编号：11 未经许可不得它用

国家信息中心2021年度青年人才基础研究项目成果

# 大数据价值评估与安全合规审查方法研究

部 门：信息与网络安全部

项目负责人：王佳慧

目 录

[一、研究计划执行情况概述 4](#_Toc93926735)

[（一） 按计划执行情况 4](#_Toc93926736)

[（二）研究目标完成情况 5](#_Toc93926737)

[二、研究工作主要进展、结果和影响 6](#_Toc93926738)

[（一）主要研究内容 6](#_Toc93926739)

[（二）主要研究进展 8](#_Toc93926740)

[三、国内外学术合作交流等情况 36](#_Toc93926741)

[四、存在的问题、建议及其他需要说明的情况 36](#_Toc93926742)

[五、项目取得成果的总体情况 36](#_Toc93926743)

[参考文献 37](#_Toc93926744)

大数据价值评估与安全合规审查方法研究

摘 要

目前，全球已经进入了数字经济时代，《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》的发布表明，大数据价值与安全合规非常重要。本课题通过梳理国内外数据安全合规评估和价值评估的研究现状，围绕大数据发展对数据价值标准化的迫切需求，主要做了以下两方面研究。

在大数据安全合规方面，本报告通过研究国内大数据安全标准为依据，提出一种数据安全合规评价的指标体系。具体分为通用指标构建，特定指标构建。特定指标构建是主要考虑不同行业的法律法规监管要求和业务发展需要不同。通用指标包括三个一级指标，分别为组织建设、制度保障、技术保障。并详述了每个指标的评估实施方法。需要说明的是，本课题的数据安全合规审查适用于内部自评或第三方评估指标构建。现场评估实施包括准备环境、实施现场评估、输出评估结果、问题回顾、复评复测五个阶段。本课题提出的指标体系从数据全生命周期着手来，结合国内国际法，行业特点，应用特点，同时关注、研究相关的执法案例，研究各个数据各个阶段的安全合规，对于具体应用而言，如果不涉及某个阶段，可以忽略相应的指标，因此通用性更强，由于数据和应用的紧相关关系，对于具体的应用场景，也需要结合实际情况增加扩展指标。

在大数据价值评估方面，提出了数据价值评估指标体系的构建方法和评估的实施流程。数据价值评估指标构建体系从市场角度来看，可通过成本法、市场法、收益法三种方法构建；从非市场角度考虑数据价值评估指标体系的构建，可通过条件价值法，即通过调查公民对数据开放共享和隐私保护的价值判断来衡量数据的社会价值。也可通过专家讨论会衡量数据的社会价值和非市场价值。同样的指标体系，使用不同的评估方法会产生不同的结果，因此数据价值量化评估不可能有通用方法，因此本课题对不同对评估方法都有研究，在实际应用阶段，价值评估指标构建完成后，应该结合数据特性、规格、评估目的以及供需双方的意见进行具体分析，确定合适的量化机制。具体方法包括层次分析法、专家打分法，以及层次分析法+模糊综合评价法等方法。分两阶段实施，第一阶段主要解决数据价值评估机制和指标体系的确定。基本确定数据价值评估的目的、范围、要求、数据类别和合规性，确定数据价值评估的指标。第二阶段结合数据特性、规格、评估目的以及供需双方的意见进行具体分析，确定合适的量化机制。应当从数据的实际场景出发，结合通用指标，具体情况具体分析。同时充分考虑分级分类分区、定性定量、主观客观、市场属性非市场属性、应用成本相结合的方法。

## 一、研究计划执行情况概述

### （一） 按计划执行情况

本项目的研究计划要点包括：

1）建立大数据价值评估框架；

2）建立大数据价值评估指标体系；

3）研究数据全生命周期的安全合规评价体系；

4）推动大数据价值评估和安全合规体系的行业示范应用；

项目组严按照原定计划进行各项工作，主要做了如下工作：

1) 提出数据安全合规的评估指标体系；

2) 提出数据安全合规评估的评估实施方法；

3) 提出数据安全合规评估实施流程；

4) 提出数据价值评估的实施流程；

5) 研究数据价值评估指标体系构建方法；

6) 针对数据价值评估适用的方法进行系统研究；

具体对比如下表1：

表1 计划与完成情况

|  |  |  |
| --- | --- | --- |
| 序号 | 计划 | 完成情况 |
| 1 | 建立大数据价值评估框架 | 分析了大数据价值评估的挑战和必要性，在此基础上提出数据价值评估的实施流程，提出适用于数据价值评估的方法。 |
| 2 | 建立大数据价值评估指标体系 | 提出数据价值评估指标体系构建方法，实际应用中根据数据的类别以及数据的不同特性选用不用的指标体系构建方法。 |
| 3 | 研究数据全生命周期的安全合规评价体系 | 深入分析了国内外数据安全合规面临的挑战，从数据全生命周期着手，结合国内国际法，行业特点，应用特点，同时关注、研究相关的执法案例。提出了数据安全合规评估体系。具体分为通用指标构建，特定指标构建。特定指标构建是主要考虑不同行业的法律法规监管要求和业务发展需要不同。通用指标包括三个一级指标，分别为组织建设、制度保障、技术保障。 |
| 4 | 推动大数据价值评估和安全合规体系的行业示范应用 | 通过具体场景的分析，和具体评估的实施，推动大数据价值和安全合规研究成果的落地和验证。 |
| 5 | 论文1 篇 | 论文1篇，评估报告1份 |

本项目取得了如下研究成果：论文《基于密钥组合的隐私数据保护方案》1篇，《数据流通平台安全合规评估》报告1份，与预期研究成果相符。

### （二）研究目标完成情况

项目组紧紧围绕本项目的研究目标开展各项研究，从以下几个方面都做了深入的探索实践，已顺利完成预期研究目标。项目组通过梳理国内外数据安全合规评估和价值评估的研究现状，围绕大数据发展对数据价值标准化的迫切需求，提出数据价值评估框架和指标体系构建方法。

取得了一系列研究成果，具体包括如下几个方面：

1. 研究数据安全合规的必要性；
2. 提出数据安全合规的评估指标体系；
3. 提出数据安全合规评估的评估实施方法；
4. 提出数据安全合规评估实施流程；
5. 提出数据价值评估的实施流程；
6. 研究数据价值评估指标体系构建方法；
7. 针对数据价值评估适用的方法进行系统研究。

完成论文《基于密钥组合的隐私数据保护方案》。

完成评估报告《数据流通平台安全合规评估》。

综上所述，项目研究已经实现了既定目标。

## 二、研究工作主要进展、结果和影响

### （一）主要研究内容

随着移动互联网、5G、云计算等技术普及和革新，数据量快速增长，数据汇聚、融合、流动与应用等场景大幅增加，催生了大数据时代。大数据时代出现之后，数字经济也得到飞速发展。近年来，数字经济在全球迎来了前所未有的高速发展。在新的经济形态中，数据成为改变市场、组织机构甚至政府和公民关系的重要因素。近年来，各国加快推进数据领域的立法活动，以期通过制度竞争获得数据资源、数据监管技术、数据规则话语权的博弈优势。全球主要发达国家把数字经济作为经济发展的重点，积极推进国家发展战略和政策，推动经济和社会持续转型。国际领域的数据竞争已经进入白热化的状态，数据成为国际竞争的重要因素。数据不仅成为重要的商业资源和生产要素，更是国家基础性战略资源。我国积极布局新基建、数据要素培育，数据经济势头发展迅猛。2020年4月9日，中共中央、国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》[1]，明确提出“加快培育数据要素市场”，包括推进政府数据开放共享，提升社会数据资源价值，加强数据资源整合和安全保护。这也给我们带来了很多新的挑战。当前我国深化数据要素市场化配置面临统筹力度弱、数据立法欠缺、交易市场瓶颈大、创新资源配置效率低、数据市场监管难、数据安全保障差等六个方面的挑战[2]。可见，数据要充分发挥其价值，也必须建立在数据安全合规的基础之上。

回顾数据发展的整个过程会发现，数据已经成为当代的战略性的资源。从上世纪四十年代到八十年代，由于计算机的昂贵、体积大、能耗高，往往只限于国防、气象、科研研究的一些领域。那时候一台计算机是有几个房子那么大，数据的存储量不是很高。而进入到了信息技术的1.0时代，也称为IT时代，这一时期是以单机应用为主要特征的数字化阶段，以数字化办公和信息管理系统逐渐代替纯手工数据，此时的数据仅限于办公等信息。信息化1.0阶段的特征是数据信息描绘（映射）现实。

从上世纪九十年代中期开始，随着网络发展，特别是互联网的兴起。以互联网为应用特征的网络化，加速了数据的传播、流通和汇聚，数据呈现海量的、多样性、时效性、低价值密度等一系列特征。网络促进了我们彼此的交流沟通，将各个方面的事情组合起来。这时候数据驱动现实模式的改变。电子商务的兴起，电子政务的广泛应用，使我们真正进入了网络的时代，就是DT（数据）时代。总的来说，主要面临以下几方面挑战：

**挑战1: 新技术催生安全新需求，冲击传统合规体系**

当下，云计算、物联网、5G、移动互联网等新技术使得时时刻刻都能收集数据。通过数据分析、数据挖掘、人工智能等信息技术，非个人数据的聚合可形成敏感数据，从碎片化的、不具有敏感性的数据中也可以分析出敏感的信息，海量数据的聚合甚至可以分析出有关国家安全的数据。这一系列的现象导致个人数据与非个人数据、敏感数据与非敏感数据、国家秘密与非国家秘密等边界逐渐模糊。传统网络环境下的统一的、集中的安全管理模式已经不能适应新环境下的数据安全需求。这就为数据合规带来新风险；另一方面导致传统数据合规策略的有效性降低甚至失效。

**挑战2: 全球化监管带来合规难题**

不论是国内还是国际领域，大数据安全的监管态势均不断增强。在此背景下，大数据安全成为组织合规的重要内容。

国内层面，整体来看，尚不完善的规则设计和执行机制难以为组织数据合规提供有效指引。目前虽然我国网络安全方面的顶层制度设计已经基本完成，网络安全法的颁布也在很大程度上填补了立法空缺，但在整个网络安全领域我国仍存在着立法不足的情况。在具体实施方面，作为网络安全基本大法的网络安全法配套制度尚不健全，可操作性和实际落地仍有待加强。此外，作为新实施的法律实践层面，网络安全法的执法案例尚不充足，执法尺度仍需进一步探索和统一。

国际层面，通观国际立法趋势，不难发现数据已成为国际空间竞相争夺的战略性资源，美欧等诸多国家和地区已经纷纷出台举措抢占国际空间数据规则的制定权，建立以本国或本区域利益为中心的数据规则体系。总的来讲，各国立法规范逐步增多，监管效力不断增强。各国的立法目标不仅在于个体权益的保障，更是关涉国家主权、国家利益在国际空间的博弈和角逐。为争夺数据话语权，扩张本国法律的适用范围，积极推行符合本国利益诉求的国际社会数据规则体系成为当前国际的立法趋势。随着国际博弈的加剧，国际法律冲突也逐渐走向常态化。网络和数据的跨国界性往往使得组织需要应对不同规则体系的合规，大大增加了组织合规的复杂性。

**挑战3: 数据价值指标体系构建研究工作不足**

数据的搜集、积累、储存、处理过程的环节多，各环节常反复出现。数据成本构成较复杂，各构成部分相互关联耦合。数据的经济效益难测算，数据的价值转化或确认过程存在不确定性等。这些特点导致数据价值评估难以标准化，也不宜考虑单一因素做简单化处理，而要紧密结合数据价值基本特性，综合多因素分阶段开展分析评估。数据价值评估指标体系主要考虑数据不同特性对价值的影响，对数据价值评估指标体系构建的研究工作较少。

**挑战4: 数据价值评估方法很难通用**

数据现在通常归类为无形资产，实际上，数据与一般无形资产价值的构成不同，数据价值的形成具有生产的一次性、加工处理的多性、成本费用的多源性、获益的较大不确定性、价值转化的风险性、数据应用的不同等特点，导致数据价值评估需要考虑诸多影响因素，具有高复杂性和高难度性，很难有通用的评估方法。

**针对上述问题及挑战，本项目的主要研究内容包括如下两个方面：**

1）研究数据安全合规的必要性，数据安全合规的评估指标体系、数据安全合规评估的评估实施方法，数据安全合规评估实施流程。

2）提出数据价值评估的实施流程。研究数据价值评估指标体系构建方法。针对数据价值评估适用的方法进行系统研究。

### （二）主要研究进展

#### 1.研究大数据全生命周期的安全合规

本部分主要研究数据安全合规的必要性，数据安全合规的评估指标体系、数据安全合规评估的评估实施方法，数据安全合规评估实施流程。

目前，在国家层面上《网络安全法》《数据安全法》《密码法》《个人信息保护法》已发布。政务领域，国家层面发布了《政务服务平台基础数据规范》、《国务院关于印发政务信息资源共享管理暂行办法的通知》等多项国家标准规范和政策文件。地方层面，各省市出台了上百份与政务数据相关的政策文件，各地都对政务数据使用、规范等工作提出了要求。但是机构和企业如何安全合规的使用数据还存在很多问题。

已有的法规在实际执行落地方面，还需要更多的规范和解释支撑。而数据安全一把手责任以及其他责任又倒逼安全合规的必要性。数据泄露要承担责任，尤其是一些数据是包含了大量与国民经济、商业机密、个人隐私等相关的信息，保障数据的安全性也是最重要的环节之一。随着数字化建设全面推进，各业务场景和业务数据流转过程也在发生巨大的变化，其安全性也是目前面临的主要挑战。目前，国际标准化组织 ISO 和国际电工委员会 IEC 已形成了较为完善的数据安全和隐私保护标准体系；国内方面相关的数据安全和隐私保护相关标准主要包括：《信息安全技术个人信息安全规范》，《信息安全技术个人信息安全影响评估指南》《信息安全技术大数据安全管理指南》《数据安全治理实践指南》[3]等。但在数据资产安全性上，还有很多需要完善的地方。

数据资产安全的标准体系，要以数据安全和隐私保护[4]为重点，在服务器、网络等基础设施安全建设的基础上，围绕数据采集、存储、利用、共享等数据活动，将数据库安全防护和政务数据全生命周期流转过程中的风险控制，在数据相关各部门形成统一的安全策略。完善自动化运维管理和常规审计中，及时对风险进行预知。数据安全防护机制总体标准架构应从技术标准、管理标准、应用标准、评估标准等多个方面构建数据安全标准体系。首先，建立完善的数据安全风险策略，通过合理授权、加密、脱敏等风控技术工具进行风险控制，并能够对风险事件进行溯源。其次，加强敏感数据控制[5]，对涉及政府机密、商业机密、个人隐私等信息必须进行脱敏，这就涉及到对敏感数据要进行良好的定义、敏感数据的监考、访问权限控制等机制，完善敏感数据管理。第三，对数据安全运营进行有效的管理。在自动运维系统上能够提供健全的风险预警、配置管理、策略管理、应急响应等，完善政务数据在运行层面的管控。随着数据大量的汇集、数据的共享开放、多应用场景的形势下，过去的安全机制也需要不断调整适应现有的状况，以应对日趋严峻的网络安全风险环境。

**1.1数据安全合规评估的必要性**

随着移动互联网、5G、云计算等技术普及和革新，数据量快速增长，数据汇聚、融合、流动与应用等场景大幅增加，催生了大数据时代。大数据时代出现之后，数字经济也得到飞速发展。近年来，数字经济在全球迎来了前所未有的高速发展。在新的经济形态中，数据成为改变市场、组织机构甚至政府和公民关系的重要因素。近年来，各国加快推进数据领域的立法活动，以期通过制度竞争获得数据资源、数据监管技术、数据规则话语权的博弈优势。全球主要发达国家把数字经济作为经济发展的重点，积极推进国家发展战略和政策，推动经济和社会持续转型。国际领域的数据竞争已经进入白热化的状态，数据成为国际竞争的重要因素。数据不仅成为重要的商业资源和生产要素，更是国家基础性战略资源。我国积极布局新基建、数据要素培育，数据经济势头发展迅猛。

2020年4月9日，中共中央、国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》，明确提出“加快培育数据要素市场”，包括推进政府数据开放共享，提升社会数据资源价值，加强数据资源整合和安全保护。2020年5月11日中共中央、国务院印发《关于新时代加快完善社会主义市场经济体制的意见》，进一步提出，“建立数据资源清单管理机制，完善数据权属界定、开放共享、交易流通等标准和措施，发挥社会数据资源价值。”可以说，互联网场景中，数据不再是一座孤岛，数据开始借助云计算、物联网、人工智能等技术集群开始流动，成为新经济形态的驱动力量。随着数据应用技术，数据大量汇聚，数据深度挖掘，人工智能技术的发展，数据安全的挑战也与日俱增。

信息社会从小数据时代进入到更高级的形态大数据时代。在此阶段，数据质量和价值通过共享、交易等流通方式价值得到更大程度的实现和提升，数据动态利用逐渐走向常态化、多元化，个人信息的权属问题和重要数据的识别问题成为这一阶段的主要争议，引发了从个人信息保护到组织数据保护、不正当竞争、著作权、网络（空间）安全等一系列法律问题。

数据从静态安全到动态利用安全的转变使得数据安全不再只是传统信息安全和网络安全时代，确保数据本身的保密性、完整性和可用性（三性问题），除了关注三性遭到破坏的数据泄漏、数据篡改、数据丢失等问题，更承载着个人、组织、国家等多方主体的利益诉求，关涉个人权益保障、组织知识产权保护、市场秩序维持、产业健康生态建立、社会公共安全乃至国家安全维护等诸多数据安全合规问题。

新技术和新应用的迭代更新也不断催生出新风险，数据安全风险日益升级，成为建设产业健康生态、保障社会公共安全和国家安全的制约因素。大数据安全已然成为超越个体，关涉国家安全的核心环节。要最大化、有效的释放数据机制，前提必须确保数据的安全和合规。如果数据是不合规的，价值可能就是零。如果数据是不安全的，也会大大降低数据的价值。对数据进行有效的加工、处理、分析是协助持续提高大数据产业发展、治理效率、实现治理现代化的重要途径。而与此同时，由于多渠道数据汇聚、数据清洗、数据安全，等各个步骤处理过程中缺乏详细的标准，数据的质量和应用在各层次、各领域标准化程度不高，成为了制约数据应用发展的重要原因。因为首要的任务是确保数据的安全合规。

在诸多的数据安全保护手段当中，数据安全合规评估作为一项能够有效监测和防范数据安全风险的制度约束，助力数据要素行业的健康与可持续发展具有重要意义。数据安全合规评估是应对数据安全合规风险的有力举措，也是数据价值评估的有力保障。国际主要发达国家围绕组织机构数据安全合规自评估、监管执法检查以及第三方评估认证等多方面积累了一些实践经验。

本项目力求在国外先进经验的基础上，结合我国的立法和实践，提出合理可落地的数据安全合规评估体系。促进数据的有序流动和安全应用，使得数据价值能合理评估，为构建数据为关键要素的数据经济保障护航。

总的来说，数据安全合规面临如下挑战：

**挑战1 新技术催生安全新需求，冲击传统合规体系**

当下，云计算、物联网、5G、移动互联网等新技术使得时时刻刻都能收集数据。通过数据分析、数据挖掘、人工智能等信息技术，非个人数据的聚合可形成敏感数据，从碎片化的、不具有敏感性的数据中也可以分析出敏感的信息，海量数据的聚合甚至可以分析出有关国家安全的数据。这一系列的现象导致个人数据与非个人数据、敏感数据与非敏感数据、国家秘密与非国家秘密等边界逐渐模糊。传统网络环境下的统一的、集中的安全管理模式已经不能适应新环境下的数据安全需求。这就为数据合规带来新风险；另一方面导致传统数据合规策略的有效性降低甚至失效。

**挑战2 全球化监管带来合规难题**

不论是国内还是国际领域，大数据安全的监管态势均不断增强。在此背景下，大数据安全成为组织合规的重要内容。

国内层面，整体来看，尚不完善的规则设计和执行机制难以为组织数据合规提供有效指引。目前虽然我国网络安全方面的顶层制度设计已经基本完成，网络安全法的颁布也在很大程度上填补了立法空缺，但在整个网络安全领域我国仍存在着立法不足的情况。在具体实施方面，作为网络安全基本大法的网络安全法配套制度尚不健全，可操作性和实际落地仍有待加强。此外，作为新实施的法律实践层面，网络安全法的执法案例尚不充足，执法尺度仍需进一步探索和统一。

国际层面，通观国际立法趋势，不难发现数据已成为国际空间竞相争夺的战略性资源，美欧等诸多国家和地区已经纷纷出台举措抢占国际空间数据规则的制定权，建立以本国或本区域利益为中心的数据规则体系。总的来讲，各国立法规范逐步增多，监管效力不断增强。各国的立法目标不仅在于个体权益的保障，更是关涉国家主权、国家利益在国际空间的博弈和角逐。为争夺数据话语权，扩张本国法律的适用范围，积极推行符合本国利益诉求的国际社会数据规则体系成为当前国际的立法趋势。随着国际博弈的加剧，国际法律冲突也逐渐走向常态化。网络和数据的跨国界性往往使得组织需要应对不同规则体系的合规，大大增加了组织合规的复杂性。在国际法律冲突的情形下，组织合规将陷入两难境地。例如，欧盟GDPR、美国CLOUD法与我国网络安全法第37条的冲突可能会导致组织在数据出境方面面临巨大的合规困境。

表2 部分国内综合法规列表

|  |  |
| --- | --- |
| 序号 | 名称 |
| 1 | 网络安全法 |
| 2 | 中华人民共和国数据安全法 |
| 3 | 数据安全管理办法 |
| 4 | 中华人民共和国个人信息保护法 |
| 5 | 关键信息基础设施安全保护条例 |

**1.2数据安全合规的评估指标体系和评估实施方法**

有学者提到大数据生命周期可以分为数据生成、存储和处理3个阶段，也有些学者把数据安全周期分为4个阶段，分别为数据发布、存储、分析和处理阶段，但采用的防护技术基本一致。因此，本报告提出的数据安全合规评估指标从数据全生命周期着手，结合国内国际法律及相关标准[6]，行业特点，应用特点，同时关注、研究相关的执法案例[5]。由于不同的研究人员在需求理解、接触的大数据实际应用场景方面存在差异，导致其在研究上产生方向、力度、关注点的不同。大数据安全合规法律法规和相关标准是规范不同研发人员研究大数据安全防护的基础。本报告将通过研究国内大数据安全标准为依据，提出一种数据安全合规评价的指标体系。具体分为通用指标构建，特定指标构建。特定指标构建是主要考虑不同行业的法律法规监管要求和业务发展需要不同。本项目主要研究通用指标的构建。

**通用指标包括三个一级指标，分别为组织建设、制度保障、技术保障。**

**1）组织建设维度：**

具体是指数据安全组织的架构建立、职责分配和各部门人员沟通协作。完善的组织建设是数据安全合规的重要环节。组织应当建立完善的、标准化的、覆盖数据全生命周期的数据组织。主要包括建立数据安全管理机构，明确数据安全管理的角色和责任，提升人员的意识，能力和素质。组织建设维度的指标评估实施方法主要是通过访谈和查验相关文件的方式实现。

**组织建设二级指标包括数据安全组织架构和人员保障。**

**➤ 数据安全组织架构：**

**包括两个三级指标：数据安全管理责任部门、数据安全管理职责分工、数据安全监督检查。**主要关注组织是否已设立数据安全管理责任部门门，负责牵头承担组织内部数据安全管理工作是否有明确独立的数据安全管理责任部门，负责牵头承担组织内部数据安全管理工作，包括但不限于制定数据安全管理整体方针策略，协调相关部门建立数据安全技术保障措施，牵头做好数据安全应急处置，组织开展数据按合规性评估等工作而且和各项安全合规工作执行落实部门有明确的责任分工界面。是否建立数据安全管理制度执行落实情况监督检查和考核问责制度。

典型的数据安全组织架构可分为决策层、管理层、执行层和监督层组成。决策层由参与业务发展决策的高管和数据安全官组成，制定数据安全的目标和愿景，在业务发展和数据安全之间做出良好的平衡；管理层是数据安全核心实体部门及业务部门管理层组成，负责制定数据安全策略和规划，及具体管理规范；执行层由数据安全相关运营、技术和各业务部门接口人组成，负责保证数据安全工作推进落地。监督层独立审计部门组成，负责监督各项措施的落实。

具体评估实施方法如下：

* **数据安全管理责任部门：**

可通过查验组织文件通报或数据安全管理办法，是否明确数据安全管理责任部门（新设部门或指定某个原部门均可），是否明确部门名称及负责人，相关文件是否已面向组织机构内部发文通报（如OA发文、纸质发文、公司领导办公会决议等），在组织内部进行流转传达。

数据安全管理责任部门是否明确，通过查验组织文件通报或数据安全管理办法，是否明确数据安全管理责任部门职责，部门职责是否包括但不限于制定数据安全管理整体方针策略，协调建立数据安全技术保障措施，牵头做好数据安全合规性评估、安全审计管理、数据安全事件应急处置、教育培训等工作。

* **部门职责分工：**

通过查验组织文件通报或数据安全管理办法，是否明确划分数据安全管理责任部门与各项工作执行落实部门分工界面，工作执行落实部门是否完整包含数据协同管理部门（信息化、客户服务、市场部门等）、数据使用部门（业务部门）、运维支撑部门（网络运维、系统集成等部门）、可能涉及的子公司等。

* **数据安全监督检查制度：**

通过访谈、文件查验是否明确由责任部门定期对执行部门数据安全管理制度执行落实情况和落实效果进行监督检查，是否能够通过监督检查及时发现问题并督促整改，是否将数据安全工作执行部门落实情况和效果纳入组织内部绩效考核体系。

**➤人员保障**：

指为实现以上组织、制度和技术工具的建设和执行其人员应具备的能力。核心能力包括数据安全管理能力、数据安全运营能力、数据安全技术能力及数据安全合规能力。根据不同数据安全能力建设维度匹配不同人员能力要求。

三级指标包括数据安全岗位职责、数据安全人员配备、数据安全人员能力。数据安全岗位职责关注是否明确相关人员数据安全工作职责，负责具体承担落实数据安全管理工作。数据安全人员配备关注是否在数据安全管理责任部门和相关部门配备数据安全管理专职人员。

具体实施方法如下：

通过对《数据安全岗位职责说明书》《人员任命书》《数据安全岗位人员名单》《数据安全岗位人员工作记录文件》等相关制度和记录文档的查验。

如数据安全岗位职责查验组织数据安全岗位职责说明文件或人员任命书，是否通过正式文件明确组织数据安全管理责任人，是否明确其职责范围，包括但不限于负责牵头制定数据安全管理制度，指导数据安全管理责任部门、协调各相关部门开展数据保护工作，提出数据安全保护的对策建议，监督管理制度和措施的执行落实情况等。

数据安全人员配备，查验组织数据安全岗位人员名单，是否梳理各部门数据安全岗位人员配备情况，包括部门名称、姓名、联系方式和工作职责等，是否在数据安全管理责任部门至少配备一名数据安全专职人员，相关工作执行落实部门至少配备一名数据安全责任人，组织开展部门内数据安全工作。相关人员工作职责是否包括但不限于权限管理、安全审计、应急响应、合规性评估、数据安全事件处置和信息报送等。查验组织数据安全岗位人员工作记录文件，验证组织数据安全管理责任部门和相关部门人员是否按照要求履职。

人员能力，评估数据安全责任人应具备数据安全专业知识和相关管理工作经历，参与有关数据处理活动的重要决策，履行以下职责：组织确定数据保护目录，制定数据安全保护计划并督促落实；组织开展数据安全影响分析和风险评估，督促整改安全隐患；依法向有关部门报告数据安全保护和事件处置情况； d) 组织受理和处置数据安全投诉、举报。

**2）制度保障二级指标包括数据识别、数据分级分类、事件应急处置、人力资源保障与考核、制度执行审计。**

**➤ 数据识别：**

网络运营者应识别数据处理活动中涉及的数据，包括个人信息、重要数据和其他数据，形成数据保护目录，并及时更新。数据识别包括数据识别、数据识别记录、数据清单、数据变更台帐。具体实施方法如下：通过检查组织数据资产梳理相关制度文件和记录文档，查验组织是否明确数据资产的安全管理目标和原则，是否明确数据资产的维护和使用责任，是否明确定期系统梳理各数据存储平台系统情况要求，是否明确数据存储系统情况梳理原则和梳理周期。

通过查验组织数据识别记录，评估组织是否明确数据识别统一规范要求，查验组织数据梳理记录，是否定期梳理各数据存储系统情况，并留存梳理记录；是否覆盖组织系统全范围，从组织收集处理用户个人信息的核心系统扩展到各数据处理活动相关系统，全面掌握组织数据资产规模和情况；是否对组织安全域内外系统或设备接入情况进行全面区分，并留存相关文档记录备查。

查验组织是否形成数据资产清单。如存在，查验组织数据资产清单，是否根据规范要求，在完成组织机构平台系统梳理的基础上，明确数据字段的指向性、关联性，是否对已形成的数据资产清单进行定期更新，建议更新周期频率不高于一年。查验组织是否形成数据资产变更台账，对数据资产使用、留存及报废等状态进行登记，并针对已形成的数据资产清单定期更新数据资产变更台账。

**➤ 数据分级分类：**

具体实施，可以参照已有法律法规和国家标准要求，以及行业标准，如金融行业[7][8][9]，根据合同规定和业务运营需要，对所识别的数据进行分类分级管理。具体评估实施方法如下：

能否形成科学可行、合理合法、完善周延的数据分级分类管理。具体查验包括制度标准策略、数据标识、差异化技术保障措施、策略变更。通过检查制度评估组织是否按照法律法规和相关标准要求，建立组织内部数据分类分级管理制度。查验组织数据分类分级管理制度，是否明确数据分类分级管理数据范围、管控技术措施、数据分类分级原则、分类分级策略标准变更流程和要求等内容；验证数据分类分级管理原则、定义、方法是否能够真实反应数据本身的属性；验证数据分类分级制度适用范围、管控系统类型是否完整覆盖组织相关数据处理活动涉及的平台系统。查验组织数据分类分级管理制度，是否按照法律法规和相关标准要求，综合考虑数据的类别属性、使用目的等，明确数据分类策略；是否在数据分类的基础上，对每一类数据类型，结合数据重要及敏感程度、安全保护需求以及一旦泄露、丢失、破坏造成的危害程度等，制定数据分级标准，明确各级数据界限，包括具体类别、子类、范围、对应的数据举例。（注：分类分级方法可参照行业内分级分类标准，目前电信、金融等领域已经有了明确的分级分类标准）

查验数据分类分级清单，是否对数据进行分类分级标识（如通过对数据字段或数据库表单打标签等形式）。查验组织数据分类分级清单，是否依据数据分类分级制度策略，结合数据分类分级管控系统对象，完成各数库表字段映射，梳理形成包含数据类别、数据定位、数据范围、对应系统数据等内容的数据分类分级清单，并根据数据分类分级变更情况进行动态更新并留存更新记录。

通过检查标识数据，如可要求组织演示组织业务和业务支撑系统，验证是否根据分类分级制度策略，实现数据资产的分类分级标识（如通过对数据字段或数据库表单打标签等形式）。

通过查验组织数据分类分级管理制度，评估组织是否建立差异化技术保障措施，是否充分考虑业务或系统平台场景需求，在数据采集、传输、存储、使用、共享、销毁等数据全生命周期各个环节中针对不同类别级别的数据明确相应的安全保障措施，包括不限于数据加密、数据脱敏、数据变更、数据销毁、操作权限管理、数据流动记录、人员操作日志记录、数据备份与恢复等技术能力和措施。

通过查验组织数据分类分级策略变更制度，是否明确关于数据分类分级策略制定、变更的流程规范，细化关于策略修订、发布、实施等具体管理要求，并对策略变更情况进行记录。

**➤ 事件应急处置：**

事件应急处置包括数据安全事件应急响应制度，数据安全应急响应预案，数据安全事件应急演练，数据安全事件投诉。评估组织是否建立数据安全事件应急响应处置机制，是否可以根据数据安全计划的变化而及时调整，确保数据安全事件得到及时有效处置。具体评估实施如下：

查验组织应急响应机制是否包括：数据安全事件分级；启动条件；启动所需的资源，如人员、设备、场所、工具、资金等；流程、人员安排和操作手册。查验应急响应机制是否配备应急响应所需的资源，确保应急响应机制能够有效实施。查验是否制定应急演练计划，按计划或者在应急响应机制发生变化后，组织开展应急演练，检验和完善应急响应机制，提高实战能力。查验应急响应记录文件，查验组织发生数据安全事件时，是否立即启动应急响应机制，并采取相应的补救和防范措施，涉及个人信息的，是否及时以电话、短信、邮件或者信函等方式告知个人信息主体，对可能危害国家安全、公共安全、经济安全和社会稳定的是否按相关要求向有关部门报告。

查验组织是否制定数据安全事件应急响应制度，明确数据安全事件应急响应牵头部门及相关执行部门的其工作职责、数据安全事件发现及报告机制、安全事件等级及相关应急措施、溯源及处置流程、事件总结等要求。查验组织数据安全事件应急响应制度，是否明确应急响应目的、依据、范围、原则、事件分级和分类、组织结构及职责、预防和预警机制、应急处置、应急响应保障措施、应急预案的宣贯、培训、演练和维护等内容。

查验组织数据安全事件应急响应方案，是否有效结合了数据安全事件场景和等级划分，是否包括但不限于数据泄露（丢失）、数据滥用、数据被篡改、数据被损毁、数据违规使用等特定场景，是否明确应急响应工作责任分工、实施环节、需配套的应急响应措施，实施环节是否包括事件监测、定位、分级、启动、响应处置、报告、事件评估、结束响应、应急总结、情况跟踪等阶段。

查验组织数据安全应急演练工作记录，验证组织业务是否根据数据安全事件应急响应预案，制定演练计划并定期组织演练，保存演练记录。每类数据安全事件场景是否至少一年开展一次演练。每个核心数据处理活动涉及的平台系统是否至少两年开展一次演练。

查验组织数据安全应急响应处置记录，是否在发生数据安全事件时及时按照应急预案实施应急措施，包括监测预警（预警分级、事件监测、信息报告、预警发布）、应急响应（先期处置、响应、信息发布、应急处置结束）、恢复重建（恢复生产、安全加固、事件总结）。是否视情况将事件情况、应急措施以及可能造成的影响等向主管部门报告。

➤**人力资源保障与考核**：

评估组织是否明确数据安全保护岗位及职责，并提供人力资源保障。查验组织是否建立人力资源考核制度，明确数据安全管理考核指标和问责机制，对相关人员特别是重要岗位人员的履职情况进行考核。出现数据安全重大事件时，对直接负责的主管人员和其他直接责任人员进行问责。

➤**制度执行审计：**

评估包括数据安全审计制度，数据安全审计规范，数据安全审计平台，数据安全审计报告。

数据安全审计制度核验是否制定了数据安全审计制度，是否针对数据生命周期各阶段（数据采集、数据传输、数据存储、数据处理、数据开放共享、数据销毁）开展安全审计，实现对数据访问和操作的有效监控和审计，防控数据生命周期各阶段中可能存在的未授权访问、数据滥用、数据泄漏等安全风险。查验组织数据安全审计制度，是否明确数据安全审计工作牵头部门和相关执行部门；是否明确审计目的、审计对象、审计内容（异常操作的定义）、审计操作规程、审计频度、审计结果规范、审计问题整改跟踪等内容；组织是否定期开展安全审计和整改工作，及时消除安全隐患。

数据安全审计规范，查验组织数据安全审计制度，核查审计对象是否完整覆盖组织相关数据处理活动涉及的平台系统。

核验组织是否建立数据安全审计平台，可要求组织演示组织是否已建设安全审计平台，并将审计对象全量接入安全审计平台；演示组织是否为审计人员开通审计平台审计账号，负责对数据生命周期各阶段的数据访问和操作进行安全监控；演示组织审计平台，验证是否根据数据安全审计内容和组织账号权限管理机制，定义异常操作的范围，配置相应的审计策略（模型）；

数据安全审计报告查验组织数据安全审计制度，核查数据安全审计的内容是否包括组织内部权限控制（数据非授权访问）、组织内部数据流向跟踪情况（批量复制或转移）、数据安全保障措施有效性等，是否能够发现和处置数据非授权访问、批量导出等异常情况。查验数据安全审计报告是否完整记载安全审计发现的问题，是否在一年内实现数据处理活动涉及的平台系统安全审计工作全覆盖。审计数据记录内容是否至少包括：操作时间、操作主体、操作类型、操作对象、操作结果；查验组织数据安全审计报告，验证组织数据安全管理责任部门是否针对有关问题协调数据安全相关执行部门提出改进方案，并要求落实解决；是否对审计问题进行跟踪审核，并留存异常情况处置记录。

3）**技术保障包括过程保障和网络安全防护保障。**

**➤ 网络安全防护保障：**

网络安全防护保障包括加密、脱敏、备份、访问控制、审计追溯、权限管理、日志管理。下面以访问控制管理和日志管理为例说明具体评估实施过程。

* **权限管理：**

包括数据访问权限管理要求，数据处理活动平台系统账号管理，数据处理活动平台系统权限管控，业务支撑系统访问控制。

具体评估实施方法如下；

数据访问权限管理要求查验组织数据访问权限管理制度，是否明确数据处理活动平台系统账号权限分配、开通、使用、销毁等安全保障原则和审批流程要求；是否明确数据处理账号操作的审批要求和操作流程；是否建立并定期更新组织数据处理活动平台系统权限分配表,是否对能够处理用户个人信息的业务系统账号进行定期梳理，并对岗位角色的权限进行规范。

数据处理活动平台系统账号管理通过演示组织账号生命周期管理流程，验证针对开发运维人员、第三方人员在创建和注销系统账号时，是否严格遵循系统账号创建和注销申请审批流程，并记录审批过程和结果。

数据处理活动平台系统权限管控通过技术验证组织数据处理活动平台系统账号权限分配是否遵循“权限明确、职责分离、知其所需、最小特权”的原则，每个账号是否按照角色或用户组进行授权，是否严格控制超级管理员权限账号数量。

业务支撑系统访问控制：通过技术验证组织业务支撑系统是否通过基于IP或MAC地址、账号口令等的方式对所有接入数据处理活动平台系统的用户或业务进行身份认证和权限控制；通过技术验证组织业务支撑系统是否配置口令复杂度策略，如：口令长度不少于8位，使用大写字母、小写字母、数字及特殊字符中至少三种的组合，且与用户名、字符顺序无相关性；通过技术验证组织业务支撑系统是否配置账号锁定策略，对系统账号口令输入尝试次数进行限制；通过技术验证组织业务支撑系统是否对口令遗忘的申请和重置流程实施严格管理，口令重置流程是否存在业务逻辑设计缺陷，是否留存申请和重置记录；演示组织业务支撑系统是否采取掩码显示、加密传输、加密存储等方式保护账号口令安全。

* **日志管理：**

包括重点日志留存管理，日志记录完整、准确、可查，日志记录时间，日志操作权限控制。具体评估实施方法如下：

重点日志留存管理查验组织日志留存相关制度文件，是否明确日志留存要求，包括日志记录范围、记录规范、留存时间以及日志记录访问权限控制等内容，重点关注但不限于数据授权访问、批量复制、开放共享、销毁及数据接口调用等环节日志。

日志记录完整、准确、可查，查验组织业务人员操作日志记录信息是否包括执行时间、操作账号、处理方式、授权情况、登录信息等；查验组织网络运行状态、网络安全事件相关的日志记录保存时间是否满足国家相关法律法规要求，不少于6个月；是否定期对网络日志进行备份，防止数据安全事件导致的日志被删除。

日志操作权限控制，查验组织是否配备日志审计人员，且审计权限与系统管理权限、策略管理权限分立设置；是否对日志操作人员操作进行权限控制，避免非法删除、修改和覆盖。

➤ **过程保障：**

主要关注涉及数据全生命周期的数据收集、存储、传输、使用、共享、出境、销毁各阶段对数据安全技术的利用和合规的落实，从而增强数据安全合规应对能力。数据收集是指从组织内部系统中新生产的数据，以及从外部组织收集数据的阶段。数据存储是指数据以任何形式在组织中进行存储的阶段。数据使用是指组织使用数据的阶段。数据加工是指在组织内部对数据进行再分析，加工的阶段。数据传输是指组织将数据传输的阶段。数据出镜是指向境外提供数据的阶段。数据公开是指向社会和市场公开数据的阶段。数据销毁是指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。数据全生命周期的指标和具体业务紧密相关，在评估过程中，对于不适用的阶段可以忽略。

**● 数据收集：**

关注数据收集合法正当，用户数据收集明示同意，其他已明确要求，停止收集。数据收集应遵循合法、正当、必要的原则，不应收集与其提供的服务无直接或无合理关联或超出个人信息主体明示同意期限的个人信息，且符合以下要求：应制定和公开个人信息保护政策并严格遵守；收集个人信息前，应明示个人信息保护政策，并征得个人信息主体同意；改变处理个人信息的目的、类型、范围、用途的，应及时告知个人信息主体，修改个人信息保护政策，并重新征得个人信息主体同意，涉及个人信息保护政策变动的应修改个人信息保护政策；明示所提供产品和服务类型，以及该类产品和服务所必需的个人信息，不应因用户拒绝提供该类产品和服务所必需的个人信息以外的信息，而拒绝提供该核心业务功能服务；不应仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为目的，强制要求、误导用户同意收集个人信息；收集个人敏感信息前，应征得个人信息主体的明示同意，确保明示同意是在完全知情的基础上 自主给出的、具体的、清晰明确的意愿表示；收集不满14周岁未成年人个人信息前，应征得其监护人的明示同意；从个人信息主体以外的其他途径获得个人信息的，应了解个人信息来源、个人信息提供方已获 得的个人信息处理的授权同意范围，并按照本标准的要求履行安全保护义务。数据提供方应在 确保其数据安全的基础上提供数据。具体评估实施方法如下：

数据收集合法正当，查验组织具体业务用户协议或隐私政策文件中业务功能及收集的个人信息，是否明确数据收集的目的、用途和范围，规范数据收集的流程和方法。查验组织数据采集相关制度文件是否明确数据采集渠道、数据格式、收集流程和收集方式；针对外部数据源，是否明确要求外部数据提供方说明数据来源，并对信息来源的合法性进行确认，确保数据收集渠道的合法性和正当性。查看隐私政策并注册使用该业务，验证是否按照国内法律法规相关要求，明示收集个人信息的目的、方式和范围，未经被收集者同意，不得收集与其提供的服务无关的个人信息。查验组织数据收集相关制度文件，是否建立数据收集的风险评估流程，针对收集的数据源、收集频度、收集渠道、收集方式、数据范围和类型进行风险评估；涉及收集个人信息的业务场景是否进一步依据相应的合规要求进行合规风险的评估，并防范收集过程中可能存在的数据泄漏风险。通过技术验证组织业务是否明确数据采集过程中个人信息的知悉范围和安全控制措施，确保收集过程中的个人信息不被泄露。查验数据收集合规报告，是否根据规则在业务系统中定期执行数据收集合规性查验。

用户数据收集明示同意，通过查验组织具体业务用户协议或隐私政策文件中业务功能及收集的个人信息，在发生用户信息收集时，组织是否按照公开透明原则，将收集规则以通俗易懂、简单明了的文字向用户明示。查验组织业务用户协议或隐私政策所述的业务功能及收集的个人信息，验证其是否存在单独以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，以默认授权、功能捆绑等形式强迫、误导用户数据主体同意收集用户数据的行为。组织如果通过在线方式进行用户个人敏感信息采集，通过技术验证业务是否使用有效加密手段保障用户在线提交信息的安全性。

停止收集，通过隐私政策或用户协议检查组织业务是否按照法律法规和相关标准要求，在停止运营产品或服务、用户终止服务等情况时，停止对用户数据的收集。通过技术验证组织业务是否为用户提供注销号码或账号的服务，并且在用户注销账号时不得设置过多不合理的注销条件（如需要提交非必要的个人敏感信息）。

**● 数据存储及传输：**

数据存储包括：存储重要数据和个人信息等敏感网络数据，应采用加密、安全存储、访问控制、安全审计等安全措施；存储重要数据和个人信息，不应超过与重要数据和个人信息主体约定的存储期限或个人信息主体授权同意有效期。 数据接收方存储数据时，应按要求采取安全措施并以合同进行约定。

数据传输，对数据传输活动采取安全措施，包括：传输重要数据和个人敏感信息时，应采用加密、脱敏等安全措施；传输向数据接收方提供的数据时，应按要求采取安全措施并以合同进行约定。

具体评估实施方法如下：

查验组织数据传输相关制度文件，是否根据法律法规、业务需求、业务系统可用性、建设成本等要求，明确需要传输加密的业务场景，明确关键网络设施的冗余部署，明确网络安全域划分策略；数据传输安全策略制定是否充分考虑了各数据存储平台系统网络规划设计、部署、维护管理和运营中的安全风险。查验组织数据传输相关制度文件，是否在数据分类分级定义的基础上，明确提出相匹配的数据加密传输要求，相关要求中是否包含对数据加密算法要求和密钥的管理要求。通过技术验证组织是否在安全边界配备数据访问控制措施；查验组织是否建立相应审批流程，对跨组织机构或使用互联网的数据传输事项进行前置审批。通过演示，查验组织业务系统是否提供对数据传输安全策略变更进行审核和监控的能力，是否部署对通道安全配置、密码算法配置、密钥管理等保护措施进行审核及监控的能力。查验组织数据接口管理规范文件，是否建立数据传输接口安全管理工作规范，明确技术管控措施；是否具备系统间接口的设备鉴权和认证能力，通过MAC地址、IP地址或端口号绑定等方式避免违规设备接入，实施数据流程控制、关键操作日志管理，包括接口名称、接口参数、接口安全要求等内容。查验组织数据接口管理规范文件，是否严格控制数据传输接口的新增需求。是否根据“安全三同步”要求，对于数据新增、改造接口在规划、设计、建设、运行、改造和维护过程中增加安全评审机制，定期对接口权限控制、传输等相关功能进行安全评估，配备相应传输接口管理和技术管控措施。查验组织数据存储环节相关制度文件，组织是否结合数据分类分级策略和管理要求明确数据存储安全策略和操作规程，包括数据存储系统差异化的安全存储保护手段（如加密、访问控制、数字水印、数字签名等）、数据存储介质安全策略和管理规定等。查验组织是否与数据存储系统管理和运维人员签订保密协议，是否在保密协议中明确数据使用范围、操作权限、违约责任等，有效约束相关人员行为，如对组织各类数据进行违规操作。

查验组织数据存储环节相关制度文件，组织是否制定各类数据存储系统的安全配置规则，明确对存储系统账号权限管理、访问控制、日志管理、加密管理、版本升级等方面的安全要求。查验组织数据存储环节相关制度文件，是否制定数据存储设备安全管理规范和操作规程，如维护操作流程、应急操作流程等。

通过技术验证组织数据存储系统及数据处理、传输设备是否部署在安全域内，是否限制直接提供公共互联网访问；查验其上线前是否经过安全验收以保证遵循统一的安全配置；对使用的外部数据存储系统是否进行有效的安全配置。"通过技术验证组织数据存储系统，是否按照数据访问权限管理制度，配备对用户或业务（应用程序）的访问控制措施，避免非授权访问。通过演示，查验组织业务涉及敏感数据存储系统的重大操作，是否纳入多人管控模式。

查验组织数据存储介质管理制度，是否明确购买或获取存储介质的规范流程，包括介质获取渠道、介质净化规程、介质销毁机制等内容。是否基于数据分类分级要求以及介质使用的要求，制定存储介质访问和使用安全策略和管理规范（含介质使用的审批、审计、异常处理等内容）。是否建立存储介质的标记规程，明确介质存储的数据对象，是否针对将数据下载到本地终端的行为进行严格审核和日志记录，对向移动介质输出数据的情况进行二次审核和日志记录。查验组织对存储介质使用的常规和随机检查流程，存储介质的使用是否遵守机构公布的关于介质的使用规范。查验组织备份恢复相关管理制度，组织是否包括数据备份的规范和操作规程，是否明确规定数据备份的周期、备份方式、备份地点规范，需要对数据恢复性验证机制进行明确说明。查验组织备份恢复相关管理制度，是否包括数据复制、备份与恢复定期检查等工作程序，工作程序说明是否包括但不限于：数据副本的更新频率、保存期限等。

* **数据使用：**

网络运营者利用个人信息和算法为用户提供定向推送信息服务的，应同时提供非定向推送信息服务的选项。应对接入其平台的第三方应用加强数据安全管理。对嵌入的第三方自动化工具，如软件开发工具包（SDK）、第三方代码、组件、脚本、 接口、算法模型等，宜开展技术检测确保其个人信息处理行为符合双方约定要求，对审计发现超出双方 约定的行为及时停止接入。开展转换、汇聚、分析等数据加工过程中，知道或者应知道可能危害国家安全、公共安 全、经济安全和社会稳定的，应立即停止加工活动，并根据相关法律法规按要求向有关部门报告。具体评估实施方法如下：

查验组织数据使用管理制度，组织是否明确了数据使用安全策略和操作规程。查验组织业务支撑系统是否提供停止定向推送信息的功能，用户选择停止接收定向推送信息时，是否停止推送信息，并为用户提供删除或匿名化定向推送所基于用户数据的必要选项。查验组织分析利用所掌握的数据资源，发布市场预测、统计信息、用户信用等信息，是否遵循国家相关法律法规要求，是否存在发布虚假信息、损害他人合法权益等情况。查验组织数据使用管理制度，是否明确大数据分析结果输出和使用的安全检查、合规风险评估和授权流程，避免分析结果输出中包含可恢复的个人信息、重要数据等数据和结构标识，从而防止个人信息、重要数据等敏感信息的泄漏。查验组织数据使用相关日志记录，是否对数据使用操作进行记录，以备对分析结果质量和可信性进行数据溯源。通过演示，查验组织业务和业务支撑系统，是否具备信息化技术手段或机制，对违规使用数据的行为进行有效的识别、监控和预警。

● 数据共享：

共享重要数据，应与数据接收方通过合同等形式明确双方的数据安全保护责任和义务，采取加密、脱敏等措施保障重要数据安全；委托第三方开展数据加工活动的，应与第三方通过合同等形式明确双方的保护责任和义务，并 要求第三方以合同中约定的形式返还、删除接收和产生的数据；发生兼并、重组、破产时，数据接收方应继续履行相关数据安全保护义务；没有数据接收方的， 应对数据作删除处理。具体评估实施方法如下：

查验组织数据开放共享相关制度文件，是否区分数据开放共享场景，对应不同的数据开放共享场景建立相应的数据开放共享安全策略和操作规程，明确数据开放共享范围、内容与有效控制机制。查验组织数据开放共享相关业务系统的审批记录，是否建立数据开放共享的审核制度和规范的数据共享审核流程，审核开放共享数据的数据内容，确认属于满足数据开放共享业务场景的需求范围及未超出授权范围开放共享数据。查验组织数据开放共享相关业务系统的审计记录，是否落实数据开放共享安全审计制度，审计结果至少留存6个月备查。查验组织保密协议或合作合同，是否通过保密协议等方式明确数据开放共享双方应承担的安全责任，应具备的数据保护手段、限制数据使用范围和场景等。通过技术验证组织数据共享相关业务系统，是否具备数据开放共享场景下的数据溯源方法（如对数据进行签名、添加数字水印等），防止数据被恶意删除、随意篡改和滥用。对于包含个人敏感信息的数据，是否能够及时跟踪、记录数据流向、数据接收者信息、处理操作等信息，保障出现数据安全问题时，能够分析问题根因，追查数据出现问题的环节和责任人。查验组织接口规范相关制度文件，是否针对涉及个人信息的应用开放接口进行有效管理，是否记录接口的访问参数，如账号、内容等信息，并进行必要的关联分析，防止数据滥用、数据窃取等行为。查验组织与数据开放共享接口调用方签署的合作协议，是否在合作协议中明确了对数据的使用目的、供应方式、保密约定等。

查验组织数据接口管理制度及数据接口清查记录，是否定期对本组织对外数据接口进行清查，是否对不符合要求的对外数据接口立刻予以关停。"查验组织对数据开放共享接收者资质审核的相关材料，是否对数据接收者资质能力进行审核、评估，确保接收者的合规性，保障用户数据在开放共享过程中的安全，是否通过合同明确用户数据接收者对用户数据的安全保密责任。通过演示，查验组织业务，是否在用户端（如网站、APP、账单、业务登记单、显示屏幕等展示场景）显示个人敏感信息时，采取去标识化处理等措施防止个人信息主体之外的其他人员未经授权获取个人敏感信息。个人信息主体身份验证通过或者主动选择后，可完整查看个人敏感信息。查验组织开放共享个人信息情况记录，比对业务用户协议或隐私政策文件，核验组织在经法律授权或具备合理事由确需开放共享时，是否违背采集阶段告知的使用目的，或超出告知的使用范围开放共享。通过系统演示，组织是否提供合理有效的措施帮助个人信息主体了解数据接收方对个人信息的保存、使用等情况，并保障个人信息主体的权利，例如，查询、访问、更正、删除、注销账户、撤回已同意的授权等。

* **数据出境：**

向境外提供个人信息或者重要数据的，应遵循国家相关规定和相关标准的要求。 境内用户在境内访问境内网络的，其流量不应路由至境外。组织存在数据传输出境时，是否按照国家网信部门、国务院等有关部门制定的办法和相关规定要求，在数据出境前进行数据跨境传输安全评估。

* **数据销毁：**

具体评估实施方法：查验组织数据销毁相关制度文件，是否结合数据分类分级管理制度和安全需求，建立数据销毁安全策略和操作规程，明确销毁对象、原因（如数据业务下线、用户退出服务、节点失效、过多备份、数据试用结束、超出数据保存期限等）和流程、存储介质销毁处理策略和操作规程。查验组织数据销毁相关制度文件，是否建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程；查验组织数据销毁记录文件，是否留存审批记录，留存时间是否满足6个月。通过演示，查验组织业务和业务支撑系统是否针对数据销毁建立完善的操作审批机制，采用多人操作模式，限制单人拥有完整操作权限。查验组织数据销毁相关制度文件，是否依据介质存储内容的重要性明确符合组织机构业务需求和法律合规需求的各类数据销毁场景、销毁手段及销毁流程，并留存销毁记录，如针对网络存储数据以及针对闪存、硬盘、磁带、光盘等存储数据所采用的数据销毁的方法和技术，采用相应的销毁策略与机制。查验数据销毁效果验证相关工作文档，数据销毁后是否保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配前得到完全清除，不可恢复。通过演示查验组织业务支撑系统是否提供了与数据销毁制度配套的各类数据销毁的技术工具（如针对网络存储数据、针对闪存、硬盘、磁带、光盘等存储数据），从而供数据销毁的执行人员执行数据的销毁，确保以不可逆方式销毁数据及其副本内容，保证对同类场景下的数据销毁效果的一致性。查验组织个人信息的销毁安全制度文件、业务用户协议或隐私政策文件，是否在制度中明确并通过业务用户协议或隐私政策文件与用户进行约定。

**1.3数据安全合规实施流程**

这部分主要说明现场评估实施流程

**现场评估实施包括准备环境、实施现场评估、输出评估结果、问题回顾、复评复测五个阶段。**

➤ 准备环境：

评估方在进行评估之前需要和被评估方展开充分沟通，形成一致意见，为评估工作做好环境准备，并对评估环境进行充分有效的说明，以保证评估方有效顺利开展评估工作。

**➤ 实施评估：**

评估方在现场评估时，应通过召开启动会了解被评估方的评估环境，以便展开评估工作。评估方应严格按照评估实施流程展开，可采取会议、询问、现场演示、配合技术手段对评估环境进行检查和核实等方式开展评估工作。被评估组织在评估过程中应积极配合评估方的工作，并及时对评估过程中出现的问题进行有效解决。

**➤ 输出评估结果：**

评估结束后，评估方应按照数据安全合规评估要求对所涉及应用场景下的各类问题进行汇总、并对问题引起的安全合规风险进行说明，出具评估结果。同时评估方与被评估方需要针对评估结果交换意见，就评估情况达成一致，完成数据安全合规评估报告。报告内容应包括评估工作总结、评分指标项、现状及整改措施等内容。

**➤ 问题回顾：**

被评估方应根据评估报告和建议，制定整改计划，落实整改措施，在整改过程中，对整改计划完成情况进行及时的总结，及时完善修改整改计划。

**➤ 复评复测：**

被评估方在规定时间内完成整改之后，向评估方提出复评申请。复评时，被评估组织应提供整改工作报告，部分整改和未完成整改的项目应逐项说明原因。评估方也应对现场评估发现的问题逐一进行查评，结束后提交数据安全合规复查评估报告。

#### 2.大数据价值评估

随着数字技术的日益成熟和应用场景的不断拓展[10]，数据的变现能力逐渐增强，成为与劳动力、土地、资本并驾齐驱的新型生产要素和驱动经济社会发展的战略资源。一方面，数据加快产业的数字化与智能化转型[11]，推动新模式新业态走向成熟，为经济增长注入新的活力。另一方面，数据成为政府管理和社会治理创新的重要驱动力，对提升政府治理效能，增进人民福祉，促进社会发展发挥了重要作用。

据统计，我国预计2021年底，数据中心市场规模会达到2486亿元。未来，随着新基建政策的逐渐落地、互联网及云计算大客户需求的不断扩张，数据中心行业将实现高速增长，预计到2025年，我国数据中心市场规模达到5952亿元，我国将成为全球最大的数据圈。麦肯锡预测，数据将成为新一代的生产要素带动生产力的增长和经济的飞速发展。贵阳大数据交易所的成立以及2021年国务院政府工作报告中提出要加快数字化发展[12]，打造数字经济新优势，协同推进数字产业化和产业数字化转型，这些都标志着我国已经真正开始正视数据所带来的价值。因此，研究如何将我国的数据资源优势转化成数据价值优势，为经济增长注入更多活力具有重要意义。

大数据价值相关的研究是从近几年才开始，还处于探索阶段，具体落地很少。国家已经从政府层面开始着力规划数据，挖掘数据背后的价值，说明未来数据一定会成为新一代的体现组织核心竞争力的信息资源，类似于组织的固定资产为组织带来经济利益的流入。

当前大数据的类别相当多，单从政务数据这一大分类开看，当前各地区大都组建了大数据管理局、政务服务数据管理局等政务数据集中管理机构，但是由于各地大数据管理机构设置的职能和权责范围都有一定的差异性，也暂未建立数据共享、数据开放、数据开发利用等具体详细的规范，导致政务数据使用、管理权限等权责规范不明确，各单位部门积极性不高，数据采集和业务部门配合度不高，最终导数据采集效率低、时间长，共享更新频次少，共享力度小、数据质量不高、开放内容范围少等问题，使其难以发挥数据应有的价值，最终即使共享了也基本无法对数据进行深入挖掘使用或不知道怎样使用。各地方、各级政务部门系统间目前依旧存在数据各项定义规范不一致等问题，上传到各政务数据共享平台的数据标准也不相同，会导致共享数据缺乏关键要素信息 , 而使数据在应用中的价值较低，制约了数据发挥应有的价值，降低了政务数据的价值，更无法为决策提供支撑。

而将数据资产列入组织的资产负债表，必然会涉及到数据资产的价值衡量，有专家学者提出利用贵阳大数据交易所数据的交易金额作为该项数据的公允价值，采用公允价值的计量模式对其进行后续计量，但是目前数据的种类繁多，虽然贵阳大数据交易所目前发展的势头相当不错，但是由于成立时间较短加上互联网近几年的发展已经产生很多种类的数据，交易所的数据所涵盖的种类还不太全面，不可能涵盖市场上出现的每一种数据，当大数据没有公允价值时，应该如何入账。研究大数据资产的估值，对于未来数据资产进入组织的资产负债表当中的所列式的金额有一定的参考作用[13]。

已有研究[14][15][16]，大多将大数据作为一种资产在定性上将其归为一项无形资产来核算。目前交易所的数据处理方法主要是拍卖法，所以在定性上将组织自行产生的大数据作为无形资产进行计量。大数据随着科技的不断进步出现的一种新型财产权客体，说明大数据资产相关权利与知识产权不同，将其归为技术型的无形资产。所以相比知识产权的价值，有其特殊性。根据无形资产的定义若是将其定义为无形资产，必须满足“能够从组织当中划分出来”和“可辨认性”的特点，数据作为资产来说，仅仅只有一小部分满足无形资产的定义，所以将其归为无形资产采用无形资产的价值评估方法不符合会计原则中的可靠性。

需要指出的是，数据价值与一般无形资产价值的构成不同，数据价值的形成具有生产的一次性、加工处理的多性、成本费用的多源性、获益的较大不确定性、价值转化的风险性、数据应用的不同等特点，导致数据价值评估需要考虑诸多影响因素，具有高复杂性和高难度性，很难有通用的评估方法。

社会数字化转型进程加快，数据管理面临的环境更加复杂，为了更好评估数据的价值，需要加强五个方面的协同：一是优化服务模式，提高一站式的数据管理能力；二是升级企业标准；三是融合新兴技术；四是创新运营机制；五是升级安全能力。

Gartner[17][18]指出，当疫情来袭时，传统技术分析公司意识到这些技术严重依赖大量的历史数据。因为这些模型中的许多模型已经不再适用。从本质上讲，疫情改变了一切，大量的数据失去作用。如何能更好的发挥数据的价值异常重要。

同时，数据的收集、传输、处理过程的环节多，各环节常反复出现。数据成本构成较复杂，各构成部分相互关联耦合。数据的经济效益难测算，数据的价值转化或确认过程存在不确定性等。这些特点导致数据价值评估难以标准化，也不宜考虑单一因素做简单化处理，而要紧密结合数据价值基本特性，综合多因素分阶段开展分析评估。数据价值评估指标体系主要考虑数据不同特性对价值的影响，对数据价值评估指标体系构建的研究工作较少。

研究数据价值评估的意义和重要性不容置疑，同时由于数据的独特特性，导致数据价值评估的挑战也非常大。因此本项目紧密结合大数据的特点构建一种复合性的大数据价值框架和评估体系，力求为现实组织之后对大数据价值评估提供一种可行的方法体系。

狭义的数据价值是指数据的经济效益，广义的数据价值是在经济效益之外，考虑数据的业务效益、成本计量等因素，我们聚焦于广义的数据价值。数据价值评估是指通过构建价值评估体系，计量数据的经济效益、业务效益、投入成本等活动。数据价值评估是数据资产管理的关键环节，是数据资产化的价值基线。目前，国内外相关标准化组织、财会领域组织、技术咨询服务企业均从多个视角开展积极探索研究，相关研究成果见下表3。

表2 国内外关于数据价值评估研究总结

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 时间 | 研究单位 | 单位性质 | 成果 | 价值 |
| 2021 | 中国信息通信研究院 | 工业和信息化部直属科研事业单位 | 数据价值化与数据要素市场发展报告[19] | 建立了数据价值化的“三化”框架，即数据资源化、数据资产化、数据资本化。 |
| 2021 | 中国信息通信研究院 | 工业和信息化部直属科研事业单位 | 数据资产管理实践白皮书（5.0版）[20] | 以数据资产赋能业务发展作为核心逻辑，阐述数据资产管理的概念内涵、演进历程、发展现状，重点讨论数据资产管理的活动职能、保障措施、实践步骤等 |
| 2020 | 国家标准化管理委员会  | 中国标 准化组 织 | 电子商务数据资产评估指标体系 （GB/T 37550-2019）[21] | 提出数据资产应用效果的分 析，考虑数据资产的使用象、 使用次数和使用效果评价在 评估数据资产的运营效果时有参考价值。 |
| 2020 | 中国资产评估协会 | 财政部下属行业组织 | 数据资产的资产评估专家指引[22] | 作为资产评估专业机构，其提出的三种评估方式在数据资产的经济价值衡量中具有权威性以及可落地性。 |
| 2020 | Gartner | 全球技术咨询服务公司 | 提出市场价值、经济价值、内在价值、业务价值、绩效价值、成本价值、废弃价值、风险价值共八大维度的信息资产价值评估模型。 | 从多角度评估数据资产的多方面价值，分析维度较完整，具有很强参考价值。具体价值评估指标设计含义模糊、数据来源及计算方式笼统，不具有落地性。 |
| 2020 | 普华永道 | 全球技术咨询服务公司 | 提出报表、BI 类应用经济价值评估方式[16] | 采用了多步式方法评估 BI 应用对组织的影响，其测算出的经济价值相关参数具有一定参考价值 |
| 2019 | 阿里研究院 | 中国技术咨询服务公司 | 数据资产化之路 数据资产的估值与行业实践[23] | 将数据资产与无形资产进行对比，探索无形资产评估方法在数据资产中运用的可行性。以方法论的形式提出评估方法，未考虑估值方法的可落地性。 |

多数企业在数据资产定价方面的尝试，具有一定的局限性，集中表现在两个方面。一是数据资产定价并未完全得到财务部门认可，尚未计入企业资产负债表；二是由于当前国内数据交易市场并不成熟，数据定价仍以合同形式对单笔交易进行约定，因此，数据定价标准的权威性与通用性受限。此外，从数据资产管理目的出发，我们在关注数据资产的“有形”价值之外，不应忽视数据资产的“无形”价值。

针对以上挑战，本部分主要做了以下工作：

● 提出数据价值评估的实施流程。

● 研究数据价值评估指标体系构建方法。

● 针对数据价值评估适用的方法进行系统研究。

**2.1数据价值评估的实施流程**

针对特定的数据价值评估项目，可以按两个阶段开展：

第一阶段，主要解决数据价值评估机制和指标体系的确定。基本确定数据价值评估的目的、范围、要求、数据类别和合规性，确定数据价值评估的指标。基本掌握数据质量（包括进展1中对数据安全合规的评估结果）情况以及数据价值影响主要因素。在数据价值量化机制确定阶段，需要对数据的生产成本形成定性认识，如：此数据的形成是人力消耗为主，还是物质、能量消耗为主，两者的大致比例如何；还需要对数据的应用价值具有基本认识，如：是否带来了成本的减少或收入的提升，产生的应用价值主要涵盖哪些方面，各方面的可量化程度及相关依据是否可获得等。

第二阶段：数据价值量化评估不可能有通用方法，价值评估指标构建完成后，应该结合数据特性、规格、评估目的以及供需双方的意见进行具体分析，确定合适的量化机制。应当从数据的实际场景出发，结合通用指标，具体情况具体分析。同时充分考虑分级分类分区、定性定量、主观客观、市场属性非市场属性、应用成本相结合的方法。

**2.2数据价值指标评估体系构建方法研究**

数据价值评估指标构建体系从市场角度来看，可通过三种方法构建：

● 成本法

在大数据价值的评估方法中，成本法是从资产的重置角度考虑数据价值的一种方法。成本法将提取数据价值的成本视为数据资产的价值，成本法从资产的重置角度出发，重点考虑资产价值与重新获取或建立该资产所需成本之间的相关程度。重置成本需要重点考虑大数据的价值与成本的关系，数据具有无时无刻都在不断变化的特性，所以依据成本法对数据价值进行评估具有一定的局限性，数据成本不易区分、贬值因素不易评估和没有办法体现数据可以产生的收益。具体使用时，通过数据成本和数据费用来确定数据资产的价值，加入AHP确定影响数据资产价值的各项因素的权重，再结合专家打分进一步确定出数据价值的评估值。目前有关成本法是否适用于大数据资产价值的评估”争议比较大。

● 市场法

市场法是在当前市场寻找相同或相似类别和应用场景的数据，对其价值进行调整的一种评估方法。市场法衡量数据资产的市场交易价格或数据密集型组织的市场溢价。目前，由于数据交易、数据服务和数据流通尚未成熟，市场法并未得到广泛的应用，多数组织将数据存储计算作为成本计量维度，将数据使用热度作为收益计量维度，并通过建立动态的估值模型，实现主观与客观相结合的数据价值评估。随着未来大数据交易市场的活跃，在市场上寻找相同或相似的数据，引入层次分析法对数据价值影响因素进行修正，最后对其进行差异化调整得到数据的价值。在评估平台数据价值时，可考虑在评估中引入平台活跃系数对其价值进行衡量，再根据市场的情况对数据价值进行调整，来最终确定数据资产的价值。此外，在市场法的基础上使用灰色关联法量化数据价值的影响因素，确定每个因素对数据价值的影响，计算被估数据的价值。鉴于目前大数据交易还不太完善，使用市场法也存在不少问题，如市场上对大数据交易大多都属于私下秘密交易，交易的信息相对不透明，可能会导致大数据的价值偏离正常的市场价值。

● 收益法

收益法是对未来预期的经济利益的流入求取现值的方法，即计算数据价值链上因数据资产产生的增量现金流，收益法基于目标资产的预期应用场景，通过未来产生的经济效益的折现反映数据资产在投入使用后的收益能力。收益法在数据价值评估的过程中主要用到未来数据所产生的收益、折现率的确定以及未来的收益时限三个主要的指标，这个指标决定着数据价值。然而由于大数据资产的特殊性和收益法使用条件的苛刻性，在数据价值实际评估中，数据超额收益难以确定导致评估难以进行，而且组织数据通常会和组织的产品一块带来收益，因此很难区分那些是数据带来的价值。

综上，从市场角度考虑的价值评估指标体系构建方法中所采用的成本法无法体现数据资产产生的收益；市场法需要存在较为成熟的市场作为基础，但目前我国数据市场还不太成熟，相应的参数指标不容易获取。相比来说，若是未来大数据的预期收益可以有更好的解决方法，解决了收益法中三个指标问题，采用收益法进行数据价值评估是一种较为成熟且评估的结果更为准确的方法。

从非市场角度考虑数据价值评估指标体系的构建，可通过条件价值法，即通过调查公民对数据开放共享和隐私保护的价值判断来衡量数据的社会价值。也可通过专家讨论会衡量数据的社会价值和非市场价值。是按数据应用后带来的直接和间接效益考虑。数据应用项带来的价值计量，围绕数据应用产生的直接、间接效益结合流通情况来估算。直接效益，是指由于数据应用给城市、组织带来经济效益的增长，这种效益与各类正向效能统计量呈正相关，包括 GDP数、组织营收、成本的降低值等。数据应用还会产生巨大的社会效益，如，促进社会资源的优化配置，数据的流动和融通加速人、物质、能量等各种要素的流动和融通等，此种效益相对间接。量化数据应用效能，可结合数据价值评估调查，对比数据应用前后的变化，在具体场景中充分探讨数据应用给使用者带来的“红利”，从而核算直接效益。一般来说有两种情况，一是给数据用户带来营收和利润增长，二是给数据用户节省成本。这两种情况都是直接效益，通过财务分析可得出。具体核计时，应结合实际情况，评判数据是否决定性或主导因素，如确为决定性因素，则通过核计营收的增加量和成本的减少量，然后据此对数据价值做量化，数据应用从宏观视角来看，还会带来社会层面的间接效益。这种效益难以直接做经济核算，但却是真实和明显的。

在政府层面，削减了公共开支，更好地发挥了政府作用；在组织层面，降低了组织制度性交易成本，便利了组织和民众。整体来说，政府通过优化办事流程、整合政务资源、融合线上线下服务，营造了稳定、公平、透明、可预期的营商环境。组织通过业务数据的应用，实现组织产品和运营的智能化，也能提高组织的整体效能。但是，这些社会效益难以量化，采用数据应用效能法做直接与间接效益量化时，可以通过简化问题，以直接效益为主，对相关各类效益分项应计尽计，然后再结合数据应用实际场景，估测间接效益相对直接效益的倍数，经过充分的市场实践，逐渐完善量化机制。

**2.3数据价值量化评估阶段**

数据价值量化评估不可能有通用方法，价值评估指标构建完成后，应该结合数据特性、规格、评估目的、以及特定行业的实践工作[15]以及供需双方的意见进行具体分析，确定合适的量化机制。数据价值评估应遵循真实、准确、客观、有效的原则，确认数据价值评估各项指标信息，并在相关利益方确认后，作为实际评估实施的输入值。评估实施者应当根据评价目的、评价对象、价值类型、信息收集情况等相关条件，分析多种方法对本次数据价值评估实施的适用性，恰当选择一种或者多种评价方法，对数据价值进行评估。同样的指标体系，使用不同的评估方法会产生不同的结果，应对所获得各种价值结论进行比较分析，形成合理的评估结论，并形成数据价值评估报告。

具体方法包括层次分析法、专家打分法，以及层次分析法+模糊综合评价法等方法。

**➤** 使用层次分析法计算数据价值指数的步骤如下。

● 构建数据价值评价指标体系。

● 构造标度表。对于各个指标的权重，采取两两因素比较的专家打分法。在对两个因素进行比较时，需要有定量的标度。可以采用标度表方法，标度表见表3。

表3 标度表

|  |  |
| --- | --- |
| 标度 | 含义 |
| 1 | 两个因素同等重要 |
| 3 | 一个因素比另一个因素稍微重要 |
| 5 | 一个因素比另一个因素明显重要 |
| 7 | 一个因素比另一个因素强烈重要 |
| 9 | 一个因素比另一个因素极端重要 |
| 2、4、6、8 | 上述相邻判断的中值 |

● 构造各级比较判断矩阵，并进行一致性检验。对评估指标采用专家打分法，按照重要程度进行两两比较，构造比较判断矩阵，

● 计算各一级指标和二级指标的权重。

● 进行二级指标评分。

● 加权计算一级指标分数。

● 加权计算数据价值评估分数。

**➤** 使用层次分析法+模糊综合评价法评估数据价值的步骤如下。

● 构建数据价值评估指标体系。

● 构造标度表。

● 构造各级比较判断矩阵，并进行一致性检验。

● 计算一级指标和二级指标的权重。

● 构造数据资产模糊评价表，得到各一级指标对应的二级模糊评价矩阵。

● 将二级指标权重向量乘以二级模糊评价矩阵，得到一级指标模糊评价向量。

● 一级指标模糊评价向量构成一级模糊评价矩阵：

● 将一级指标权重向量乘以一级模糊评价矩阵，得到数据资产价值综合模糊评价向量：

● 构造分数对照表。

● 将综合模糊评价向量乘以分数对照表，得到数据价值评估分数。

**➤** 专家打分法是指通过召开专家研讨会，为评估指标打分。采用专家打分法，如打分规则确定为百分制：81~100分记为强；61~80分记为较强；41~60分记为较弱；40分及以下记为弱。邀请10位专家进行打分，根据打分结果构造数据价值评估维度的模糊评价表。

## 三、国内外学术合作交流等情况

在项目实施期间，项目组有序组织项目参与人员进行了多次系列研讨，开了4次内部学术交流和讨论；

参加全球智慧城市会议。

参加国内外知名学者举办相关学术报告。

## 四、存在的问题、建议及其他需要说明的情况

我们下一步工作的研究重点是继续实践现有数据安全合规体系评估。构建价值评估体系的实践应用，并通过实际应用来检验评估体系。

## 五、项目取得成果的总体情况

项目组按照本项目的申报计划书开展各项研究工作取得了一系列的创新性研究成果。

依托本项目，已形成相关论文1篇，评估报告1份。

论文《基于密钥组合的隐私数据保护方案》

《数据流通平台安全合规评估》报告

## 参考文献

1. [1]中共中央 国务院. 关于构建更加完善的要素市场化配置体制机制的意见[EB/OL]．http://www.gov.cn/zhengce/2020-04/09/content\_5500622.htm，2020年3月30日.
2. [2]于施洋．我国构建数据新型要素市场体系面临的挑战与对策［J］．电子政务，2020(03)：P2-12．
3. [3]中国信息通信研究院. 数据安全治理实践指南［R］. 北京：中国信息通信研究院，2021.
4. [4]凃云杰. 大数据时代的数据安全与隐私保护问题研究[J]. 无线互联科技,2019(08):155-156.
5. [5]DAMA中国分会. DAMA数据管理知识体系指南［M］. DAMA国际. 北京：机械工业出版社, 2020年版.
6. [6]GB/T 36073-2018．数据管理能力成熟度评估模型[S].北京：国家标准化管理委员会，2018.
7. [7]JR/T 0218-2021．金融业数据治理能力建设指引[S].北京：中国人民银行，2021.
8. [8]JR/T 0158-2018．证券期货业数据安全分级[S].北京：中国人民银行，2018.
9. [9]GB/T 18391.1-2009．信息技术 元数据注册系统(MDR) 第1部分：框架[S].北京：国家标准化管理委员会，2009.
10. [10]周良军、邓斌. 华为数字化转型［M］. 北京：人民邮电出版社，2021年版.
11. [11]IBM. Deliver Business Ready Data Fast with DataOps[EB/OL]. https://www.ibm.com/downloads/cas/GLNAZBXN，2020.
12. [12]贵阳大数据交易所. 中国大数据交易产业白皮书[Z], 2016.
13. [13]戴炳荣 , 闭珊珊 , 杨琳 , 纪婷婷，陈美. 数据资产标准研究进展与建议[J]. 大数据 , 2020(3): 36-44.
14. [14]朱晓武、黄绍进. 数据权益资产化与监管［M］. 北京：人民邮电出版社，2020年版.
15. [15]上海浦东发展银行，IBM，中国信息通信研究院. 商业银行数据资产管理体系建设实践报告［R］. 北京：上海浦东发展银行，IBM，中国信息通信研究院，2021.
16. [16]普华永道．数据资产化前瞻性研究报告［R］. 北京：普华永道，2021．
17. [17]Gartner. 2021年十大数据和分析趋势[EB/OL]. http://www.eepw.com.cn/article/202103/423843.htm，2021．
18. [18]Gartner. Hype Cycle for Data Management,2021[EB/OL]. https://www.gartner.com/en/documents/4004072-hype-cycle-for-data-management-2021，2021．
19. [19]中国信息通信研究院. 数据价值化与数据要素市场发展报告［R］. 北京：中国信息通信研究院，2021.
20. [20]中国信息通信研究院. 数据资产管理实践白皮书（5.0版）［R］. 北京：中国信息通信研究院，2021.
21. [21]GB/T 37550-2019．电子商务数据资产评估指标体系 [S].北京：国家标准化管理委员会，2020.
22. [22]中国资产评估协会. 数据资产的资产评估专家指引［R］. 北京：中国资产评估协会，2020.
23. [23]阿里研究院．数据资产的估值与行业实践［R］. 杭州：阿里研究院，2019．

|  |
| --- |
| **项目组成员** |
| 王笑强 | 信息与网络安全部，高级工程师 |
| 张 羽 | 信息与网络安全部，高级工程师 |
| 李 冉 | 信息与网络安全部，工程师 |