

## 业务驱动的数据跨境风险机理研究

荣景峰<sup>1,2</sup>, 陈思宇<sup>1,2</sup>, 王艺洋<sup>2,3</sup>, 牛俊<sup>3</sup>, 刘徐杰<sup>4</sup>, 周安顺<sup>5,6</sup>, 付安民<sup>7</sup>, 曹春杰<sup>1</sup>, 张玉清<sup>1,2,3</sup>

(1. 海南大学网络空间安全学院, 海南 海口 570228; 2. 国家计算机网络入侵防范中心 (中国科学院大学), 北京 101408;

3. 西安电子科技大学网络与信息安全学院, 陕西 西安 710126; 4. 中国移动通信集团海南有限公司, 海南 海口 570311;

5. 南京邮电大学信息与通信学院, 江苏 南京 210023; 6. 中讯邮电咨询设计院有限公司, 北京 100089;

7. 南京理工大学计算机科学与技术学院, 江苏 南京 210023)

**摘要:** 针对当前数据安全风险机理研究未能充分考虑跨境数据特有的风险形成原因及要素, 难以全面揭示跨境数据风险的全貌与内在联系等问题。为此, 提出了基于业务驱动的数据跨境风险机理研究。首先, 应用 Petri 网抽象业务流程并收集过程资料数据。然后, 基于过程资料数据抽取相关概念范畴并映射成演化网络叶子节点, 同时依据风险因果理论构建风险演化网络。在此基础上, 分析计算风险演化网络的相关系数, 确定风险要素并系统阐释数据跨境风险机理的形成与演化过程。最后以调查问卷和历史数据分析方式验证分析结论, 结果表明研究结论符合调研数据统计结果且与历史风险诱因高度契合。总体而言, 所提研究可以为数据跨境风险量化评估提供理论支持, 并为数据跨境风险应对提供决策依据。

**关键词:** 数据跨境风险机理; 风险要素; 数据跨境有序流动; 数据安全

**中图分类号:** TP309.2

**文献标志码:** A

**DOI:** 10.11959/j.issn.1000-436x.2025105

## Business driven data cross border risk mechanism research

RONG Jingfeng<sup>1,2</sup>, CHEN Siyu<sup>1,2</sup>, WANG Yiyang<sup>2,3</sup>, NIU Jun<sup>3</sup>, LIU Xujie<sup>4</sup>, ZHOU Anshun<sup>5,6</sup>,  
FU Anmin<sup>7</sup>, CAO Chunjie<sup>1</sup>, ZHANG Yuqing<sup>1,2,3</sup>

1. College of Cyberspace Security, Hainan University, Haikou 570228, China

2. National Computer Network Intrusion Protection Center (University of Chinese Academy of Sciences), Beijing 101408, China

3. School of Cyber Engineering, Xidian University, Xi'an 710126, China

4. China Mobile Communications Group Hainan Co., Ltd., Haikou 570311, China

5. School of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

6. China Unicom (Hainan) Innovation Research Institute, Beijing 100089, China

7. School of Computer Science and Technology, Nanjing University of Technology, Nanjing 210023, China

**Abstract:** Existing research on data security risk mechanisms had not fully accounted for the unique formation causes and elements of cross-border data risks, limiting our understanding of their overall landscape and internal connections. In response, a business-driven approach was proposed to analyze cross-border data risk mechanisms. Firstly, Petri nets were employed to abstract business processes and collect process data. Then, relevant conceptual categories were extracted and mapped to the leaf nodes of an evolving network. A risk evolution network was constructed based on risk causation theory, and its correlation coefficients were analyzed to identify key risk elements and elucidate the formation and evolution processes of cross-border data risks. Questionnaire surveys and historical data analysis validate the research findings, showing alignment with survey statistics and historical risk drivers. Overall, the proposed research offers theoretical support for the quantitative assessment of cross-border data risks and provides a decision-making basis for their management.

**Keywords:** data cross-border risk mechanism, risk factor, orderly cross-border flow of data, data security

收稿日期: 2024-10-27; 修回日期: 2025-03-31

通信作者: 张玉清, zhangyq@nipc.org.cn

基金项目: 国家重点研发计划基金资助项目 (No.2023YFB3106400)

**Foundation Item:** The National Key Research and Development Program of China (No.2023YFB3106400)

## 0 引言

数据要素已经成为继土地、劳动力、技术和资本之后的第五大生产要素，其价值体现在数据流通、数据资源交换等方面。在文化、经济、贸易等领域的国际交流不断加深的背景下，数据要素作为各项活动的重要载体，彰显出其重要地位。根据调研机构麦肯锡的一项调查测算显示，全球数据流动量每增加 10%，将带动国内生产总值显著提升 0.2 个百分点<sup>[1]</sup>。可见数据的跨境流动已经成为推动全球化发展的重要驱动力。

目前，各国政府已经将数据要素的安全保护提升至国家战略级别，如欧盟推出通用数据保护条例（GDPR, general data protection regulation）法案<sup>[2]</sup>，旨在保障欧盟范围内个人数据安全以及数据主体在数据跨境过程中的权益。美国政府依据《国际紧急经济权力法》<sup>[3]</sup>（IEEPA, international emergency economic powers act）发布一项行政命令，限制向中国和俄罗斯等 6 国出售美国所谓的“敏感数据”。截至 2025 年 4 月，全球已经有超过 120 个国家已经完成或即将完成数据保护和隐私立法，其充分表明各国政府对数据要素安全保护的重视程度。

尽管相关各国相继出台了数据要素保护方案。但是跨境数据因其参与方较多、供应链路长、场景复杂多变等特点，其安全薄弱环节较多，容易引发数据安全风险事故甚至危及国家主权和政治安全。为此，相关学者专家从法学、经济学、计算机科学、图书情报等多学科视角<sup>[4]</sup>，对数据跨境安全展开深入研究。

为全面掌握数据跨境风险机理的研究进展，本文分别对国内外相关研究文献进行系统性梳理与检索，检索时间截至 2025 年 4 月。在国内，本文依托中国知网、万方数据等主流知识数据库，检索近五年内与“风险机理”主题相关的核心期刊文献。结果显示，中国知网收录相关核心期刊论文 181 篇，万方数据收录 25 篇。在此基础上，进一步以“数据”为主题检索相关论文，结果显示，中国知网收录论文 58 篇，万方数据收录论文 13 篇。对上述论文进行人工筛选，发现与数据跨境风险机理直接相关的论文 0 篇。在国外，依托 IEEE Xplore、EI、SCI、arXiv 等主流学术数据库进行检索，并结合人工筛查。结果显示所获文献均未与数据跨境风险机理主题形成直接关联。综上所述，当前国内外尚未有针

对数据跨境风险机理开展专项研究的文献成果。

风险机理是风险研究的基础，可以丰富相关领域风险研究的理论基础。当前已有数据安全风险机理研究，因其未能充分考虑跨境数据特有的风险形成原因和关键要素。同时，在风险相关者方面亦未充分考虑跨境数据风险对国家层面安全威胁的潜在影响，进而导致现有文献在数据跨境风险机理方面存在显著不足，难以全面揭示跨境数据风险的全貌与内在联系，特别是内部隐患、外部威胁以及自身脆弱性等关键问题。

为解决上述问题，本文基于 Petri 建模语言对数据跨境业务流程展开建模分析，并在此基础上采用扎根理论（GT, grounded theory）、复杂网络分析法和风险事故致因“2-4”模型<sup>[5]</sup>，完成风险致因的因果关系演化网络构建，进一步抽取风险主要致因因素，即风险要素，分析风险要素导致风险发生的路径，支撑数据跨境风险机理研究，刻画数据跨境风险机理及其演化过程，从而为数据跨境的风险研究提供支持。本文主要贡献如下。

1) 首次提出了基于业务需求分析的数据跨境业务流程抽象模型。旨在系统性地识别数据跨境业务需求，梳理跨境相关业务流程及相关的过程数据资料，该模型可以清晰和直观地描述数据跨境业务流程。

2) 基于扎根理论等方法，完成由过程数据资料向风险致因因素的系统演化，应用复杂网络分析等方法，进一步对风险致因因素进行筛选，从而抽取出数据跨境风险要素，揭示跨境数据风险的全貌与内在联系。

3) 在数据跨境安全领域，首次基于业务驱动针对数据跨境风险机理展开研究。以数据跨境风险要素体系为基础，结合风险演化过程以及相关数据风险理论，揭示风险要素的危害对象以及数据安全根基传导风险过程。本文针对数据跨境风险机理展开研究可为数据跨境风险研究提供基础理论支持。

## 1 相关工作

### 1.1 风险机理研究动机

风险机理研究在于探索风险形成的路径，可以从剖析、挖掘风险的形成因素入手。本文检索数据跨境领域风险研究的相关文献，发现当前的研究方向主要集中在法律、机制体系以及风险评

估等方面。在数据安全相关领域风险机理研究方面,本文在国内主要文献数据库中,检索2021—2025年计算机软件及应用领域中关于“风险机理”主题的核心期刊文献。在国外检索IEEE、ACM等主流文献库中同样年限,关于“风险机理”“隐私安全”等相关主题文献。并对上述文献进行人工筛选,选取与风险机理相关文献进行汇总分析,结果如表1所示。在表1中,列举了25篇相关文献。其中48%文献为国内核心期刊论文,52%文献为国外期刊论文。在数据跨境安全相关领域类别中,100%文献涉及数据跨境政策相关主题,96%文献涉及数据跨境管理相关主题,64%文献

涉及数据跨境风险相关主题,54%文献涉及数据跨境风险要素相关主题。

然而,关于数据跨境风险机理的系统研究仍较为匮乏,仅有董克等<sup>[16]</sup>在其论文中对风险形成机理进行了简要描述,但未对风险机理的传导机制进行深入分析。在数据安全相关领域类别中,数据安全风险机理研究和风险形成相关研究覆盖了该类别中全部文献。然而涉及数据跨境政策和管理的文献相对较少,关于数据跨境风险要素的探讨几乎为空白。由此可见,当前的数据安全风险机理研究尚未充分涵盖跨境数据流动所特有的风险要素特征,难以全面揭示跨境数据风险的全貌与内在联系,故有

表1 风险机理相关研究跨境要素对比

类别	文献	风险机理研究	数据跨境政策	数据跨境管理	数据跨境风险	数据跨境风险要素	数据跨境风险机理	
数据跨境安全相关领域	文献[6]	×	√	√	×	×	×	
	文献[7]	×	√	√	√	√	×	
	文献[8]	×	√	√	×	×	×	
	文献[9]	×	√	×	×	×	×	
	文献[10]	×	√	√	√	√	×	
	文献[11]	×	√	√	√	√	×	
	文献[12]	×	√	√	√	√	×	
	文献[13]	×	√	√	√	×	×	
	文献[14]	×	√	√	√	√	×	
	文献[15]	×	√	√	√	√	×	
	文献[16]	○	√	√	√	√	○	
	数据安全相关领域	文献[17]	×	√	√	√	×	×
		文献[18]	×	√	√	×	×	×
		文献[19]	×	√	√	×	×	×
		文献[20]	×	√	√	√	×	×
		文献[21]	×	√	√	×	×	×
文献[22]		√	○	×	×	×	×	
文献[23]		√	×	×	×	×	×	
文献[24]		√	○	×	×	×	×	
文献[25]		√	×	×	×	×	×	
文献[26]		√	√	√	×	×	×	
文献[27]		○	×	×	×	×	×	
文献[28]		√	○	√	√	○	×	
文献[29]		√	×	×	×	×	×	
文献[30]		√	○	×	×	×	×	

注:√表示包括,×表示不包括,○表示部分包括。

必要针对数据跨境风险机理展开深入研究。

## 1.2 数据跨境业务流程

数据跨境业务流程通常是指数据从一个国家（地区）转移到另一个国家（地区）的过程。依据中国数据安全及数据跨境相关法律规定，数据出境制度包括数据出境安全评估、个人信息出境标准合同、个人信息保护认证、自贸区跨境数据“白名单”等方式。同时，还可以根据特殊出境业务场景的规定，免于上述方式的申报。

## 1.3 Petri 建模

传统的业务流程建模使用自然语言文字描述业务流程，不可避免会存在语义异构、系统间互操作困难等问题<sup>[31]</sup>。Petri 建模语言有效地解决了上述问题，具有严格的数学表示性<sup>[32]</sup>，侧重对整个系统过程的描述，是广泛使用的流程建模语言之一。同时，Petri 网图形化的布局能够准确地模拟业务活动、决策点以及节点状态转换，为复杂的业务环境提供清晰的可视画面。相比传统流程，Petri 网可以更精确地描述业务并发、子网结构等业务形态。

## 1.4 扎根理论

扎根理论是 Glaser<sup>[33]</sup>提出的一种理论方法，对扎根理论的定义是“一种与数据收集相关的通用分析方法，使用一套系统应用的方法来生成关于某个实质性领域的归纳理论”<sup>[34]</sup>。本文根据当前数据跨境风险机理的研究现状与实践之间存在较大落差等特点<sup>[35]</sup>，对实际业务资源展开近距离剖析，凝练扎根理论的范畴概念结论。针对业务过程中的法律、法规、标准等资料数据进行汇总分析，并浓缩抽取概念和范畴，支撑数据跨境风险机理研究。

## 1.5 复杂网络分析算法

复杂网络是一种具有复杂结构和特征的特殊网络结构，将复杂现实世界系统中的元素抽象为节点，将元素之间的关系抽象为边。在复杂网络分析过程中，通过计算网络中相关参数，可以进一步分析引发风险的风险要素，即通过分析复杂网络可以发现网络中的重要节点和传播路径。

本文将采用复杂网络形式构建数据跨境风险演化网络，清晰直观地揭示数据跨境风险致因因素之间的内在关联，并通过算法分析抽取数据跨境风险要素。

## 2 数据跨境风险机理研究

### 2.1 风险机理研究的可行性与合理性

风险机理是风险研究的基础，可以丰富相关领域风险研究的理论基础，为进一步研究风险控制提供理论支持<sup>[36]</sup>。当前，诸多行业已经完成各自领域范围内的风险机理研究，如表 2 所示。

表 2 其他行业领域风险机理理论支撑

行业	文献	主要研究方法	被引用次数/次
金融	文献[37]	文献挖掘、扎根理论	61
经济	文献[38]	系统风险分析、联结经济、合经济效应	260
社科	文献[39]	风险演化因果关系分析、系统动力学	80
财政	文献[40]	多学科维度风险分析	200
医疗	文献[41]	识别风险、分析和评估、风险评估矩阵	101
海事	文献[42]	文献综述、机器学习	93
地质	文献[43]	层次分析	80
工程	文献[44]	系统动力学、解释结构	63
交通	文献[45]	马尔可夫算法、高斯混合算法	32

表 2 中列举了金融、经济、社科等风险研究较为成熟行业领域的风险机理研究相关论文。其主要采用文献挖掘、风险演化因果关系分析及多学科维度风险分析、扎根理论、系统动力学等研究方法。上述方法在实际研究中展现出良好的适用性与可行性。同时，由相关文献被引用次数表明，风险机理研究不仅为相关领域的风险识别与管理提供了重要的理论支撑，在推动风险研究体系的完善与发展方面也具有显著意义。

综合上述风险机理研究意义与可行性的分析结果，结合当前数据跨境风险机理尚未展开深入研究的现状。可以确定，针对数据跨境风险机理展开研究具有重要的学术价值和现实意义，且具有较强的可行性。同时，为提高论文的合理性，本文借鉴《信息安全技术数据安全风险评估方法》中关于风险发生过程的描述，并在其基础上根据数据跨境的特点，结合数据跨境风险相关法规要求进行完善和补充，旨在针对数据跨境领域展开风险机理研究，为数据跨境领域风险研究提供支撑。

### 2.2 数据安全风险评估模型

风险机理可以描述风险形成的过程，当前数据跨境安全领域尚未对风险机理展开深入研究。数据跨境安全与数据安全、计算机信息安全等领域存在较大的交集和相似性。故此，借鉴数据安全、计算机信息安全等领域风险评估模型研究成果，可以支撑数据跨境风险机理的深入研究，进而为数据跨境风险研究奠定基础。在数据安全、信息安全等领域，相关研究人员针对风险评估展开研究。Wang 等<sup>[46]</sup>基于数据挖掘和关联分析方法对信息安全展开度量。马冬青等<sup>[47]</sup>应用优劣解距离法和灰色关联分析法对信息安全展开风险评估。Zhang 等<sup>[48]</sup>提出了基于马尔可夫链的高级长期威胁（APT, advanced persistent threat）攻击风险传播评估模型。马梓刚等<sup>[49]</sup>应用改进的 petri 网对系统功能安全和信息安全一体化风险进行建模。Chen 等<sup>[50]</sup>应用层次化方法评估电网信息资产安全威胁。耿文莉等<sup>[51]</sup>应用灰色神经网络对云平台大数据安全风险展开评估。Cao 等<sup>[52]</sup>提出了基于计算机技术和熵权法实现信息化安全风险评估。上述风险评估模型的研究成果可以为数据跨境风险机理研究提供重要的理论框架和方法支持。

### 2.3 数据跨境风险机理研究路线

考虑到数据跨境业务流程的复杂性，以及相关风险的未知性，为了充分挖掘数据跨境风险要素，掌握风险因素触发风险的机理和形成过程。在数据跨境领域，本文基于业务驱动首次针对数据跨境风险机理展开研究。该研究以业务流程驱动，基于业务过程的数据跨境风险机理研究路线，如图 1 所示。

在图 1 中，首先基于收集的相关数据、已识别的数据资产等数据资源集合，创建业务流程抽象模型，并向构建复杂分析网络过程输出业务过程数据资料。其可以作为过程文档资料支撑扎根理论分析，包括跨境业务涉及的相关法律、法规、标准要求、操作日志等资料数据。其次，在构建复杂分析网络过程中，根据输入的业务过程数据资料，借鉴扎根理论的范畴概念，输出范畴列表，进一步将范畴作为网络节点，输入给复杂分析网络。同时，基于风险事故致因理论，建立网络节点因果逻辑关系，进而构建风险演化网络。在此基础上，应用复杂网络分析方法，分析挖掘风险要素。最后，刻画数据跨境风险机理。

## 3 数据跨境业务抽象模型

在研究型工作中，通常会选择 Petri 建模语言作为业务流程的输出工具<sup>[53]</sup>，充分发挥其善于应对复杂流程且具有强大的系统分析能力。本文提出基于 Petri 技术对数据跨境业务流程进行抽象建模。

### 3.1 数据跨境业务流程概述

业界公认数据跨境出境全过程包括数据跨境前、跨境中和跨境后 3 个阶段<sup>[54]</sup>。基于上述 3 个阶段，本文依据业务流程阶段特点，在数据跨境前引入启动阶段。该阶段包括跨境数据需求分析、资产识别等步骤。其意义在于将数据跨境发生与资产识别联系起来，进而推动数据处理者在数据安全监管措施与数据跨境合规性要求之间实现制度性协同与有机对接。数据跨境业务流程如图 2 所示，详细如附录 1 所示。

### 3.2 数据跨境业务流程分析

根据图 2 中的详细描述，应用 Petri 网分析软件 PIPE 对数据跨境业务流程进行抽象建模，如图 3 所示。在图 3 中，圆圈表示库所，方块表示变迁，黑色实心点表示 Token，其在 Petri 网中代表系统的某种状态或条件。尽管 Petri 网结构是以静态方式表示，但是在触发规则的控制下，Token 是可以流经网络描述系统的动态行为<sup>[55]</sup>。系统状态因为事件或行为发生转变称为变迁，在图 3 中由矩形表示。数据跨境业务抽象模型中的库所和变迁定义如表 3 和表 4 所示。在数据跨境业务流程的抽象模型中，将业务流程划分 4 个阶段，即启动阶段、数据跨境前、数据跨境中和数据跨境后。

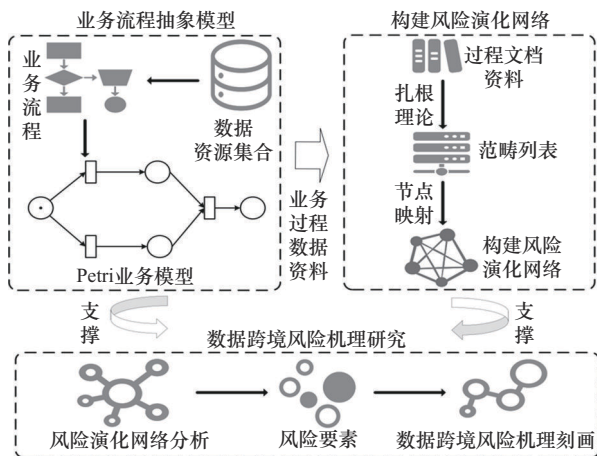


图 1 数据跨境风险机理研究路线

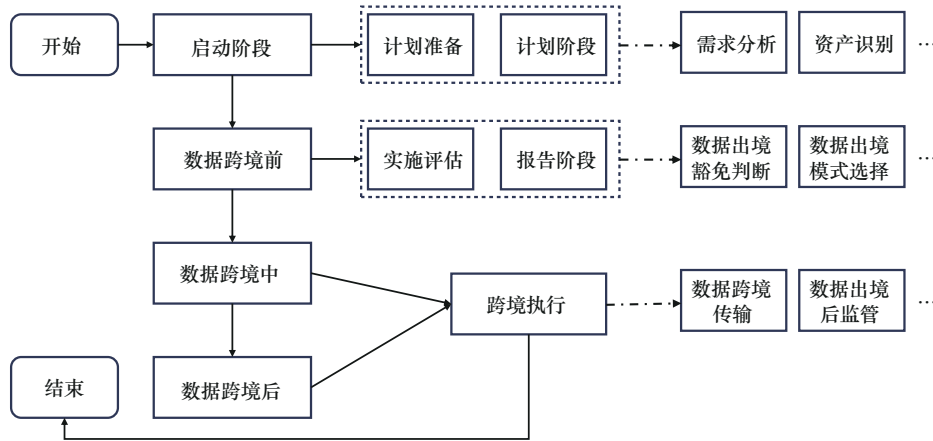


图2 数据跨境业务流程

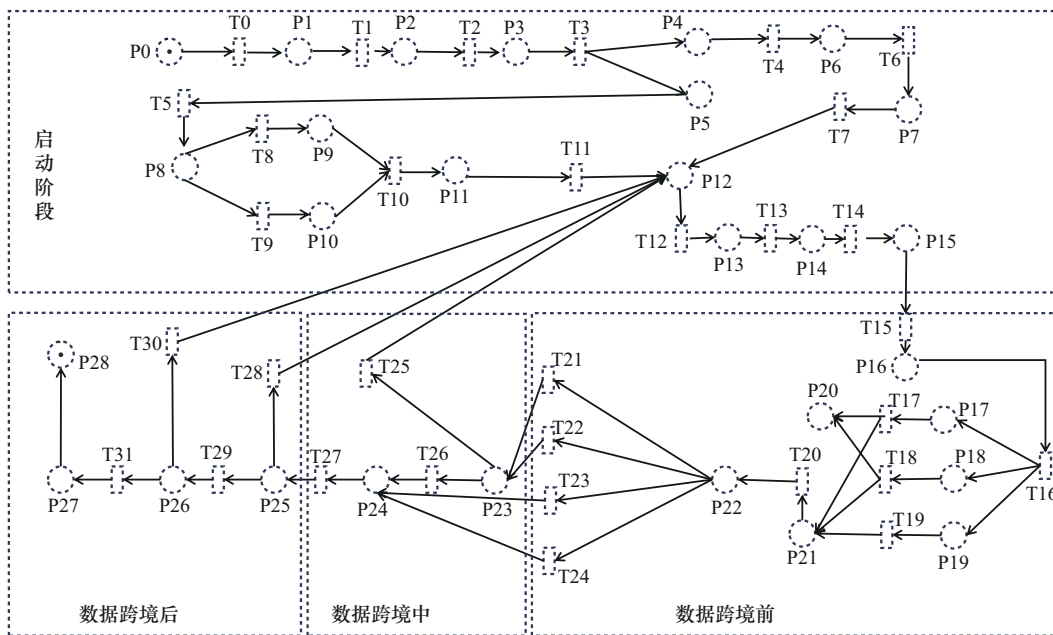


图3 数据跨境Petri网抽象模型

表3

库所定义

库所	含义	库所	含义	库所	含义
P0	起始库所	P10	人员评估相关管理制度	P20	指定信息数据保护机构
P1	数据处理者基本情况分析	P11	管理制度审计	P21	跨境数据合规性审查、评估风险
P2	境外接收者基本情况分析	P12	数据资产识别	P22	数据跨境方式选择
P3	可行性分析	P13	数据跨境业务场景分析	P23	提交网信管理机构评估
P4	涉及信息系统	P14	数据跨境字段与业务场景匹配	P24	发生跨境数据
P5	涉及业务条线及部门	P15	跨境数据量统计	P25	评估有效期
P6	外部数据收集	P16	全年数据跨境发生量预测	P26	是否发生影响数据安全情形
P7	内部数据收集	P17	重要数据	P27	境外数据接收及数据处理
P8	是否引入三方评估机构	P18	(敏感) 个人信息	P28	结束
P9	三方评估协议	P19	一般数据		

**表4** 变迁定义

变迁	含义	变迁	含义	变迁	含义
T0	分析需求	T11	审计管理制度	T22	订立个人信息出境标准合同
T1	分析数据处理器基本情况	T12	分析数据跨境业务场景	T23	个人信息保护认证
T2	分析境外接收者基本情况	T13	匹配数据跨境字段与业务场景	T24	免于申报出境
T3	涉及部门分析	T14	统计跨境数据量	T25	未通过审核
T4	收集外部数据	T15	预测全年数据跨境发生量	T26	通过审核
T5	收集内部数据	T16	进行跨境数据分类信息判定	T27	跨境数据发生
T6	汇总数据资源	T17	重要数据	T28	期满
T7	确认涉及业务、技术等人员	T18	(敏感) 个人信息	T29	未期满
T8	引入第三方风险评估机构	T19	一般数据	T30	发生影响数据安全情形
T9	筛选评估人员	T20	审查跨境数据合规性	T31	未发生影响数据安全情形
T10	数据操作权限管理	T21	数据出境风险自评估报告等		

1) 启动阶段。P0是起始库所，开始执行需求分析工作，经过P1、P2和P3库所，以及T1、T2和T3的变迁，通过对数据处理器和数据接收者基本情况进行分析，初步完成数据跨境业务的可行性分析工作。其余步骤主要完成业务条线相关部门、人员、权利、物资等资源调配工作，判断是否需要三方评估机构介入，以及三方评估机构介入后的评估协议等方面工作。汇总相关数据进入数据资产识别阶段，该阶段通过对数据资产库存进行管理，可以为后续的跨境数据分析提供数据资产清单等资料，支撑数据跨境前阶段。

2) 数据跨境前。基于数据资产清单和人员数据操作权限等资料，对出境业务与出境数据字段进行梳理，并基于相关规定，对出境数据实施跨境风险和合规性检查，并根据适用条件选择数据的跨境方式。

3) 数据跨境中。主要包括跨境数据的传输以及相关安全监控等任务。

4) 数据跨境后。主要包括跨境后数据加工处理的管理、安全环境保障以及跨境合同或安全评估有效期、出境范围变更等风险的监管。同时，针对突发风险、残余风险等安全事件展开监控，如发生上述或其他风险，T30将引导模型流转至启动阶段，对风险展开分析。

#### 4 数据跨境风险演化网络

风险研究主要方法包括系统动力学、风险场理论、复杂网络分析等方法。其中，Forrester<sup>[56]</sup>阐述了模型对数据的敏感性特点，常用语通过因果关系

和反馈机制揭示系统的非线性特征与长期演化规律。当前，数据跨境风险研究起步较晚，在历史风险案例累计方面薄弱，不足以支撑该方法的仿真数据验证对比，以及长期演化规律总结。风险场理论作为衡量风险状态的参数，最早由秦雅琴等<sup>[57]</sup>提出并应用于机器人路径规划。随着理论体系的不断完善，该方法在智能交通系统、自动驾驶决策等领域中展现出显著的理论优势。复杂网络分析方法可以适应多种学科和场景，可以更好地理解网络的拓扑结构和动态行为，且可以直观地展现局部节点与整体网络的关系。Liu等<sup>[58]</sup>提出了基于风险相互作用网络(RIN, risk interaction network)的风险传播效应新型风险评估框架。故此，本文选用复杂网络分析方法，旨在揭示网络中各个风险要素节点的关系结构以及内在关联，充分发挥数据跨境领域评审人员的专业经验，为跨境数据风险研究奠定初步基础。

本节将在4.1节至4.3节中，以“点-链路-网络”结构阐述数据跨境风险演化网络的构建过程。

##### 4.1 构建数据跨境风险演化网络节点

###### 4.1.1 数据跨境业务过程资料的扎根理论分析

在扎根理论编码过程中，本文在研究团队内部以名义小组方式对抽取内容进行讨论。并将讨论结果递交给法学相关研究人员，以焦点访谈方式对讨论结果进行审核。即以不同人群调研、不同领域交叉、不同调研方法等措施降低主观因素对抽取结果的影响。扎根理论具体步骤如下。

1) 开放性编码阶段。对原始数据进行拆解分析、对比和归纳，并在此基础上完成初始概念和副

范畴的提炼工作。在本文中，概念是附着于数据跨境相关法律法规资料等原文内容的概念性标签。副范畴是针对概念内容的进一步信息提取和浓缩。

2) 主轴性编码阶段。分析范畴间的类属关系，归纳主范畴。主范畴是一组概念，组内信息均指向同一对象，由一个层次较高也较抽象的概念统摄即称为范畴。表 5 摘选了部分数据，展现数据跨境相关副范畴向主范畴归集的过程。

表 5 主轴式编码结果(摘选)

主范畴	副范畴	初始概念
敏感、重要数据分类界定	敏感数据、重要数据定义不同	普通数据与重要数据重要程度不同
		数据出境申报数量方面要求不同
	保护措施不同	个人信息与个人敏感信息定义不同
		保护措施不同，泄露导致的后果也不相同
数据主体具有的权利和途径	告知数据主体应有的权利	
	告知数据主体行使权力的途径和方式	
单独同意	获取数据主体单独同意	

3) 选择性编码阶段。对主范畴进一步提炼，确定核心范畴。选择性编码的目标是通过假设或关系图，分析主范畴之间的内部关系，确定一个核心范畴，并围绕该核心范畴构建理论框架。因风险具有因果特性和传播特性，故在选择性编码阶段采用风险演化网络等方法进一步分析核心范畴，即风险主要致因因素。

4.1.2 基于范畴构建风险演化网络节点

基于扎根理论提炼抽取 87 条初始概念和范畴全部数据，本节将这些数据中的范畴投影为网络节点，使其成为数据跨境风险演化网络中的叶子节点，如图 4 所示。

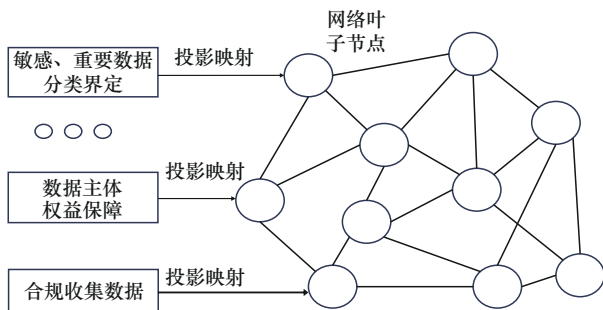


图 4 范畴投影构建风险演化网络叶子节点

4.2 构建数据跨境风险演化网络的致因链路

某一风险的发生可能是由一个或者多个风险因

素共同触发。Wang 等<sup>[59]</sup>基于因果循环图理论，直观表达不同因子变量之间的因果关系，并支撑风险影响因子分析、风险后果分析、风险反馈回路识别等相关研究。

结合上述风险理论，基于数据跨境业务流程中的关键风险节点和节点间的因果关联，构建风险演化网络的致因链路。以某个致因链路为例，如图 5 所示。图中列举出了安全管理缺失导致数据安全事件发生的传导过程，即安全管理缺失导致相关人员培训不足和安全意识不足，叠加环境影响因素导致忽视安全措施和危险评估不足，进而产生数据安全潜在威胁和安全预案缺失等问题，最终导致数据安全事件发生。

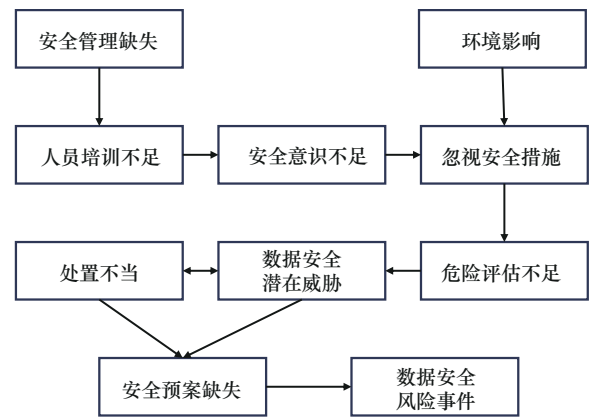


图 5 安全管理缺失导致事故致因链路

4.3 构建数据跨境风险演化关系网络

风险的复杂性和因果性，决定风险致因链路并非单链路形态。Liu 等<sup>[60]</sup>基于对关键因果因素的复杂网络分析，以事故案例中的因素和结果表示为网络节点，节点之间的因果关系表示为边。Garvey 等<sup>[61]</sup>根据风险之间的相互关联关系，构建供应链网络风险传播模型。由此可判定，数据跨境风险的演化关系呈现为多条风险链路交织而成的复杂网络形态。基于 4.1 节中对风险节点的系统梳理，以及 4.2 节中关于致因链路的构建，进一步结合风险因果理论，最终构建形成数据跨境风险演化网络，如图 6 所示。

5 数据跨境风险机理演化路径

5.1 数据跨境风险要素

风险要素是引发风险的主要或者关键风险致因因素，是风险关系网络中的关键节点。基于 4.3 节中调研结果并应用复杂网络分析软件 Gephi，针对



图6 数据跨境风险演化网络

每一个风险致因因素节点，逐个计算风险节点的PageRank系数（PR），计算式如式(1)所示。

$$PR(a)_{i+1} = \sum_{i=0}^n \frac{PR(Ti)_i}{L(Ti)} \quad (1)$$

其中，PR(a)表示当前节点a的PR值，PR(Ti)表示其他各个节点（能够指向a）的PR值，L(Ti)表示其他各个节点（能够指向a）的出链数，i表示当前时刻或迭代次数。风险主要致因因素如表6所示，结果表明，数据跨境安全管理、人员因素、数据安全技术保护和环境因素4个风险致因因素是网络核心节点。

表6 风险主要致因因素

编号	风险致因因素	度	PageRank系数
55	数据处理机构情况	5	0.016 926 082 300 790 4
32	接收方法律环境	8	0.018 143 481 929 381 9
85	境外加工处理数据	10	0.019 337 525 961 016 3
53	数据安全审计	9	0.020 205 368 922 962 9
14	合规数据处理	12	0.022 573 704 436 727 2
2	重要敏感数据界定	12	0.027 016 781 097 489 3
87	环境因素	17	0.037 065 820 977 878 6
23	数据安全技术保护	15	0.038 314 881 956 182 2
76	人员因素	20	0.041 974 904 133 130 3
51	数据跨境安全管理	23	0.047 137 304 855 316 9

该计算结果符合傅贵等<sup>[5]</sup>提出的风险事故致因“2-4”模型。基于上述模型理论以及表6的各项计算结果，可以确认数据跨境风险要素是管理措施、环境影响、技术限制和人员因素。

### 5.2 数据跨境风险演化网络分析

#### 5.2.1 内生风险威胁

内生风险是指由系统中单一或多个独立风险因素可能引发风险的过程，其特点是处于风险致因链路的最初节点。在数据跨境风险演化网络中，该类型节点游离在核心节点群之外，距离风险要素节点距离较远。本节以风险要素中的环境影响为例说明。计算式如式(2)所示。

$$centrality(i) = \frac{N - 1}{\sum_{n=1}^N distance_i^n} \quad (2)$$

其中，N表示图顶点的个数，distance<sub>i</sub><sup>n</sup>表示顶点i到顶点n的最短距离。接近中心性的取值范围是[0,1]，数值越大越靠近中心。表7列举了前10条环境相关致因因素。由表7可知，各项致因因素是环境影响相关节点中各项中心性排名最低的10项，其中，34、35和36号节点的加权接近中心性较低，表明其处于数据跨境风险演化网络的边缘位置，是风险的初期隐含。

表7 环境相关致因因素

编号	致因因素	加权接近中心性
34	接收方政府加入国际信息保护组织	0.331 349
35	接收方地区具有约束力的国际承诺	0.331 349
36	与中国签订数据安全双边协定	0.331 349
37	数据接收方政治环境	0.343 056
39	数据接收方社会环境	0.343 056
38	数据接收方外交环境	0.354 96
55	数据处理者机构基本情况	0.359 921
25	接收方基本情况	0.375 794
80	累计发生数据跨境数量	0.376 984
40	数据接收方宗教信仰	0.400 198

### 5.2.2 风险聚集

风险聚集是不同传播路径的风险汇聚在同一处节点。在数据跨境复杂的业务场景背景下，数据自身风险因素以及其他风险因素始终处于不断发展或变化过程中，通过风险网络传导加持，相关风险因素最终完成汇集，进而形成风险聚集。

本节以风险要素中的技术限制为例说明。表8列举了由Gephi软件计算前10条技术限制相关致因因素。加权中介中心性数值介于30至578之间，表现出比较重要的中介传递原则。网络边缘的致因因素节点通过传递，在上述节点完成风险聚集。

表8 技术限制相关致因因素

编号	致因因素	加权接近中心性	加权中介中心性
29	合规销毁数据	0.473 214	103.272 2
27	合规储存数据	0.489 087	135.583 4
43	数据接收方风险管控	0.470 238	186.912 8
53	数据安全审计	0.470 238	217.822 7
19	数据目的与范围一致	0.455 357	30.582 59
18	出境数据最小范围描述	0.446 429	32.652 79
44	跨境数据流量异常监控	0.444 444	56.749 82
23	数据安全技术保护	0.499 206	577.412 1
13	合规处理数据	0.459 325	83.799 6
4	合规收集数据	0.463 294	95.274 47

可见，对数据跨境风险演化网络的风险聚集和跃迁分析，可以确定引发风险发生的关键致因节点。

### 5.2.3 风险触发

Huang等<sup>[62]</sup>认为，当一个网络中至少出现2个风

险因素时，由2个或多个风险因素引起的2个或多个风险场相互作用，并形成耦合风险场，使系统状态上升到较高的风险状态，最终导致风险事故的发生。

由此可见，在数据跨境风险演化网络中，一个或多个边缘节点风险因素受到激发，传递风险给关键节点，关键节点在接收相关激发后，则会触发数据跨境相关风险事件。

### 5.3 数据跨境业务驱动的风险机理刻画

网络空间安全领域权威表示，安全性、可用性和合规性是数据安全保护的3个元属性，不可被其他属性替代，是数据安全的根基。其中安全性进一步可以分解为可鉴别、机密性和可控性；可用性包括持久保护、业务连续和应急响应；合规性包括数据治理、隐私保护和合规使用。

在《信息安全技术数据安全风险评估方法》的征求意见稿中，将风险源描述为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性、脆弱性、问题、隐患等。基于数据跨境业务抽象模型以及复杂网络分析结果，综合上述3个元属性以及相关法规标准的风险源描述，总结出基于业务流程驱动的数据跨境风险机理演化路径，如图7所示。

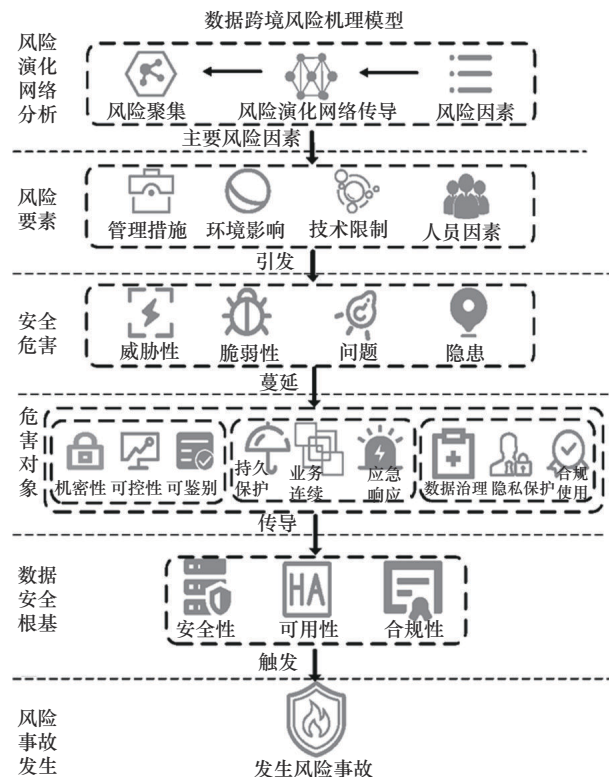


图7 基于业务流程驱动的数据跨境风险机理演化路径

由图7可知,数据跨境风险机理演化路径基于业务流程,共分为6个阶段。在风险演化网络分析阶段,如4.1节~4.3节描述基于扎根理论等方法构建风险演化网络。在第5节阐述风险演化网络分析的过程,确认网络核心节点向风险要素转化的过程。在第二阶段风险要素阶段之后,5.3节进一步阐述第三至第六阶段,即由风险要素引发安全危害的过程,并基于该过程向危害对象蔓延,最终传导至数据安全根基,触发风险事故。

## 6 实例分析

### 6.1 验证方案设计

为验证本文提出的研究工作,设计验证方案如下。

1) 采用调研问卷方式,验证本文提出的管理措施、环境影响、人员因素和技术限制四大类风险要素的合理性。调研当前金融领域中,数据跨境风险产生影响较大的致因要素。最终对比本次调研结果与本文抽取风险要素的相似关系,印证本文抽取风险要素的合理性。

2) 统计并分析历史数据,验证管理措施、环境影响、人员因素和技术限制四大类风险要素是触发风险事故发生的主要原因。6.3节以数据泄露为例,收集近些年风险事故发生案例,根据官方发布的事由原因进行归纳总结,以数据统计形式验证本文提出的数据跨境风险机理研究,即管理措施、环境影响等风险要素会通过安全危害等传导机制,最终触发风险事故发生。

### 6.2 金融行业数据跨境风险要素实例分析

金融是数据密集型行业,同时也是强监管行业,金融部门数据跨境流动有特殊性,本节以金融行业数据跨境安全为研究对象,应用调查问卷方式收集相关人员专业意见,汇总并构建本文实验数据来源。最终,通过线性回归算法对统计数据进行分析。整个调查过程分为6个步骤,具体如下。

1) 调查问卷设计。第一部分为调查人员基本信息,包括文化程度、年龄、从事相关专业时间、职称或职级;第二部分包括被调查者对当前金融行业数据跨境安全现状总体评估,如表9所示;第三部分包括具体风险要素,根据金融行业特点,列举部分风险要素作为调研对象。

表9 金融行业数据跨境安全现状

等级	描述	分数
A	非常安全	100~80
B	较安全	80~60
C	安全	60~40
D	弱安全	40~20
E	不安全	20~0

金融行业数据跨境安全风险致因因素评价分数如表10所示。

表10 致因因素评价分数

等级	该因素对金融行业数据跨境安全风险影响	分数
A	影响非常大	100~80
B	影响较大	80~60
C	影响一般	60~40
D	影响较弱	40~20
E	无影响	20~0

调研对象可以根据因素对风险事故的影响或者贡献对项目进行评分,或者直接给出等级评价。最终数据收集时,会将调研对象的评分转换成为评价等级,并针对评价等级进行验证分析。

2) 调研对象。调研对象包括金融行业从业者、相关数据接触者、金融科技研发者、专业研究人员、高校相关专业老师以及学生等群体中随机挑选。具体调研群体基本属性信息统计如表11所示。

表11 调研群体基本属性信息统计

调研群体基本属性	属性数值范围
学历	大专、本科、研究生(硕士、博士)
年龄	20~55岁
相关从业年限	3~15年
职称	初级职称、中级职称、高级职称
职级	科员、中层领导

3) 实验数据收集。随机挑选调研对象24人,收集并挑选出样本的80%为数据样本,即20人数据作为本次验证数据。

表12为金融行业数据跨境总体安全现状评价调研结果。表13摘选部分金融行业数据跨境风险致因调研样本,全量样本如附录2所示。

表 12 金融行业数据跨境总体安全现状评价调研结果

样本序号	评价	样本序号	评价	样本序号	评价
1	A	9	A	17	A
2	A	10	A	18	B
3	B	11	B	19	A
4	A	12	B	20	A
5	A	13	C	21	A
6	A	14	A	22	D
7	C	15	C	23	A
8	A	16	D	24	A

表 13 金融行业数据跨境风险致因调研结果(摘选)

编号	致因因素	评价 样本 1	评价 样本 2	评价 样本 3
1	敏感、重要数据分类界定	D	B	A
2	人员因数	A	A	C
3	合规收集数据	B	B	C
4	结构化数据	E	B	C
5	数据确权	A	B	B
6	数据跨境安全管理	B	B	C
7	数据主体权益保障	A	B	C
8	数据安全技术保护	C	C	C
9	出境数据与申报数据是否一致	C	A	B
10	数据脱敏、去标识	B	B	B

4) 调研数据处理方法。本文采用 SPSS 26.0 统计软件对调研数据进行分析处理,应用线性回归算法对调研数据进行分析,以验证本文提出的数据跨境风险要素,计算式如式(3)所示。

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \dots + \beta_i x_i + \varepsilon \quad (3)$$

其中,  $y$  是因变量,会受到自变量影响;  $i$  为致因因素编号; 自变量系数  $\beta$  为线性拟合系数;  $\varepsilon$  为误差项。基于线性回归算法可以分析出致因因素对金融行业数据跨境安全风险的影响,筛选出主要的影响因子,计算结果如表 14 和表 15 所示。

表 14 摘要

模型	$R$	$R$ 方	调整后 $R$ 方	标准估算的错误	德宾-沃森
1	0.889 <sup>a</sup>	0.790	0.778	0.509	—
2	0.928 <sup>b</sup>	0.861	0.845	0.426	—
3	0.947 <sup>c</sup>	0.897	0.878	0.378	—
4	0.968 <sup>d</sup>	0.937	0.921	0.304	1.883

自变量包括数据跨境安全管理、人员因素、数据安全技术保护和环境因素 4 个风险要素。在表 14 中,  $a$  表示预测变量:(常量),数据跨境安全管理;  $b$  表示预测变量:(常量),数据跨境安全管理和人员因素;  $c$  表示预测变量:(常量),数据跨境安全管理、人员因素和数据安全技术保护;  $d$  表示预测变量:(常量),数据跨境安全管理、人员因素、数据安全技术保护和环境因素。其模型  $R$  方以及  $R$  方调整系数接近拟合度 1,表现较好,德宾-沃森系数为 0~4,表现出较好的独立性。 $B$  是自变量的系数,  $t$  值代表每个自变量对因变量的单独影响程度,可见调研对象在金融行业数据跨境安全方面,更重视数据跨境安全管理因素。显著性表明,4 个自变量均会对因变量产生影响。

5) 调研结果分析。根据上述数据计算结果,数据跨境安全管理、人员因素等风险要素对金融行业数据跨境安全总体现状影响较大,即金融行业领

表 15 系数

模型	自变量	$B$	标准错误	标准化系数 Beta	$t$	显著性
4	(常量)	-0.654	0.436	—	-1.499	0.155
	人员因素	0.450	0.097	0.531	4.613	<0.001
	数据跨境安全管理	0.485	0.122	0.467	3.975	0.001
	数据安全技术保护	0.262	0.067	0.277	3.897	0.001
	环境因素	0.170	0.055	0.229	3.112	0.007

域更加重视数据跨境过程中的数据跨境安全管理、人员因素、数据安全技术和环境因素4个方面的风险要素。

6) 专家评审。邀请2022—2025年曾在核心期刊上发表关于数据跨境安全、隐私保护等领域研究成果的5位学者及专家,对调研结果进行评审。专家评审可以确保对调研结果的深入分析和多角度验证,从而提升研究的科学性与权威性。

综上所述,金融行业在数据跨境方面更加重视数据跨境安全管理、人员因素、数据安全技术和环境因素等4个方面因素。其风险要素关注点与本文提出的数据跨境安全四大风险要素的分析结果对比基本一致,即表明本文提出的数据跨境风险要素分析结论对相关行业的数据跨境风险研究具有一定支撑价值。

### 6.3 基于数据安全风险事故的风险机理验证

为了验证本文提出的数据跨境风险要素是触发数据跨境安全风险的关键因素。本文以数据安全风险事故分析角度入手,挖掘已发生风险事故的风险原因,并进一步分析风险原因类别,最终通过数据统计完成风险机理的验证工作。

当前,典型数据跨境风险案例较少,难以支撑数据验证实验。但是数据泄露风险是数据跨境安全风险事故的子集,数据泄露通常会引发数据跨境流通,进而触发数据跨境风险,对数据跨境风险机理研究结果的验证具有一定研究价值。本文收集了近些年典型的数据泄露案例,尽管其中一些数据泄露事件并不是发生在数据跨境过程中。但是,导致其发生泄露的风险要素也可导致发生跨境数据泄露,且其传播过程也可触发数据跨境风险。

本文检索相关新闻、资料、历史记录以及文献等公开历史资料,应用Google、百度等搜索引擎,对“数据安全”“数据风险”“数据泄露”等相关主题进行检索。被收集数据要求有官方的正式通告以及风险原因调查结论。经过人工筛选和统计,该数据集合计记录68件风险事故,逐条记录风险事故的事件名称、事件描述、事件影响、事件原因、事件发生时间、事件来源以及风险归类。本文将其开源分享于Github社区中。

针对上述风险事件官方发布原因展开分析发现,人员因素导致的风险事故占据相当一部分比

例,如安全意识不足导致人员泄露账户信息、长期不更新密码导致密码撞库事件发生、人员恶意行为导致源代码或其他识别信息泄露等,该类风险原因占比12%。同时,数据保护技术限制导致的网络攻击、数据抓取、软件攻击、恶意软件以及API渗透等风险原因占比超过50%。管理不足导致的配置错误、管理漏洞、保护措施不足等风险原因占比12%,政治斗争等环境因素导致的风险原因占比较低。上述各项风险事故原因详细占比信息如图8所示。

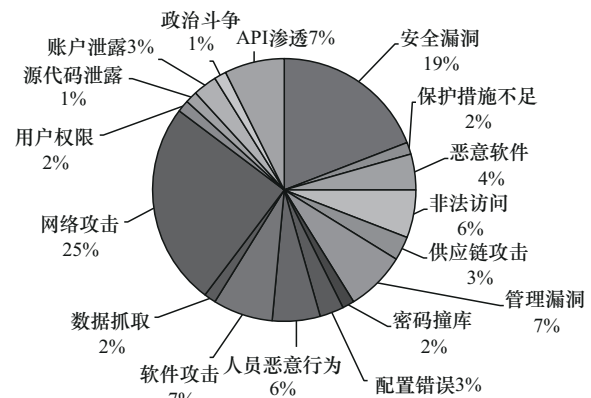


图8 风险事故原因占比信息统计

综上所述,近些年发生的数据安全风险事故原因以及影响范围信息记录表明,风险均系因人为、管理、技术和环境四大因素所引发,而其风险影响范围会导致数据的无序跨境流动,亦会触发数据跨境风险。

## 7 讨论

### 7.1 基于数据跨境风险机理研究现状的意义讨论

风险机理是风险理论的重要内容,只有掌握风险机理,才能掌握风险规律,进而实现风险管控。在风险研究相对成熟的领域中,如工程、经济、社科等领域均有风险机理相关的研究成果,且研究成果对该领域的风险研究提供了较好支撑。

为此,本文在数据跨境安全领域基于业务驱动,针对数据跨境风险机理展开研究,意义如下。

1) 本文针对数据跨境风险机理展开研究,可以为数据跨境风险研究提供新颖的视角和扎实的理论基础。

2) 本文具有跨学科合作优势,既研究基于相

关法律、法规以及运营日志等数据,也可为法律、信息技术等相关领域研究人员提供共同的研究平台,促进跨学科的知识融合。

3) 数据跨境风险机理研究具有指导实践优势,即通过对跨境数据相关法律法规的深入分析,可以帮助跨境数据相关角色更好地理解和遵循相关法规与标准,降低合规风险成本。

4) 依据数据跨境风险机理研究中已识别的风险要素,可以实施风险重点管控,阻断风险演化路径。进而达到预防风险事故发生和降低风险损失的目标。

## 7.2 数据跨境风险机理指导风险措施的优势

本文提出数据跨境风险机理研究,一方面可以在理论上支持数据跨境风险研究,另一方面可以为规避风险或降低风险损失提供支持。

应用典型案例:以广州互联网法院审理的“个人信息跨境案”为例,在该案件中数据主体在某咨询机构 APP 上预订境外酒店,并提交了个人信息。数据主体在事后阅读《客户个人数据保护章程》规定时,发现其个人信息被泄露至境外,随即向广州互联网法院提起诉讼,指控酒店集团和咨询公司未经充分告知,将其个人信息传输境外。案件审判结果该机构未履行告知和同意,侵害数据主体权益,需承担侵权责任。

针对上述案例,结合本文提出的数据跨境风险机理,可以从管理措施、人为因素等角度制定风险应对措施,以达到降低风险损失的目的。例如,在风险措施角度,可以制定如下风险管控措施。

1) 针对数据主体权益风险,强化管理体系,关系到数据主体单独同意授权管理以及其他数据主体权益管理。

2) 围绕合规收集、处理数据制度。应当强化履行告知数据主体义务,明确告知数据跨境的目的、方式等信息。制定相关业务操作流程,以流程管理规范风险行为。

3) 制定事前风险评估管理机制。针对发生跨境的数据,数据接收方以及数据流转的第三方的风险展开事前评估。

在人员因素方面,可以制定如下风险管控措施。

1) 积极开展人员数据跨境安全培训,提高相

关人员数据跨境风险防范意识。

2) 多项措施辅助相关人员实施跨境数据管理,提升数据跨境安全管控能力。

3) 开展数据跨境业务能力考核,以此督促相关人员提升数据跨境风险管控能力。

## 7.3 数据跨境风险机理研究的局限性

在数据跨境安全领域,本文基于业务驱动,首次针对数据跨境风险机理展开研究,该研究主要适用于专业性不强的“泛化的业务场景”。针对专业性较强的跨境业务场景,如医疗体系中的个人健康数据、金融领域的交易、征信或授信数据、信息基础设施的敏感数据等场景,其蕴含的风险不仅包括跨境数据风险,也包括医疗风险、金融风险和国家安全风险。因此,本文研究的局限性主要体现在高度抽象概括数据跨境风险机理,在各个行业领域内的针对性研究较弱。

## 7.4 工作展望

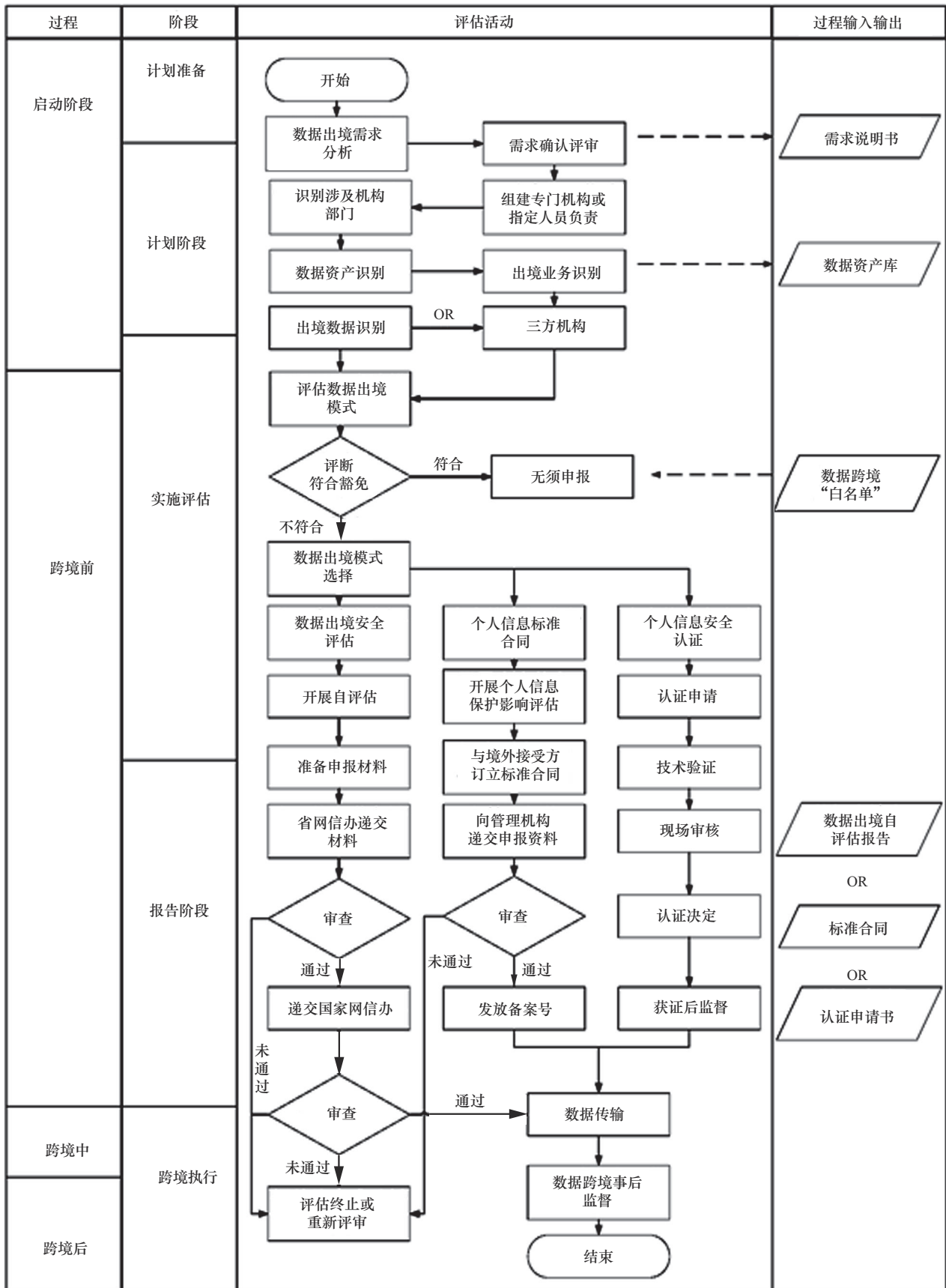
针对本文研究存在局限性问题,未来将围绕数据跨境典型业务场景展开具体化的分析研究,并在此基础上丰富和完善相关研究成果,以此支撑数据跨境安全体系建设,推动风险研究的深入发展。

本文研究拟基于数据跨境风险机理,以本文提出的风险要素为基础,进一步识别风险致因因素,并据此构建数据跨境风险要素体系。同时,筛选风险量化的研究方法,完成风险因素的指标分配,进而支撑构建数据跨境风险评估研究,为数据安全有序的跨境流动提供科学、客观的风险评估依据。

## 8 结束语

针对当前已有数据安全风险机理研究未能充分考虑跨境数据特有的风险形成原因以及关键要素,难以全面揭示跨境数据风险的全貌与内在联系,特别是内部隐患、外部威胁以及自身脆弱性等关键问题。本文基于 Petri 网建模、扎根理论、网络复杂分析等方法。在数据跨境安全领域,首次针对数据跨境风险机理展开研究。该研究基于数据跨境业务流程,面向跨境数据相关法律、法规、标准等规则要求,旨在为数据跨境风险研究提供基础支撑。

附录 1 金融行业数据跨境业务流程



### 附录 2 金融行业数据跨境风险致因调研结果

调研	风险程度	敏感、重要数据分类界定	人员因素	合规收集	结构化数	数据确权	数据跨境	数据主体	数据安全	出境数据	数据脱敏	环境因素	发生数据	出境目的	出境数据	出境频率	数据等级保护方案	处理个人信息规模	境内外储存安全环境
调研 1	A	D	A	B	E	A	B	A	C	C	B	D	B	B	C	D	C	C	D
调研 2	A	B	A	B	B	B	B	B	C	A	B	B	C	C	B	B	C	C	C
调研 3	B	A	C	C	C	B	C	C	C	B	B	D	D	D	D	D	C	A	C
调研 4	A	A	B	A	D	B	A	A	B	B	B	E	E	E	B	E	E	D	C
调研 5	A	D	A	A	A	D	A	B	C	C	B	D	B	A	D	A	B	C	D
调研 6	C	B	D	E	A	C	C	C	B	E	A	D	C	A	C	D	C	C	B
调研 7	A	C	A	A	D	A	B	A	A	C	C	D	B	C	A	D	E	D	C
调研 8	A	C	C	D	C	A	B	B	A	B	B	A	C	D	D	A	A	E	E
调研 9	A	C	A	C	C	A	A	A	C	E	E	D	C	B	A	D	C	D	A
调研 10	B	B	B	A	A	B	B	B	C	B	B	D	B	D	D	D	A	E	A
调研 11	C	C	C	B	B	C	C	D	E	A	A	A	B	B	A	A	A	A	B
调研 12	A	C	A	D	B	A	B	A	C	C	D	B	B	A	A	B	D	C	C
调研 13	C	A	C	B	A	A	D	B	D	A	A	B	C	B	C	B	A	A	C
调研 14	D	A	E	B	B	E	D	D	E	B	C	A	C	A	A	A	A	B	A
调研 15	A	A	A	A	A	A	A	B	E	A	A	A	E	C	C	A	B	B	C
调研 16	A	D	B	D	D	C	B	A	B	C	A	A	C	C	B	A	B	B	A
调研 17	A	B	A	E	A	C	A	A	C	A	A	D	C	A	A	D	B	E	E
调研 18	A	C	A	C	C	A	B	B	C	B	B	C	B	B	B	C	A	B	A
调研 19	D	D	D	D	D	D	D	D	B	D	D	D	D	D	B	D	B	B	C
调研 20	A	E	A	C	D	A	A	A	C	A	E	E	B	D	D	D	C	B	A

#### 参考文献:

[1] GUO B N, WANG Y, ZHANG H, et al. Impact of the digital economy on high-quality urban economic development: evidence from Chinese cities[J]. *Economic Modelling*, 2023, 120: 106194.

[2] 孙雯倩, 徐天辰, 余佩厚, 等. 基于《个人信息保护法》的 APP 隐私政策合规性检测[J]. *计算机工程*, DOI: 10.19678/j.issn.1000-3428.0069804.

[3] 张焕波, 毛天羽. 须高度重视美国《国际紧急经济权力法》[C]//中国智库经济观察(2019). 北京: 社会科学文献出版社, 2020: 183-187.

[4] 李卓卓, 刘子轶. 从分野到融合: 多学科视角下的数据跨境研究综述[J].

情报杂志, 2024, 43(12): 198-207.

LI Z Z, LIU Z Y. From divergence to convergence: a review of cross-border data research from a multidisciplinary perspective[J]. *Journal of Intelligence*, 2024, 43(12): 198-207.

[5] 傅贵, 陈奕燃, 许素睿, 等. 事故致因“2-4”模型的内涵解析及第 6 版的研究[J]. *中国安全科学学报*, 2022, 32(1): 12-19.

FU G, CHEN Y R, XU S R, et al. Detailed explanations of 2-4 model and development of its 6<sup>th</sup> version[J]. *China Safety Science Journal*, 2022, 32(1): 12-19.

[6] 徐拥军, 王兴广. 总体国家安全观下的跨境数据流动安全治理研究[J]. *图书情报知识*, 2023, 40(6): 20-30.

XU Y J, WANG X G. Security governance of cross-border data flow under the holistic view of national security[J]. *Documentation, Information & Knowledge*, 2023, 40(6): 20-30.

[7] 来小鹏, 马诗雅. 我国商业数据跨境流动合规治理的问题与完善[J]. *行政管理改革*, 2024(4): 43-53.

LAI X P, MA S Y. Reform path of compliance governance of cross-

- border flow of commercial data in China[J]. *Administration Reform*, 2024(4): 43-53.
- [8] 吴晓明, 初佳玉, 付剑玫. 企业数据跨境流动的风险防控研究[J]. *征信*, 2024, 42(4): 41-49.  
WU X M, CHU J Y, FU J M. Research on the risk prevention and control of cross-border flow of enterprise data[J]. *Credit Reference*, 2024, 42(4): 41-49.
- [9] 刘益灯, 宋歌. DPF 美欧数据跨境流动规则博弈及其镜鉴[J]. *世界经济研究*, 2024(7): 29-42.  
LIU Y D, SONG G. The implications of cross-border data flow between the EU and the U. S. through data privacy framework[J]. *World Economy Studies*, 2024(7): 29-42.
- [10] 李金, 徐姗, 卓子寒, 等. 数据跨境流转的风险测度与分析: 基于数据出境统计信息的实证研究[J]. *管理世界*, 2023, 39(7): 180-201.  
LI J, XU S, ZHUO Z H, et al. Risk measurement and analysis for cross-border data flow: an empirical study based on statistics of outbound data[J]. *Journal of Management World*, 2023, 39(7): 180-201.
- [11] 李金, 张黎明, 李建平, 等. 跨境数据传出机构的风险分类管控和影响因素分析[J]. *系统科学与数学*, 2022, 42(9): 2347-2366.  
LI J, ZHANG L M, LI J P, et al. Classified control and influencing factors for risks management in institutions with cross-border data flow[J]. *Journal of Systems Science and Mathematical Sciences*, 2022, 42(9): 2347-2366.
- [12] 陈统. 数据出境风险自评估机制的理解与适用[J]. *企业经济*, 2023, 42(4): 143-152.  
CHEN T. Understanding and application of self-assessment mechanism of data export risk[J]. *Enterprise Economy*, 2023, 42(4): 143-152.
- [13] PASCUAL H, ALAMO J M D, RODRIGUEZ D, et al. Hunter: tracing anycast communications to uncover cross-border personal data transfers[J]. *Computers & Security*, 2024, 141: 103823.
- [14] LI J, DONG W T, ZHANG C, et al. Development of a risk index for cross-border data movement[J]. *Data Science and Management*, 2022, 5(3): 97-104.
- [15] GUAMÁN D S, RODRIGUEZ D, ALAMO J M D, et al. Automated GDPR compliance assessment for cross-border personal data transfers in android applications[J]. *Computers & Security*, 2023, 130: 103262.
- [16] 董克, 吴佳纯, 马廷灿. 我国数据出境安全风险要素体系研究[J]. *情报理论与实践*, 2024, 47(6): 49-59.  
DONG K, WU J C, MA T C. Research of outbound data transfer security risk element system in China[J]. *Information Studies (Theory & Application)*, 2024, 47(6): 49-59.
- [17] MINIADOU K, LEONIDIS A, PAPADOPOULOS G T, et al. Encrypted biometric search: a deep learning approach to scalable and secure cross-border data exchange[C]//*Proceedings of the 2024 IEEE International Conference on Big Data (BigData)*. Piscataway: IEEE Press, 2024: 2794-2800.
- [18] ZHANG C, LIU Y, XU M D, et al. Trans-border trusted data spaces: a general framework supporting trustworthy international data circulation[J]. *IEEE Access*, 2025, 13: 30481-30496.
- [19] KULKARNI M S, NAIK H L, BHARATHI S V. Textual analysis of privacy policies to understand the effect of GDPR[C]//*Proceedings of the 2023 2nd International Conference on Futuristic Technologies (INCOFT)*. Piscataway: IEEE Press, 2023: 1-5.
- [20] HUANG X L, XIN C S, JI H J, et al. Cross-border data security risk analysis and development suggestions of the protection technologies for intelligent connected vehicles[C]//*Proceedings of the 2024 5th International Conference on Information Science, Parallel and Distributed Systems (ISPDS)*. Piscataway: IEEE Press, 2024: 257-262.
- [21] ZHUANG Z X, LEE X D, WEI J Q, et al. CBCMS: a compliance management system for cross-border data transfer[C]//*Proceedings of the 2024 IEEE International Conference on Big Data (BigData)*. Piscataway: IEEE Press, 2024: 4789-4798.
- [22] 张璐. 个人信息保护风险规范的建构机理与实现路径[J]. *江西财经大学学报*, 2022(3): 126-136.  
ZHANG L. The construction mechanism and realization path of risk specifications for personal information protection[J]. *Journal of Jiangxi University of Finance and Economics*, 2022(3): 126-136.
- [23] 陈朝兵, 吴钟灿. 政府数据开放中隐私风险的形成: 一个理论分析框架[J]. *内蒙古社会科学*, 2023, 44(2): 38-46.  
CHEN C B, WU Z C. Formation of privacy risk in government data opening: a theoretical analysis framework[J]. *Inner Mongolia Social Sciences*, 2023, 44(2): 38-46.
- [24] 王向明, 王炳涵. “数据要素×”助力新质生产力形成的作用机理与风险防范[J]. *河南社会科学*, 2024, 32(7): 10-21.  
WANG X M, WANG B H. The mechanism and risk prevention of “data elements ×” promoting the formation of new quality productive forces[J]. *Henan Social Sciences*, 2024, 32(7): 10-21.
- [25] 石江瀚, 佟泽华, 孙晓彬, 等. 科研大数据风险传导的机理研究[J]. *情报理论与实践*, 2022, 45(4): 17-26.  
SHI J H, TONG Z H, SUN X B, et al. Mechanism on risk conduction for scientific research big data[J]. *Information Studies (Theory & Application)*, 2022, 45(4): 17-26.
- [26] WAIRIMU S, IWAYA L H, FRITSCH L, et al. On the evaluation of privacy impact assessment and privacy risk assessment methodologies: a systematic literature review[J]. *IEEE Access*, 2024, 12: 19625-19650.
- [27] HUSSAINI S S, RAHARJO B. Comprehensive risk evaluation model for data center security risk assessment[C]//*Proceedings of the 2024 10th International Conference on Wireless and Telematics (ICWT)*. Piscataway: IEEE Press, 2024: 1-6.
- [28] FANG Z, ZHANG K, DIAO Y G, et al. Risk assessment based on data-flow dynamic hypergraph for cross-border data transfer[C]//*Proceedings of the 2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. Piscataway: IEEE Press, 2024: 2504-2509.
- [29] JIAO Z S, JIA W B, WANG H J, et al. Research on data security risk assessment methods for automobile enterprises[C]//*Proceedings of the 2024 4th International Conference on Big Data, Artificial Intelligence and Risk Management*. New York: ACM Press, 2024: 1020-1024.

- [30] JIN M. Research on building of scientific data security risk governance capability maturity model[C]//Proceedings of the 2023 3rd International Conference on Big Data, Artificial Intelligence and Risk Management. New York: ACM Press, 2023: 773-780.
- [31] 梁燕, 文泽鹏, 刘丽, 等. 基于本体的动态业务流程建模方法[J]. 计算机仿真, 2022, 39(11): 350-354.  
LIANG Y, WEN Z P, LIU L, et al. A dynamic business process modeling method based on ontology[J]. Computer Simulation, 2022, 39(11): 350-354.
- [32] COOK J E, WOLF A L. Automating process discovery through event-data analysis[C]//Proceedings of the 1955 17th International Conference on Software Engineering. Piscataway: IEEE Press, 1995: 73-82.
- [33] 吴肃然, 李名荟. 扎根理论的历史与逻辑[J]. 社会学研究, 2020, 35(2): 75-98.  
WU S R, LI M H. Grounded theory: history and logic[J]. Sociological Studies, 2020, 35(2): 75-98.
- [34] EVANS G L. A novice researcher's first walk through the maze of grounded theory: rationalization for classical grounded theory[J]. Grounded Theory Review, 2013, 22(1): 145-163.
- [35] SUDDABY R. From the editors: what grounded theory is not[J]. Academy of Management Journal, 2006, 49(4): 633-642.
- [36] 付玮琼. 核心企业主导的供应链金融模式风险机理研究[J]. 企业经济, 2020, 39(1): 136-143.  
FU W Q. Research on the risk mechanism of supply chain finance model led by core enterprises[J]. Enterprise Economy, 2020, 39(1): 136-143.
- [37] 杨海珍, 程相娟, 李妍, 等. 系统性金融风险关键成因及其演化机理分析: 基于文献挖掘法[J]. 管理评论, 2020, 32(2): 18-28.  
YANG H Z, CHENG X J, LI Y, et al. An analysis of the key causes and evolution mechanism of systemic financial risk: based on literature mining method[J]. Management Review, 2020, 32(2): 18-28.
- [38] 李晓英, 陈维政. 供应链风险形成机理研究[J]. 中国流通经济, 2003, 17(9): 10-13.  
LI X Y, CHEN W Z. A study on mechanism of the formation of supply chain risks[J]. China Business and Market, 2003, 17(9): 10-13.
- [39] 叶琼元, 夏一雪, 窦云莲, 等. 面向突发公共卫生事件的网络舆情风险演化机理研究[J]. 情报杂志, 2020, 39(10): 100-106.  
YE Q Y, XIA Y X, DOU Y L, et al. On the evolution mechanism of online public opinion risk for public health emergent events[J]. Journal of Intelligence, 2020, 39(10): 100-106.
- [40] 黄国桥, 徐永胜. 地方政府性债务风险的传导机制与生成机理分析[J]. 财政研究, 2011(9): 2-5.  
HUANG G Q, XU Y S. Analysis on the transmission mechanism and generation mechanism of local government debt risk[J]. Public Finance Research, 2011(9): 2-5.
- [41] PASCARELLA G, ROSSI M, MONTELLA E, et al. Risk analysis in healthcare organizations: methodological framework and critical variables[J]. Risk Management and Healthcare Policy, 2021, 14: 2897-2911.
- [42] RAWSON A, BRITO M. A survey of the opportunities and challenges of supervised machine learning in maritime risk analysis[J]. Transport Reviews, 2023, 43(1): 108-130.
- [43] AYDIN M C, BIRINCIOĞLU E S. Flood risk analysis using gis-based analytical hierarchy process: a case study of Bitlis province[J]. Applied Water Science, 2022, 12(6): 122.
- [44] ETEMADINIA H, TAVAKOLAN M. Using a hybrid system dynamics and interpretive structural modeling for risk analysis of design phase of the construction projects[J]. International Journal of Construction Management, 2021, 21(1): 93-112.
- [45] ZHANG Y, ZOU Y J, SELPI, et al. Spatiotemporal interaction pattern recognition and risk evolution analysis during lane changes[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(6): 6663-6673.
- [46] WANG J, ZHANG K, LI J Y. Network awareness of security situation information security measurement method based on data mining[J]. Journal of Intelligent & Fuzzy Systems, 2024, 46(1): 209-219.
- [47] 马冬青, 崔涛. 基于 TOPSIS 和 GRA 的信息安全风险评估[J]. 信息安全研究, 2024, 10(5): 474-480.  
MA D Q, CUI T. Information security risk assessment based on TOPSIS and GRA[J]. Journal of Information Security Research, 2024, 10(5): 474-480.
- [48] ZHANG J C, ZHENG J, ZHANG Z, et al. ATT&CK-based advanced persistent threat attacks risk propagation assessment model for zero trust networks[J]. Computer Networks, 2024, 245: 110376.
- [49] 马梓刚, 麻荣宽, 李贝贝, 等. SSPN-RA: 基于 SS-petri 网的工业控制系统安全一体化风险评估方法[J]. 计算机科学, 2024, 51(10): 380-390.  
MA Z G, MA R K, LI B B, et al. SSPN-RA: security integration risk assessment method for ICS based on SS-petri net[J]. Computer Science, 2024, 51(10): 380-390.
- [50] CHEN X H, ZHANG K S, CHEN B J, et al. Research on evaluation techniques for security threat levels of critical information assets in power grids[C]//Proceedings of the 2025 IEEE 8th Information Technology and Mechatronics Engineering Conference (ITOEC). Piscataway: IEEE Press, 2025: 828-833.
- [51] 耿文莉, 高梦瑜. 基于灰色神经网络的云平台大数据安全风险评估[J]. 科学技术与工程, 2021, 21(28): 11932-11937.  
GENG W L, GAO M Y. Security risk assessment of big data on cloud platform based on grey neural network[J]. Science Technology and Engineering, 2021, 21(28): 11932-11937.
- [52] CAO Z Y. Research on the application of building engineering informatization and security management based on BIM technology[C]//Smart Infrastructures in the IoT Era. Berlin: Springer, 2025: 495-511.
- [53] 邓汉年, 周杰, 杨波, 等. 基于随机 Petri 网的民机审定试飞实施流程建模与分析[J]. 计算机科学, 2024, 51(S1): 1075-1080.  
DENG H N, ZHOU J, YANG B, et al. Modeling and analysis of the implementation process of civil aircraft approval flight test based on stochastic Petri net[J]. Computer Science, 2024, 51(S1): 1075-1080.
- [54] 来小鹏, 郭子詠. 金融数据跨境流动的法律风险量化分析与规制建议[J]. 金融监管研究, 2024(4): 1-19.

LAI X P, GUO Z H. Quantitative analysis and regulatory recommendations on the legal risks of cross-border financial data flows[J]. *Financial Regulation Research*, 2024(4): 1-19.

- [55] 姚可欣, 付长军, 郑伟明, 等. 基于着色Petri网的离散事件动态系统建模与仿真[J]. *新型工业化*, 2021, 11(9): 101-104.

YAO K X, FU C J, ZHENG W M, et al. Modeling and simulation of discrete event dynamic systems based on colored Petri nets[J]. *The Journal of New Industrialization*, 2021, 11(9): 101-104.

- [56] FORRESTER J W. Industrial dynamics[J]. *Journal of the Operational Research Society*, 1997, 48(10): 1037-1041.

- [57] 秦雅琴, 董帅, 谢济铭, 等. 基于行车风险场的高速公路交织区车辆轨迹预测方法[J]. *汽车安全与节能学报*, 2024, 15(6): 952-961.

QIN Y Q, DONG S, XIE J M, et al. Methods for predicting vehicle trajectories in motorway weaving zones based on driving risk fields[J]. *Journal of Automotive Safety and Energy*, 2024, 15(6): 952-961.

- [58] LIU H, SHEN D, DABIĆ M, et al. A novel methodology for risk assessment considering risk higher order interactions and propagation effects[J]. *IEEE Transactions on Engineering Management*, 2025, 72: 907-924.

- [59] WANG X F, WANG T, ZHOU X, et al. Research on strategic risk identification method of equipment system development based on system dynamics[J]. *Journal of Systems Engineering and Electronics*, 2023, 34(5): 1225-1234.

- [60] LIU D, WANG K, DAI F X, et al. Network analysis on key causes of chemical accidents considering structural characteristics[J]. *Journal of Safety Science and Technology*, 2021, 17(7): 71-76.

- [61] GARVEY M D, CARNOVALE S, YENIYURT S. An analytical framework for supply network risk propagation: a Bayesian network approach[J]. *European Journal of Operational Research*, 2015, 243(2): 618-627.

- [62] HUANG W C, SHUAI B, ZHANG R, et al. A new system risk definition and system risk analysis approach based on improved risk field[J]. *IEEE Transactions on Reliability*, 2020, 69(4): 1437-1452.

#### [作者简介]



荣景峰 (1986-), 男, 辽宁沈阳人, 海南大学博士生, 主要研究方向为数据安全、数据分级分类、数据跨境安全等。



陈思宇 (2000-), 男, 四川成都人, 海南大学硕士生, 主要研究方向为数据安全、人工智能安全等。



王艺洋 (2001-), 男, 湖北襄阳人, 西安电子科技大学硕士生, 主要研究方向为数据安全等。



牛俊 (1992-), 女, 陕西西安人, 博士, 西安电子科技大学在站博士后, 主要研究方向为人工智能安全等。



刘徐杰 (1982-), 男, 广东普宁人, 中国移动通信集团海南有限公司工程师, 主要研究方向为网络安全渗透、APT攻击、数据安全跨境流动等。



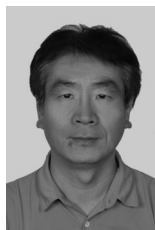
周安顺 (1975-), 男, 河南洛阳人, 南京邮电大学博士生, 中讯邮电咨询设计院有限公司正高级工程师, 主要研究方向为网络安全等。



付安民 (1981-), 男, 湖北通城人, 博士, 南京理工大学教授、博士生导师, 主要研究方向为数据安全、密码学和隐私保护。



曹春杰 (1977-), 男, 河北衡水人, 博士, 海南大学教授、博士生导师, 主要研究方向为无线网络安全、区块链、人工智能安全等。



张玉清 (1966-), 男, 陕西宝鸡人, 博士, 中国科学院大学教授、博士生导师, 主要研究方向为网络与系统安全等。