保密性、完整性、可用性和数据处理合理性等事件的威胁、脆弱性、问题、隐患等，也称“风险隐患”），并同样指出了数据安全风险评估需要通过信息调研，识别数据处理者、业务和信息系统、数据资产、数据处理活动、安全措施等相关基本要素，从数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面识别风险隐患，最终形成风险源清单，分析、评价数据安全风险并给出整改建议。



来源：国家标准《数据安全风险评估方法（征求意见稿）》，数据安全推进计划整理

图1 数据安全风险基本要素关系

评估流程方面，“准备-实施-总结”已成为共识。数据安全风险评估工作主要围绕数据处理者的数据和数据处理活动，对可能影响数据保密性、完整性、可用性和数据处理合理性的安全风险进行分析和评价。通过对比、总结国内《数据安全风险评估方法（征求意见稿）》《网络数据安全风险评估实施指引》《电信网和互联网数据安全风险评估实施方法》等风险评估标准，可以发现，风险评估工作目前已形成一套覆盖“准备-实施-总结”三大阶段的流程，具体分为评估准备、信息调研、风险识别、综合分析、评估总结五个环节。各环节的工作任务以及产出物也基本明确，具体流程与产出物见表2。

表2 数据安全风险评估实施流程与产出物

环节	工作任务	产出物
评估准备	• 确定评估目标 • 确定评估范围 • 组建评估团队 • 制定工作计划 • 确定评估依据与内容 • 制定评估方案	• 评估调研表 • 评估方案 • 数据处理者基本情况 • 业务清单 • 信息系统清单 • 数据资产清单 • 数据处理活动清单
信息调研	• 数据处理者调研 • 业务和信息系统调研 • 数据资产调研 • 数据处理活动调研 • 安全措施调研	• 数据流图 • 安全措施情况
风险识别	• 数据安全管理风险识别 • 数据处理活动风险识别 • 数据安全技术风险识别 • 个人信息处理风险识别	• 人员访谈记录文档 • 文档查验记录文档 • 安全核查记录文档 • 技术测试报告
综合分析	• 梳理问题清单 • 风险分析与评价 • 提出整改建议	• 数据安全风险源清单 • 数据安全风险清单 • 数据安全风险整改建议
评估总结	• 报告风险评估结果 • 处置数据安全风险	• 数据安全风险评估报告

来源：国家标准《数据安全风险评估方法（征求意见稿）》，数据安全推进计划整理

三.实务问题剖析与解决思路

尽管大量法律法规、部门规章以及标准提供了丰富的理论指引，组织在数据安全风险评估工作实务中仍然面临重重阻碍。这些阻碍分布在整个评估过程的各个阶段，成因错综复杂。因此，本章节将通过系统梳理数据安全风险评估的各阶段面临的典型问题，深入分析问题成因，充分参考业内优质经验，形成问题解决思路，为相关数据处理者、服务机构纾难解惑。

(一)评估准备

1.如何确定评估触发条件

《网络安全法》提出网络运营者应开展网络安全认证、检测、风险评估等活动，并通过网络安全等级保护、信息安全风险评估等一系列标准对组织的网络、信息安全风险评估工作进行落地指导。相较于网络、信息安全风险评估，数据安全风险评估的工作要求、标准依据或正在征求意见，或尚未正式发布——这导致许多数据处理者的数据安全风险评估工作仍处于起步阶段，面临着评估触发条件不明确的“0号困境”。

部分组织将同地区、同行业的组织遭遇数据安全事件或受到监管部门处罚作为自身开展风险评估的触发条件：通过将这些公开的事件或处罚信息内化形成风险信息检查表单，对业务部门逐个开展数据安全风险排查专项工作。然而，此类专项排查工作投入高、收效低：不同的组织对数据安全风险的承受能力与管理需求存在较大的差异，公开的信息披露有限且存在一定的滞后性，导致组织难以有规划地开展数据安全风险评估工作，评估内容参考性较低，对组织的风险启示性不足。

解决思路：梳理适用情形

针对这一问题，组织或评估机构可以参考国家标准《数据安全风险评估方法（征求意见稿）》的“5.4 评估适用情形”。评估适用情形列出了数据处理者开展数据安全风险评估的一些具体适用情形，具体见表3。

表3 数据安全风险评估适用情形

适用情形	适用情形来源
a） 重要数据处理者、关键信息基础设施运营者、处理100万人以上个人信息的个人信息处理者、大型互联网平台运营者、赴境外上市的数据处理者、党政机关、网络安全等级保护三级及以上运营者，应**每年开展一次**数据安全风险评估。	国家法规

适用情形	适用情形来源
b）数据处理者在重要数据共享、交易、委托处理或向境外提供前，应开展数据安全风险评估。	国家法规
c）数据处理者开展高风险数据处理活动前，宜开展数据安全风险评估，高风险数据处理活动包括但不限于： （1）重要数据和个人信息处理者合并、分立、解散、被宣告破产进行数据转移。 （2）承载重要数据处理活动的信息系统发生架构调整、下线等重大变更。 （3）数据处理者利用生物特征进行个人身份认证。 （4）基于不同业务目的的数据汇聚融合。 （5）委托处理、向他人提供未成年人、老年人数据。 （6）新技术应用可能带来数据安全风险的。 （7）法律法规或有关部门规定要评估的情形。 （8）其他可能直接危害国家安全、公共利益或者大量个人、组织合法权益的数据处理活动。	标准方建议
d）重要系统上线前，可根据实际需要开展数据安全风险评估。	标准方建议
e）对于已经评估过数据安全风险评估的数据处理活动，当数据范围、数据处理活动、环境、相关方等发生重大变更时，需重新开展数据安全风险评估。	标准方建议
f）当被评估对象的政策环境、外部威胁环境、业务目标、安全目标等发生重大变化时，应重新开展风险评估。	标准方建议

来源：国家标准《数据安全风险评估方法（征求意见稿）》，数据安全推进计划整理

这些情形**一是**引述了国家法律法规中有关开展风险评估的要求与场景（例如：数据处理者在重要数据共享、交易、委托处理之前），在明确数据安全风险评估活动开展的必要性的同时，也提供了评估活动开展的法规依据；**二是**总结了组织常见的高风险数据处理活动（例如：基于不同业务目的的数据汇聚融合），为组织或评估机构提供了更为明确、直接的工作指引与建议；**三是**回应了如何持续开展评估的关切，已开展过风险评估的数据和数据处理活动一旦发生重大变更或变化，组织或评估机构应重新实施风险评估，将风险评估融入组织的数据安全运营机制。

实务操作上，组织或评估机构可通过持续梳理数据安全风险评估的适用情形，从评估要求的来源、内容等角度入手，分析、判断自身适宜开展评估活动的触发条件、实施时机以及具体评估项的必要性，推动数据安全风险评估工作的常态化开展。示例见表4。

表4 评估适用情形检查表（示例）

适用情形来源		适用情形内容	触发评估条件		评估时机	是否必要
国家法律法规	数据安全法	第三十条 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。	特定对象	重要数据	定期开展	必要项

适用情形来源		适用情形内容	触发评估条件		评估时机	是否必要
国家法律法规	网络数据安全管理条例（征求意见稿）	第二十五条 数据处理者利用生物特征进行个人身份认证的，应当对必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的个人身份认证方式，以强制个人同意收集其个人生物特征信息。	特定对象	高风险数据处理活动	特定场景	必要项
行业主管部门要求	工业和信息化领域数据全风险评估实施细则（试行）（征求意见稿）	第六条［评估期限］重要数据和核心数据处理者每年完成至少一次数据安全风险评估，并形成评估报告。数据安全风险评估结果有效期为一年，自评估报告首次出具之日起计算。	特定对象	重要数据和核心数据	定期开展（1年）	必要项
国家标准	数据安全风险评估方法（征求意见稿）	5.4评估适用情形 c）数据处理者开展高风险数据处理活动前，宜开展数据安全风险评估，高风险数据处理活动包括但不限于：重要数据和个人信息处理者合并、分立、解散、被宣告破产进行数据转移。	特定对象	高风险数据处理活动	特定场景	建议项
国家标准	数据安全风险评估方法（征求意见稿）	5.4评估适用情形 e）对于已经评估过数据安全风险评估的数据处理活动，当数据范围、数据处理活动、环境、相关方等发生重大变更时，需重新开展数据安全风险评估。	重大变化	/	特定场景	建议项

来源：数据安全推进计划

2.如何制定评估工作目标

数据处理者开展数据安全风险评估工作的主要目标可以被分为三层：**一是落实监管要求**，满足国家法律法规关于开展风险评估的要求；**二是摸底数据现状**，摸清自身数据和数据处理活动基本情况；**三是提升安全能力**，检查重要的数据处理活动中是否存在管理、技术风险隐患，推动完善数据安全保护措施。三层目标共同促进数据处理者履行法定义务、建立健全数据安全制度、排查解决漏洞隐患，使数据处于有效保护和合法利用、持续安全的状态。

然而，大量组织未能正确、全面地认识数据安全风险评估的价值与目标：多数组织将第一层目标作为开展风险评估或其他风险治理工作的唯一目标——这导致一旦缺少了国家法规或监管部门的强制性要求，这些组织开展数据安全风险评估工作的意愿与动力也会随之丧失。

此外，由于大量组织前期未能全面掌握业务、数据和数据处理活动的特点以及潜在的漏洞隐患，其制定的数据安全风险管理策略无法反映组织的风险管理需求与准则，这也导致组织即使开展了数据安全风险评估工作，也无法基于评估结果准确地衡量风险问题整改措施的投入产出比、实施优先级，甚至产生内部多方对风险评估结果难以达成共识、风险问题整改推进困难等问题，长远来看，不利于组织数据安全风险的防范与治理。

解决思路：建立风险准则

针对这一问题，组织可以参考数据安全推进计划发布的《数据安全治理实践指南3.0》（以下简称《实践指南3.0》），开展数据安全风险评估及治理专项，通过系统化的数据安全风险治理，建立组织的数据安全风险准则。

数据安全风险治理是以风险为中心的方法论，提炼了组织管理数据安全风险时需要重点关注的五大环节，即：风险准则建立、风险要素识别、风险评估分析、风险处置解决、风险治理改进。其中，风险准则建立是指通过分析组织数据安全风险需求，识别组织的关键业务、数据和数据处理活动，形成风险治理准则，帮助组织将注意力与资源集中在那些超出自身承受能力的数据安全风险，在明确了风险治理重点对象的同时，也为风险评估、整改等具体活动提供了判断与执行标准。

实务操作上，组织一是通过分析风险需求，具体任务包括收集、整理自身适用的数据安全、隐私保护法律法规，识别组织的关键业务、数据和数据处理活动，明确数据安全风险治理的范围与重点对象；二是创建数据安全风险治理愿景、使命，这一步需要与组织高层人员进行沟通、协商，在获得其批准与支持之后，形成基本的风险准则，明确组织的风险管理偏好；三是制定数据安全风险治理政策，这一步需要与内部相关方（例如：人力资源、法务、安全、营销、IT团队）进行商议，在充分了解相关方的业务与合规需求之后，制定风险管理政策，为后续风险评估以及其他风险治理相关的工作提供实施方针、标准。

此外，针对组织或内部相关方无法正确理解风险评估的价值与目标这一问题，组织还可以通过工作动员会、研讨会、培训讲座等方式，宣贯组织的风险治理政策，解读评估标准，讨论评估方案，加强业务部门对数据安全风险评估及其目标、价值的认知与理解，提升内部相关方对风险评估工作的参与程度，持续强化各方在数据安全风险评估以及治理工作的协同能力。

3.如何规划评估实施范围

组织数据安全风险的边界持续扩展：传统的安全防护通常采用边界防护策略保障静态数据的安全。然而，**一方面**，组织的业务活动必然伴随着数据的流动，而数据广泛存在于数据中心、云端、终端等位置，数据资源暴露面的扩大意味着其面临的威胁也成倍增加；另一方面，组织数据在多个业务、数据处理活动中与大量设备、人员产生交互，异

常的行为隐匿于海量的数据访问行为中，不仅变得更加隐蔽、难以识别，也无形中扩大了数据安全风险可波及的范围。

因此，组织如何在日益复杂的业务及数据处理活动中，规划数据安全风险评估的范围，在既定的评估时间、范围内识别出组织最为关注的数据安全风险，是广大数据处理者、评估机构在筹备评估工作过程中需要重点思考的问题。

解决思路：识别重点对象

为了避免风险边界过大导致的评估“失焦”问题，提高数据安全风险评估的投入产出比，组织可以参考《网络数据安全风险评估实施指引》，在规划评估范围时，首先明确评估工作中的重点评估对象。

实务操作上，组织可以参考数据分类分级的成果，将个人信息、重要数据、核心数据以及这些数据的处理活动作为重点评估对象，并抽样选取一般数据及其数据处理活动，一并纳入本次风险评估的范围，在确保识别出重点评估对象面临的风险的同时，也保障了评估的全面性，具体示例见表5。由于一般数据涵盖范围较广，数据处理者可结合组织自身安全需求，对一般数据进行细化分级，本报告将一般数据从低到高分为1级、2级、3级。

表5 重点评估对象（示例）

<table>
<tr><th colspan="2">数据级别</th><th colspan="2">数据描述</th><th>是否风险评估对象</th></tr>
<tr><td colspan="2">核心数据（L5）</td><td colspan="2">关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据</td><td>是</td></tr>
<tr><td colspan="2">重要数据（L4）</td><td colspan="2">一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据</td><td>是</td></tr>
<tr><td rowspan="3">一般数据</td><td>L3</td><td rowspan="3">一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人、组织合法权益造成危害，但不会危害国家安全、公共利益的数据</td><td>如：财务信息等内部机密信息、敏感个人信息</td><td>待定</td></tr>
<tr><td>L2</td><td>如：一般个人信息</td><td>待定</td></tr>
<tr><td>L1</td><td>如：组织已公开数据</td><td>否</td></tr>
</table>

来源：数据安全推进计划

如果组织尚未开展数据分类分级工作，则可以参考信息系统等级保护的相关要求，根据业务、信息系统的重要程度，选取核心业务系统或内部的重要信息系统（例如：大数据平台、人力资源系统、供应链系统）的数据和数据处理活动作为重点评估对象，重点评估其承载的数据和数据处理活动面临的风险。这一解决思路目前已应用于许多组织的数据安全风险评估

实践：组织选取某一重要的信息系统作为评估实施的“原点”，将其数据的来源、去向系统作为评估的范围边界，梳理该系统涉及的数据、数据处理活动并绘制数据流向图，识别数据流转过程中的操作人员、操作行为以及操作结果等信息，从而分析潜在的数据安全风险问题。

(二)评估实施

1.如何获取有效评估信息

信息调研是数据安全风险评估工作中最为重要的环节，组织的评估执行人员通过文档审阅、配置核查、人员访谈等不同的方式，收集组织的数据和数据处理活动、数据安全管理、技术等方面的信息。

数据安全风险评估涉及到组织的业务及其数据应用场景，需要评估执行人员实地调研业务和数据情况，多轮访谈组织业务人员，掌握数据处理活动的背景——这意味着评估执行人员不仅需要熟练掌握数据安全风险评估要点，还要通过专业的协作迅速了解组织的业务、数据和数据处理活动的关键信息，从而更好地识别出潜在的威胁、脆弱性以及已有安全措施的不完善之处。然而，许多组织在开展数据安全风险评估的过程中发现，由于组织前期开展的网络、信息安全评估通常由安全部门发起、主导，执行人员同样来自安全部门，主要负责网络结构、信息资产、威胁检测工具安全情况的调研、核查，对业务、数据处理活动的了解不够深入。

因此，人员执行数据安全风险评估的信息调研时，产生了新的问题：**一方面**，评估执行人员对业务、数据情况理解欠佳，对于业务、数据及其处理活动的风险识别不全面，且不同人员可能对于同一风险问题的判断存在较大的差异；**另一方面**，受访人员未能充分理解风险评估的依据与要点，在访谈或调研过程中反馈大量的无关信息，直接导致了返工或者评估进度延期等问题。

解决思路：完善协作机制

针对这一问题，组织可以通过完善组织协作机制，从团队、工具、协商三方面入手，规避上述在信息调研过程中的问题。

实务操作上，针对评估执行人员可能存在的业务掌握度低、自由裁量等问题，**一方面**，组织可以在组建评估团队时，选取业务人员加入评估执行团队，由业务人员负责整理本次风险评估涉及的业务和信息系统、数据信息，并适时向团队其他成员介绍这一部分信息，在执行团队内部实现优势互补；**另一方面**，完善评估信息调研表等工具，在逐步固化、标准化数据安全风险评估依据中的评估项、查验方式以及访谈问题等内容的同时，完善对于不同角色的受访人员或者证明材料的信息判断标准，确保评估执行人员之间具备相对统一的评估尺度。**同时**，针对受访人员可能无效响应的问题，组织可以在实施访谈工作前，邀请计划受访的人员参与本次风险评估的研讨会，由评估执行人员对风险评估方案、依据以及要点进行解读，双方对评估内容进行充分协商，输出、分发评估研讨会问答合集，以免在风险评估的实施过程中出现人员理解偏差的问题。

2.如何应用风险评估工具

组织调研当前的数据资产情况、发现潜在威胁与脆弱性、检查安全防护措施状态都离不开评估工具。数据安全风险评估中，评估工具能够提供更为客观的信息，在降低人力成本的同时，也极大地提高了评估结果的可信度。

整个评估实施的过程中，评估执行人员需要调研覆盖组织数据安全管理、技术以及大量数据处理活动的各类信息，故需要通过应用组织内部已部署的安全产品或者使用其他技术检测工具，收集、整合以上多方甚至多维度的信息，从而回答风险评估工作的核心问题，即：组织的何种数据、分布何处、如何流转、谁在使用、如何防护。

然而，大量组织反馈，当前数据安全产品种类多且功能各异，在缺乏工具应用指导的背景下，组织开展数据安全风险评估时倾向于沿用传统的信息安全风险评估工具，因此仅能识别网络、信息安全方面的风险问题，很难识别出隐藏在具体业务场景和数据处理活动中的安全风险问题，严重影响了数据安全风险问题检出的全面性。因此，在当前数据安全产品工具发展迅速、种类多样，而风险评估实施的必备工具尚未明确的背景下，如何选取合适的评估检测工具同样是组织实施数据安全风险评估面临的重要问题。

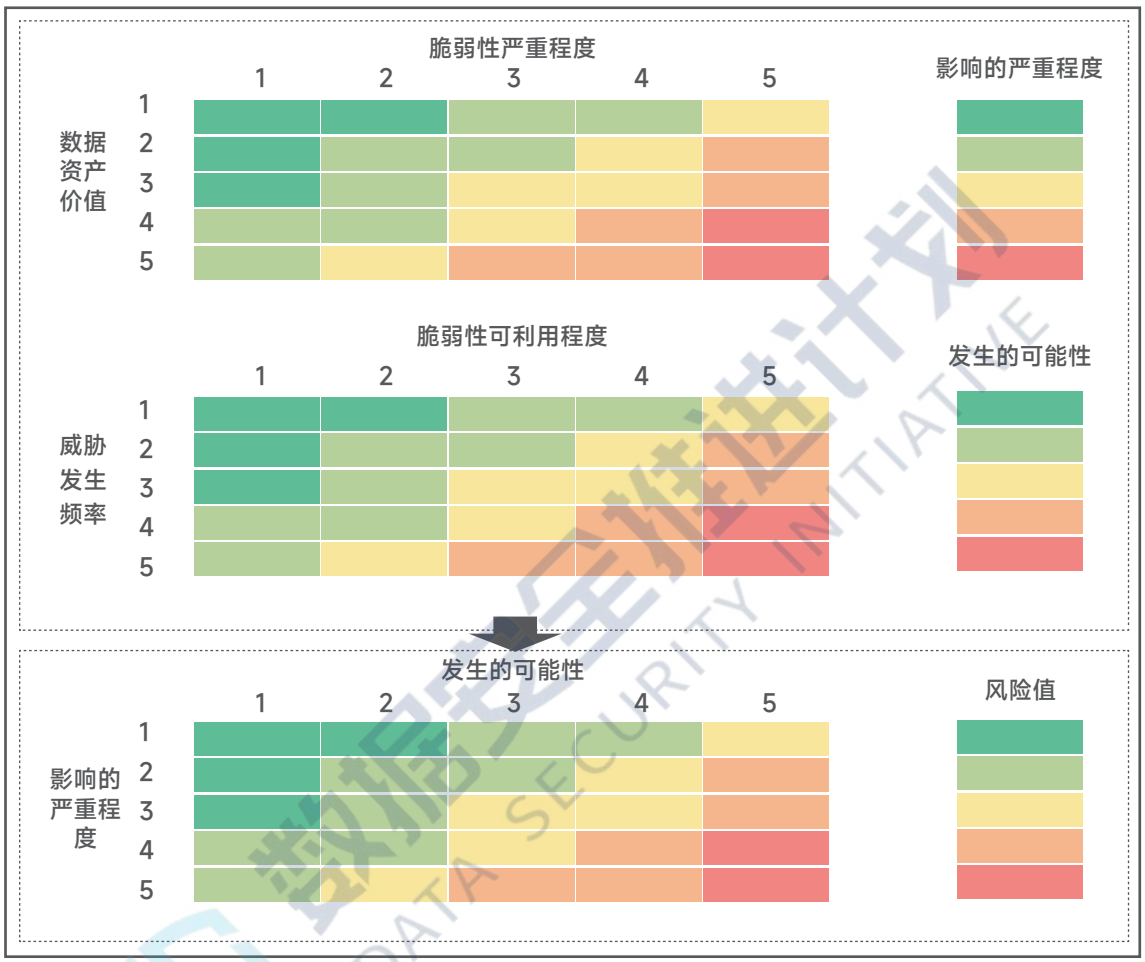
解决思路：认识工具功能

针对这一问题，组织可以结合前期规划的评估范围、重点评估对象等信息和风险评估实施各个环节的目标，明确工具在各个阶段内应发挥的功能，从而选取适宜的数据安全产品工具。

实务操作上，组织首先可以参考数据安全推进计划2023年发布的《数据安全产品与服务观察报告》以及其他业内研究报告，初步掌握主流的数据安全产品工具及其功能。在数据安全风险评估的实践中，可应用的评估工具主要分为三类：**一是扫描类工具**，主要负责提供针对数据、风险源（例如：脆弱性）等风险要素的扫描服务，为数据安全风险评估提供要素识别的功能，具体包括资产扫描类、数据识别类、漏洞检测类工具等。目前市面上许多数据分类分级、数据资产管理以及部分数据安全防护类工具（例如：API数据防泄露）都具备这一部分的功能；**二是流量分析类工具**，主要负责提供对数据处理活动的识别与监测能力，用于关联应用、数据库、人员的敏感数据操作，分析潜在的风险行为，具体包括应用层流量分析、全流量分析等数据风险监测类工具；**三是自动化评估类工具**，主要负责自动化评估流程管理、评估对象的信息填报、证明文件的上传和查阅、评估结果的生成及报告的输出等，具体包括合规检测工具、在线评估系统等。随着产品工具的平台化、一体化趋势日益明显，上述的三类工具在数据安全风险评估中提供的能力也已在一些平台型产品中得以集合。

3.如何开展风险评估分析

风险分析是组织基于前期的信息调研、风险识别的情况，对风险的影响程度、发生的可能性进行赋值、分析，最终通过风险矩阵输出风险值的过程。风险矩阵如图2所示。



来源：数据安全推进计划

图2 风险矩阵（示例）

风险分析的方法主要为定性分析、定量分析、综合分析（定性与定量相结合）。定性分析不要求各个风险要素被严格地量化，在风险要素的评价上主要依靠评估执行人员的个人经验、专业知识等，因此对于评估执行人员的专业能力要求较高。定量分析（包括半定量分析）则是对风险要素进行赋值，依据数值建立数学模型，量化风险分析的过程与结果，确保输出清晰的风险分析结论，但其存在将复杂问题过度简化或模糊化的缺陷，同样易造成风险分析结论的偏差。

目前业内的数据安全风险分析方法以定性分析为主，例如《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）》提出，针对风险发生的影响程度可以结合数据价值、安全问题严重程度等因素进行分析，从不同的影响对象、危害程度高低分别提供了定性的描述，以便评估执行人员参考、对照分析，具体见表6。然而，在实务操作上依然存在分析过程严重依赖执行人员经验、分析结论主观性过高等问题。

表6 数据安全风险危害程度（节选）

影响对象	危害程度	参考说明
国家安全	很高	直接危害国家安全重点领域，如政治安全。
经济运行	高	1.直接影响宏观经济运行状况和发展趋势，如社会总供给和总需求、国民经济总值和增长速度、国民经济主要比例关系、物价总水平、劳动就业总水平与失业率、货币发行总规模与增长速度、进出口贸易总规模与变动等。 2.直接影响一个或多个地级市、行业内多个企业或大规模用户，对行业发展态势、技术进步和产业生态等造成严重影响，或者直接影响行业领域核心竞争力、核心业务运行、关键产业链、核心供应链等。
公共利益	高	1.直接危害公共健康和安全，如严重影响疫情防控、传染病的预防监控和治疗等。 2.可能导致重大突发公共卫生事件（II级），造成社会公众健康严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒等严重影响公众健康的事件。 3.导致一个或多个地市大部分地区的社会公共资源供应较长期中断，较大范围社会成员（如100万人以上）无法使用公共设施、获取公开数据资源、接受公共服务。
组织权益	中	可能导致组织遭到监管部门严重处罚（包括取消经营资格、长期暂停相关业务等），或者影响重要/关键业务无法正常开展的情况，造成重大经济或技术损失，严重破坏机构声誉，企业面临破产。
个人权益	中	个人信息主体可能会遭受重大的、不可消除的、可能无法克服的影响，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害。如遭受无法承担的债务、失去工作能力、导致长期的心理或生理疾病、导致死亡等。

来源：国家标准《数据安全风险评估方法（征求意见稿）》，数据安全推进计划整理

解决思路：建立分析模型

针对这一问题，组织可以建立数据安全风险分析模型，通过明确判断尺度、丰富评价维度、提升赋值精度三方面的措施，提高分析过程和结果的客观性。

一是制定风险分析过程的判断尺度。组织采用定性分析方法进行风险分析时，人员的主观判断将直接影响风险分析的结论。因此，明确评估执行人员的判断尺度，提供判断某项风险是否属于重大风险的“红线”、“基线”——这在一定程度上能够防止风险分析结论与实际情况偏差过大。以汽车行业的实践为例，汽车自身及其业务属性决定了其在风险分析的过程中聚焦可能直接影响行车安全、财产安全等方面的风险要素，因此在开展数据安全风险评估的过程中，组织将“是否为极端威胁行车、财产安全等方面的风险”与“是否为大多数人群所适用的风险”作为人员分析风险时的重要尺度。

二是完善风险分析过程的评价维度。组织开展风险分析时，通常使用风险矩阵图对风险发生的可能性和影响程度进行评价。然而，风险本身具有不确定性，组织评价风险发生的可能性时缺乏成熟的参考依据，赋值易流于形式，对风险分析结论缺乏参考价值。因此，组织可以丰富风险评价的维度，提升风险分析结论的实用性。例如，目前组织面临的数据安全风险不仅包括了数据保密性、完整性、可用性遭到危害，还包括了数

据被违法、违规处理带来的合规风险，基于这一问题，组织可以在风险矩阵中补充“可罚性”这一维度，即：从组织的合规管理角度出发，评价组织数据一旦被泄露、破坏、滥用可能引发的监管处罚、违约追责等问题的严重程度。

三是提升风险分析过程的赋值精度。组织采用定量分析方法开展风险分析时，最大的难点问题在于风险发生的可能性和危害程度的定级、赋值和计算。针对风险发生的危害程度，组织可以从数据的重要程度、数据资产价值、脆弱性严重程度等具体风险要素进行相对精准的赋值：《江苏省数据安全风险评估规范》从数据遭到泄露或损害时，可能对国家安全、经济运行、社会稳定、公共利益、个人权益造成的影响程度入手，提出了组织可以参考的一般、重要与核心数据赋值。具体赋值方法如表7。未来，组织在风险分析的过程中，也可以参考数据的流通价值，进一步提升数据这一风险要素的赋值精度。

表7 数据级别赋值（示例）

数据级别		数据级别赋值	数据重要程度定义
数据等级	定性描述		
核心数据	很高	5	该级别数据的安全属性被破坏后: 1.会对国家安全造成特别严重危害或严重危害; 2.或对经济运行、社会稳定或公共利益造成特别严重危害。
重要数据	高	4	该级别数据的安全属性被破坏后: 1.会对国家安全造成一般危害; 2.或对经济运行造成严重危害或一般危害; 3.或对社会稳定、公共利益造成严重危害。
一般数据	中	3	该级别数据的安全属性被破坏后: 1.会对社会稳定、公共利益造成一般危害: 2.或对组织权益、个人权益造成特别严重危害。
	低	2	该级别数据的安全属性被破坏后，会对组织权益个人权益造成严重危害。
	很低	1	该级别数据的安全属性被破坏后，会对组织权益个人权益造成一般危害。

来源：国家标准《数据安全风险评估方法（征求意见稿）》，数据安全推进计划整理

针对风险发生的可能性，实务操作上存在一定的困难：风险源（例如：威胁和脆弱性）的发生频率、安全措施有效性和完备性等因素难以预测、量化。组织可以“以系统为单位”，默认同一信息系统、数据库中的威胁与脆弱性赋值保持一致，避免风险分析过程引入错误的关联关系，提升定量分析的可落地性、可操作性。如果组织在近期开展过网络安全等级保护测评等评估评测，也可以参考其脆弱性识别结果进行赋值。

此外，针对数据安全风险危害程度与发生的可能性的量化分析与评价，《数据安全风险评估方法（征求意见稿）》在附录B中按照统计学中的均匀分布，给出了“很高”、“高”、“中”、“低”、“很低”级别可参考的得分取值范围，这也一定程度上为风险值的计算提供了参考，具体见表8。

表8 数据安全风险危害程度等级参考（节选）

等 级	得 分
很高	[80%,100%]
高	[60%,80%)
中	[40%,60%)
低	[20%,40%)
很低	[0%,20%)

来源：《数据安全风险评估方法（征求意见稿）》，数据安全推进计划整理

(三)评估总结

1.如何充分应用评估结果

数据安全风险评估的结果能够直接影响组织的风险处置策略、措施，产生大量的人力、物力成本。因此，评估执行人员提供的分析结论可能会受到组织内部相关方的质疑与挑战，这也要求风险评估的结果具备较高的可信度与说服力。然而，风险本身具有不确定性、随机性，评估执行人员难以在当下的评估时点对未来是否会发生该风险进行证明，而相关方可能对风险的真实性、紧迫性缺乏认知，这也使许多组织在完成风险评估工作后陷入了新的困境与僵局。

解决思路：发布安全声明

针对这一问题，组织可以借鉴网络安全风险评估实践，通过将数据安全风险清单与安全声明相结合的方式，向相关方解释评估方给出的评估结论和建议相关方采取某项处置措施的原因，分析处置措施执行后可预期达到的效果——这能够有效提升数据安全风险评估结论的可信度，为相关方判断是否采纳评估结论和处置建议提供了参考，明确评估执行方与风险处置方的责任，最终推动风险评估结果在组织内部的充分应用。安全声明模板见表9。

表9 安全声明（模板）

风险名称	风险等级	风险描述	风险处置建议	处置原因	安全声明
说明：评估方填写	说明：评估方填写	说明：评估方填写	说明：评估方填写	说明：评估方填写	说明：相关方填写
示例：数据泄露风险	示例：高	示例：未建立监控与审计机制，应用系统管理部门自行对其应用系统涉及数据访问、使用等情况进行监控，存在较高的数据违规使用、泄露风险。	示例：引入日志审计平台等产品或技术工具，将日志审计平台与承载敏感数据的各应用系统进行对接，对各应用系统日志的统一的收集、管控与审计。	示例：风险等级高于预设的风险准则	示例：接受处置建议

来源：数据安全推进计划

安全声明的价值在于：**一方面**，评估执行人员向相关方分发评估结果的同时，需要通过安全声明一并发布各评估项的国家法规或标准来源，注明评估过程中所收集的证明材料情况，对不符合项进行特别批注，明确风险问题与处置建议，声明因忽略风险评估结论引发的安全问题由相关方自行承担；**另一方面**，各相关方需要在获得评估结果后从风险处置的成本、优先级等方面，对风险问题与处置建议进行评估，并声明是否实施风险处置方案。如确认开展风险处置工作，相关方还需要进一步明确处置计划与具体责任人、处置时限，并由组织的监督层人员、评估执行人员跟踪评估处置措施的效果，定期向组织决策层、管理层人员汇报。

四.数据安全风险评估工作建议

组织环境与业务需求、新型攻击威胁持续变化，数据安全风险的边界不断扩大，数据安全风险的评估与治理将成为组织不断探索的重要课题。本报告建议：

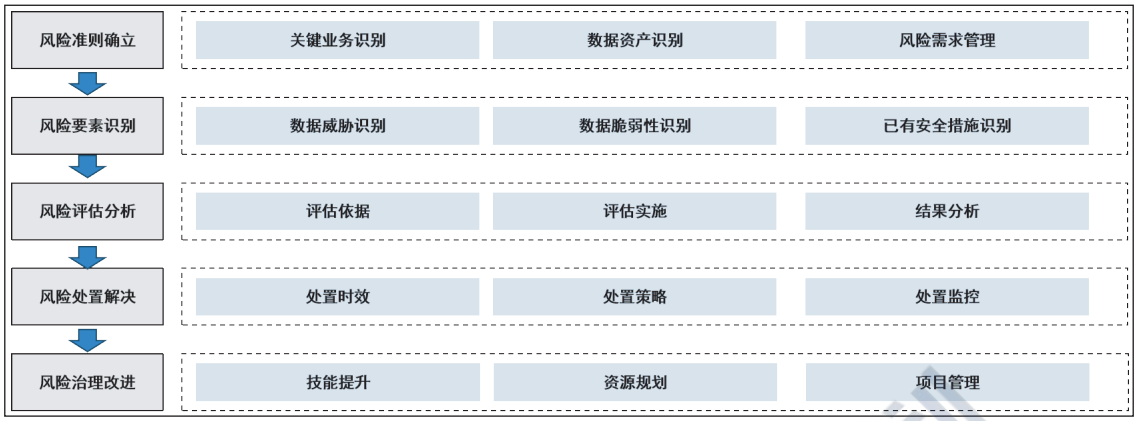
(一)建立数据安全风险评估机制

随着国家法律法规和监管部门、行业主管部门要求的不断细化，数据安全风险评估工作也将持续在各行业推进、落地。数据安全风险评估以法律法规遵从性为准则，围绕数据和数据处理活动，重点关注数据安全的管理、技术以及个人信息保护等方面问题，是组织权衡数据价值释放与数据安全保障的“标尺”。因此，组织应建立常态化的数据安全风险评估机制，明确实施数据安全风险评估的场景，将评估的实施频次、实施要求、评价标准等内容固化到内部的管理要求中。

(二)构建数据安全风险治理框架

数据安全风险评估的结果不仅是组织前期数据安全建设水平的验证，也是未来数据安全建设的输入：数据安全风险评估的结果作为组织开展数据安全风险处置、治理改进的依据，也将持续用于完善数据安全风险治理的准则，以推动对更多未知风险的识别、评估。

为了更好地串联数据安全风险识别、评估、处置、监控以及后续改进等工作，推动基于风险评估的数据安全风险治理框架建设：2022年，中国信息通信研究院云大所数据安全团队在CCSA TC601携手近三十家企业，牵头开展了《数据安全风险治理成熟度评价模型》预研。2023年，中国信息通信研究院云大所数据安全团队基于行业服务实践，对内容进行优化，目前形成《电信和互联网 数据风险治理成熟度评估模型》标准草案，并在CCSA TC1成功立项。《电信和互联网 数据风险治理成熟度评估模型》首次将组织的数据安全风险治理按照风险治理的阶段分为五大能力域15个能力项，并划分了五级能力等级，提出组织应以风险为核心，构建覆盖风险准则建立、风险要素识别、风险评估分析、风险处置解决、风险治理改进的全面治理框架，从要素识别的全面性、评估分析的准确性、处置解决的有效性等方面持续优化风险治理能力，致力于推动企业事前明确数据安全风险关键要素，事中建立全面的风险治理体系，事后健全风险治理的监控与管理改进，具体见图3。



来源：《电信和互联网 数据风险治理成熟度评估模型》标准（草案）

图3 数据风险治理基本框架

(三)完善数据安全风险治理体系

组织识别、评估数据安全风险，依据风险准则制定不同的风险处置策略，并通过持续监控、评价风险的状态，判断是否追加新的处置措施。由此可见，数据安全风险将持续驱动组织完善自身的数据安全治理体系，组织的数据安全建设工作也将从单一的“合规驱动”走向“合规+风险”的双轮驱动。

数据安全风险治理的各个环节与风险准则息息相关，因此，组织应将风险准则的确立作为风险治理的开始——这意味着组织应基于自身发展的需要，充分考虑组织的发展目标以及当前所处的环境、利益相关方诉求等方面，将数据安全风险治理的体系建设渗透进数据安全的组织建设、制度流程、技术工具、人员能力等各个方面，明确数据安全风险治理的准则，并以准则引导组织内部的风险识别、评估与处置机制完善，使数据安全风险治理战略与组织的整体发展与风险管理战略始终保持一致。

附录：中国信通院云大所实务索引

表10 实务索引

数据安全风险评估及治理实务			实务经验主要来源
1 数据安全风险评估工作背景	/	(1) 数据安全风险形势日益严峻	数据风险治理相关标准研制、数据安全风险监测与评估相关课题研究
		(2) 组织风险防范面临监管考验	
		(3) 新技术应用暗藏新型风险	
2 数据安全风险评估工作现状	/	(1) 风险评估已成业界焦点	数据风险治理相关标准研制、数据安全风险监测与评估相关课题研究
		(2) 评估标准编制进程加快	
		(3) 评估实施方法逐渐成熟	
3 实务问题剖析与解决思路	3.1 评估准备	3.1.1 如何确定评估触发条件-梳理适用情形	汽车企业数据安全风险评估实践
		3.1.2 如何制定评估工作目标-建立风险准则	数据风险治理相关标准研制工作实践
		3.1.3 如何规划评估实施范围-识别重点对象	银行、保险、运营商企业数据安全风险评估实践
	3.2 评估实施	3.2.1 如何获取有效评估信息-完善协作机制	银行、保险企业数据安全风险评估实践
		3.2.2如何应用风险评估工具-认识工具功能	银行数据安全风险评估实践
		3.2.3如何开展风险评估分析-建立分析模型	金融支付企业数据安全风险评估实践
	3.3 评估总结	3.3.1如何充分应用评估结果-发布安全声明	汽车企业数据安全风险评估实践
4 数据安全风险评估工作建议	/	(1) 建立数据安全风险评估机制	数据风险治理相关标准研制、数据安全风险监测与评估相关课题研究
		(2) 构建数据安全风险治理框架	
		(3) 完善数据安全风险治理体系	