高校数据安全治理的模型研究*

巫莉莉，黄志宏，何斌斌
（华南农业大学　信息网络中心，广东　广州　510642）

摘　要：在分析我国高校数据安全面临的严峻挑战的基础上，提出了以目标为导向、内涵式发展、合理的指标体系、多元协同和基于业务场景的治理思路，通过数据安全治理能力、数据安全过程、业务场景三个维度将数据安全治理框架映射至高等教育领域，构建了贯穿数据生命周期的高校数据安全治理模型，指导数据高效、有序、可信流通，并建立了管理、技术、运营为一体的高校数据安全治理能力评估体系，支撑模型的应用发展，为提升高校数据安全治理水平提供科学的指引。

关键词：数据安全治理；治理模型；评估体系；评估指标；数据生命周期
中图分类号：TP309　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2025.07.007
引用格式：巫莉莉，黄志宏，何斌斌. 高校数据安全治理的模型研究［J］. 网络安全与数据治理，2025，44(7)：43-49.

Research on the model of data security governance in universities

Wu Lili，Huang Zhihong，He Binbin
(Information Network Center，South China Agricultural University，Guangzhou 510642，China)

Abstract：On the basis of analyzing the severe challenges faced by data security in Chinese universities，a goal oriented，connotative development，reasonable indicator system，diverse collaboration，and business scenario based governance approach is proposed. The data security governance framework is mapped to the field of higher education through three dimensions：data security governance capability，data security process，and business scenario. A university data security governance model that runs through the entire data lifecycle is established to guide the efficient，orderly，and trustworthy flow of data. And a university data security governance capability evaluation system that integrates management，technology，and operation is also constructed to support the application and development of the model，providing scientific guidance for improving the level of university data security governance.

Key words：data security governance；governance model；evaluation system；evaluation indicators；data lifecycle

0　引言

随着高校数字化转型的发展和数据价值的释放，与之而来的数据安全风险也越来越大。国内外已有很多学者开展了数据安全治理研究，但这些研究主要围绕数据安全治理能力评估、策略、体系框架等，对于高校数据安全治理模型的研究较少。其中，周林兴等[1]构建了档案数据安全治理能力成熟度模型，并划分了5个成熟度等级。杨晓琪等[2]从数据安全评估的角度出发，提出了一种“管理+技术”的数据安全评估模型。阙天舒等[3]立足于全球视野指出在数据安全治理方面的困境与存在的问题，并提出我国数据安全治理的优化策略。崔益峰等[4]针对国内高校面临的数据安全治理问题，提出了建立全生命周期的安全控制策略、技术防护体系以及治理机制，但并未提出一个完整的治理模型。王玉等[5]基于国产化安全需求，提出了适用于我国政务数据安全治理的体系框架。专门针对高校业务场景的数据安全治理比较欠缺。本文在高校数据治理的基础上，在以数据为核心的方法论框架下，构建一个多维一体的高校数据安全治理模型，全力打造科学化、精细化、规范化的高校数据安全治理新范式，通过数据安全工作建设高校数字化转型安全合规的数字底座。并结合高校数字化转型过程中对数据安全的要求，探索一条符合中国高校特色的数

*基金项目：教育部产学合作协同育人项目（231105921100023）

据安全实施路径，在充分发挥数据价值的同时保障数据在高校各部门、各应用、各业务中高质、高效、可信的流通，将高校自身发展需求与数据安全战略相融合，促进高校数据安全新生态和新格局的形成，保障高校数字化的安全转型。

1 数据安全治理内涵

数据安全强调的是数据的合法利用和有效保护之间的动态平衡与持续保护。2019 年《信息安全技术 数据安全能力成熟度模型》（GB/T 37988—2019）将数据安全定义为：通过管理和技术措施，确保数据有效保护和合规使用的状态[6]。2021 年《中华人民共和国数据安全法》将数据安全解释为：通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。从数据安全定义的发展来看，主体开始意识到数据安全是一个动态的、不断发展完善的过程，应该更加关注数据安全建设、发展的持续性。

数据安全治理是依据组织顶层数据安全战略，内外部相关方协作实施的一系列治理措施和活动的集合，在此基础上确保组织的数据安全，使数据价值最大化，以此来支撑组织业务目标的实现，推动业务与数据安全一体两翼、平和发展。数据安全治理可以分为宏观和微观两个层面。宏观层面，为了利用数据促进国家数字经济和社会的有序发展，治理主体通过国家战略、法律和政策，进行顶层设计、制度完善、组织建设，保障数据安全技术体系和人才队伍等的建设；微观层面，治理主体为了有效保护数据、保障数据的合法利用，在国家相关政策和战略的指导下，针对数据资源的采集、存储、开放、共享和利用等环节，通过相关技术手段，实施数据安全管理及评估等工作[7]。

1.1 以数据为中心

随着 2020 年发布的《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》（以下简称《意见》），数据已成为具有重要价值和战略意义的新时代资源，对社会发展、国家治理、个人生活等方方面面均产生了重大而深远的影响。2024 年国家数据局等 17 部门印发《“数据要素 ×”三年行动计划（2024—2026 年）》，指出为了更好地落实《意见》，发挥数据要素的放大、叠加、倍增作用，构建以数据为关键要素的数字经济，是推动高质量发展的必然要求[8]。因此，顺应数字经济时代发展的大趋势，建设以数据为中心的全方位的数据安全治理模型，是保障数据有效利用和健康发展的根基。

1.2 以数据生命周期为要素

数据安全治理贯穿了数据的整个生命周期，从采集、存储、传输、处理、交换到销毁的完整闭环，跟随着数据的流动使其具有动态性和持续性的特点[9]。由于不同环节不同主体之间的利益驱使，导致每一个环节都极易产生流动的数据安全威胁和风险。因此，以数据生命周期为要素，根据生命周期各环节的任务，结合具体的业务场景进行全流程保护，识别生命周期中存在的数据安全问题并有指向性、有目的性地解决问题，达到以数据为中心的更加细粒度的安全防护要求，更易确保数据安全防护机制的整体性。

1.3 以促进数据安全和数据开发利用均衡发展为目标

在数字化转型的关键期，高校应着眼全校信息化和数据安全全局，把握好安全与开发之间的动态平衡。《数据安全法》第十三条明确了安全与发展是一个相辅相成的关系，两者不能只顾其中之一，而是要并重齐驱，形成数据开发利用与数据安全相互促进发展的局面。安全是发展的根本、前提和基础，在数据驱动的时代更要时刻守好安全这一底线[10]。数据的流通让其成为具有生命力的生产要素，只有在安全的土壤环境下，才能结出健康发展的果实，从而推动数字经济高质量的发展，反作用于数据安全的实现。

2 高校数据安全面临多重挑战

国内大部分高校经过多年的网络安全建设，普遍建成了校园内外网安全防护模式的边界防御体系。随着国家数据安全法制进程的推进，目前校园网络安全防护的措施已不能满足数据安全的要求。高校数据安全的问题集中体现在：一方面，高校数据安全治理是推动数据安全合规使用的重要保障，必须满足体系化、持续化的整体需求；另一方面，高校数据安全工作面临着碎片化、滞后化等多重挑战，落地情况与规划相差甚远，严重制约了数据安全治理能力的提升。

2.1 重视度不够，建设滞后性突出

2.1.1 顶层规划缺乏布局

部分高校制定规划时重视国家的大政方针，却忽视结合学校的实际情况，造成战略制定得偏高或是制度架空的现象。高校的数据安全治理需要整合学校当前和未来的发展需要进行布局，在制定数据安全治理方针时要达成共识，并结合具体的业务场景将数据安全的工作任务和可用资源进行合理配置，减少重复性建设和资源投入，根据学校战略规划的变化适时演进，逐步促进顶层规划的实施与落地。

2.1.2 缺乏数据安全文化

高校的数据安全治理要取得成功，需要建立校园数据文化氛围。师生作为数据安全工作中重要的核心主体，

缺乏将数据安全意识主动融入工作和学习中的观念，缺乏提升数据安全意识和素养的使命感，导致数据安全工作长期集中在信息化部门，提升师生数据安全意识和素养成为口号，造成数据安全事件层出不穷。将数据安全教育融入日常工作和学习中，强化高校自身的数据安全文化软实力，数据安全治理工作推进起来才能事半功倍。

2.2 组织保障不足，运营管理困难

2.2.1 缺乏专业的运营人员

人员的不稳定是造成数据安全风险的因素之一。高校业务数据多、业务系统分散、数据存储介质多样，负责数据安全的专业技术人员不足，存在重设备轻技术的现象。管理人员缺少数据安全法律法规、知识技能培训，相关技术和技能存在明显的滞后性，面对数据安全建设和处理数据安全事件时人手和经验双重紧张，难以达到数据安全发展的要求。

2.2.2 缺乏多元主体的协作

数据安全涉及整个数据生命周期，必然涉及多个主体的协作，建立健全各主体的常态化协作机制至关重要。高校各主体缺乏协作共赢的开放性思维，各主体之间难以形成合力，主体角色缺位、错位甚至掣肘的现象屡见不鲜，导致难以形成一套跨部门、跨场景协同发展的数据安全管理机制保障数据安全治理工作的落地。

2.3 技术能力缺失，合规性风险增高

2.3.1 数据底数不清

高校作为培养高层次人才和发展科研创新的重要战略基地，拥有大量的师生个人信息、教学、管理等数据，以及高价值的科研数据等，数据资产规模大。高校业务部门和业务系统众多，数据使用方式多样、使用人群庞大，导致数据资产梳理难度增大，难以掌握高校拥有的准确数据量和数据流向，同时还存在数据越权使用的风险，严重制约了数据安全治理工作的有效开展。高校需配置专职的数据安全人员，借助专业的技术手段和工具协助完成数据资产分布的摸查，形成校级数据资源目录，基于目录明确数据安全管理的权责，强化数据安全治理的依据。

2.3.2 分类分级不到位

数据安全工作有序开展的前提是进行数据的分类分级。2024 年《数据安全技术 数据分类分级规则》（GB/T 43697—2024）国标的实施，开启了“数据安全技术”系列国家标准的新纪元，为各领域数据分类分级的标准化工作提供了清晰的方法论和系统化指导。数据分类分级是保障高校数据安全治理有效落地实施的极为重要的一环，但目前还缺乏标准化、自动化的分类分级工具，仍然需要人工投入大量时间对数据进行手动分类分级，导致执行效率及准确度低下。目前教育行业的数据分类分级标准缺乏，高校首先应制定符合学校业务发展的数据分类分级原则，通过对数据进行分类分级摸清学校的数据家底，形成数据地图，基于数据地图形成高校的重要数据资源目录，持续推进数据分类分级的场景应用，将数据安全防护工作落在实处。

3 高校数据安全治理思路

高校数据安全治理聚焦高校数据安全工作中普遍关切的突出问题和主要矛盾，以“全局统筹规划，技术保障落地，运营加强实施，业务场景牵引，评估助力优化”的实践理念为指导思想，激励、引导高校数据安全治理工作的落实推进，形成成熟、完善的高校数据安全治理模型，加快实现高等教育的现代化。

3.1 明确数据安全的目标导向

目标导向决定了模型的应用方向。《信息安全技术 数据安全能力成熟度模型》（GB/T 37988—2019）的提出为数据安全能力的提升指明了发展方向，可以此为依据指导教育行业开展数据安全治理。高校的数据安全目标群体是师生，目标对象是数据，而目标是要基于高校的校情，构建支撑高校业务场景实施的数据安全治理模型，从保障数据生命周期各阶段安全的角度出发，确保数据安全合规地流动和使用，同时利用数据促进业务的发展。

3.2 坚持内涵式发展的理念

准确把握教育强国、网络强国、数字强国的基本内涵，结合新时期国内高校的发展重心和高等教育的特点，形成“数据为主、安全导向、持续加强”的内涵式发展理念。一是要强化以数据为中心的理念，利用数据安全治理保障数据合规可用，以数据驱动业务发展为核心，坚持安全贯穿数据的整个生命周期，打造安全可信的高校数据底座，推动数据的流通。二是要以业务为抓手，开展场景化的数据安全防护，敏捷落地相关数据安全能力，平衡数据安全与业务发展的关系，在发展中重安全，在安全中促发展。三是要加强保障机制和能力评估，把常态化检测和阶段性评估有机结合，督促高校建立健全数据安全治理的保障体系[11]。

3.3 构建合理的指标体系

合理的指标体系为认识和评估高校数据安全治理水平提供全面的指导框架。数据安全治理模型没有统一的评估指标体系，须针对高等教育领域的特点，对指标进行合理的选择和重构，构建一个有利于形成数据安全治理绿色生态的评估指标体系。指标的选取总体上数量要适中，须兼顾指标导向性、代表性、可延续性，注重指

标数据获取的可行性[12]，为高校组织实施数据安全治理提供科学、有效的指导依据和评估指南；同时还要考虑指标的可量化性，通常以定性和定量的方法进行综合评估，便于整个评估体系的精准化、持续化评估，更好地辅助支持高校管理层的决策。

3.4 完善多元协同的保障机制

获得数据安全治理全新价值的关键在于协同共生。在高校数据安全治理过程中，需注重总体布局，推动高校各主体在各方面、各环节、各因素之间的协调联动。一是从学校层面建立稳定、有效的数据安全治理组织，加快形成权责明晰、分工协作、保障有力的组织架构，为业务部门和技术部门的协作提供组织保障。二是形成多元协同共治的常态化工作机制，通过做好对内学校部门之间，对外学校和企业、社会之间的各方协同，集合各主体的优势和资源，提升解决问题的效率，最终形成共同治理的良好生态[13]。

3.5 基于业务场景开展治理

数据安全的本质是保护数据在开放、共享、流动和使用过程中的安全。在发展过程中往往会出现“重建设、轻应用”的状态，业务上聚焦在工具平台或信息系统，容易忽视在业务的开展应用过程中数据流动产生的安全风险。高校发展过程中业务活动是数据的载体，在统筹兼顾数据安全与业务发展的前提下，基于业务场景开展数据安全治理，根据业务场景的重要性进行差异化的安全管控，以“点－线－面”的形式编织数据安全一张网，以保障业务战略目标为前提，促进高校教学、科研、管理、服务中各项业务的安全性、连续性，驱动数据安全治理的常态化开展。

4 高校数据安全治理模型的构建

数据安全治理是一个动态的、持续演进的过程。为了贯彻落实国家的总体安全策略，统筹高校的数字化发展和安全，在大量实践标准和策略研究的基础上，借鉴数据安全治理（Data Security Governance，DSG）和数据安全能力成熟度模型（Data Security Capability Maturity Model，DSMM）的理念和架构，结合网络安全等级保护制度2.0的要求，本文提出了一个具有科学性、指导性的高校数据安全治理模型（Universities Data Security Governance Model，UDSGM）。UDSGM包括数据安全治理能力、数据安全过程、业务场景三个维度（如图1所示），旨在通过模型应用帮助高校了解自身的数据安全治理水平，提升数据安全治理的能力。

4.1 高校数据安全治理能力

因各个学校发展程度各异，在数据安全建设管理、技术和运营等方面的能力也有所不同，亟需通过打造一把能够衡量各高校数据安全治理能力水平的“标尺”，推进共性治理能力的标准化建设，形成一个可量化的评估体系，以评估工作为抓手促进数据安全治理能力的提升与业务发展。数据安全治理能力维度明确了高校在数据安全治理中应具备的能力，构建了基于能力支撑的数据安全治理评估体系，分为评估指标体系和能力等级两部分。

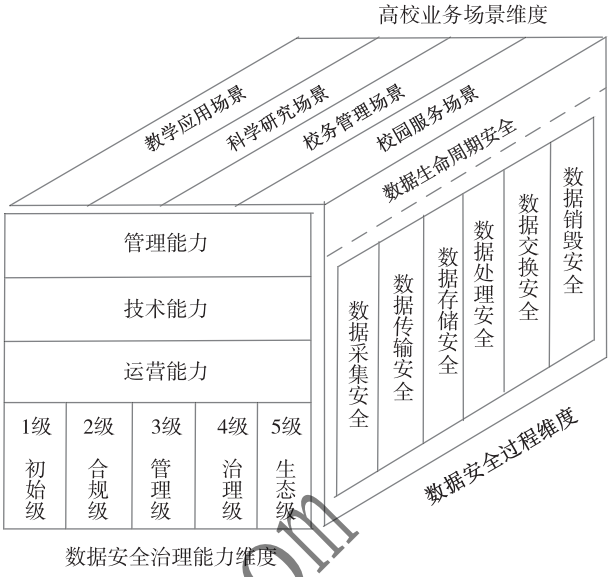

图1 高校数据安全治理模型

4.1.1 高校数据安全治理能力评估指标体系

通过高校数据安全治理能力评估指标体系将能力拆分为多维指标进行评估，进而掌握每项指标的实现能力。从系统论的角度出发，高校数据安全治理能力评估指标体系分为3个层级，包括3个一级能力指标、10个二级能力指标和30个三级能力指标，如表1所示。整个指标体系由下一级指标对上一级指标进行内涵式的阐述，形成有机整体，全方位、多层次地展现高校数据安全治理能力的整体状态。

高校数据安全治理能力评估指标体系包括管理能力、技术能力和运营能力三个方面。管理能力是前提，主要是通过制定、执行、改进学校的数据安全治理战略、标准、制度，夯实管理制度和架构基础，从组织上保障数据安全治理的有序开展；技术能力是关键，表现为通过构建校园网络等基础设施安全防护、平台安全防护和培养技术人才队伍等措施，提升数据安全的技术防护水平，保障数据安全治理的精准施策；运营能力则是基础，通过全方位的运营管理，保障高校数据安全的规划、实施、运行、监督的全程监控，最大化安全业务的价值，驱动管理和技术的可持续融合发展。三个能力彼此相辅相成，相互促进，形成高校数据安全治理的闭环[14]。在具体落

地上，针对三个一级能力指标建立相应的管理、技术和运营体系，三个体系协同配合、逐步实现完善的数据安全保护能力。

表 1　高校数据安全治理能力评估指标体系

一级能力指标	二级能力指标	三级能力指标
管理能力	战略规划	规划设计
		经费保障
	组织机构	组织架构
		人员配置
		协同机制
	制度流程	方针政策
		规章制度
		流程规范
技术能力	校园网络安全	设备安全
		通信安全
		应用安全
		终端安全
	能力平台	安全资质
		平台规模
		扩展能力
	数据管控	数据合规利用
		教育数据分类分级
		科研数据出境安全
	技术人才	专业队伍
		专业能力
		安全素养
运营能力	运营机制	安全协同
		监控预警
		风险防范
		应急处理
	人员保障	安全教育
		技术培训
		技能考核
	考核监管	评估检查
		运营绩效

4.1.2　高校数据安全治理能力等级

UDSGM 对高校的数据安全治理水平进行了分析和总结，将数据安全治理能力划分为 5 个等级，从低到高依次为：初始级、合规级、管理级、治理级、生态级，分别代表高校数据安全治理的不同阶段，是一个逐级上升的过程[15]，如图 2 所示。

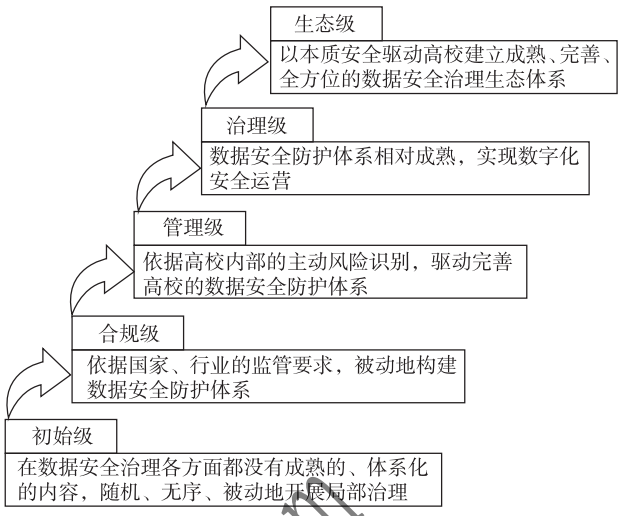

图 2　高校数据安全治理模型阶梯进化图

（1）初始级

高校对数据安全治理的意识浅薄，没有制定数据安全治理战略和规划，没有相应的组织负责，数据安全治理能力方面处于管理无序、无专业人员、专业设备欠缺的状态，属于高校数据安全治理的起步阶段。

（2）合规级

高校开始重视数据安全治理的建设，主要聚焦于满足国家监管机构或行业的合规要求，从战略、组织、基建、技术、人员、文化等方面具备了基本规范的数据安全治理能力，实现从无到有的转变。

（3）管理级

管理级是高校数据安全治理建设从被动防御转为主动防御的阶段。关注数据生命周期的安全，基于教学、科研、管理、服务等业务场景，依据当前主动探索的安全风险进一步完善数据安全防护体系，在一定范围内不同程度地实现了数据安全治理战略和规划。

（4）治理级

治理级注重精细化管理、技术的有效应用和量化的运营考核，通过常态化的数据安全运营，从“被动合规”转为“主动治理”，实现持续的数据安全保障能力。数据安全技术基于业务场景的应用程度较高、范围较广，基本覆盖了数据生命周期的全过程。

（5）生态级

生态级代表高校达到具备向行业输出成功经验的高水平数据安全治理能力。高校基于健全的组织架构和机制、先进的技术支撑、可靠的人员队伍、良好的数据安全文化氛围等，以持续优化为主要目标，形成了成熟、完善、全方位的高校数据安全治理生态体系。

4.2 数据安全过程维度

基于数据生命周期开展数据安全治理，贯穿数据处理流转的各个环节，主要目标在于发掘数据风险的真正源头，对数据流动的轨迹、状态的变化进行追踪。根据DSMM生命周期各阶段的过程域，基于学校已有的网络安全防护能力，结合高校实际的业务流程和数据安全风险，梳理了技术防护措施和对应的技术工具（如表2所示），便于依据数据风险变化做出细粒度的、动态的、精准的控制，持续提升数据安全的事前风险预警能力、事中防护能力、事后追溯能力。其中在技术防护措施方面，针对贯穿数据生命周期的基线核查、身份验证和访问控制等通用数据安全措施没有在表中一一列明。

表2 高校数据生命周期的技术防护措施和工具

数据生命周期阶段	DSMM过程域	技术防护措施	技术工具
数据采集	数据分类分级 数据采集安全管理 数据源鉴别及记录 数据质量管理	数据加密 数据脱敏 真实性保障 质量管理 分类分级	分类分级工具 数据脱敏系统 数据加密系统 数据中台
数据传输	数据传输加密 数据可用性管理	真实性保障 完整性保障 审计监控	数据库审计系统 数据加密系统 数据防泄露系统
数据存储	存储媒体安全 逻辑存储安全 数据备份和恢复	数据冗余 密码加盐 数据加密 完整性保障 数据备份 数据恢复 数据归档	灾备系统 数据加密系统 数据库运维管控 数据库防火墙 数据归档软件
数据处理	数据脱敏 数据分析安全 数据正当使用 数据处理环境安全 数据导入导出安全	系统容灾 数据校正 不可抵赖性保障 数据脱敏 数据加密 隐私计算 安全计算	数据库防火墙 数据库运维管控 数据脱敏系统 灾备系统 数据加密系统 数字签名
数据交换	数据共享安全 数据发布安全 数据接口安全	数据脱敏 数据加密 安全计算 隐私计算 API监测	数据脱敏系统 数据水印系统 数据加密系统 数据库防火墙 数据库运维管控 API监测系统 数据库审计系统
数据销毁	数据销毁处置 存储媒体销毁处置	安全销毁	数据销毁工具

4.3 高校业务场景维度

高校普遍开展了不同程度的数据治理，梳理出高校的数据资源目录，可为数据安全治理建设奠定数据底座基础。根据数据安全需求侧的分析，将高校业务场景划分为教学应用场景、科学研究场景、校务管理场景和校园服务场景四类（如表3所示）。

表3 高校业务场景划分及数据安全风险

场景名称	场景描述	数据安全风险
教学应用场景	教学应用场景不仅涵盖了传统的教学方式，还融入了AI技术，通过多样化和现代化的智慧教学，实现学生个性化的培养方式，为培养全面发展的人才提供有力支持	1. 系统漏洞风险 2. 数据泄露风险 3. 权限控制风险 4. 数据篡改风险 5. 数据出境风险 6. 数据丢失风险 7. 法律法规合规风险
科学研究场景	科学研究场景涵盖实验室、科研平台、数字化应用、学术交流与合作、智慧校园基础设施建设等方面，为高校科研人员提供了研究环境和丰富的资源支持	
校务管理场景	校务管理场景涵盖师生管理、财务管理、资产管理、科研数据管理、行政管理、校园安全与后勤管理以及智慧校园平台建设等多个方面，为高校的正常运转和持续发展提供了有力保障	
校园服务场景	校园服务场景涵盖师生的衣食住行一站式服务、图书借阅服务、健身运动服务、心理咨询服务、学生就业服务等，为师生提供全方位、便捷、高效的服务，提升校园生活质量和教育教学水平	

高校教学应用、科学研究、校务管理、校园服务场景由一系列相关联的业务活动组成，如图3所示。图中的活动1～N是指学校教学、科研、管理、服务等业务中某个业务场景中的具体流程节点，是业务场景的基本业务元素单元，通过数据流转串联或并联，最终构成满足某个业务场景的连续业务行为的集合[16]。每一个业务活动满足5W元素，即Who（谁）、What（什么）、When（何时）、Where（何地）、Why（为什么），例如高校教师

职称评审，从用户需求侧来看提交评审申请这个业务活动，涉及参与评审的教师（Who）参加职称评审（Why），通过职称评审系统（Where）提交职称评审申请（What），并在评审期内（When）可随时访问系统。数据安全方面需要规避表3中数据安全风险的描述，防止用户对职称评审系统数据的越权查询、下载以及增、删、改等数据操作。

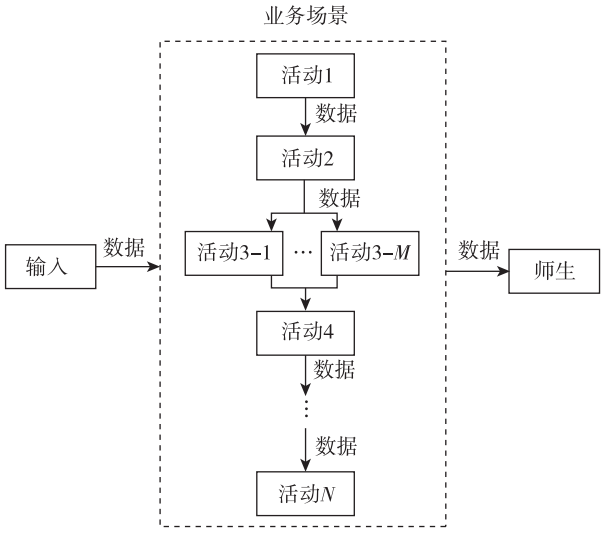

图3　业务活动与数据流转模型

5　结束语

本研究构建了一个融合高校业务场景的数据安全治理模型，可作为高校数据安全治理水平发展的一种指南。数据安全治理非常重要，具有长期性、战略性的特点，模型的建立具有重要的理论意义、实践意义和现实意义，既可以指导高校对标进行数据安全治理，又可以为高校提升数据安全治理水平明确方向和实施内容。高校的数据安全治理是一种实践，其本质不在于知而在于行。高校数据安全治理模型给出了高校数据安全治理的建设框架，如何将整套框架切实应用于建设过程，还需要经过不断实践来探索一条可实施路径。通过不断探索、验证、迭代和完善模型，以用促建，切实守住高校的数据安全底线，推进数据安全治理与业务持续同步发展，让高校数据安全治理能力标准化、模式化，形成高等教育行业可以通用的数据安全治理参考标准。

参考文献

[1] 周林兴，韩永继. 档案数据安全治理能力成熟度模型构建研究［J］. 档案与建设，2020（7）：24－27.
[2] 杨晓琪，白利芳，唐刚. 基于DSMM模型的数据安全评估模型研究与设计［J］. 信息网络安全，2021，21（9）：90－95.
[3] 阙天舒，王子玥. 数字经济时代的全球数据安全治理与中国策略［J］. 国际安全研究，2022，40（1）：130－154.
[4] 崔益峰，袁先珍，张斌. DSMM框架下高校数据安全治理研究［J］. 电子测试，2022，36（22）：87－89.
[5] 王玉，安鹏，栗文科，等. 政务数据安全治理体系研究与实践［J］. 信息安全研究，2023，9（9）：900－907.
[6] 信息安全技术 数据安全能力成熟度模型（GB/T 37988－2019）［S］. 2019.
[7] 杨蕾，袁晓光. 数据安全治理研究［M］. 北京：知识产权出版社，2020.
[8] 国家数据局. 十七部门关于印发《“数据要素×”三年行动计划（2024—2026年）》的通知［EB/OL］.［2025－03－01］. https://www.cac.gov.cn/2024－01/05/c_ 1706119078060945.htm.
[9] 刘隽良，王月兵，覃锦端，等. 数据安全实践指南［M］. 北京：机械工业出版社，2022.
[10] 张平. 中华人民共和国数据安全法理解适用与案例解读［M］. 北京：中国法制出版社，2021.
[11] 范唯. 高等教育评估制度体系建设的未来构想［EB/OL］.［2025－03－01］. https://m.gmw.cn/baijia/2021－02/08/34606387.html.
[12] 胡俊平，曹金，李红林，等. 全民数字素养与技能评价指标体系构建研究［J］. 科普研究，2022，17（6）：25－31.
[13] 陈永杰. 多元协同 推进高校数字化转型［J］. 中国教育网络，2023（12）：18－20.
[14] 吕毅. 主动构建数据安全体系，稳步推进数据安全治理［J］. 中国信息安全，2019（12）：54－55.
[15] 林宝晶，钱钱，翟少君. 网络安全能力成熟度模型［M］. 北京：机械工业出版社，2021.
[16] 李雪莹，王玮. 基于业务场景的数据安全治理模型［J］. 信息安全研究，2022，8（4）：392－399.

（收稿日期：2025－03－07）

作者简介：

巫莉莉（1979－），女，硕士，高级工程师，主要研究方向：数据治理、数据安全、大数据分析。

黄志宏（1981－），通信作者，男，硕士，正高级工程师，主要研究方向：网络安全、数据安全。E-mail：huangzh@scau.edu.cn。

何斌斌（1982－），男，本科，高级工程师，主要研究方向：网络安全、数据安全、大数据分析。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部