构建前中后台多方协同安全治理模式

——建设银行数据安全管理的思考与实践

文/谢　坤*

摘要：在数字化转型浪潮中，数据安全是数据应用和数据价值实现的护城河。如何同时实现数据安全保护和数据要素加速释放，已成为监管机构、社会各方关注的热点，也成为金融机构探讨的课题。本文从数据安全管理体系建设和数据安全生命周期保护等方面，介绍建设银行数据安全管理工作开展的整体思路，分享建设银行数据安全管理机制和技术防护等实践经验。

关键词：数据安全　数据分类分级　数据生命周期

近年来，建设银行以数据为关键生产要素，立足新发展阶段、贯彻新发展理念、践行新金融行动，着力推进三大战略，强化数据、技术双轮驱动，在数字化转型领域不断探索和发展，以先进的企业级数据能力和一体化系统支撑能力为全行业务发展保驾护航。可以说，数字化转型早已成为全行的共识，数据文化也已渗透到建设银行经营管理的方方面面。当数据成为新的驱动力，数据安全管理的重要性日益凸显。数据安全是数据要素有序开发利用与价值释放的重要前提和保障，是商业银行实现数字化转型的重要基础。作为国有大行，建设银行始终坚持统筹发展和安全，着力提升数据治理能力，通过搭建一体化的数据安全保障体系，为新金融行动保驾护航。

* 作者单位：中国建设银行股份有限公司。本文是根据作者2023年9月在第12届中国支付清算论坛数据安全分论坛上的发言整理。

一、理解与思考

近年来，《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》相继颁布，数据信息安全领域的法律法规体系逐步完善。党中央、国务院先后印发了“数据二十条”“数字中国建设规划”等，组建了国家数据局，数据要素的价值发现将进入快速发展的轨道。国务院政府工作报告连续三年强调“数据安全”。党的二十大报告明确了数据安全是总体国家安全观的重要组成部分。“数据二十条”的指导思想也确定要以维护国家数据安全、保护个人信息和商业秘密为前提，以促进数据合规高效流通使用、赋能实体经济为主线。因此，“数据安全”已成为关乎国家安全和社会稳定大局的重要因素。

然而，当前数据安全形势不容乐观，无论是在国际上还是国内，数据安全事件频发。据媒体从天津的国家计算机病毒应急处理中心获悉，2023 年第一季度，涉及我国的数据泄露事件仍呈现高发态势，受影响较大的行业包括教育、卫健、金融等。其中，单次遭泄露数据量在 10 万至 100 万条区间内占比最高，接近总量的一半，而遭泄露数据仍以公民个人信息为主。在社会层面，数据安全问题极易传播和发酵，从而导致声誉风险。实践中，既有机构因“存在数据泄露风险”被处罚，也有互联网平台因涉及数据安全与保护被调查。

金融行业作为科技驱动型和数据密集型行业，一直以来都是监管机构重点关注的行业。近年来，监管机构陆续出台了一系列数据安全制度规范，指导商业银行贯彻党中央、国务院决策部署，落实法律法规要求。可以说，监管要求逐步明确细化，也更加严格。

从支付产业来看，数字经济背景下，支付领域数据共享开放场景更为复杂，金融与非金融场景融合发展，用户与金融机构的触点更加广泛，进一步加速了数据要素的流动，数据治理环境更加复杂多样，传统数据治理框架下的管理机制需随之优化，数据安全意识有待进一步宣贯，数据安全保护技术和工具需不断升级，这些都是支付产业高质量发展面临的挑战。

那么，如何平衡好数据安全与数据应用，在守好安全底线前提下满足业务发展需求。首先要构建前中后台多方协同安全治理模式，落实三道防线管理职责，

压实数据安全责任，牢固树立数据安全红线意识。其次要建立健全企业级的数据安全治理体系，将数据安全管控要求和措施贯穿于数据生命周期全过程，保障数据合规、安全、高效流通，释放数据要素价值。

二、探索与实践

建设银行确立了数据安全管理的基本原则，即“合法合规、全面覆盖、各尽其职、保护有效、保障应用”。围绕“组织架构、制度体系、技术防护体系、运营管理以及培训宣贯”五个方面推进数据安全管理体系的完善。

（一）组织架构方面

建设银行建立了覆盖管理层、执行层和监督层三个层次数据安全组织架构。管理层，明确了总行党委的数据安全责任，金融科技与数字化建设委员会统筹数据安全工作。执行层，数据管理部门牵头管理全行数据安全工作，科技部门负责在信息科技领域落实数据安全工作，各业务部门负责在所管辖业务领域工作中落实数据安全管理要求。监督层，风险管理部门、内控合规部门在职责范围内落实数据安全风险管理、内控评价、问责处置等工作，审计部门开展数据安全审计工作。同时，建设银行将数据安全风险纳入全面风险管理体系，压实“三道防线”责任，加强协同联动，确保数据安全风险管控“横向到边，纵向到底”。

（二）制度体系方面

建设银行构建了数据安全制度规范体系，对标数据安全法律、法规及监管要求，在数据管理、科技管理、业务管理三大领域，推进一系列数据安全管理相关制度和流程机制的建立，形成了网络安全、信息安全、数据安全和个人信息保护协同一致的制度规范体系。同时，进一步细化制定了分类分级保护、应急管理等专项制度和实施细则。

（三）技术防护体系方面

建设银行依托新一代企业级安全即服务（SaaS）的安全架构，建立了“外防攻击窃取、内防数据泄露、全面安全监控”的数据安全技术防护体系。在抵御外部攻击窃取方面，通过构建“四道防线”的纵深防御技术防护措施，实现不法分子网络“进不来”；通过向上层应用统一提供身份认证、授权、数据加密、安全监控等安全技术措施，实现非授权信息“看不懂”和“拿不走”，有效应对和

防范外部渗透窃取、数据库“拖库”、第三方数据泄露等客户信息安全风险。在内部数据使用管控方面，通过建立安全封闭的数据专用环境，严控终端设备和网络数据泄露途径，及时阻断内部操作导致的数据泄露风险。数据安全技术防护体系覆盖数据全生命周期，通过数据访问控制平台、隐私计算平台等技术平台沉淀了数字脱敏、加密权限、访问控制、数字水印、隐私计算等数据安全核心技术，为后台生产数据、前端分析数据等场景的数据保护提供技术支撑。

（四）运营管理方面

建设银行主要开展了以下八个方面的工作。

一是建立全域数据资产运营管理平台。数据资产全域管理是实现数据全生命周期和业务全流程数据安全保障的重要基础，建设银行通过全面盘点梳理入库全行数据资产，构建了企业级数据资产目录，做到“心中有数”，助力用户厘清数据资产分布及关联关系，勾勒企业级数据资产全貌，并提供数据地图和数据溯源等能力，为数据安全管理向“自动化、智能化”的转变夯实数据基础。

二是建立全域数据集成管理能力。建设银行依托数据湖和云化数仓两大数据中台基础设施，建立了内外部数据采集、整合和服务的规范与流程，进一步提高内外部数据的整合共享和供应效率，实现了对行内外数据的全量统一管理，做到“一网打尽”。遵循新一代标准规范，数据湖仓累计接入百余个上游组件库表数据，涵盖了交易流水、借记卡、信用卡等主要业务领域相关数据；持续提升数据时效性，入湖的批量数据中90%以上实现T+1供数；初步建立数据驱动入湖机制，将原先根据业务需要被动加载数据的模式转变为预判业务价值主动整合数据。

三是建立数据资产全链路数据流转监测机制。实现了从数据产生、加工整合到服务应用的全链路数据关系的全覆盖，全面掌握端到端数据流转情况及健康状态，包括数据的流入流出、所在节点等，确保所有敏感数据的流转都可被监测、记录、分析和溯源。

四是实施全域数据生命周期安全分级保护。在数据资产盘点整合的基础上，进行数据分类分级。依据行业标准和监管指导，确定了数据分类分级规则；面对海量数据，自主研发了数据安全自动化辅助定级模型，通过机器学习等方法实现数据安全等级的自动化初判，并对初判结果进行人工复核，将数据安全级别落实到每个数据项上，为数据分级管控打下基础。同时，结合监管要求和管理实际，

细化数据安全分级管控策略，明确数据分类分级保护要求，让安全管理有据可循，将数据安全分级保护贯穿数据采集、传输、存储、处理、销毁的全过程。

五是建立统一数据授权使用管控机制。搭建了覆盖所有信息系统的全行统一用户权限管控体系，确保按照“最小必要”原则设立使用权限。同时，围绕“数据湖仓用数”和“个人客户的隐私授权”两个重要场景建立企业级的授权管理机制，为全行“快捷用数、安全用数、合规用数”提供保障。打造个人隐私授权统一管理平台，把全行个人客户的安宁权授权、个人隐私授权、个人单独授权等场景进行统一管理，确保数据分析活动均在个人客户授权下进行，加强个人数据使用合规管理及安全管控，充分保护个人客户的相关权益，并最大限度地减少对客户的打扰。

六是探索利用隐私计算技术促进数据安全共享。积极探索联邦学习、多方安全计算等技术应用，支持联合计算、联合建模等丰富功能，支持集团内外部各机构快速部署和使用，在确保“数据不出域”的前提下，实现数据“可用不可见”，充分发掘跨机构数据在建设银行风控、营销、监管等场景的价值，促进数据融合应用。

七是建立数据安全风险评估机制。组织开展全集团数据安全风险评估，推进常态化数据安全评估联动机制建设，强化数据风险管控。围绕重点场景开展影响评估，加强对个人信息保护、第三方合作、数据出境、产品创新等多种场景下的数据安全评估，做到风险早发现，早预防，早解决，从而保障建设银行数据创新应用的正当性和合规性。例如，互联网贷款产品上市前，通过开展数据安全评估，分析创新产品的数据应用与自动化决策模型是否存在数据安全隐患，数据采集是否取得了相应的授权，数据传输、处理是否采取了必要的保护措施，确保产品充分考虑了对客户隐私和伦理道德的保护，有效防范数据泄露风险。

八是建立数据安全应急管理机制。完善应急管理体系，制定数据安全事件应急管理制度，明确了职责分工和报告流程，事件分级和重点场景，指导全行对数据安全事件进行识别和差异化响应，并建立了覆盖各级机构的应急联系通信录，确保联系到人。强调了数据安全事件与网络和信息安全事件、业务连续性事件、声誉事件等协同处置，确保各方密切配合，一旦有事件发生，能够快速响应、各司其职、相互协作、处置得力。

（五）培训宣贯方面

建设银行开展数据安全人才培养与文化建设。数据安全其实和生产安全一

样，必须做到人人有责，个个有心。为了牢固树立企业级的数据安全意识，建设银行在“建行学习”网络平台和企业微信等渠道，面向全行员工提供法律标准解读分析、数据安全管理要求解读等相关课程，编制信息安全警示录、技能手册等培训教育材料，让全体员工都成为数据安全的守卫者。同时，加强对数据安全专业岗位人员的培训，提升专业人员的数据安全技能，让其成为关键时刻的“消防员”。此外，通过跟踪数据安全监管动态、业界实践、行内进展等，形成数据安全工作定期简报，加强行内宣贯，促进全行数据安全文化建设。

三、未来展望

建设银行作为国有大行，在推进自身安全体系建设的同时，还积极参与金融行业数据安全标准的制定。同时与领先的金融机构和互联网公司一道深度参与中国信息通信研究院发起数据安全推进计划，共同开展相关领域学术交流研究，携手建设数据安全治理生态。

未来，建设银行将继续坚持总体国家安全观，以高度的政治责任感落实数据安全各项要求，完善数据安全顶层设计，推进各项保障工作落地，不断提升数据安全保护水平。作为支付清算协会成员，积极与监管机构、金融同业、行业协会等各方共同构建数据安全协同治理模式，保障支付产业数据安全流通，助推高质量发展。