2025

银行保险机构数据安全合规落地最佳实践

指导单位：DCMM金融行业社区技术委员会

参编单位：

平安银行股份有限公司
华夏银行股份有限公司
浙商银行股份有限公司
河南农村商业银行股份有限公司
南京银行股份有限公司
四川银行股份有限公司
浙江稠州商业银行股份有限公司
中国太平洋保险（集团）股份有限公司
人保信息科技有限公司
泰康保险集团股份有限公司
平安人寿保险股份有限公司
上海翰纬信息科技有限公司
数责科技（上海）有限公司
奇安信科技集团股份有限公司
北京明朝万达科技股份有限公司
绿盟科技集团股份有限公司
深圳市联软科技股份有限公司
江苏江南农村商业银行股份有限公司

序言

刘 巍

DCMM金融行业社区技术委员会
秘书长

数据作为数字经济时代的核心生产要素，正深刻重塑银行保险行业的业务模式与竞争格局。从开放银行的生态共建到保险线上化的服务革新，从联合建模的风控升级到数据要素流通的价值释放，数据的深度应用已成为金融机构数字化转型的核心驱动力。随之，数据安全风险也呈现出“多场景渗透、多主体交织、多维度爆发”的复杂态势。《个人信息保护法》《数据安全法》筑牢法律底线，国家金融监督管理总局《银行保险机构数据安全管理办法》更以“细则化、场景化、问责化”的监管要求，将数据安全从“技术合规”升级为“治理刚需”。在此背景下，行业亟需一部兼具契合监管与实操落地特质的指南，破解“业务高速流动与合规风险可控”“技术平滑升级与存量系统改造”“数据价值释放与安全底线守护”的三重矛盾。

作为中国电子信息行业联合会DCMM金融行业社区技术委员会（DCMM金数社），我们一直关注金融机构在数据安全合规领域的探索与突破。自DCMM金数社成立以来，我们始终以“推动金融行业数据管理能力成熟度提升”为使命，通过调研问卷、专题研讨、标准共建等形式，深度链接监管机构、金融机构、技术厂商与咨询服务方，洞察关键领域的共性痛点，联合探索解决方案。其中，《2025银行保险机构数据安全合规落地最佳实践》的编写，正是对该领域智慧的系统沉淀与价值升华。

这份报告绝非“大而全”的理论白皮书，而是一套“按图施工”的实战工具箱。编写组以《银行保险机构数据安全管理办法》为主线，将法规条文拆解为“制度流程-技术工具-组织文化”的全链路落地方案，更可贵的是，报告直面中小机构“资源有限、经验不足”的现实困境，通过“案例+模板+指标”的呈现形式，让不同规模、不同技术基线的机构都能“拿来即用”，少走弯路、少花冤枉钱。

数据安全合规不是“成本中心”，而是“信用资本”与“业务准入证”。头部机构已通过“数字化+智能化”实现风险秒级响应，中小机构正加速补齐“制度+流程”的基础短板。恰逢此时，我们更需清醒认识到：数据安全的终极目标，是实现安全与发展的动态平衡——让合规要求融入业务流程，让安全能力支撑创新实践，让数据在可控范围内充分流动，真正成为驱动银行保险行业高质量发展的核心动能。

谨以此报告，献给每一位在金融数据安全领域深耕的从业者。愿这份凝聚行业智慧的实践指南，能成为连接监管意图与业务末梢的桥梁，推动更多机构从合规达标走向韧性成长，共同守护金融数据安全的生命线，为数字经济时代的金融高质量发展保驾护航。

编写组

张兵
翰纬科技

周越博
河南农商银行

马波勇
太平洋保险

李欣韦
翰纬科技

江志辉
兴业银行

韩佶卿
浦发银行

王岩
泰康保险

师俊强
翰纬科技

孟彦飞
翰纬科技

参编专家

华桑兴
平安银行

赵亮
平安银行

丁世宁
华夏银行

燕晓晓
华夏银行

孙钢
浙商银行

钱正旸
浙商银行

蔡栋
河南农商银行

荆彪
河南农商银行

徐小锋
南京银行

吴迪
南京银行

周胜
四川银行

王桐根
四川银行

任方娟
稠州银行

周炜
稠州银行

杨凯
江南农商银行

安丙春
泰康保险

参编专家

徐周
太平洋保险

卢西昌
太平洋保险

王达波
人保科技

王爽
人保科技

李瑞荣
泰康保险

陶蓉
泰康保险

张扬
平安人寿

李乃增
平安人寿

楚赟
奇安信

梅成伟
奇安信

曲彦儒
明朝万达

黄乃田
明朝万达

王喆
绿盟科技

任鸿钰
绿盟科技

张建耀
联软科技

王贤智
合规社

目 录 Contents

前 言

一、编写背景与目的

过去五年，金融数字化以“加速度”改写行业版图：开放银行、保险线上化、联合建模、数据要素流通等新场景层出不穷，数据已从“业务副产物”跃升为“核心生产要素”。与此同时，《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》及国家金融监督管理总局《银行保险机构数据安全管理办法》相继落地，监管要求从“原则性指引”转向“细则化、场景化、问责化”。银行保险机构普遍面临“三重压力”：

- 业务侧要求数据高速流动与共享，追求极致客户体验；
- 合规侧要求风险可控、可追溯、可审计，责任到人；
- 技术侧要求在不中断现有系统的前提下，补齐短板、平滑升级。

在此背景下，行业急需一份兼具“监管契合度”与“落地操作性”的实战指南——既能把法规条文翻译成可复制的流程，又能把头部机构的先行经验提炼成可落地的模板，帮助中小机构“少走弯路、少花冤枉钱”。

2024 年，电子联合会 DCMM 金融行业社区技术委员会牵头发布的《银行保险机构数据安全合规调查研究报告》首次系统梳理了行业现状、痛点与成熟度分布，引起监管部门与从业机构的高度关注。为了延续并深化这一成果，原班主编团队再次集结，启动《2025 银行保险机构数据安全合规落地最佳实践》编写工作，并携手“合规社”作为唯一深度合作媒体。

本报告旨在：

- 以监管办法为纲，拆解经实战验证的最佳实践，覆盖“制度－流程－技术－文化”全链路；
- 用“案例+模板+指标”的形式，为不同规模、不同技术基线的机构提供“拿来即用”的落地方案；
- 通过合规社全媒体矩阵，打通“监管－机构－第三方”信息壁垒，形成持续迭代的行业知识库。

我们期望这份报告不仅是一本“操作手册”，更是一座“桥梁”——让监管意图精准传导至业务末梢，让先行者的经验快速复制到全市场，最终推动整个金融行业在数据安全与合规的道路上行稳致远。

二、报告的价值与定位

《2025 银行保险机构数据安全合规落地最佳实践》不是又一份“大而全”的白皮书，而是一套“按图施工”的实战工具箱。其核心价值与独特定位体现在以下四个维度：

- 监管对齐的“说明书”

以国家金融监督管理总局《银行保险机构数据安全管理办法》为主线，映射到制度、流程、技术三大模块，帮助机构快速完成差距分析与整改路线设计，避免“合规盲区”。

- 可复制的“样板间”

案例全部来自头部银行、保险、咨询公司、科技公司的真实项目，均经过编写组现场访谈、数据核验和合规性验证。每个案例配套流程图、控制矩阵，可直接落地，实现“开箱即用”。

- 全生态的“连接器”

报告将监管方、金融机构、咨询服务商、技术厂商纳入同一张能力图谱，列出“谁在用、怎么用、效果如何”三张清单，为中小机构提供“一键对接”生态资源库。

- 持续迭代的“活文档”

依托合规社独家内容平台，报告将以“纸质书 + 线上知识库 + 季度更新补丁”的形式持续演进；读者可通过合规社公众号实时查看法规更新、补丁模板和新增案例，确保合规策略始终在线。

这是一本让监管“看得懂”、机构“用得上”、厂商“对得准”的金融行业数据安全合规“施工图”。

三、阅读对象说明

本报告主要为以下四类专业读者量身定制，内容深度与呈现形式均围绕其工作场景与痛点展开：

- 金融机构决策层

董事长、行长、总裁、首席风险官（CRO）及董事会风险管理委员会成员，可借助报告中的同业最佳实践，快速决策数据安全预算与路线图。

- 合规与数据安全治理负责人

首席合规官（CCO）、数据保护官（DPO）、数据安全治理负责人及法务、内控、审计条线人员，可参考引用报告提供的案例内容，实现“制度－流程－技术”一键对齐监管要求。

- 科技与业务落地团队

首席信息官（CIO）、首席信息安全官（CISO）、架构师、安全工程师及业务条线数字化负责人，可通过案例的技术栈、实施路径，缩短方案设计周期，降低试错成本。

- 生态合作伙伴

数据安全咨询、培训、技术厂商及投资机构，可依据报告中的“能力图谱”与“需求清单”精准定位自身产品/服务在金融场景的切入点，快速对接潜在客户与合作伙伴。

无论您是制定战略的“掌舵者”、把控合规的“守门人”、落地实施的“工程师”，还是寻求商机的“生态伙伴”，翻开本报告，都能找到可直接复用的答案与可即刻启动的下一步行动。

第一章　银行保险机构数据安全合规政策解读

第一节　从管理视角理解《银行保险机构数据安全管理办法》

数据安全从来不是“买几套安全设备”就能一劳永逸的技术题，而是一道持续运转的管理题。Gartner 提出 Data Security Governance（DSG）框架，把“谁对什么数据承担什么责任”放在技术选型之前；国家金融监督管理总局的《银行保险机构数据安全管理办法》把同一逻辑写进了银保行业。通读《办法》第二章至第七章，可以清晰地看到一套“管理闭环”——目标、组织、对象、方法、评估五要素依次展开，与成熟的管理体系（ISO 9001、COSO、COBIT）高度同构。

一、谁来管：第二章 数据安全治理

这是整套办法的“组织架构图”。监管首次以条款形式要求党委（组）和董事会承担最终责任，高级管理层承担实施责任，并明确归口管理部门牵头，业务、风控、科技、审计、合规等多部门协同。它回答的是“权责利”——数据安全不是归口管理部门的独角戏，而是横贯前中后台的“矩阵式管理”。

二、管什么：第三章 数据分类分级和第六章 个人信息保护

这两章把“管理对象”从模糊的“所有数据”收敛为可操作的“目录”。先分类（客户数据、业务数据、经营管理数据、系统运行和安全管理数据等），再分级（核心、重要、一般）。不同级别数据匹配不同强度制度、流程与技术措施，避免“一刀切”带来的资源浪费或保护不足。

三、如何管：第四章 数据安全管理 + 第五章 数据安全技术保护

这是办法的“操作手册”。第五章聚焦制度与流程：数据全生命周期（采集、存储、使用、加工、传输、删除）和数据应用场景；第六章聚焦技术，但所有技术条款都带有“管理接口”——加密、脱敏、访问控制、日志审计不是“买最好的产品”，而是“按分级要求配置并持续运营”。一句话：技术必须服从管理规格，而非相反。

四、管得怎样：第七章 数据安全风险监测与处置

管理需要“闭环验证”。本章要求建立风险监测、事件报告、应急处置、事后评估的完整流程。只有当“事件数量、响应时长、改进完成率”成为管理层 KPI，数据安全才真正成为企业治理的一部分。

把《办法》从第二章到第七章串起来看，它实质上是给金融机构一套“数据安全管理体系”的管理蓝图：先搭班子（治理架构），再盘点资产（分类分级），接着建章立制（管理办法+技术规范），最后持续度量与改进（监测处置）。这与传统网络安全“以攻防为中心”的技术逻辑截然不同——数据安全首先是党委（党组）、董事会和高管层的治理责任，其次才是数据安全部门的落地工程。理解并践行这一点，是金融机构从“合规达标”走向“韧性成长”的关键第一步。

第二节　数据安全体系框架解析

一、数据安全体系框架对机构开展数据安全合规建设的意义

（一）提供全面指导

数据安全体系框架为企业机构的数据安全合规建设绘制了清晰的路线图。它涵盖了从法律法规遵循到具体技术实施的各个方面，使机构能够系统地识别自身的数据安全需求，明确在不同业务场景下应采取的合规措施。例如，当面临《银行保险机构数据安全管理办法》和《中国人民银行业务领域数据安全管理办法》等监管要求时，框架可以帮助机构梳理出关键的合规要点，避免因疏忽而出现违规行为。

（二）降低风险

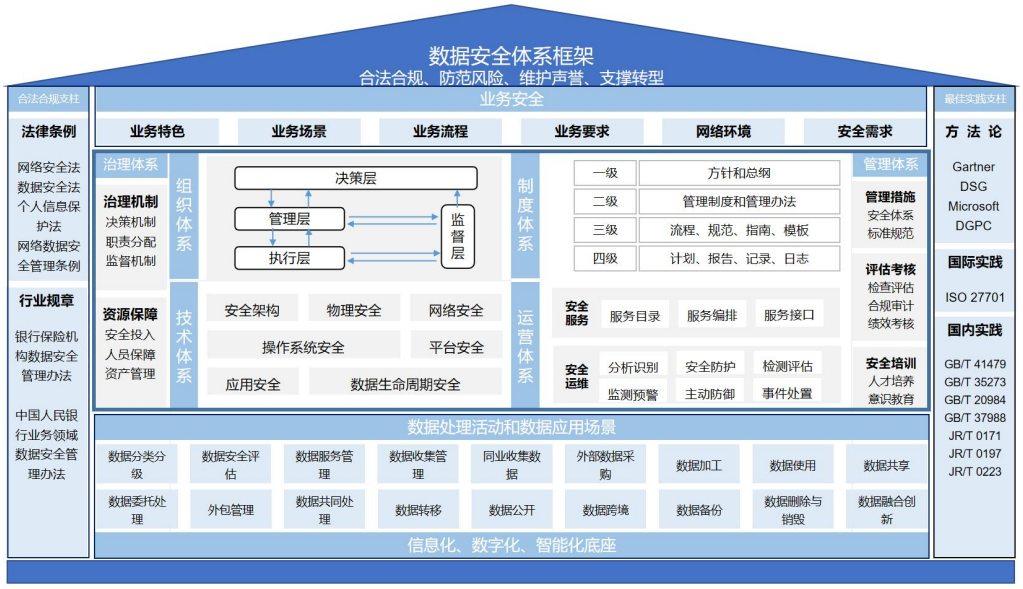
通过强调合法合规、风险防范等目标，该体系框架有助于机构提前识别和评估数据安全风险。机构可以依据框架中的风险评估方法，对自身的数据处理活动进行全面检查，发现潜在的安全漏洞，如数据泄露风险、网络攻击隐患等。然后，根据框架建议的管控措施，采取相应的技术手段和管理策略进行风险处置，从而有效降低数据安全事件发生的概率，减少可能带来的经济损失和声誉损害。

（三）保障业务连续性

数据是机构业务运营的核心驱动力，数据安全体系框架以业务安全为中心，确保数据在业务流程中的安全流转。当机构在开展数据安全合规建设时，遵循框架中的业务安全原则，可以在保障数据安全的同时，维持业务的正常运行。例如，在数据备份和恢复策略方面，按照框架要求建立完善的机制，能够在数据遭受破坏或丢失时，快速恢复数据，使业务尽快恢复正常，避免因数据安全问题导致业务中断。

（四）提升竞争力

在当今数字化竞争激烈的环境中，能够有效开展数据安全合规建设的机构更具优势。数据安全体系框架有助于机构向客户、合作伙伴和监管机构展示其在数据安全方面的专业性和可靠性。这不仅有助于增强客户对机构的信任，吸引更多的业务机会，还能使机构在行业内树立良好的声誉，从而提升其市场竞争力。



二、体系框架的结构

（一）数据安全合规建设的目标

数据安全合规建设的核心目标是合法合规、防范风险、维护声誉和支撑转型。合法合规要求机构严格遵守国家法律法规和行业规范，确保数据处理活动的合法性；防范风险是通过各种措施降低数据安全事件的发生概率；维护声誉强调数据安全工作对于机构品牌形象的重要性；支撑转型则是为机构的数字化转型提供安全保障，使其能够放心地利用数据进行业务创新和升级。

（二）两个支柱

合法合规支柱：这是数据安全体系的基础。它包括法律法规（如《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》等）和行业规范。法律法规为机构的数据安全工作提供了基本的法律遵循，明确了数据处理的红线；行业规范则针对特定行业的数据特点和业务需求，提出了更具针对性的合规要求，使机构能够在符合行业监管的基础上开展数据安全工作。

最佳实践支柱：汇聚了国内外在数据安全管理方面的先进理念和方法。例如国际上的 Gartner DSG、Microsoft DGPC 等方法论，以及国内的相关标准和实践案例。这些最佳实践为机构提供了可借鉴的经验和成熟的技术解决方案，帮助机构更快地提升数据安全管理水平。

（三）以业务安全为中心

业务安全是数据安全体系的核心导向。机构需要深入分析业务特点、业务场景、业务流程和业务要求，将数据安全措施与业务紧密结合。例如，在金融业务中，对于网上交易业务，要考虑在保障交易数据安全的同时，不影响交易的实时性和效率。

（四）数据安全的底座

信息化、数字化和智能化是现代机构运营的基础，也是数据安全的依托。信息化为数据的产生、存储和传输提供了技术平台；数字化使数据成为机构的核心资产，推动业务流程的优化和创新；智能化则通过大数据分析、人工智能等技术，为数据安全提供更精准的风险识别和防护手段。数据安全工作必须建立在这个底座之上，才能适应机构的发展需求。

（五）建立在数据处理活动和数据应用场景上的安全管控

数据安全的管控措施需要与实际的数据处理活动和应用场景相结合，才能发挥实效。数据处理活动贯穿数据的整个生命周期，包括数据收集、存储、使用、加工、传输、提供、公开、删除与销毁等环节。机构应根据不同数据处理环节的特点和风险，采取相应的管控措施。例如，在数据收集环节，要确保数据来源合法，并对收集的数据进行分类分级；在数据传输环节，要采用加密技术保障数据的保密性。同时，针对不同的数据应用场景（如数据共享、数据跨境、数据融合创新等），制定个性化的安全策略。

（六）数据安全管理体系的六大核心子体系

组织体系：明确机构内部数据安全管理的组织架构和职责分配。确定哪个部门或团队负责数据安全战略规划、哪个部门负责具体的数据安全运营等，确保数据安全工作有专人负责，避免职责不清导致的管理漏洞。

制度体系：建立一系列数据安全管理制度和规范。从方针政策到具体的操作流程，如数据访问控制制度、数据加密制度、安全事件应急响应制度等，为数据安全工作提供制度保障。

技术体系：涵盖安全架构、物理安全、网络安全、操作系统安全、平台安全、应用安全、数据生命周期安全等技术层面。通过部署防火墙、入侵检测系统、加密技术、脱敏技术等安全产品和技术手段，构建多层次的技术防护屏障，抵御外部攻击和内部威胁。

运营体系：包括安全服务、安全运营和安全培训等内容。提供数据安全相关的服务支持，如安全咨询、安全评估等；开展日常安全监测、分析和应急响应工作；对员工进行数据安全培训，提高全员的数据安全意识和技能。

治理体系：涉及数据安全的决策机制、监督机制和资源保障等方面。确保数据安全重大决策的科学性和合理性，对数据安全工作进行有效监督，并为数据安全项目提供必要的资金、人力等资源支持。

管理体系：侧重于对数据安全工作的评估考核和持续改进。建立科学的评估指标体系，定期对数据安全工作进行检查和考核，根据评估结果及时调整和优化数据安全策略和措施，实现数据安全管理体系的持续有效运行。

第三节　银行保险机构的数据安全合规制度体系

《银行保险机构数据安全管理办法》第二十条对银行保险机构数据安全制度建设进行了规定：

第二十条 银行保险机构应当按照国家数据安全与发展政策要求，根据自身发展战略，制定数据安全保护策略。银行保险机构应当制定数据安全管理办法，明确管理责任分工，建立包括数据处理全生命周期管控机制，落实保护措施。

银行保险机构应当对数据外部引入或者合作共享、数据出境等，制定安全管理实施细则。

银行保险机构的数据安全管理制度体系可按照四级架构搭建：

图：数据安全治理制度体系示例

一级：一级文件为数据安全管理的方针政策。一级文件应简洁明了，例如数据安全管理十六字方针：“合法合规、防范风险、维护声誉、支撑转型”。

二级：二级文件为管理规定，是详细的管控策略，通常是《数据安全管理办法》。二级文件《数据安全管理办法》是承接全部监管要求的纲领性文件，核心在于阐明“需要做什么”。

三级：三级文件为操作手册和指南，包括数据安全管理的流程、规范及细则等。三级文件由若干流程、规范及细则组成，其核心在于明确“如何执行”，用以指导日常数据安全工作的具体开展。

四级：四级文件为数据安全管理所需的说明、记录、表单等工具。

依据《银行保险机构数据安全管理办法》，对标梳理所需三级文件，各机构可结合自身管理要求与管理文化进行编制。

办法：章	办法：节	制度流程	
		二级	三级
第二章 数据安全治理	第九条（数据安全治理架构）	L2-数据安全管理办法	
	第十条（数据安全责任制）		L3-数据安全违规处罚管理细则
	第十一条（数据安全归口管理部门）		
	第十二条（业务部门）		
	第十三条（风险合规与审计部门）		
	第十四条（数据安全技术保护部门）		
	第十五条（数据安全文化建设）		L3-数据安全教育和培训管理规范
第三章 数据分类分级	第十六条（总体要求）		L3-数据分类分级实施流程
	第十七条（数据分类）		
	第十八条（数据分级）		
	第十九条（动态调整）		
第四章 数据安全管理	第二十条（管理体系）		
	第二十一条（数据资产管理）		L3-数据资产管理细则
	第二十二条（数据安全评估）		L3-数据安全评估规范
	第二十三条（数据服务管理）		L3-数据服务规范
	第二十四条（数据收集）		
	第二十五条（数据收集）		
	第二十六条（外部数据采购）		L3-数据外部引入安全管理实施细则
	第二十七条（数据加工）		L3-数据加工审批流程
	第二十八条（数据使用）		L3-数据访问管理流程 L3-数据提取操作流程
	第二十九条（数据共享及集团内部共		L3-数据合作共享安全管理实施细则

	享）		L3-数据外发安全管理流程
	第三十条（数据委托处理）		L3-数据外发安全管理流程
	第三十一条（外包管理）		L3-信息科技外包管理细则 L3-供应商安全管理实施细则
	第三十二条（数据共同处理）		L3-数据外发安全管理流程
	第三十三条（数据转移）		
	第三十四条（数据转移）		L3-数据外发安全管理流程
	第三十五条（数据公开）		L3-数据对外公开披露的审批流程
	第三十六条（数据跨境）		L3-数据出境安全管理实施细则
	第三十七条（数据备份）		L3-数据备份及恢复性测试管理细则
	第三十八条（数据删除与销毁）		
第五章 数据安全技术保护	第三十九条（数据安全技术保护体系）		L3-数据安全技术保护策略和体系架构
	第四十条（信息系统生命周期的数据安全）		L3-信息系统生命周期安全管理细则
	第四十一条（网络安全与数据安全保护）		L3-网络安全管理规范
	第四十二条（数据安全保护基线-信息系统保护）		L3-信息系统安全管理细则 L3-数据安全保护基线-信息系统保护
	第四十三条（数据安全保护基线-数据访问控制）		L3-数据安全保护基线-数据访问控制 L3-数据操作日志审计规范
	第四十四条（数据安全保护基线-数据传输保护）		L3-数据安全保护基线-数据传输保护
	第四十五条（数据安全保护基线-数据存储保护）		L3-数据安全保护基线-数据存储保护
	第四十六条（数据安全保护基线-数据销毁管理）		L3-数据安全保护基线-数据销毁管理
	第四十七条（数据安全基础设施）		
	第四十八条（数据安全测试）		L3-信息系统安全测试管理细则
	第四十九条（大数据平台安全）		L3-大数据平台安全管理规范
	第五十条（数据加工）		L3-人工智能模型开发应用安全管理规范
	第五十一条（数据加工）		L3-模型算法/信息系统数据安全审查流程
	第五十二条（数据加工）		
	第五十三条（外部交互数据安全）		L3-外部数据交互安全操作规范 L3-数据接口安全管理规范
第六章 个人信息保护	第五十四条（处理原则）		L3-个人信息保护管理细则
	第五十五条（处理原则）		
	第五十六条（告知义务）		

	第五十七条（告知义务）		
	第五十八条（影响评估）		L3-个人信息保护影响评估管理规范
	第五十九条（共享和外部提供）		L3-个人信息对外传输操作规范
	第六十条（跨境传输）		
	第六十一条（委托处理）		
	第六十二条（自动化决策）		
	第六十三条（个人信息风险报告）		L3-个人信息安全事件管理规范
第七章 数据安全风险监测与处置	第六十四条（数据安全风险管理机制）		
	第六十五条（风险监测）		L3-数据安全风险监测规范
	第六十六条（风险评估与审计）		L3-数据安全风险评估细则 L3-数据安全审计流程
	第六十七条（数据安全事件分级）		L3-数据安全事件管理流程
	第六十八条（应急响应与处置）		
	第六十九条（事件监管报告）		

第四节　数据安全管理部门的日常工作

在数字化浪潮下，数据已成为银行保险机构的关键资产，其安全性直接关系到机构的稳健运营和声誉。Gartner 理论指出，数据安全工作更多依赖于管理而非单纯的技术手段。技术是基础，而管理则是通过制度、流程和人员的协同作用，构建起全面的数据安全防护体系，确保数据在机构内外部流转、使用和存储等各个环节的安全性。

根据金监局《银行保险机构数据安全管理办法》第十一条规定，银行保险机构需指定数据安全归口管理部门，作为本机构数据安全工作的主责部门。以下是数据安全归口管理部门日常工作的详细说明：

一、 数据安全制度体系建设和完善

数据安全归口管理部门负责跟踪国家和行业监管部门发布的数据安全法律法规和监管要求，形成数据安全合规文件库。同时，根据业务环境、组织架构或监管要求的变化，及时更新数据安全管理制度流程。例如，每月跟进法律法规变化情况，确保机构的数据安全工作符合最新要求。体现了办法第十一条中“组织制定数据安全管理原则、规划、制度和标准”的要求，以及第二十条中关于制定数据安全保护策略、明确管理责任分工、落实保护措施的规定。

二、 数据分类分级管理

部门需制定数据分类分级标准，组织各部门对数据资产进行全面盘点，实施数据分类分级，建立数据目录，并定期复审和调整数据分类分级结果，动态管理和维护数据目录。例如，分阶段开展数据分类分级工作，根据数据的敏感程度和重要性采取差异化安全保护措施，符合第十一条中“组织建立和维护数据目录，推动实施数据分类分级保护”的要求，以及第二十一条中关于建立企业级数据架构、明确数据保护对象的规定。

三、 数据安全流程管理

数据安全归口管理部门负责对数据安全制度流程的执行情况进行监督管理，及时处理数据安全团队相关的授权、审批任务，监控流程执行情况，对发现问题及时通知责任人整改，并定期评估流程的效率和效果，进行优化。具体流程包括数据安全评估和审查、数据访问、数据提取、数据共享、外部数据引入、数据对外提供、数据出境、数据供应商安全评估、数据安全需求管理等。

四、 数据安全风险监测

虽然风险管理部门是数据安全风险监测的主责部门，但数据安全归口管理部门需提供必要的支持和配合，包括协助风险管理部门建立和完善数据安全风险监测系统，提供技术工具和平台支持；及时向风险管理部门提供数据安全相关的数据和信息，确保风险监测的全面性和准确性；与风险管理部门共同制定数据安全风险监测指标体系，确保监测指标能够全面覆盖数据安全风险点；在风险监测过程中发现异常情况时，协助风险管理部门进行快速响应和处置，确保风险事件能够及时得到控制；与风险管理部门共同对数据安全风险监测情况进行分析和总结，提出改进建议。

五、 数据安全风险评估

同数据安全风险监测一样，数据安全风险评估由风险管理部门主责，数据安全归口管理部门需提供支

持和配合，包括协助风险管理部门制定数据安全风险评估计划，明确评估范围、评估方法和评估流程；在风险评估过程中，协助风险管理部门进行数据安全风险的识别、分析和评估；根据风险评估报告，协助风险管理部门督促相关部门落实整改措施，确保风险问题得到及时解决；协助风险管理部门编制数据安全风险评估报告，确保报告内容全面、准确、符合监管要求。

六、 数据安全事件处置

发生数据安全事件后，归口部门需启动应急处置，按要求及时向监管部门报告事件，并进行调查与总结，符合办法第六十八条和第六十九条中关于应急响应与处置、事件监管报告的要求，确保在数据安全事件发生时能够迅速、有效地应对。

七、 数据安全宣贯培训

归口部门负责制定数据安全培训计划，定期组织培训课程，开展宣传活动和知识竞赛等，提升员工数据安全保护意识与技能。例如，每年制定培训计划，按需开展培训，体现了第十一条中“组织开展数据安全宣贯培训，提升员工数据安全保护意识与技能”的要求，营造全员重视数据安全的良好氛围。

八、 配合内外部数据安全检查工作

部门需配合内外部审计部门开展数据安全审计或检查工作，配合监管部门开展数据安全检查工作，并对检查发现的问题及时督促相关部门整改，提交整改报告。这符合第六十六条和第七十五条中关于风险评估与审计、现场检查与事件处置的要求，确保机构的数据安全工作符合监管要求。

九、 数据安全事项报告

定期向党委（党组）、董（理）事会、高管层报告数据安全重要事项。例如，每季度、半年或一年进行一次报告，确保高层能够及时掌握数据安全动态，做出正确决策，体现了第十一条中“向党委（党组）、董（理）事会、高管层报告数据安全重要事项”的要求。

十、 数据安全规划

根据机构的战略目标和业务发展需求，部门需制定中长期的数据安全管理规划，明确规划期内的目标、重点任务、实施步骤、资源需求等内容。例如，每三年制定一次数据安全规划，为机构的数据安全工作提供明确的方向和计划，体现了第十一条中“组织制定数据安全管理原则、规划、制度和标准”的要求，确保数据安全工作与机构整体战略相匹配。

十一、 数据安全考核

部门需明确数据安全考核指标和权重，定期对部门和个人的数据安全管理工作进行考核评价。例如，

每年进行一次考核，通过考核激励员工积极参与数据安全工作，体现了第十一条中“组织制定数据安全管理原则、规划、制度和标准”的要求，通过考核机制提升数据安全管理的执行力。

十二、 数据安全合作和交流

部门需组织内部跨部门会议，协调解决数据安全工作中遇到的问题，并与外部同业机构、科研机构、数据安全厂商建立合作机制，定期开展交流。例如，每月组织一次跨部门会议，促进内部协作，同时通过外部合作获取最新的数据安全技术和经验，通过合作和交流提升机构的数据安全能力。

在当前银行保险机构数据安全建设过程中，数据安全归口管理部门承担着核心的统筹协调职责。其需要与机构内部多个部门密切合作，形成协同作战的工作格局。例如，与信息技术部门合作，确保数据安全技术措施的有效落实；与业务部门合作，将数据安全要求融入业务流程；与合规部门合作，确保数据安全工作符合监管要求；与人力资源部门合作，将数据安全纳入员工绩效考核体系。

数据安全归口管理部门的工作职责广泛且重要，其通过制度建设、风险管控、人员培训等多方面工作，构建起银行保险机构的数据安全防线。同时，在数据安全建设过程中，与各部门协同合作，共同推动机构数据安全管理水平的不断提升，为机构的稳健发展提供有力保障。

第二章　银行保险机构数据安全现状与挑战分析

第五节　行业整体数据安全态势概述

一、市场规模：从“百亿级”迈向“千亿级”

- 2023 年中国数据安全市场规模约 97.5 亿元，占网络安全总市场的 12.1%，已连续 7 年保持增长。
- 工信部等十六部门提出“到 2025 年产业规模突破 1,500 亿元、年复合增长率 30%”的目标。
- 2024—2026 年，“数据要素×”三年行动计划叠加行业示范场景落地，预计数据安全投入再提速，金融、政务、医疗、能源等关键行业贡献主要增量。

二、威胁图景：数据泄露“量升件降”，地下交易仍在暗流涌动

- 2024 年国内监测到 3,510 起数据泄露事件，涉及 581 亿条记录，事件数同比下降，但单次泄露规模明显增大。
- 金融、电商、医疗、教育仍是重灾区，10 万—100 万条规模的泄露占比近半，脆弱人群与高净值人群成为精准攻击目标。
- 暗网交易活跃度虽下降三成，但数据售卖单价上涨，勒索病毒相关成本 2024 年全球平均达 487 万美元，同比增长 10%。

三、政策与合规：立法“组合拳”持续收紧

- 《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》《网络数据安全管理条例》形成高位阶法律矩阵；“数据出境安全评估”“关基保护条例”等配套制度细化落地。
- 金融行业专属法规《银行保险机构数据安全管理办法》2024 年正式生效，首次把“数据安全治理”写入监管条文，明确党委（党组）和董事会最终责任。
- 工信部、国家数据局、国家密码局等多部委同步推进“数据要素×”行动、工业领域数据安全能力提升方案，形成“横向到边、纵向到底”的监管闭环。

四、需求与技术：从“单点防护”走向“平台化治理”

- 需求侧：金融机构数字化业务上云、开放 API、联合建模导致数据流动路径复杂化，“合规+业务”双轮驱动对“可管、可控、可审计”提出更高要求。
- 供给侧：
  - 平台化、集约化成为主流：数据安全运营平台（DSOP）、数据安全管理平台（DSMP）快速替代碎片化工具。

– 隐私计算商用化加速：联邦学习、多方安全计算、同态加密在金融风控、联合营销场景落地，预计 2025 年市场规模破百亿元。

– AI 与零信任深度融合：AI 用于威胁检测、分类分级自动化；零信任架构（ZTA）在金融云、混合云环境渗透率预计 2027 年达 60%。

五、行业结构：金融稳居第二梯队，投入增速领跑

- 2023 年政府、电信、金融三大行业贡献数据安全市场 60% 以上份额；其中金融行业投入增速 35%，高于平均水平。
- 等保 2.0、关基保护、数据出境评估等合规要求，推动银行、保险、证券机构年均数据安全预算占 IT 总投入比例由 3% 提升至 8% 以上。
- 金融云、开放银行、数字保险、跨境理财通等创新场景，带动加密、脱敏、API 安全、隐私计算等新赛道需求爆发。

六、未来展望：2025-2027 关键窗口期

- 政策红利：数据安全产业顶层设计完成，金融、医疗、工业等行业细则将密集出台，预计带动 2,000 亿元级市场增量。
- 技术拐点：隐私计算互联互通标准落地、国产密码全面替代、AI 驱动的数据分类分级与威胁狩猎进入规模商用的临界点。
- 产业格局：平台型厂商通过并购加速整合，金融客户将优先受益“一站式+托管式”服务；中小机构则通过“合规 SaaS”降低门槛，形成分层竞争新生态。

金融行业正处于“强监管+高威胁+快创新”的三重交汇点。对银行保险机构而言，数据安全已从“成本中心”升级为“信用资本”和“业务准入证”。抓住 2025-2027 年政策与技术的双重窗口期，建立“治理－技术－运营”一体化能力，将成为下一阶段核心竞争力的分水岭。

第六节　数据安全管理面临的挑战和问题

一、治理架构：责任虚化、协同断档

（一）“董事会负总责”停留在纸面，缺乏量化考核指标，风险事件后难以追溯。

（二）数据安全牵头部门多为兼职，横向协调权不足，业务部门“各唱各调”。

（三）分支机构、子公司、科技子公司职责边界模糊，“母行－分行”“总-子”之间存在大量监管盲区。

二、资产盘点：底数不清、口径不一

（一）数据目录依赖人工填报，更新滞后，新业务系统上线 3-6 个月仍无准确清单。

（二）分类分级标准“多套并行”——监管口径、行业惯例、厂商模板互不兼容，导致“同一字段今天敏感、明天不敏感”。

（三）个人信息、衍生指标、外部采购数据缺乏统一标识，跨境场景下无法快速识别需评估字段。

三、制度落地：重编制、轻运营

（一）制度“墙上挂、纸上放”，缺少与业务流程的嵌入式接口；一线员工仍按“经验”操作。

（二）数据生命周期制度碎片化：采集阶段要求最小够用，使用阶段却缺少审批留痕；归档与销毁无人认领。

（三）问责体系“重事后、轻事前”，违规成本低于合规投入，反向激励“先上车后补票”。

四、技术与管理脱节：工具孤岛、能力断层

（一）加密、脱敏、DLP、API 网关各自为政，策略无法联动，出现“高加密－低权限”或“强脱敏－弱审计”的真空地带。

（二）大量存量系统改造难度大，老旧核心、外包 SaaS 无法接入统一密钥管理平台，形成“木桶短板”。

（三）AI 分类分级、UEBA 等新工具误报率高，运营人员陷入“告警疲劳”，最终回归人工复核。

五、风险监测与应急：看见不等于看懂

（一）日志分散在众多系统，格式不统一，威胁狩猎需跨多个平台拼接数据。

（二）数据泄露场景模型缺失，无法区分“正常批量下载”与“异常窃取”，平均 MTTD（发现时间）较长。

（三）应急演练重“技术恢复”轻“业务止损”，一旦出现重大事件，公关、法务、客服三线协同不足，次生舆情风险高。

六、第三方与供应链：影子资产、失控接口

（一）联合建模、云托管、联合营销等场景下，第三方接口数量年均增长 40%，但 60% 以上缺少安全评估与持续监测。

（二）采购合同模板更新滞后，缺少数据安全 SLA、违约赔偿及溯源条款，导致“数据出行先上车后评估”。

（三）外部数据供应商分级管理流于形式，高风险供应商仍在“白名单”中享受绿色通道。

七、人才与文化：短缺与疲劳并存

（一）全行业数据安全复合型人才缺口明显，中小机构以“一人多岗”硬扛，人员流动率持续增高。

（二）培训内容停留在法规宣贯，缺少场景化演练，员工“知道不对，但不知道怎么改”。

（三）业务部门 KPI 与数据安全指标无挂钩，“业绩优先”文化导致安全投入被持续挤压。

八、成本与 ROI 衡量：投入易、见效难

（一）数据安全投入短期无法带来直接收益，CFO 视角“花大钱买看不见的安全”，预算审批层层打折。

（二）行业缺少统一 ROI 模型，无法量化“减少一次泄露事件带来的罚金、诉讼、品牌损失”，导致“预算年年砍”。

（三）存量改造与增量创新并行，重复建设、重复采购现象突出，全行级“数据安全一盘棋”难以落地。

上述八大挑战相互交织，使得数据安全管理从“技术命题”升级为“组织变革命题”。唯有以治理架构为支点、资产盘点为抓手、制度流程为骨架、技术平台为支撑、风险运营为闭环，才能真正把监管要求转化为可持续的竞争力。

第七节　常见数据安全风险与威胁分析

以下风险按照“威胁场景—攻击手段—影响面”三维结构梳理，覆盖银行保险机构日常运营、外包协同、跨境流通等全生命周期场景，可直接用于风险识别、评估与内控对标。

一、数据泄露（Confidentiality 风险）

威胁场景：外部攻击、内部人员无意或故意泄露、第三方接口失控

攻击手段：SQL 注入、撞库、爬虫、钓鱼邮件、移动介质摆渡、API 弱口令

影响面：客户隐私曝光、监管罚款、声誉受损

二、数据篡改（Integrity 风险）

威胁场景：交易数据、风控模型参数被恶意修改

攻击手段：中间人攻击、SQL 注入、模型投毒、越权调用 API

影响面：业务决策错误、资金损失、监管问责

三、数据破坏 / 丢失（Availability 风险）

威胁场景：勒索软件、供应链植入恶意代码、运维误操作

攻击手段：勒索病毒、逻辑炸弹、误删库、备份失效

影响面：业务中断、数据无法恢复、SLA 违约

四、数据滥用 / 越权使用

威胁场景：内部人员超范围查询、合作方二次使用

攻击手段：权限漂移、账号共享、接口未按最小化原则返回数据

影响面：个人信息主体权利受损、合规处罚

五、数据伪造与深度伪造

威胁场景：身份冒用、虚假交易、欺诈理赔

攻击手段：AI 换脸、合成语音、虚假数据源注入

影响面：欺诈损失、反洗钱误判、监管通报

六、违法违规出境 / 存储

威胁场景：跨境业务、云托管、灾备

攻击手段：未经评估的跨境专线、境外 SaaS 默认数据中心

影响面：违反《数据出境安全评估办法》，最高可处 1,000 万元罚款

七、第三方不可控风险

威胁场景：联合建模、外包开发、API 开放

攻击手段：第三方缓存数据、超期接口、特权后门

影响面：数据在供应链环节失控、连带责任

八、数据推断攻击

威胁场景：公开或匿名数据集被交叉关联

攻击手段：差分攻击、成员推理、模型逆向

影响面：去标识化失效、个人信息再识别

九、内部威胁

威胁场景：离职人员、权限滥用、商业间谍

攻击手段：U 盘摆渡、打印带走、日志擦除

影响面：核心算法、客户名单外泄

十、移动端与物联网风险

威胁场景：移动展业、智能终端、车联网

攻击手段：App 违规收集、无线键盘监听、固件漏洞

影响面：终端成为跳板、客户位置泄露

银行保险机构的数据安全威胁已从单一“网络入侵”演化为“多场景、多主体、多维度”的系统性风险。任何忽视治理、流程、人、第三方环节的“纯技术视角”都将留下致命缺口。下一步，应基于《银行保险机构数据安全管理办法》生命周期管控要求，建立“威胁库—风险矩阵—控制措施—监测指标”的闭环管理体系，把上述十大威胁转化为可量化、可审计、可改进的管理动作。

第三章　银行数据安全合规落地实践案例

第八节　平安银行 数据分类分级双向打标方法与 AI 打标实践

一、背景介绍

（一）实施的背景和起因

随着信息技术的飞速发展，20 世纪 90 年代开始数据库技术日益成熟，各行各业凭借计算机技术的支撑，在日常经营运作的过程中产生了海量数据，包括政务数据、公共数据、金融数据、地理信息数据、刑事司法数据、企业数据等，数据已然成为新技术环境下的关键生产要素。特别是近年来全球经济数字化发展力度持续加强，以大数据、5G、云计算、区块链、人工智能等新技术为代表的数字经济规模持续扩大，企业数字化转型趋势逐步升温。量变引发质变，庞大体量的数据中蕴含的商业价值或可为企业带来可观的收益。然而其中隐藏的数据安全问题日益凸显，如何保护数据挖掘技术不被滥用，如何保护公众隐私不被泄露等等问题求解成了当务之急。

金融数据的安全应用关系到广大人民群众的切身利益，涉及大量个人信息，成为黑产组织、电信诈骗团伙等不法分子密切关注的领域。由于不同类型的数据其价值和影响程度均不同，对其采取的安全管理保护措施和付出成本也不尽相同。数据安全分类分级管理是推动数据安全治理的重要前提，也是安全防护的基础，可有针对性地对数据采取保护措施。对数据进行分类分级有利于加强金融消费者个人信息保护、提高企业机构内部数据的合理规划、便利企业或行业之间数据资源共享以及提升国家数据安全保护能力。

国家层面对数据安全的高度重视，可以追溯到 1994 年颁布的《计算机系统安全保护条例》，提出了信息安全保护的概念。随着信息实践操作的不断发展，逐渐产生了数据分级保护的理念，2007 年公安部发布的《信息安全等级保护管理办法》将信息安全分为五个等级。2008 年我国制定了《信息安全技术 信息系统安全等级保护基本要求》，针对不同的等级提出了相应的技术要求。近几年颁布的《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》等明确要求建立数据安全分类分级制度，从立法的角度，建立数据分级保护制度体系。金融数据具有数据体量大、数据价值高的显著特征，需要对金融数据中的高价值、高敏感程度数据进行重点保护，因此金融领域十分重视金融数据的分类分级和安全保护。当前，全国信息技术标准化技术委员会与金融标准化管理技术委员会联合其行业主管部门已发布多项数据安全分类分级与保护相关的标准，如《信息安全技术 个人信息安全规范》（GB/T 35273-2020）、《信息安全技术 个人信息安全影响评估指南》（GB/T 39335-2020）、《个人金融信息保护技术规范》（JR/T 0171-2020）、《金融数据安全 数据安全分级指南》（JR/T 0197-2020）以及《金融数据安全 数据生命周期安全规范》（JR/T 0223-2021）等，相关国家与行业标准领域还有多项处于研制阶段，如《信息安全技术 网络数据分类分级要求（征求意见稿）》《信息安全技术 重要数据识别指南（征求意见稿）》以及《金融数据安全 数据安全评估规范（征求意见稿）》。现有标准分别从全量个人信息、个人信息安全影响、个人金融信息、金融业数据、数据生命周期、网络数据、重要数据以及数

据安全评估的维度对金融数据安全分类分级与保护做出了规定。

数据安全的重要性日益提升，金融监管机构对数据安全提出了更高的要求，国家金融监督管理总局发布《银行保险机构数据安全管理办法》、人民银行发布了《中国人民银行业务领域数据安全管理办法》。

（二）我行的基本情况

平安银行作为一家全国股份制商业银行，同时还是人行与银保监会划定的系统重要性银行，历来对客户信息和数据安全高度重视，严格遵从国家和监管机构的相关法规和要求，鉴于数据安全分类分级的基础性和重要性，平安银行投入充足资源和力量，在充分学习和交流的基础上，结合平安银行自身数据治理条件和数据特点，研究探索出“平安银行数据安全分类分级双向打标方法”，并在该方法指导下，积极研发 AI 模型，开发出数据安全分类分级 AI 打标及管理平台。

（三）我行数据安全数据分类挑战与问题

1.海量金融数据安全分类分级面临成本与时效的巨大挑战。

数据安全分类分级的对象需要细化到字段级，才能够满足数据生命周期各阶段对数据进行分级管控和保护的要求。金融行业的内外部数据历来都是海量的，这是由金融企业客户的普遍性、产品与服务的丰富性、业务与管理的线上化所决定的。面对百万级数据表和千万级的数据项，且每日都有惊人增量的背景下，如果采用传统的人工方法实施数据安全打标，势必长期投入大量人工，且无法在短期内完成，因此海量的金融数据实施安全分类分级打标面临成本与时效的巨大挑战。要解决数据安全分类分级应用困难的问题，就必须从源头制定对策。

2.数据全生命周期安全保护全覆盖和有效性存在巨大挑战。

金融企业在数据全生命周期实施安全保护，实现全面覆盖和有效，是存在非常大的挑战。作为庞大的金融企业，上千的系统运行，数万甚至数十万的员工队伍，千万级甚至数亿级的客户群，确保数据在采集、传输、存储、加工、使用、退役销毁等众多环节及成千上万的场景，真正实现对数据的安全保护，绝对不是一件容易的事情。实现这一目标可能要采取全方位的、立体的多项措施。

3.数据安全分类分级结果准确性的挑战。

近些年来，伴随着全球数字经济的高速发展，金融行业的业务领域不断扩大，网络系统规模不断增加，资产分布越来越广，这就容易导致存在扫描死角、敏感数据可能潜藏在众多脏数据、非结构化数据的包围之中，这些都会导致资产探测周期长、效率低的问题，进而导致数据字段识别不完整，在数据安全分类分级时导致数据资源缺失，数据打标不全面的情况。同时，在对数据进行分类分级时，有些数据可能同时属于几个类别，如果在进行数据安全分类时维度不清晰，可能会导致分类分级结果出错，影响后续基于数据安全分类分级的各种操作产生错误。

二、实施过程

（一）解决思路

面对数据安全法规和监管要求，面对数据安全分类分级打标的种种挑战，我们必须回答好如下三个问题：

1.数据安全分类怎么分，依据什么原则分，谁来分？

2.安全等级如何定，有没有参考依据，准确性怎么保证？

3.面对海量数据，如何在成本可控与时间可控的前提下完成分类分级？

我们的解决思路首先是要区分存量和增量，存量的特点是数据量庞大，且元数据质量参差不齐，甚至缺乏足够了解数据的人员，分类分级的时间紧迫且传统方法成本高昂；增量数据虽然每天也有大幅增长，但是相比存量数量有限，并且在需求分析和系统设计阶段，不乏熟悉数据的业务和开发人员，并具有准确识别数据和打标的时间窗。鉴于上述特点，平安银行提出对存量数据实施自下而上打标和对增量数据自上而下打标的双向打标方法，所谓自下而上打标，是指通过 AI 分类模型+逻辑判定规则相结合的机器模型扫描存量数据，依据存量数据的元数据或者存储的数据值特征，识别和判定为某类安全标签（从数据安全视角划分的数据项），并对机器扫描结果进行人工复核；所谓自上而下打标，是指数据建模期间，依靠需求分析和模型设计人员对新增数据项的理解，人工识别和判定这些新增数据项的数据安全标签，并将设计结果传导至生产数据，实现对增量数据的安全打标。

（二）解决方案

1.数据安全分类分级保护矩阵

首先是制定标准，一套细化到数据项（字段级）的分类分级标签，以及与之对应的全生命周期各环节的保护措施。严格按照我国法律法规要求，结合我行实际情况，制定我行数据安全分类分级规范条文，明确数据安全管理的基本原则，分类分级的管理要求，使数据安全分类分级有据可依。

2.自上而下与自下而上双向打标

专业的事情交给专业的人员，繁琐的劳动交给机器。基于这样的原理，我们可以采取自下而上和自上而下的双向打标模式，双向打标的整体介绍思路如下：

自上而下，即数据库模型设计阶段，从逻辑模型进行打标，对应物理表继承安全标签，数据建模人员是最了解数据的人，也是最专业的人；

自下而上，即扫描物理表数据，对物理表字段进行分类分级打标，海量的存量数据打标工作交给机器；

3.数据安全 AI 打标与管理平台

双向打标方法需要一个支撑平台实现智能打标和流程管理，该平台具有 AI 模型训练和扫描的能力，具有扫描结果人工复核的能力，具备数据安全保护矩阵的建立和维护能力，打标结果向外提供服务的能力。

（三）技术应用

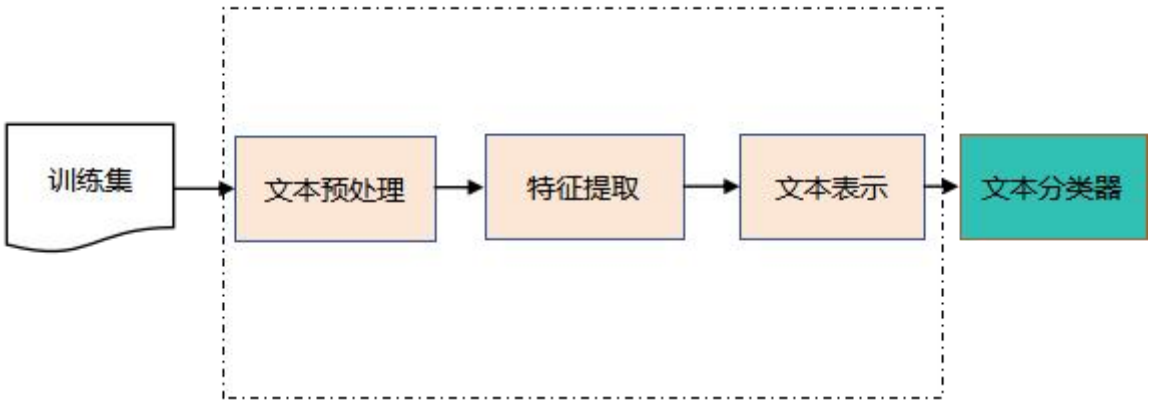
1. AI 模型的应用

数据安全分类分级可以将其抽象为多类别文本分类问题，即用计算机对文本（或其他实体）按照一定的分类体系或标准进行自动分类标记。在本例中输入是数据表名、数据字段和数据字段描述，输出是数据安全标签。其中库名、表英文名、表中文名、表定义、字段英文名、标准中文名、业务定义、字段类型均为输入，输出是数据安全标签序号和数据项名称。

库名	表英文名	表中文名	表定义	字段英文名	标准中文名	业务定义	字段类型	数据安全标签序号	数据项名称
客户信息管理子系统(BECIF-CORE)	BLACKLIST_BILL_INFO	支票黑名单	支票黑名单	ORG_NAME	出票人名称	个人客户或对公客户出票人名	VARCHAR2	DACU000693	登录用户名
客户信息管理子系统(BECIF-CORE)	ATTENTION_ACCOUNT	运营关注账户	运营关注账户	ACCOUNT_NO	对方账号	涉及零售活期、定期、对公定	VARCHAR2	DACU000148	个人网络账号
客户信息管理子系统(BECIF-CORE)	BLACKLIST_BILL_INFO	支票黑名单	支票黑名单	SZ_ARTIF_PERSON_NAI	法定代表名称	是指依法代表法人行使民事权	VARCHAR2	DACU000699	个人基础标签
客户信息管理子系统(BECIF-CORE)	CLIENT_TELECOM_FRAUD_INFO	电信诈骗名单管理	电信诈骗名单管理	ID_NO	个人证件号码	个人使用的有效的、被核实证	VARCHAR2	DACU000699	个人基础标签
客户信息管理子系统(BECIF-CORE)	ATTENTION_ACCOUNT	运营关注账户	运营关注账户	BANK	开户行名称	账户开户行名称，例如：北京	VARCHAR2	DACU000699	个人基础标签

图表 1 数据安全标签输出示例

传统方法文本分类方法如专家规则（Pattern）进行分类，如通过业务知识编写正则表达式的方式，此类方法可以短平快的解决 Top 问题，但是随着文本规模和设计的场景复杂多变会导致规则非常多，不仅费时费力而且覆盖的范围和准确率都非常有限，而且随着统计学习方法的发展，特别是互联网在线文本数量增长和机器学习的兴起，逐渐形成了一套解决大规模文本分类问题的经典玩法，这个阶段主要的套路是人工特征工程和浅层分类模型。基本上大部分机器学习方法都在文本分类领域有所应用，比如朴素贝叶斯分类算法（Naïve Bayes）、KNN、SVM、最大熵和神经网络等等。



图表 2 机器学习示例

以上机器学习在 2012—2015 年作为较为成熟的技术广泛应用在各个领域和商业公司，但是随着千万级别大数据发展，主要问题的文本表示是高纬度高稀疏的，特征表达能力很弱，而且神经网络很不擅长对此类数据的处理；此外需要人工进行特征工程，成本很高。而深度学习最初之所以图像和语音取得巨大成功，一个很重要的原因是图像和语音原始数据是连续和稠密的，有局部相关性。应用深度学习解决大规模文本分类问题最重要的是解决文本表示，再利用 CNN/RNN 等网络结构自动获取特征表达能力，去掉繁杂的人工特征工程，端到端（end2end）的解决问题。

TextCNN 在实际文本分类任务应用中有不错的表现，特别适用于短文本任务，但是 CNN 有个最大的

问题是 filter_size 视野，一方面无法建模更长的序列信息，另一方面 filter_size 的超参数很繁琐。CNN 本质是做文本特征的表达任务，而自然语言处理任务中更常用的循环神经网络，因为其能够更好地表达上下文信息。本次方案具体在文本分类任务中，Bi-Direction RNN （本方案使用的是双向 LSTM，又称长短期记忆网络），从某种意义上可以理解为可以捕获变长且双向的“N-gram”信息。

关于循环神经网络可以参考 Recurrent Neural Network for Text Classification with Multi-Task Learning。RNN 在计算机视觉领域用于视频分类、图像标注、视频标注和最近的视觉问答。在文本任务中如序列标注、命名实体识别、文本翻译、文本摘要、词性标注、语音识别、文字生成语音等都有比较广泛的应用。LSTM 因为独创记忆序列，成为目前最火的神经网络底层建模方案和经典算法。大量应用在文本生成、情感分析、机器翻译、语音识别、生成图像描述、自动驾驶和视频标记。目前已知的公开消息有：应用 LSTM 搭建的神经网络模型赢得了 ICDAR 手写识别比赛冠军；相关学者应用 LSTM 处理机械设备震动信号；谷歌公司应用 LSTM 做语音识别和文字翻译，对超过 20 亿部 Android 手机和其他设备的语音识别采用 LSTM 算法模型；苹果公司使用 LSTM 优化 Siri 应用；Facebook（现改名为 Meta 公司）曾公开宣布使用 LSTM 每天处理高达 45 亿个翻译等。神经网络中的 LSTM 在各公司 AI 领域均有广泛应用，LSTM 也正在渗透到现代工作任务。

2. 另外，结合实际情况，由于测试集和训练集的任务分布本身相差较大、预训练模型参数较大而样本数量受限、文本出现缺乏语义信息或样本跨域情况，导致深度学习框架下训练结果出现一定程度的过拟合问题，初级阶段并不能实现模型的泛化能力。在人力有限的情况下，通过正则判定和规则判定手段强行矫正深度学习的强大计算能力，能够初步应用在实际业务场景，极大提高解决业务效率。其中，正则判定：是根据字段本身包含的数据内容的鲜明特点进行判断，例如：性别分类中，除男女之外很难出现其他数据形式或内容，即可判断分类，规则判定：是根据专家法，对提取分类和存在训练集进行正面和反面判断，根据关键词判断是否极大概率正确或极大概率错误，再通过数据工程进行加工，形成最终结果。两个手段辅助深度学习模型因客观原因导致部分不可解释的结果现象，使得结果更加准确且可靠。最后，结果又可以反哺训练集和预测集分布相差较大问题，循环反复，不断提高深度学习模型的效果，形成以模型为主导的数据安全分类任务，剔除 90%无效数据且对安全字段自行打标，极大提高人工识别安全分类分级效率，利用技术降本增效。

（四）成果实施步骤

1.数据安全分类分级保护矩阵

根据方案，首先是制定标准，一套细化到数据项（字段级）的分类分级标签，根据我国《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》等基本法律，参照《金融业数据安全分类分级指南》和《个人金融信息保护技术规范》等行业标准作为参考内容，结合我行数据情况，梳理形成数据项+安全级别+保护措施形成全方位数据安全分类分级保护矩阵，指导全行数据安全分类分级工作有据可依。矩阵内容如图所示：

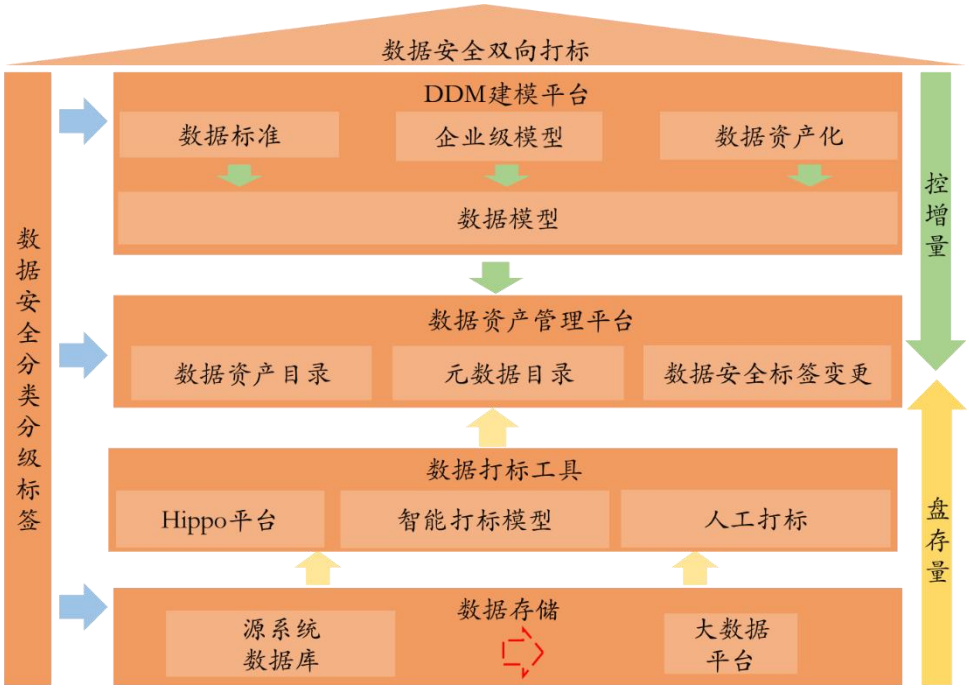
信息安全标签ID	数据主题	一级分类	二级分类	标签项	个人金融信息类别	数据安全等级	数据生命周期																																					
							数据采集		数据传输		数据存储		数据使用-数据导出		数据使用-数据访问		数据使用-数据加工		数据使用-数据展示		数据使用-开发测试数据使用-汇聚融合		数据使用-公开披露		数据使用-数据转让		数据使用-委托处理		数据使用-数据共享		数据删除		数据销毁											
							法律依据	保护措施	法律依据	保护措施	法律依据	保护措施	法律依据	保护措施	法律依据	保护措施	法律依据	保护措施	法律依据	保护措施	法律依据	保护措施	法律依据	保护措施	法律依据	保护措施	法律依据	保护措施	法律依据	保护措施	法律依据	保护措施	法律依据	保护措施										
DAC1000168	客户	个人客户	个人自然信息籍贯		C2	机密(3)	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0物理擦除	《JR/T0彻底销毁										
DAC1000251	客户	个人客户	个人自然信息家庭净资产		C2	机密(3)	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0物理擦除	《JR/T0彻底销毁										
DAC1000187	客户	个人客户	个人自然信息家庭人口		C2	机密(3)	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0可以展示	《JR/T0物理擦除	《JR/T0彻底销毁										
DAC1000700	客户	个人客户	个人自然信息家庭住址		C2	机密(3)																																						
DAC0002427	客户	单位客户	单位资讯信息介质号码			机密(3)																																						
DAC1000352	客户	个人客户	个人身份信息卡密码		C3	绝密(4)	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0物理擦除	《JR/T0彻底销毁										
DAC1000353	客户	个人客户	个人身份信息卡有效期		C3	绝密(4)	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0强制屏蔽	《JR/T0物理擦除	《JR/T0彻底销毁										

图表 3 数据安全分类分级保护矩阵示例

2.制定自上而下与自下而上双向打标方案

自上而下：数据库模型设计阶段，从逻辑模型进行打标，对应物理表继承安全标签；

自下而上：扫描物理表数据，对物理表字段进行分类分级打标；



图表 4 数据安全双向打标示例

3.自下而上打标

平安银行的数据安全分类分级按照以下路径开展，第一步是制订标准，一套细化到数据项（字段级）的分类分级标签，以及与之对应的全生命周期各环节的保护措施；第二步是 AI 模型数据集数据的自动采集与整合，以及全量数据元数据的完善和补充，根据第一步制订标准，通过正则判定和规则判定手段，在数据资产管理平台进行大范围数据采集，获得模型所需初步数据训练集；第三步是数据预处理，划分为训练集、验证集和测试集，做好脏数据脏符号处理以及标准化等预处理工作，提高数据集质量；第四步是搭建 AI 模型接口及配置文件处理，搭建经典 LSTM 深度学习网络架构，包含卷积层、降采样层和全链接层，配

置文件包含外公司已经训练好的 npz 词向量，根据超参数设定导入词典再导入词向量，最终导入网络架构。为进一步提高模型效果，采用双向 RNN 改进算法，双向保存权重参数，进一步提高隐藏层输出信息。第五步是反向传播及分类，计算每个神经元误差，通过激活函数计算每个权重梯度，因采用 LSTM 模型，完美解决了梯度爆炸和梯度消失的问题，使得模型更具有广泛性，最终根据之前确定的验证集评估方法保存最佳训练权重参数。第六步运用 AI 模型，模型对预测集数据进行安全分类打标，并最终导出输出结果。第七步调参，针对局部可优化的训练组 batch_size、长度 seq_len、LSTM 层 num_layers、时间步长 time_step、学习率 learning_rate、激活函数等进行微调，测试最佳配置参数。第八步规则定义，这是鉴于机器扫描的结果虽然在理想环境（训练集）已经达到 95%准确率，但由于测试集和训练集的任务分布本身相差较大、预训练模型参数较大而样本数量受限、文本出现缺乏语义信息或样本跨域情况，导致深度学习框架下训练结果出现一定程度的过拟合问题，初级阶段并不能实现模型的泛化能力。因此根据实际情况制订规则定义，将离群值或因前训练的数据集质量低的影响因子削弱，最终达到理想效果。第九步人工复核，金融安全十分重要，即使有 0.1%的误差也可能造成不可估量的泄露风险，因此通过熟悉数据的开发人员或者业务人员进行人工复核纠正，确保最终结果可以应用在实际数据应用层面；第十步模型循环训练，根据第九步人工复核结果的数据进行反哺 AI 训练模型，重复二至九步，进一步提高模型效果；第十一步是应用打标结果，把复核后的数据安全标签打标结果在数据资产管理平台上架，向各类用数场景提供数据安全分类分级服务。

上述步骤不是单向的，我们通过信息反馈机制不断完善前面环节的质量，比如把复核确认后的打标结果反馈到 AI 模型进行补充训练，持续提升模型准确率；而通过不断检视全量数据项打标结果，发现一些新的数据安全分类分级标签，反馈到第一步持续补充完善标准。

4.自上而下数据安全打标

自上而下的数据安全打标方案作为管控增量数据库表进行数据安全打标的重要手段，在各系统进行数据库建模阶段即进行数据安全标签的打标，由该库表的设计人员进行数据安全打标，设计人员对该库表即将存储的数据尤为清楚，也是数据库表产生的“第一站”，既保证了数据安全标签的准确性，在该数据安全标签打标以后，又保证了数据安全保护措施在整个数据全生命周期安全保护措施的可落地性。

三、成果与效益

（一）打标范围全面覆盖—覆盖全

双向打标方案不分数据库类型，无论是关系型数据库还是大数据平台，该打标策略可覆盖全行所有系统，实现“存在即打标”的目标。

（二）打标时效与资产上架同步—时效快

双向打标的措施都具备时效快的特点，自上而下打标：数据库表落地即实现资产上架，资产上架即意味着数据安全标签的正式生效。自下而上打标：机器自动扫描，每天实现跑批任务，T+1 可实现数据安全

标签上架和服务的提供。

（三）打标成本低廉可控—成本低

自上而下打标方案中，由设计人员在库表设计之初进行数据安全打标，继承到整个数据全生命周期安全保护流程中，避免后续返工。自下而上的数据安全打标策略由 AI 智能模型进行打标，只需部署跑批任务即可实现打标，极少人工介入成本。

（四）打标质量满足要求—质量高

自上而下打标由数据库表设计人员打标，保证数据安全准确率；自下而上由智能打标模型进行打标后，人工复核，实现高质量打标。

（五）模型优化良性循环—可持续

双向打标后的打标成果，在实现全覆盖和高质量的情况下，将打标结果反哺给 AI 智能打标模型，实现良性循环，数据安全管理可持续。同时自上而下打标模式融入打标过程与开发设计之中，实现开发治理一体化，实现数据安全打标流程的可持续。

四、经验与启示

首次分类分级，优先识别敏感等级高的数据，这样在人力有限的情况下，可以基于敏感信息的识别保护敏感信息，以及对存储敏感信息的系统开展评估和网络安全保护。

打标优先使用就高原则，在使用过程中二次复核，通过数据内容辅助判断准确调整。

迭代训练，持续完善 AI 智能打标模型，提升准确率。辅助其他正则扫描、血缘继承自动化扫描工具，提升敏感信息的准确率和一致性。

第九节　华夏银行 数据分类分级和数据安全评估实践

一、背景介绍

（一）监管要求

随着数字化转型的推进，数据在金融行业的重要性日渐提升，但安全威胁日益复杂。网络攻击和数据泄露频发，威胁金融机构声誉并可能引发系统性风险，数据安全形势愈发严峻。

2024 年 12 月，国家金融监督管理总局《银行保险机构数据安全管理办法》正式施行，要求银行保险机构全面构建数据安全治理体系，涵盖数据安全治理、数据分类分级、数据安全管理、数据安全技术保护、个人信息保护、数据安全风险监测与处置、监督管理等方面。其中数据分类分级和数据安全评估为两项关

键基础性工作，数据分类分级作为实施差异化安全管控的基础，明确了“银行保险机构应当制定数据分类分级保护制度，建立数据目录和分类分级规范，动态管理和维护数据目录，采取差异化安全保护措施”。通过划分核心数据、重要数据、敏感数据和其他一般数据并实施差异化的安全防护策略，强化个人信息保护，确保数据全生命周期的安全性；数据安全评估作为检验防护效果和持续改进的重要抓手，明确了“银行保险机构在处理敏感级及以上数据的业务活动时，或者开展数据委托处理、共同处理、转移、公开、共享等对数据主体有较大影响的活动时，应当事先开展数据安全评估。数据安全评估应当根据数据处理目的、性质和范围，按照法律法规和伦理道德规范要求，分析数据安全风险和对数据主体权益的影响，评估数据处理的必要性、合规性，评估数据安全风险及防控措施的有效性。”等要求。

中国人民银行《中国人民银行业务领域数据安全管理办法》同样高度重视数据分类分级、数据安全评估工作，要求数据处理者建立健全业务数据分类分级制度和操作规程，细化数据分类并标识安全级别，定期更新数据资源目录，适应数据的动态变化；对于涉及个人信息的业务数据提供活动，应当评估是否遵守法律、行政法规要求等。

（二）行内现状

我行数据资产通过推送元数据文件的形式，登记至信息系统并在此基础上开展分类分级。在开展分类分级盘点和应用过程中，结合各业务部门反馈和内部审查，实际工作中发现，安全等级存在偏低或偏高情况，部分数据未完成定级，数据安全分级结果的关键要素缺失，以及百万级数据表标识不够准确等问题。

同时，随着业务合作、特殊数据处理场景的增多，结合各项监管检查、内部审计、年度数据安全风险评估，需要进一步提升数据安全评估的规范性并提升效率。

依据监管分类分级标准，我行正持续探索符合实际情况的分类分级方式和管理流程，稳步提升分类分级的覆盖率和准确性；持续推动数据分类分级结果对接业务系统、管理平台、数据类系统以及安全工具平台，推动分级管控措施的有效落实，防范潜在风险；围绕合规性、安全性、规范性，持续探索统筹管控及常态化开展数据安全评估，推动数据安全评估的标准化、线上化、智能化。

二、实施过程

（一）数据分类分级

1.数据资产登记

我行已组织各部门全面梳理在业务及经营管理过程中获取和产生的各类数据，遵循完整性、正确性等资产管理规范，按月推送元数据信息文件至数据资产管理系统，登记内容包括系统名称、schema、数据表中文名称、数据表英文名称、字段中文名称、字段英文名称、所属部门等业务、技术要素，纳管应用系统资产信息。

2.分类分级框架构建

（1）监管标准分析融合

依据中国人民银行《JR/T 0197-2020 金融数据安全 数据安全分级指南》和国家金融监督管理总局《银行保险机构数据安全管理办法》等制度文件，结合本行数据情况，整理形成了《典型数据分类分级参考表》，确保分类分级标准符合多方监管要求。

《典型数据分类分级参考表》涵盖了客户数据、业务数据、经营管理数据、系统运行和安全管理数据四个一级分类，各一级分类下又逐步细分，如将标准中“监管”分类的“数据报送”信息融合至“经营管理－数据报送－监管报送信息”；将“经营管理”的“技术管理”信息融合至“系统运行和安全管理”分类下。

（2）梳理分类分级标准的内容示例

分类分级依据和标准形式确定后，需结合《JR/T 0197-2020 金融数据安全 数据安全分级指南》中“金融业机构典型数据定级规则参考表”，梳理标准中的内容示例，在查看标准时能够结合内容示例进行分类和分级，如客户－个人－个人自然信息－个人基本状况信息中，内容示例包括个人姓名、性别、国籍、《海外账户纳税法案》（FATCA）有关个人身份数据、民族、婚姻状况、证件类型、证件号码、证件生效日期、证件到期日期、家庭住址等，对应数据安全级别为敏感数据。

（3）构建分类分级映射框架

梳理出分类分级标准中各分类下包含的内容示例，筛选具有代表性的重要应用系统，结合系统简介、表中文名、字段中文名等信息，逐个分析数据表及字段，与标准中的内容示例建立映射，形成安全词库的数据元依据，如客户－个人－个人自然信息－个人基本状况信息中，敏感性层级为 3 级，标准里的词汇“个人姓名”，梳理行内系统相关字段包括“客户姓名”“对方姓名”“用户姓名”等，可以结合数据命名共性提取共性的数据元“姓名”，以此类推形成完整的分类分级映射框架。

3.词库规则梳理

基于分类分级框架，筛选部分重要应用系统的数据表及字段，通过人工对照“内容示例”与表及字段注释的方式，总结字段共性特征，构建规则化安全词库。词库包含完整的分类体系（安全一级至四级分类）、词汇名称、安全等级、数据元等核心属性，并与数据资产管理系统的自动化盘点任务集成，实现对数据资产字段中文注释信息的扫描分析。

首先，梳理映射关系。梳理每个数据元映射的词汇，每个数据元可映射多个词汇，尽量避免一个词汇对应多个数据元；其次，确定词汇及数据元的识别规则。如是否参与模糊匹配、匹配优先级等；再次，分析含义相近字段的命名情况。如交易时间，在字段中包括：“交易开始时间”，“交易结束时间”，“交易处理时间”，“交易”，“时间”等相关描述，提取词汇过长容易出现漏扫，过短容易跟其他时间相关词汇冲突导致误扫。因此，根据多条件确定，如：含“交易时间”或同时存在“交易”和“时间”或存在“交易”且字段类型为时间类型。

4.盘点算法开发

采用词库匹配方法，应用智能拆词技术，加入精准与模糊匹配标识以及优先级标识，开发形成完善的分类分级盘点算法。首先，将字段中文注释与安全词库中的词汇名称进行完全匹配，匹配成功则结束盘点；

其次，未匹配成功则进行模糊匹配且排除不参与模糊匹配的词汇；最后，依据词汇优先级，优先选择高级别的词汇进行匹配。

在过程中持续排查分类分级结果，多角度优化配置规则，提高安全词库的准确性。同时，建立分类分级结果的更新机制，当数据资产增量更新或安全词汇变更的情况下，通过定时任务实现自动化分类分级盘点及结果更新。

5.结果校验与优化

对分类分级结果进行人工校验和业务沟通复核，持续探索新技术的辅助优化。

筛选部分重要应用系统的分类分级结果进行校验，主要校验敏感级及以上的数据字段，分析误扫、漏扫的字段及原因，对词汇或算法进行优化。

其次，与业务沟通复核。构建分类分级确认调整的线上申请审批流程，由系统所属部门组织技术开发部门开展分类分级结果的线上确认，提出并沟通存在问题，以此持续优化安全词汇或盘点算法。经过确认调整的分类分级结果，后续不再进行自动化盘点，并推动各单位加强数据安全级别的时效管理，及时动态调整。

最后，借助人工智能强大的语义理解能力，精准剖析业务场景需求和上下文的深层逻辑。通过人工智能对业务场景和上下文内容的动态学习和智能分析，不断优化分类分级标准及盘点逻辑体系，提升结果准确性。

（二）数据安全评估

1.明确评估场景及内容

根据监管明确的评估要求，结合同业实践案例，分析我行存量数据出行清单，总结以业务场景为触发条件的数据安全影响评估内容，包括系统上线和数据出行两大场景：

系统上线：包含我行新开发的涉及数据收集、存储、使用、加工、传输、提供、共享、转移、公开、删除、销毁等处理活动的信息系统或产品上线，或在原有信息系统的基础上开发的涉及数据处理活动的新功能上线的场景，应从数据全生命周期保护、数据安全运维保护、产品协议合规等方面开展数据安全影响评估。

数据出行：包含委托处理、共同处理、对外提供等将数据提供至我行之外的业务场景，应从数据处理活动的合法、正当、必要性；合作协议合规；数据安全保护机制；数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利益或者个人、组织合法权益带来的风险；合作方的诚信、守法等情况；合作方的安全能力检查等方面开展数据安全影响评估。

2.梳理标准化评估要素

分析不同业务场景的评估内容，总结提炼必要的评估要素，形成标准化评估模板，包括记录基本的数据处理信息和评估场景信息，涉及系统上线，则评估系统信息、数据安全功能、安全协议等；涉及数据出行，则评估出行数据信息、数据传输安全管理、对接的行外第三方基本情况、合同管理、报备管理、合作

方安全能力检查等。

华夏银行数据安全影响评估模板

填表日期	
填表部门（单位）	
填表人	
数据处理目的	
相关方	

评估模块	评估域	评估项（*必填项）	评估结果	备注
基本信息	数据处理信息	*数据内容 （列出涉及我行信息的关键字段，如：个人客户数据：姓名、手机号、身份证号；客户交易数据：付款账号、转账金额、收款账号）		
		*数据最高安全级别		
		*出行数据规模		
		*数据保存期限（或项目持续时间）		
		*是否涉及个人数据？		若为“是”，请继续填下面一个问题
		是否告知数据主体，并在实施中获取数据主体同意？		
		*是否以“最小授权”原则使用数据？		

图表 6 数据安全影响评估模板

针对所对接机构的不同性质，划分差异化的评估要素，如对接监管机构及政府部门：银行业主管机构、监管机构、政府部门，则无需填写合同管理、报备管理、合作方安全能力检查等；对接专业组织：金融标准组织机构，则无需填写合作方安全能力检查等；对接业务合作：因业务合作需要与我行建立信息系统互联的机构，则需要进行合同签订、报告监管、合作方安全能力检查等。

3.制定评估流程

由业务需求部门根据实际情况按要求填写评估事项的自评结果，并提供支持自评结果的佐证材料，经领导审批后提交数据安全统筹部门。数据安全统筹部门与数据安全技术保护统筹部门对评估结果进行审核，如审核发现自评结果不符合实际情况或所提供的佐证材料不充分的情况，则退回修改或补充。对于达到要求的评估，业务需求部门可开展后续业务；未达到要求的评估，业务需求部门需要进行整改，在整改完成后重新开展评估。

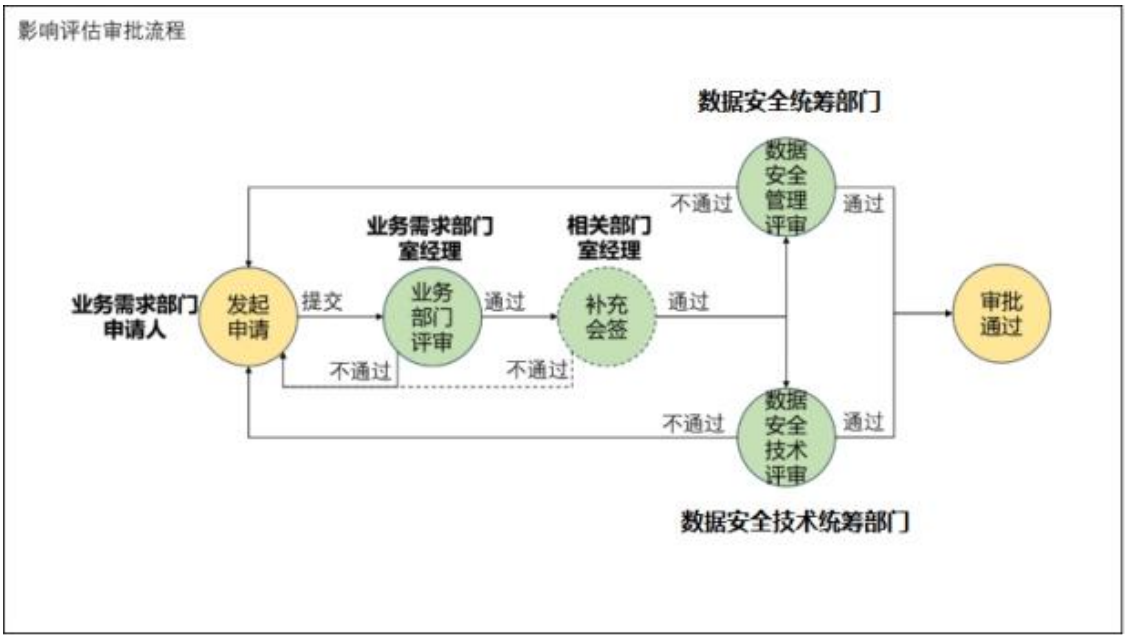
4.在制度中明确评估要求和流程

通过修订并印发数据安全管理办法、细则，构建了由决策层、统筹管理层和执行层组成的“金字塔”式数据安全组织架构，数据安全统筹部门统筹推进数据安全管理工作，规范数据处理活动、开展数据安全影响评估。同时，进一步明确数据安全影响评估的管理要求、评估流程、评估模板等，指导各单位遵循“谁管业务、谁管业务数据、谁管数据安全”的原则，在处理敏感级及以上数据的业务活动时，或开展数据委托处理、共同处理、转移、公开、共享等对数据主体有较大影响的活动时，事前开展数据安全影响评估工作。

5.建设线上化数据安全评估功能

结合已在制度中明确的评估要素和评估流程，搭建线上化数据安全评估功能模块，涵盖数据安全评估的清单查看、申请、审批、会签等环节。支持需求提出部门发起数据安全评估申请，填写涉及系统上线、

数据出行等相关信息，上传相关证明材料；经过业务部门、数据安全管理、数据安全技术三道审批，必要时会签相关部门。



图表 7 数据安全影响评估流程

6.开展日常数据安全审查

组织开展信息科技项目、业务需求、数据应用中数据安全需求识别，针对涉及敏感级及以上数据处理活动的新需求，以及数据委托处理、共同处理、对外提供等特殊业务场景，在需求评审环节提出要求，引导需求提出部门通过线上化功能开展数据安全评估，审查数据安全评估情况，督促业务需求提出部门按要求进行整改，并在整改完成后重新开展评估。

7.持续完善数据安全评估体系

数据安全评估作为数据安全管理体系建设中重要的一环，对组织的敏感数据和信息系统进行全面分析的过程，旨在识别潜在的安全风险，存在关键数据定义难、场景依赖度高、控制点繁杂等难点。评估过程中涉及信息核对、文档查阅、配置查验、技术检测、编制报告等多个步骤，要求评估审核人员具备丰富的领域专业知识和实践经验。

因此，需结合监管制度要求及数据安全评估实践，持续完善评估要素，厘清自动化预评估规则，提升系统评估效率，减少人工校验的工作量。同时，积极探索人工智能大模型语义分析的智能化，将人工智能大模型应用到数据安全影响评估过程中，根据评估模板和规则自动生成安全评估报告，降低实施、审核人员的技术门槛，节约数据安全运营人力成本和工具购买成本；动态适应监管要求变化，生成标准化分析报告，在满足监管审计要求前提下，提升全行数据安全管理水平和效率，实现数据高效流动应用。

三、成果与效益

（一）运营效率革新

通过建立分类分级管理体系，优化分类分级自动化盘点逻辑，有效减少了人工识别和标注的工作量，成功实现百万级结构化数据的分类分级，支持各业务部门进行结果的线上确认和调整申请审批，显著提升了分类分级管理的运营效率。

数据安全评估的线上化有效减少传统线下模式中纸质文档的使用、人工审核的低效以及跨部门沟通的延迟；线上平台支持数据的实时更新和共享，便于查看分析和快速决策，减少因人为操作失误导致的额外成本。

（二）推进落实分级管控

基于业务确认的分类分级结果，持续推动监管对于数据分级管控的合规要求落地，在数据全生命周期各环节的数据处理活动中，根据数据安全级别落实对应的数据安全处理要求，实现业务需求和安全需求之间的平衡。

（三）精准识别安全风险

已形成常态化的数据安全评估和审查机制，组织信息科技项目、业务需求开展安全审查，审查特定业务场景下的数据安全评估情况。将数据安全评估作为开展特殊业务场景的前置条件，通过“以评促改”，辅助业务需求提出部门组织排查、梳理清楚在项目、业务开展过程中的潜在的数据安全威胁和合规风险，并提前采取应对措施，有针对性地整治到位，切实防范数据安全风险。

四、经验与启示

（一）强化规范管理，提升运营能力

通过构建科学完善的数据分类分级体系，建立统一的分类分级标准，持续规范数据管理流程，确保数据理解的一致性与准确性，能够为精细化运营提供可靠的数据支撑，进一步助力提升数据安全运营效率与决策水平。

数据安全评估的难点在于其对具体场景的高度依赖性，不同业务场景下的数据处理方式和安全需求各不相同，增加了评估的复杂性和挑战性。因此，需要深入掌握新项目、新需求的业务特性、数据处理传输机制等，以提升对特殊场景的识别和应对能力。

（二）深化技术赋能，驱动智能化升级

通过应用人工智能等先进技术，在数据分类分级方面，结合语义分析、业务知识图谱与动态学习机制的协作模式，深入解析字段语义，精准理解业务场景，提升灵活性与准确性；赋能业务准确识别高风险数据，确保安全合规前提下，推进业务创新，实现从“人工标注”转换到“智能解析”的全面升级。在数据

安全评估方面，重点把控数据“出系统”“出行”“出境”三道关键关口，推进数据安全影响评估的标准化、线上化、智能化，规范数据处理活动，有效防范和抵御金融数据安全风险。

（三）打造生态共建，推动可持续建设

构建企业间数据安全实践案例共享机制，为同业提供实践参考与经验借鉴。通过提炼经验、创新实践，助力金融行业整体提升数据安全管理水平；通过构建数据安全共享机制，既能降低试错成本，提升管理效能，又能推动数据安全生态的良性发展与可持续建设。

第十节　浙商银行 大数据平台安全管理的探索与实践

一、背景介绍

近年来金融业数据安全形势日趋严峻，数据安全事件频发，国家与监管部门密集出台数据安全法律法规以强化监管，而金融机构数字化转型、做好金融 “五篇大文章” 又高度依赖数据支撑，如何实现数据安全使用与共享成为金融机构亟待解决的核心命题。

金融机构数据安全防护体系建设和运营面临多项挑战。在建设层面，一是金融机构数据安全防护能力建设以外购产品为主，而不同厂商产品兼容性不足导致安全管控易形成“竖井”，缺乏统筹联动；二是数据安全防护与业务场景深度绑定，复合型专家人才紧缺；三是第三方供应商安全水平参差不齐，供应链风险突出。在运营层面，一是数据资产类型复杂多样、海量安全告警掩盖真实数据安全风险；二是数据安全风险处置难度大，数据追踪溯源困难；三是数据安全风险与业务关联性强，跨部门协作存在机制性障碍。

企业级大数据平台作为数字化转型的核心基础设施，其作用贯穿业务运营、决策支持、技术架构优化等多个维度，具有数据体量大、敏感性高、用途广泛等特性，一旦发生数据泄露或滥用，可能对业务运行、用户权益及数据资产安全造成严重损失。因此，在大数据平台建设和运营过程中，对数据安全管理的需求尤为迫切，需从多层面构建覆盖数据全生命周期的防护体系，平衡数据价值释放与安全风险管控的关系。

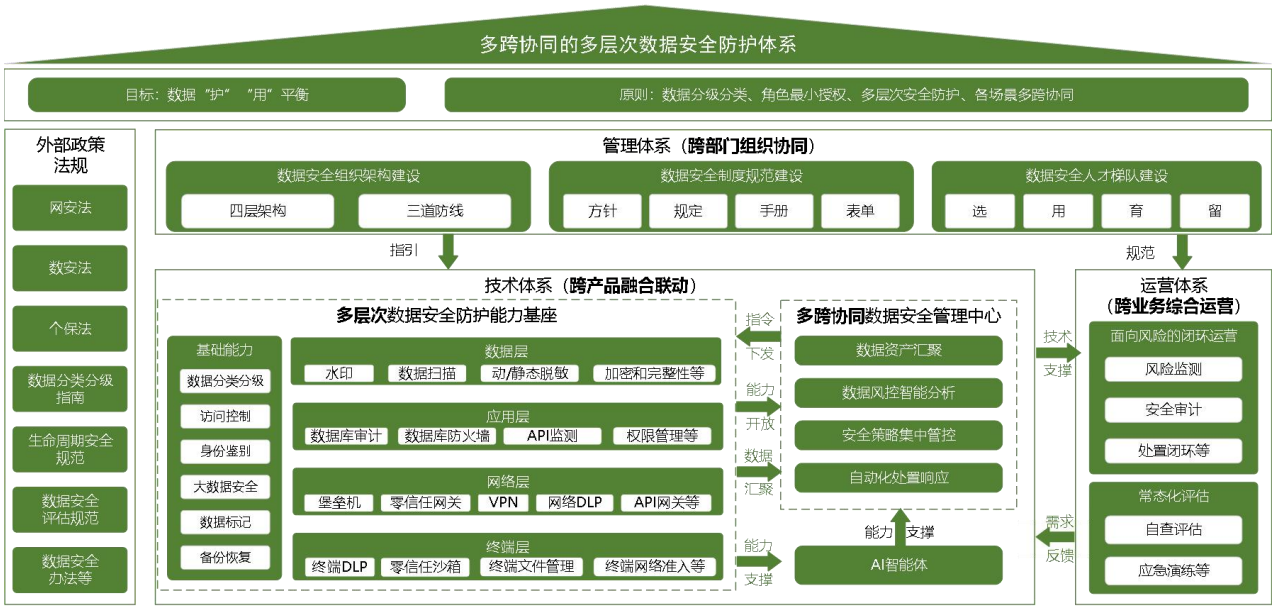
本行基于多年数据安全防护体系化建设经验，逐步形成管理、技术、运营联动的**多跨协同多层次的数据安全防护体系**，为数据的安全流转和监管合规保驾护航。本文旨在抛砖引玉，介绍本行多跨协同多层次的数据安全防护体系概况，并结合本行大数据平台数据安全管理实践说明数据安全防护体系的意义和价值。

二、实施过程

（一）多跨协同多层次的数据安全防护体系

本行数据安全防护体系（如下图）以数据的全生命周期、全应用场景、全维度风险覆盖为需求，划分为管理、技术、运营三大维度，涵盖组织、流程、人员、技术、运营等数据安全事务，考虑跨部门、跨业务、跨产品联动融合，在宏观层面贯彻多跨协同的思路，管理体系、技术体系、运营体系相辅相成。数据

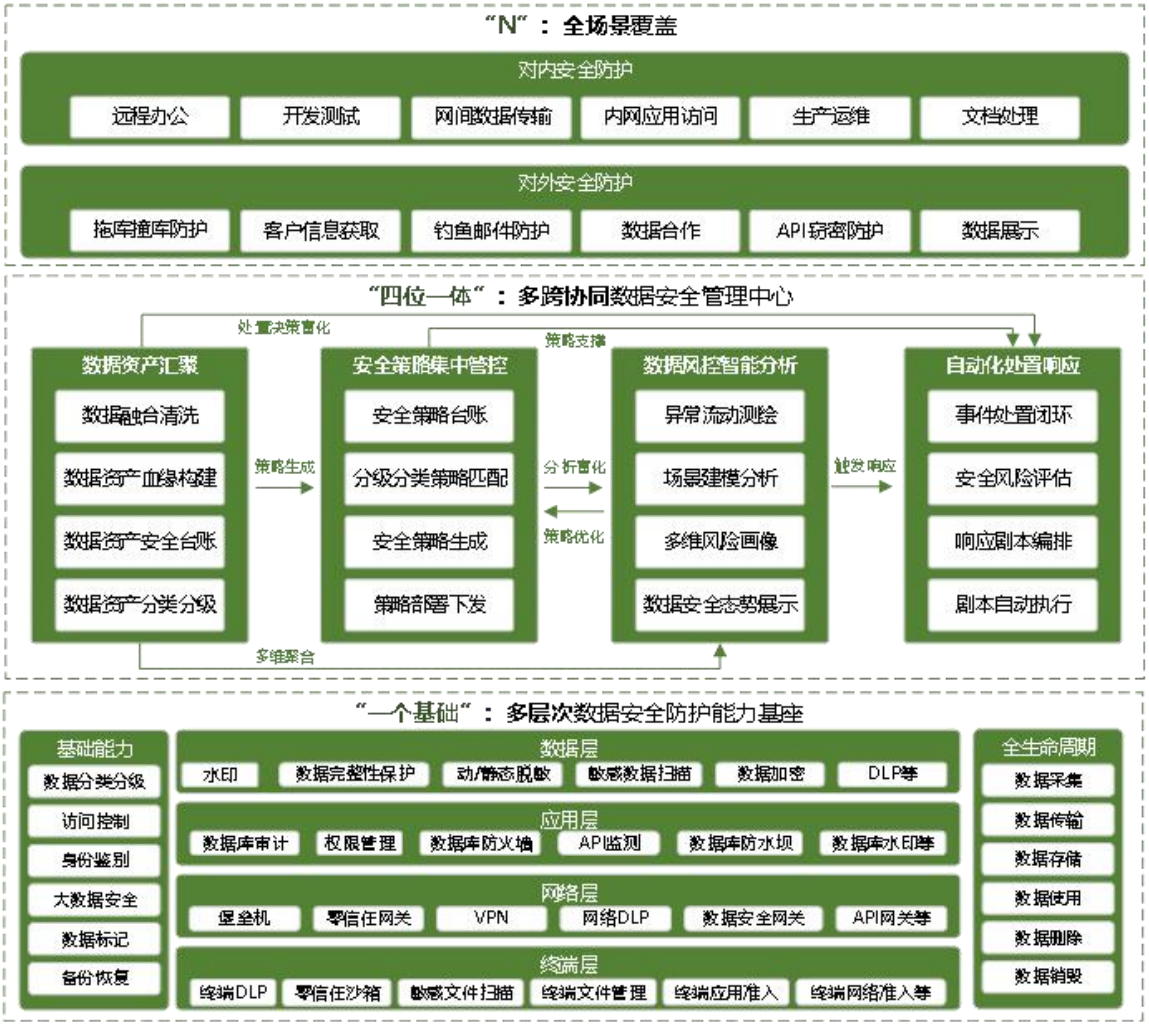
安全防护管理体系作为数据安全防护工作的基础保障，落实组织架构、制度规范、人才梯队建设的管理工作。数据安全防护技术体系针对金融核心场景，围绕数据全生命周期，以安全技术能力落地来实现场景化、差异化防护目标。数据安全防护运营体系依托技术和管理体系，实现智能化、一体化的数据安全风险运营闭环和数据安全风险常态化评估。



图表 8 多跨协同的多层次数据安全防护体系架构

（二）“1+4+N”数据安全技术防护体系

具体来看，本行构建了“1+4+N”数据安全技术防护体系（如下图），以一个多层次数据安全防护能力基座为基础，通过集成**数据资产汇聚、安全策略集中管控、数据风控智能分析、自动化处置响应**的四位一体数据安全管理平台，覆盖对内、对外数据使用的 N 个场景，实现数据全生命周期、全应用场景、全维度覆盖的安全防护。



图表 9“1+4+N”数据安全技术防护体系

数据资产汇聚实现安全视角数据资产识别。基于数据分类分级结果融合多项数据安全日志源，对数据资产进行解读分析和精确打标，实现全量数据的自动化分级标定与智能语义分类，融合安全资产日志，分析资产关联关系、流转链路，精准定位数据来源、属主、责任人，高效辅助策略调整、风险预警与自动化处置。

安全策略集中管控形成场景化策略管理能力。将法律法规等外规内化形成内部制度规范，依据制度制定策略基线，形成数据安全策略矩阵。同时针对不同数据使用场景对安全策略矩阵进行裁剪，根据数据访问主客体、平战切换等维度动态调整安全策略，在面对复杂的金融业务时，能够自适应调整防护措施，显著提升数据安全管理效率。

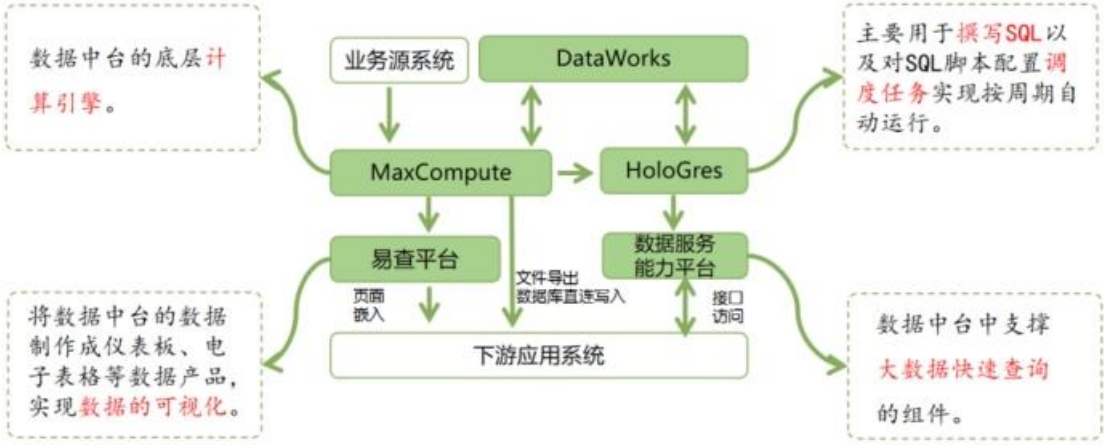
数据风控智能分析实现一体化数据安全预警。全面汇聚各个安全产品的多源异构日志，进行数据的关联、清洗、标准化并结合 AI 进行融合分析，挖掘深层次的风险。打破数据安全产品竖井式建设带来的数据和能力孤岛问题，建立动态风险画像和态势感知视图，实现数据安全态势可视化监控。

自动化数据安全风险处置响应。基于 IPDRR 模型构建五大基础能力模块，在传统安全运营平台自动化

响应处置能力的基础上强化数据安全风险处置能力。聚焦风险闭环，利用 AI 智能体赋能业务专家经验，显著提升数据安全运营的自动化水平与处置效能。

（三）大数据平台安全管理实践

本行大数据平台采用阿里大数据底座，服务均为容器化部署，具备高可用能力，通过源数据库实现数据备份。平台包含 MaxCompute、DataWorks、Hologres、QuickBI 四大组件（如图 3），现已汇集行内主要应用系统数据，实现“批量+实时+在线”交互平台一体化，形成一站式全链路数据研发体系。大数据平台的推广使用全面提升了行内数据采集、数据研发效率。



图表 10 大数据平台结构图

因大数据平台涉及大量业务数据，可能面临数据越权访问、终端留存敏感信息、敏感数据外发等隐患引发的客户隐私泄露、核心业务数据外流及系统权限被滥用的风险。本行基于“1+4+N”数据安全技术防护体系，聚焦大数据平台数据资产整合、安全加固防护、风险动态监测、事件响应处置及访问行为审计，落实大数据平台的数据安全管控（如下图）。

图表 11 基于大数据平台的安全防护能力关联图

三、成果与效益

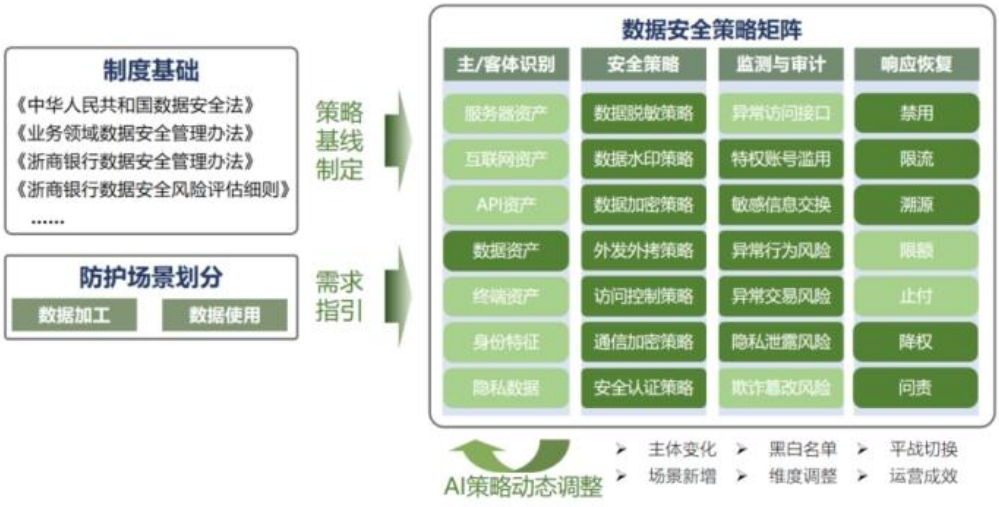
（一）大数据平台数据资产整合

大数据平台数据量大、敏感性高、用途广泛，需根据数据类型与安全级别施加不同的安全防护策略。传统识别方式准确率低、耗费人力、效率低下，可能导致敏感数据未准确识别产生的滥用、越权使用、泄露等安全风险。我行使用规则模型与分级分类智能结合的技术方式，基于动态数据敏感度评估模型、业务价值权重算法及语义特征识别等技术（如下图），并通过 AI 智能体提高数据识别准确率，实现数据的自动化分级标定与智能语义分类，有标注数据准确率可达 97%以上，无标注数据也可达到近 80%准确率。

图表 12 大数据平台数据资产安全管理技术及应用图谱

（二）大数据平台安全加固防护

大数据平台通过将组织划分为多个工作空间限制数据知悉范围，并按照用户角色不同划分数据加工和数据使用两个场景，分配不同工作空间权限。根据平台数据的分类分级结果，结合场景对数据安全策略矩阵进行裁剪（如下图），针对不同类型和敏感级别的数据设置安全防护、访问控制等策略。

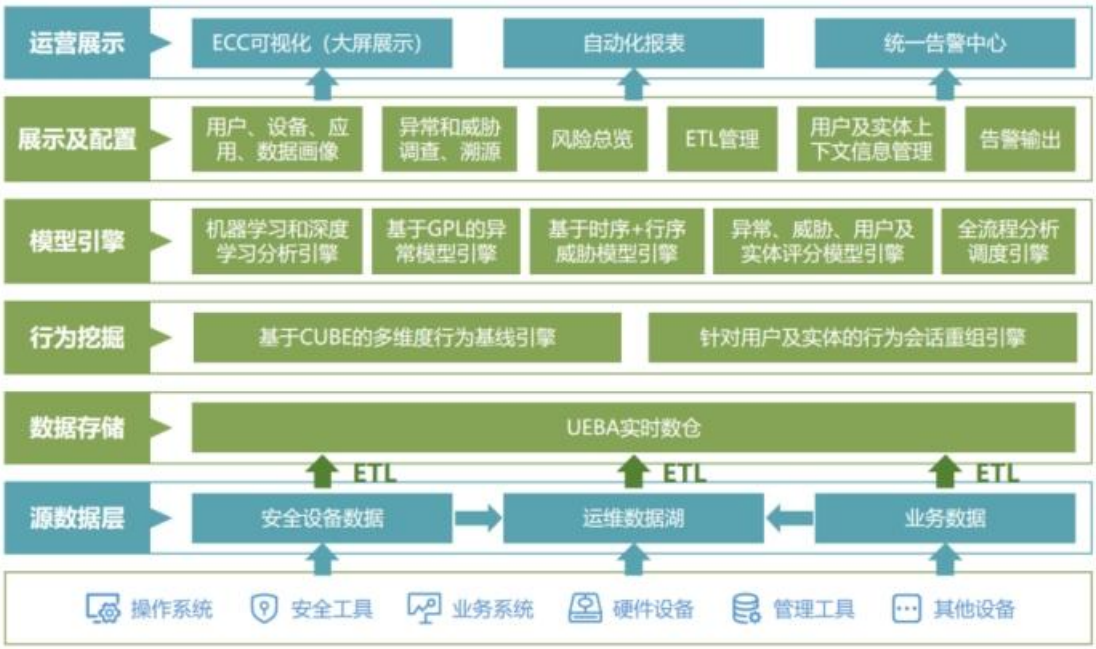


图表 13 大数据平台数据安全策略矩阵

针对普通用户访问使用大数据平台，平台以反向代理形式部署 API 动态脱敏系统，从大数据平台应用侧统一管控，默认采取高敏感性数据项动态脱敏、文件下载拦截等数据访问控制策略，提升大数据平台安全基础保障能力。针对特权用户访问大数据平台，因其具有文件下载权限及部分高敏感性数据项访问需求，由零信任沙箱统一纳管访问，借助沙箱隔离文件特性，刚性管控敏感数据文件不直接落地办公终端，实现敏感数据访问的封闭化管理，杜绝大数据平台敏感数据外泄。针对数据分析人员，在数据加工场景下需访问使用原始数据，可能涉及大量敏感数据，仅依靠动态脱敏、零信任沙箱无法满足需求，为此配备专门的数据建模间，采取独立物理操作环境、独立门禁、视频监控，网络访问控制上采取独立网段、堡垒机记录建模操作行为和数据访问行为，在满足便利性的同时最大程度保障数据安全。

（三）大数据平台风险动态监测

建设数据安全集中管控平台，实现大数据平台的风险动态监测（见下图）。数据安全集中管控平台通过采集、清洗、标准化大数据平台的数据访问相关日志，借助多源数据融合分析和风险建模能力构建大数据平台用户的多维度行为基线，建立用户访问风险画像，针对异常访问、异常登录等潜在风险隐患强化监测。目前已建立大数据平台数据访问相关的风险模型 41 个，例如建立周期内用户访问大数据平台的频次基线，当某天用户访问大数据平台的频次远超自身的历史访问基线参考值，会标记为异常行为产生告警，并对用户风险评分进行核减。



图表 14 数据安全集中管控平台结构图

（四）大数据平台事件响应处置及审计

通过数据安全流程自动化与响应平台处置闭环安全设备告警和用户需求申请，在大数据平台中实施通用、快速、有效的数据安全运营策略，并结合技术、管理、运营等多方面的措施，确保大数据平台的数据全生命周期安全。事件闭环主要流程可见下图。平台部署后，数据安全风险处置效率明显提升，将告警分析研判等风险处置耗时由原来人工处置时的几天、几小时降低至分钟级甚至秒级。

图表 15 大数据平台事件响应处置流程图

四、经验与启示

本行大数据平台安全管理通过引入数据分级分类智能体、大模型多模态处理引擎等智能化技术，突破传统人工识别瓶颈，实现数据资产的高效梳理。基于数据类型与安全级别制定差异化防护方案，覆盖多源异构数据与众多应用系统并定期动态调整，确保策略与业务场景实时匹配。经由数据安全集中管控平台全面汇聚各个安全产品的多源异构日志，实现数据的关联、清洗、标准化并结合 AI 进行融合分析，挖掘深层次的风险。依托数据安全流程自动化与响应平台，将安全设备告警处置与用户需求申请纳入闭环管理，整合技术、管理、运营措施，实现风险处置效率从 “人工耗时 ” 到 “机器响应” 的大幅提升。该数据安全防护体系在本行落地应用以来，大幅度提升全行数据安全防护水平与安全运营能力，实现数据保护与数据流动利用的动态平衡，激活数据要素潜能，推进数据安全使用与共享，同时助力本行在各大重要活动中取得优异成绩，圆满完成北京冬奥会、杭州亚运会等重保任务。

第十一节　河南农商银行 数据安全三同步实践

一、背景介绍

2025 年，河南农商银行实现从“联合银行”到“统一法人”的转变，坚定“三农”使命仍然是河南农商银行的核心责任，基于对未来发展趋势的研判，管理层制定了为期三年的科技战略发展规划。随着信息科技的迅速发展及业务系统的规模化建设，网络和数据安全方面也同步面临诸多挑战，如整体数据安全建设规划不完善，数据分类分级工作的落地成效不足，安全运营机制有待优化等，如何有效应对各类数据安全风险，成为我行亟待解决的重要课题。

（一）外部因素

法律法规和条例：《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》《网络数据安全管理条例》等法律法规相继发布，对规范数据处理活动、个人信息保护等提出了明确要求。针对网络和数据安全的监管要求持续提升，我行的数据安全管理工作面临新的挑战。

行业监管办法：中国人民银行、国家金融监督管理总局（金监局）陆续出台了一系列行业标准和监管办法。2024 年 12 月 27 日，金监局发布了《银行保险机构数据安全管理办法》，这是金监局挂牌成立后发布的首部数据安全管理方面的部门规章。

金监局《办法》规定银行保险机构应当建立数据安全责任制，党委（党组）、董（理）事会对本单位数据安全工作负主体责任。银行保险机构主要负责人为数据安全第一责任人，分管数据安全的高级管理人员为直接责任人，明确各层级负责人责任，细化违规情形和责任追究事项，健全落实问责处置机制。金监局《办法》同时明确，其及派出机构将对银行保险机构的数据安全保护情况实施监督管理，并将数据安全管理纳入监管评级评估体系，依法对数据安全事件进行处罚和处置。

2025 年 4 月，中国人民银行发布了《中国人民银行业务领域数据安全管理办法》，该办法自 2025 年 6 月 30 日起施行。旨在规范中国人民银行业务领域数据的安全管理并促进数据的开发利用，对其业务领域数据相关的处理活动及其安全监督管理作出明确规定。

安全事件：数据泄露、数据勒索等安全事件频发，监管机构对银行“数据安全管理不足”等违规行为的处罚力度不断加大，这些都显著增加了银行在法律合规、声誉和财务方面的风险。因此，强化数据安全管理，预防和减少数据安全事件的发生，对我行来说尤为迫切。

（二）内部因素

我行需根据信息科技业务发展态势，遵循最新监管要求，并借鉴行业最佳实践，构建一个有效的数据安全管理框架，细化各项措施，积极落实“三同步”机制，从源头构建安全防线，在当前推进开展数据分类分级等基础工作阶段，将其融入业务全生命周期，有效弥补安全规划不足、运营机制滞后等短板，为数据安全防护体系提供系统性保障，提升我行的数据安全防护能力，确保数据处理的合规性和安全性。

二、实施过程

（一）同步规划：构建全方位数据安全蓝图

1. 结合监管与内部需求制定规划

在同步规划阶段，我行紧密围绕最新监管要求，将《银行保险机构数据安全管理办法》《中国人民银行业务领域数据安全管理办法》等法律法规作为规划的重要依据。同时，充分结合自身在数据安全自评中发现的薄弱环节，制定了全面且贴合我行实际的数据安全规划，明确了未来 3 至 5 年数据安全建设的总体目标。以满足监管合规要求为基础，聚焦数据泄露高风险领域，逐步构建“外部攻击防窃取、内部数据防

泄漏、全面安全监控”三位一体的数据安全防护体系。

2. 融入业务全生命周期规划

将数据安全规划融入业务全生命周期，制定针对性的安全防护措施。同步规划数据分类分级、数据防泄漏、API 安全监测、数据库审计等技术手段，确保业务数据在全生命周期的安全。同时，结合业务特点，对不同业务系统的数据进行分类分级规划，明确不同级别数据的安全管理要求和防护措施，为后续的数据安全建设提供清晰的实施指引。

（二）同步建设：打造多层次数据安全防护体系

1. 组织同步建设

（1）完善治理架构。成立网络与数据安全管理工作组、网络和数据安全领导小组，明确领导小组的职责权限，使其成为数据安全工作的最高决策机构和监督主体。构建“领导小组－管理工作组－执行部门－岗位人员”四级治理架构，清晰划分各级架构在数据安全管理中的职责，形成上下联动、高效协同的工作机制。领导小组负责审定数据安全战略规划和重大决策；管理工作组负责统筹协调日常数据安全管理工作；执行部门负责具体落实各项数据安全措施；岗位人员则对本岗位的数据安全负直接责任。

（2）明确多方责任。针对组织建设中存在的分工责任不明确问题，制定详细的责任清单，明确监督层、管理层、执行层、合作方、数据提供方、处理方、运营方、接收方等各方在数据安全管理中的具体责任。对于合作方，签订数据安全协议，明确其在数据获取、使用、存储等环节的数据安全责任和合规义务，并定期对其数据安全管理情况进行审计和评估。要求合作方不得将获取的我行数据用于协议外的其他用途，如发生数据泄露等安全事件，合作方需承担相应的赔偿责任。

（3）配备专职人员。参考同业经验，在总行及各分行设置专职的数据安全管理岗位，配备具备专业知识和丰富经验的数据安全管理人员。专职人员负责数据安全策略的制定与执行、数据安全事件的应急处置、数据安全培训的组织等工作。同时，建议各业务部门指定至少一名数据安全兼职人员，协助专职人员开展本部门的数据安全管理工作，形成覆盖全行的数据安全管理网络。

2. 制度同步建设

（1）完善核心制度。加快《数据安全管理办法》《个人金融信息安全保护办法》等制度的制定、印发与实施，并根据实际运行情况进行动态修订和完善。在核心制度中明确数据安全管理的总体目标、基本原则、组织架构、责任分工、管理流程等内容，为全行数据安全管理工作提供基本制度遵循。在制度中明确数据全生命周期的安全管理要求，包括数据的采集、存储、使用、传输、销毁等环节的具体规定。

（2）制定配套细则。针对制度建设中缺少细化落实的制度体系问题，围绕核心制度制定一系列配套的细则和操作指南。制定《数据分类分级管理细则》，明确数据分类分级的标准、方法和流程，以及不同级别数据的安全保护措施；制定《数据安全风险评估操作指南》，规范风险评估的频率、方法、内容和报告格式；完善应急预案中的数据安全事件应急处置细则，明确应急响应的组织架构、处置流程、责任分工和保障措施等。通过配套细则的制定，确保各项制度能够落地执行。

（3）建立制度更新机制。建立数据安全制度动态更新机制，定期对现行制度进行梳理和评估，根据法律法规、监管要求、业务发展和技术变革等动态变化，及时修订和完善相关制度。当新的法律法规出台或监管要求发生变化时，及时对现有制度进行调整，确保制度的合规性；当业务模式创新或引入新技术时，补充针对性的数据安全管理规定，防范新型数据安全风险。

3. 文化同步建设

（1）开展分层培训。每年组织开展网络和数据安全意识培训，并根据不同岗位人员的工作特点和数据安全需求，实施分层分类精准培训。对于管理层，培训内容侧重数据安全战略、监管要求和风险管理等方面；对于技术人员，培训内容侧重数据安全技术、安全工具的使用和安全漏洞的修复等方面；对于普通员工，培训内容侧重数据安全基础知识、岗位操作规范和安全事件的识别与报告等方面。通过分层培训，提高培训的针对性和实效性。

（2）丰富培训形式。采用多元化培训形式，如讲座、案例分析、答题竞赛等，提高员工的参与度。定期举办数据安全案例分析会，通过分析行业内发生的数据泄露、数据勒索等安全事件，让员工深刻认识到数据安全的重要性；开展数据安全模拟演练，让员工在实践中掌握数据安全事件的应急处置流程和方法。

（3）营造安全氛围。通过内部网站、宣传栏、公众号等多元传播渠道，广泛宣传数据安全知识、法律法规和我行的数据安全管理制度，营造“人人重视数据安全、人人参与数据安全”的良好氛围。定期发布数据安全警示信息，提醒员工注意防范数据安全风险。

4. 技术工具同步建设

（1）多源数据自动化分类分级

依托分类分级平台，构建大模型分类引擎，并结合规则驱动技术，通过历史数据训练优化算法模型，对结构化数据采用规则匹配快速分类。开发多数据源接入模块，支持关系型数据库、国产数据库、大数据平台及多种格式文件接入，并同步制定分类分级标准。同步分类结果至其他安全工具，核心技术包括分布式扫描架构、机器学习与大模型技术、规则驱动、多数据源接入及分类结果联动技术，提升分类效率与精准度。

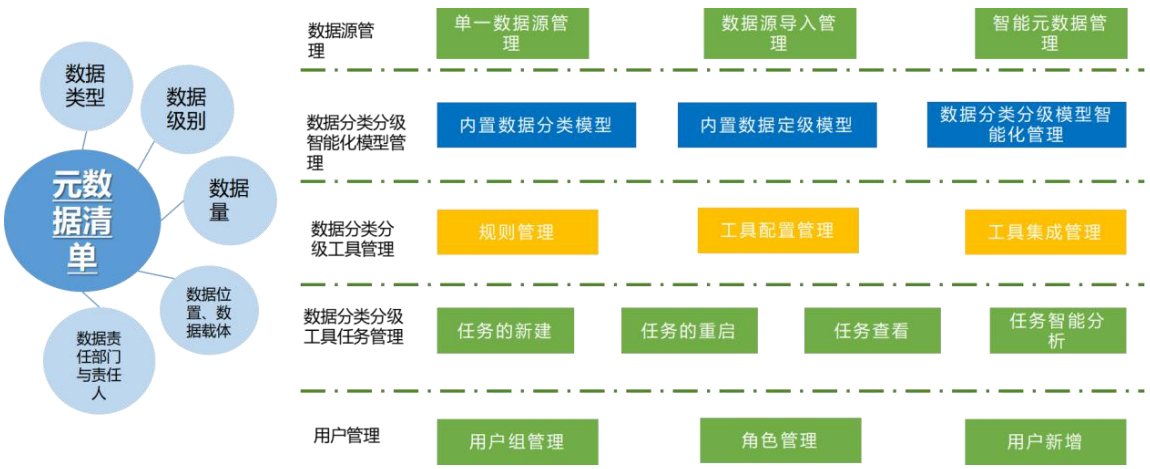


图 1 数据分类分级平台架构图

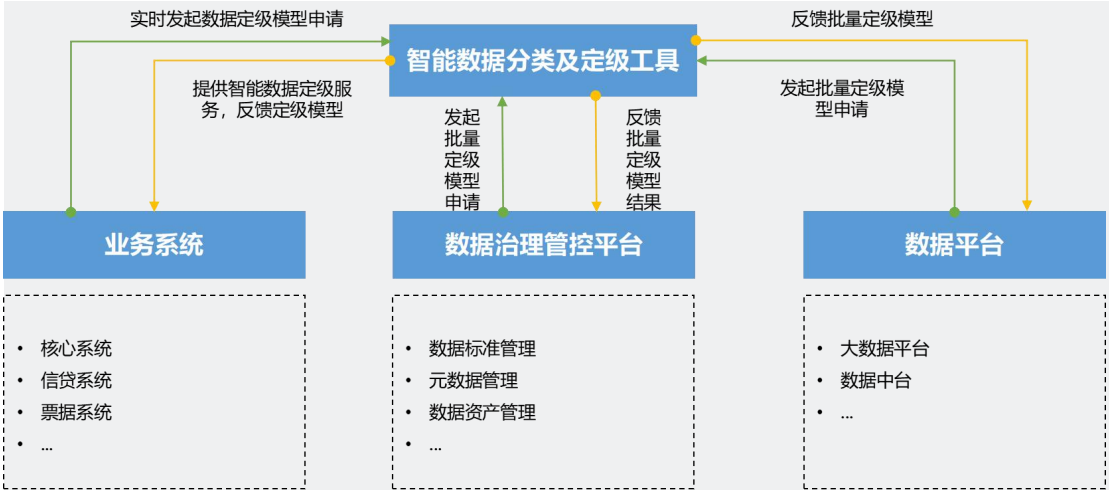


图 2 数据分类分级平台数据对接图

（2）全量 API 识别与多维风险智能防护

通过对生产和灾备金融互联网区域网络出口 API 流量进行监控，及时发现未授权、未脱敏等风险隐患。利用监控系统的自动化 API 识别技术，结构化还原网络流量中的 API 请求和响应，提取参数配置，识别 API 的技术设计格式，包括 RESTful、SOAP、gRPC、GraphQL、Dubbo3.0。

通过持续监测和分析 API 交互数据，识别 API 请求和返回内容中包含的敏感数据，并及时更新敏感数据暴露的细节，以便更好地了解 API 的功能、使用情况、数据暴露面情况和潜在的安全风险。

结合 API 携带的数据和 API 分类分级算法，对 API 进行分类定级，从功能层面，类型包括登录 API、注册 API、短信验证码发送 API、导出 API、文件上传 API、文件下载 API 等，从 API 数据暴露面层面，类型包括数据暴露 API、数据采集 API 等，在其他层面，包括服务调用 API、人机访问 API 等。级别包括高敏感、中敏感、低敏感、非敏感。

通过 API 持续发现能力，自动监测和跟踪 API 的变化，API 状态包括新增 API、活跃 API、失活 API 和复活 API。及时了解和管理 API 的变化，进行相应的验证和评估。

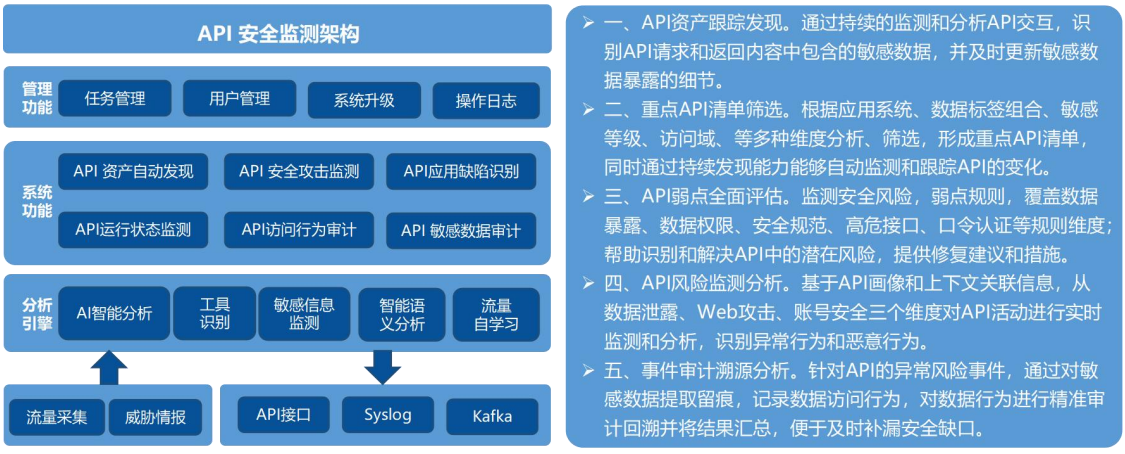


图 3 API 监测工具架构图

（3）多端协同的敏感数据防泄漏

构建网络数据防泄漏体系，对互联网出口外发数据进行安全监测。整合关键词匹配、正则表达式等近 20 种技术，建立敏感数据识别规则库，针对敏感信息制定专属规则，通过 MD5 算法生成文件指纹，实现网络与终端协同联动，可追溯敏感数据外发源头。对接统一安全平台实现策略集中配置与下发，通过多维度敏感数据识别、基于 DPDK 的网络流量线速解析、终端行为监控、文件指纹关联及流式碎片防护技术，有效预警多渠道敏感数据泄露。实时监测大屏同步呈现各网口流量、事件趋势、风险等级分布等多维度数据，支持事件数据分析大屏与海量数据分析大屏的灵活切换，动态展示最新风险事件，为运营决策提供实时态势支撑。

图 4 数据防泄漏部署示意图

（4）数据全生命周期精准审计与风险防控

通过在生产中心机房和灾备中心机房部署数据库审计系统，对重要三级系统的数据库操作进行监控、记录和分析，可全面捕获数据库访问操作流量，依托数据库协议解析和完全 SQL 解析技术，即便面对超长语句、多层嵌套、多表关联等场景，仍能精准识别审计元素并准确分析操作类型和对象，同时具备加密审计能力，可对 Oracle 高级安全加密、SSL 等通讯链路加密场景进行解密审计，且不影响正常加密传输，从而确保数据的安全性和合规性。该系统功能可覆盖数据全生命周期的审计需求，可自动发现网络内未知数据库并形成资产清单，无需人工干预即将其纳入审计范围，内置近 500 种针对异常登录、高危操作、SQL 注入等风险行为的识别规则且支持自定义配置，一旦监测到风险，能通过邮件、短信、企业微信等多种方式及时告警，日志管理采用在线、备份、外送三种存储机制，结合高压缩处理技术满足日志信息保留半年以上的要求，还可对接 Syslog 和 Kafka 以便第三方平台进行二次分析。

- 全方位审计：面向应用调用数据库、数据库横向访问、运维访问等行为，从来源、时间、结果、操作、风险多维度监测审计。
- 安全风险监测：提供数据库漏洞攻击实时监测预警能力，对高危操作行为、高权限账户行为、敏感数据访问行为进行实时告警。
- 异常行为分析：通过高耗时语句、失败的登录、不认识的新操作、失败的新操作、失败的登录、客户端信息的变化、超量访问等多维度关联分析，快速感知异常访问风险。
- 语句耗时分析：提供数据安全分析报表，实时监测数据库的性能状态，助力开发、运维过程中的应用优化。

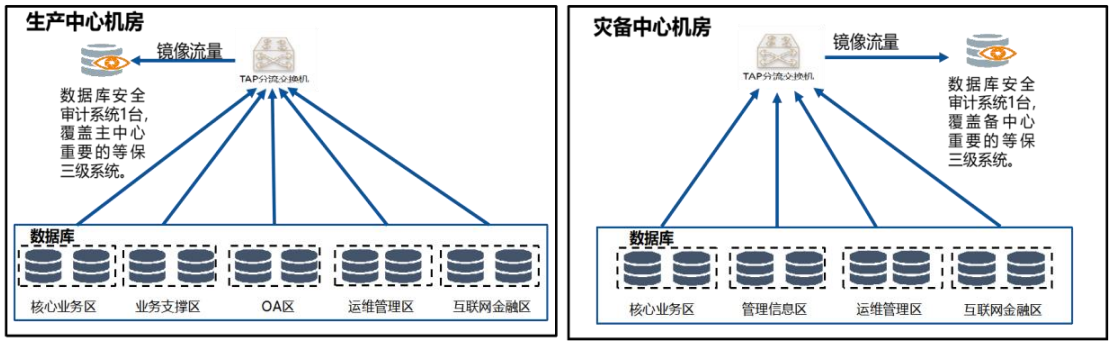


图 5 数据库审计系统部署示意图

（三）同步运行：实现全流程安全管控

1. 技术工具协同运行

各类数据安全技术工具实现协同运行，形成一个有机的整体。数据分类分级平台作为基础支撑工具，将数据分类分级结果实时同步至其他安全工具，为其他安全工具提供精准的防护依据。数据分类分级工具通过向 API 安全监测工具推送敏感数据标识，使其针对含高敏感数据的 API 接口提高监测频率并提升防护等级，一旦发现未脱敏传输等违规行为立即告警；为数据防泄漏工具提供敏感数据识别规则补充，助力其更精准地识别外发数据中的敏感信息，提升发现效率。

网络数据防泄漏工具结合 MD5 算法、文件指纹技术、接口等方式，追溯泄露文件来源。当 API 安全监测工具发现异常的 API 调用行为可能导致数据泄露时，可将相关信息同步至网络数据防泄漏工具，使其加强对该类数据传输的监测。同时，数据库审计工具也会重点关注与该 API 相关的数据库操作，共同形成全方位的安全防护闭环。

2. 制度与流程落地运行

将数据安全制度和流程融入日常业务运营中，确保制度的有效执行。在数据处理的各个环节，如数据采集、存储、使用、传输、销毁等，要求相关岗位人员严格按照相关制度和流程进行操作。定期检查和评估制度执行情况，及时发现问题并进行整改。

建立数据安全事件应急处置机制，当发生数据安全事件时，按照既定的流程快速响应、科学处置，最大限度降低事件造成的影响。同时，推动数据安全风险评估常态化开展，根据评估结果及时调整安全策略和防护措施，确保数据安全防护能力与业务发展需求和风险变化态势相适应。

通过同步规划、同步建设、同步运行的“三同步”实践，我行逐步构建起完善的数据安全防护体系，有效弥补了安全规划不足、运营机制滞后等短板，提升了数据安全防护能力，确保了数据处理的合规性和安全性，为业务的稳定发展提供了坚实的安全保障。

三、成果与效益

（一）合规性显著提升

围绕《银行保险机构数据安全管理办法》等法规开展工作，数据安全合规工作取得重大突破。完成数据分类分级，清晰界定核心、重要和一般数据，实施差异化保护措施，完全符合监管要求。数据处理全环节严格遵循制度流程，确保合法规范，有效规避监管处罚风险。

（二）防护能力大幅增强

“三位一体”数据安全防护体系作用显著。多源数据自动化分类分级平台精准识别敏感数据，为防护提供依据；全量 API 识别与风险防护工具拦截未授权等风险，降低 API 漏洞泄漏风险；多端协同防泄漏体系管控办公网敏感数据外发；数据库审计系统监控分析操作，预警异常行为。技术工具协同运行，全方位提升防护能力，有效抵御内外部威胁。

（三）业务稳定性有力保障

完善的防护体系为业务稳定发展提供支撑。建立数据安全事件快速响应机制，确保在最短时间内评估处置，降低对业务影响。常态化风险评估及时解决潜在风险，保障业务系统稳定。新业务开展前做好安全评估与防护，为上线和运营创造良好环境，保障银行资产增长、存贷款业务稳健运行，巩固行业领先地位。

（四）成本效益优化明显

初期投入的资金用于技术采购、人员配备和制度建设，长期来看成本效益显著。精准防护减少数据安全事件导致的直接赔偿、业务中断及间接声誉损失。风险评估和常态化监测及时解决潜在风险，避免演变为重大事件的高额成本。高效管理体系提高运营效率，减少业务非正常停滞时间，间接创造经济效益。

四、经验与启示

（一）紧跟监管导向是关键

监管法规为银行数据安全管理指明方向。我行重视监管导向，规划阶段以监管要求为依据，确保建设与运行符合监管标准。启示金融机构需关注监管动态，调整管理策略，将监管要求融入日常经营，以合规构建安全防线，避免监管不合规困境。

（二）全生命周期管理是核心

将数据安全规划融入业务全生命周期，从起始阶段考虑风险并制定措施，可避免后期大规模整改的高成本高风险。数据全生命周期各环节需严格监控与管理，要求金融机构建立完善治理体系，明确责任与规范，实现全流程管控，确保数据安全合规。

（三）协同建设与运行是保障

数据安全建设需组织、制度、文化和技术多方面协同。我行同步建设中，完善架构、明确责任、配备人员提供组织保障；完善制度、制定细则、建立机制确保有章可循；开展培训、营造氛围提升员工素养；部署工具并协同运行构建技术体系。各方面协同形成整体，提升防护能力，启示金融机构要注重协同，打破壁垒，整合资源形成合力。

（四）持续优化与创新是动力

数据安全形势变化，新风险不断出现。我行定期梳理评估制度，结合法规、业务和技术变化修订完善，保持有效性；技术上引入新工具方法，优化防护体系。启示金融机构要敏锐洞察新技术新趋势，持续优化管理体系，通过创新提升防护能力，应对动态变化的安全风险。

第十二节　南京银行 数据安全运营体系建设实践

一、背景介绍

（一）案例企业

南京银行成立于 1996 年，于 2007 年在沪市主板成功上市，是全国 20 家系统重要性银行之一，位列英国《银行家》杂志公布的全球 1000 家大银行第 86 位。成立 29 年来，始终坚守“做强做精做出特色，致力于打造国内一流的区域综合金融服务商”的战略愿景。

南京银行数字银行管理部成立于 2018 年，以数字力量持续推动南京银行“数字化转型”战略建设，强化数字赋能的同时，筑牢数据安全屏障，以“擦亮数字银行名片，成为一流的区域性数字化赋能标杆”为愿景。

（二）案例背景

随着数字经济成为推动当前经济整体增长的核心引擎，我们迎来了产业数字化与数字产业化融合变革的数字经济新时代。数据成为数字中国建设的关键与基本要素，起到了全国经济稳定器与缓冲器的作用。持续演进的大数据技术、云计算技术、AI 技术、区块链技术、IoT 技术等科技创新不断在商业银行业务领域落地生根，催生了不断深化交织的商业银行金融数据开发与共享利用的新局面。然而，数据的流动性远远高于其他传统要素，数据流动过程中无处不在的数据安全潜在问题，极大地制约了数据的有序共享与价值赋能，特别是关系国家安全问题的核心数据与重点数据安全，以及关系个人金融信息主体的隐私数据保护问题等。

为规范数据安全管理，国家相继出台了《中华人民共和国网络安全法》《中华人民共和国数据安全法》及《中华人民共和国个人信息保护法》等相关法律法规。在此框架下，国家金融监督管理总局、中国人民

银行以及全国金融标准化技术委员会等机构进一步发布了适用于金融行业的具体的数据安全相关标准，如《银行保险机构数据安全管理办法》《中国人民银行业务领域数据安全管理办法》《金融数据安全 数据安全分级指南》（JR/T 0197-2020）、《金融数据安全 数据生命周期安全规范》（JR/T 0223-2021）等。逐步建立和完善的数据安全监管体系表明，做好商业银行的数据安全工作对于维护商业银行客户的合法权益、推动国家数字经济健康发展具有重要意义。

基于上述背景，南京银行高度重视数据安全工作，统筹发展与安全，围绕五大板块日益旺盛的信息系统建设与迭代需求，面向信息系统建设数据安全运营体系，实现数据边界管控、数据安全定级、存量系统盘点、新建系统介入以及对外提供评估五大核心能力，为进一步推动全行“知重负重、担责尽责，以新发展理念推动南京银行高质量发展”贡献数据安全力量。

数据安全运营体系围绕五大核心能力展开：

· **数据边界管控：**为数据要素的流通提供办公与测试环境敏感数据的智能识别与管控能力，从而加大人为泄露行内敏感数据的难度，提升了全行数据要素流通的边界管控安全能力。

· **数据安全定级：**为各类用数场景提供数据项自动化打标能力，从而降低敏感数据的手工打标难度，提升数据安全资产维护效率。

· **存量系统盘点：**针对全行存量系统开展数据安全盘点，采用调研技术双驱动方式，为各类业务系统的数据安全水平提供有效的闭环验证能力。

· **新建系统介入：**将数据安全管控纳入全行新建系统的项目管理阶段，开展数据安全架构评审、数据安全测试，不断推进全行数据安全左移。

· **对外提供评估：**制定《南京银行数据对外提供安全管理办法》，构建数据对外安全评估、受托方数据安全监督检查等能力。

二、实施过程

（一）整体策略

近些年，国家及行业监管机构出台了覆盖数据生命周期安全规范、数据安全能力成熟度评估、个人信息安全影响评估等的相关标准，然而，相关标准有一个最大的共同特点就是通用性，至于各机构如何建设适合组织自身资源禀赋的数据安全运营体系，则需要各机构自行思考。

因此，我们首先需要选择适合组织自身资源禀赋的数据安全运营体系建设策略。关于数据安全运营体系建设策略选择的观点是分歧与共识并存的。共识在于数据安全运营体系建设的切入点就两个，面向信息系统建设或面向业务场景建设。分歧主要体现在一个组织究竟是走面向信息系统的数据安全运营体系建设策略，还是走面向业务场景的数据安全运营体系建设策略，这是最优先需要想清楚的问题。为了防止可能出现重复投入人力物力、开展多次业务场景对齐与技术能力评估却又无功而返的不利结果，考虑到可操作性、投入产出比等因素，我们建议城商行等中小金融机构在现阶段优先走面向信息系统的数据安全运营体

系建设道路。

（二）解决方案

数据安全运营体系具有五大核心能力，具体来看：

1.数据边界管控

建立覆盖生产、办公、测试三大环境的数据边界管控能力，赋能数据要素的对内使用与对外流通。针对生产到测试环境的数据流转，通过静态脱敏流程进行管控；针对测试到办公室环境的数据流转，通过文件上传下载审批流程进行管控；针对生产环境到办公环境的数据流转，通过数据提取审批流程进行管控。同时，我们对可能出现数据泄露的渠道，包括邮箱、安全 U 盘进行管控。邮箱方面，根据不同敏感词，设置了差异化的词频阈值限制策略，同时给予了白名单发件人、白名单收发件人组合等多种例外途径；安全 U 盘方面，设置敏感字段扫描及准出的管控策略。此外，我们对于办公终端、数据库中留存的敏感数据进行定期扫描，严格限制敏感数据的留存比例，进一步降低拍照、摘录等途径的数据外泄风险。

2.数据安全定级

建设基于算法的字段级分类分级智能打标系统，建立智能化的数据安全定级能力。分类分级既是数据安全运营体系的地基，也是全行数据安全管控措施落地的基础。在建立智能化的数据安全定级能力之前，数据安全定级工作主要依靠人工录入的方式进行手工打标，耗费非常高的人工成本，且定级质量难保证，引入智能打标系统后，可以实现数据字典的自动打标，高效打标数据项类型与级别，大幅降低手工打标成本。目前，该系统已在全行广泛推广应用，可有效支撑数据管控平台、数据开发平台等系统平台的数据安全定级工作。同时，平时注重积累自动打标与人工检核结果的差异数据作为补充训练数据，持续提升模型准确率。

3.存量系统盘点

设计存量系统盘点的调研问卷，建设数据安全测试环节，建立存量系统数据安全盘点的闭环验证能力。基于我行制定的 18 条数据安全管控基线，按照业务与技术分别制定了存量系统盘点的调研问卷，通过数据安全测试相关技术手段对调研结果进行闭环验证，并形成专业的数据安全测试报告，辅助各系统完成相关数据安全问题的整改。

4.新建系统介入

在信息系统建设的 7 个阶段纳入数据安全管控重点事项，介入项目管理的立项阶段、需求阶段、架构设计阶段、设计阶段、非功能测试阶段、投产阶段与验收阶段。立项阶段主要在项目业务可行性分析报告与项目技术可行性分析报告中做好风险提示；需求阶段通过情景式平台智能生成软件需求说明书的数据安全需求部分；架构设计阶段迭代设计了多版的数据安全评审项清单；设计阶段通过情景式平台智能映射需求，完成设计分析；非功能测试阶段启用全新的数据安全测试环节，验证上线评审系统的数据安全基线满足情况；投产阶段，将数据安全管控纳入上线评审流程；验收阶段，增设了新建系统的数据安全后评价指标。

5.对外提供评估

设计数据对外提供安全评估表与受托方数据安全监督检查表，建立业务数据对外提供的数据安全评估能力与受托方监督检查能力。全行的数据对外提供安全管理严格遵循“谁提供，谁负责”的原则，对委托处理、数据外部共享等数据对外提供的情形进行数据安全管控，包括对数据对外提供的目的、传输方式、数据范围、敏感数据类型与等级、数据规模、留存时间的合理分析，以及对数据接收方数据安全资质、涉及的数据生命周期环节、对应的数据安全保护措施，业务处理目的实现后的数据处置方式等的全面评估。

三、成果与效益

通过建设企业级数据安全运营体系，南京银行破解数据要素的“粗放流动、低效定级、局部防护”等数据安全难题，实现数据安全“边界守护、智能定级、整体覆盖”，支撑全行海量数据的安全使用。具体来看：

第一，从粗放流动到边界守护。过去各业务系统按照自己制定的非标准化的、较为粗放的规则管理自身数据要素的流动安全，通过建设数据安全运营体系，实现跨生产、办公、测试、外部多域的标准化与精细化管控，打造涉及数据对外提供应用的数据安全评估与受托方监督检查能力。

第二，从低效定级到智能定级。过去的数据安全定级主要是针对数据项开展人员手工定级，依赖专业人员对定级标准与行内制度的熟悉程度，打标效率较低，通过企业级数据安全运营体系，以算法为中心，覆盖各业务系统，实现各系统数据字典相关数据项的自动化智能定级。

第三，从局部防护到整体覆盖。过去各业务系统的安全能力主要依赖零星的数据安全合规要求，例如禁用弱密码等较为基础的局部防护措施，通过建设数据安全运营体系，将数据安全需求、数据安全架构评审、数据安全设计、数据安全测试等作为独立模块驱动全行新建与存量业务系统数据安全保护能力的提升，起到与网络安全、消费者权益保护协同发展的作用。

数据安全运营体系为南京银行带来如下价值：

第一，成效显著。南京银行数据安全运营体系有效落实监管政策制度要求，支撑全行业务数据要素的安全有序发展，实现数据安全管理能力质效双增。

第二，全面覆盖。南京银行数据安全运营体系覆盖总分行各级机构的全面管控，包括数据安全定级、新建系统介入、存量系统盘点、对外提供评估等。

第三，周期贯穿。南京银行数据安全运营体系覆盖数据全生命周期，体系闭环，并且通过了 DCMM 四级认证，具备较强的领先性。

四、经验与启示

在数据安全运营体系建设过程中，南京银行总结如下实践经验：

第一，明确数据安全运营体系建设目标，与同业及咨询机构进行充分的沟通和交流，深入调研全行的数据安全现状，挖掘全行数据安全痛点，形成数据安全现状评估报告，综合选取适合我行自身资源禀赋的

建设策略。

第二，不断推动全行信息系统建设的数据安全管控左移，智能适配各类业务场景与数据安全保护需求，降低全行数据安全运营体系落地的整体建设成本。

第三，以实际问题为导向，依托 PDCA 循环，形成数据安全运营体系迭代演进路径，将数据安全运营与用数场景深度融合，加强数据安全风险的管控能力。

后续，南京银行数据安全运营体系进一步向三个方向提升：第一，重点建设统一的数据安全定级体系，综合数据项、信息系统与操作人员的多维定级，为数据安全运营体系的安全监测提供有力支撑。第二，重点提升智能化数据安全运营能力，多技术融合提升数据安全运营效率。同时，开展模型评估以保障数据要素在 AI 应用中的有序安全赋能，保障训练过程合规，模型部署安全，提升算法可解释性。第三，重点提升集团联防化能力，加强与集团子公司的走访交流、威胁情报共享、数据安全风险评估及认证项目共建，建设全集团的数据安全联防联控机制，实现数据安全运营管理的降本增效。

第十三节　四川银行 数据分类分级实践

一、背景介绍

随着金融科技的深度应用及新一代系统工程投产，四川银行数据资产规模呈指数级增长。数据类型涵盖结构化数据、半结构化数据、非结构化数据，其中包含大量涉及客户隐私、资金安全的敏感信息。在数据规模快速扩张的同时，数据安全管理面临双重核心挑战：

（一）合规压力持续升级

近年来，《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》《银行保险机构数据安全管理办法》《中国人民银行业务数据管理办法》等法律法规密集出台，对金融机构数据分类分级提出明确要求。国家金融监督管理总局四川监管局在 2024 年专项检查中强调，“银行业金融机构需建立与业务匹配的数据分级标准，对客户敏感信息实施差异化保护”。四川银行作为省级法人银行，亟需加快推进数据安全分类分级建设工作。

（二）传统管理模式效率低下

一是人工分类分级模式存在明显短板，单系统数据梳理需业务人员与数据安全管理人员联合操作 5～10 天。二是人工判定依赖个人经验，抽查显示敏感数据“漏判率”达 45%、“误判率”达 55%，例如将“客户联系电话”误定为 2 级（内部数据），可能导致非授权人员可查询，引发客户投诉。

为破解上述困境，四川银行于 2024 年 3 月启动“新一代数据安全管理平台建设项目”，通过引入智能化工具、重构管理流程，实现数据安全与业务发展的协同增效。计划将漏判率、误判率降低至 5%以下。

二、实施过程

（一）基础体系搭建：构建“组织－标准－工具”三位一体框架

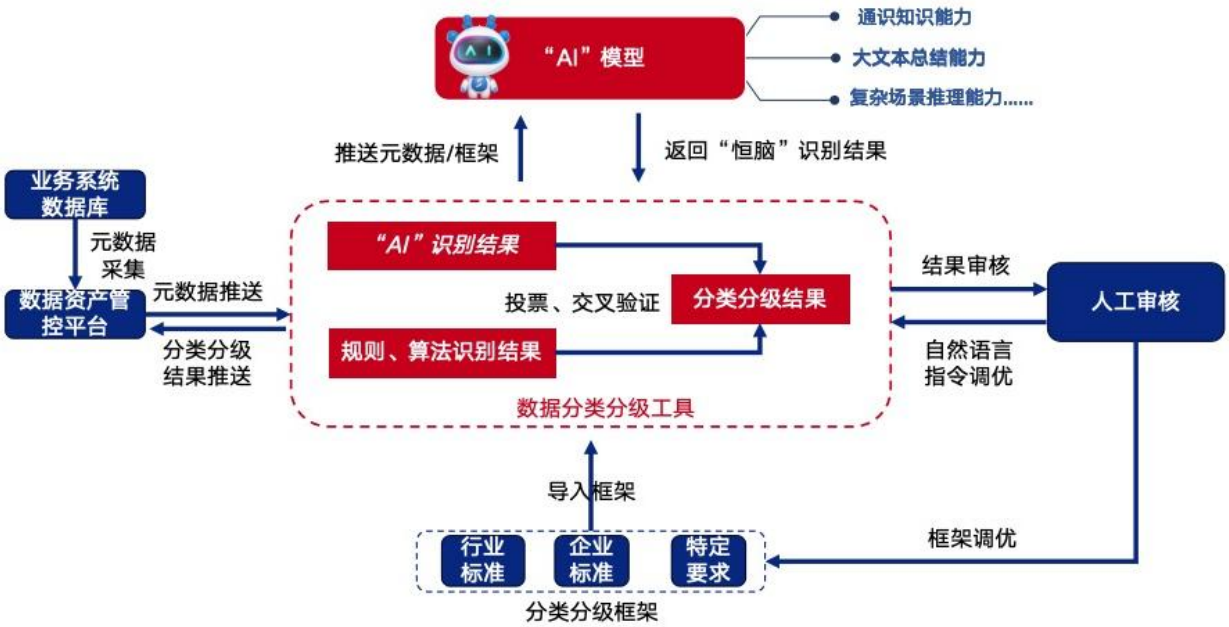
一是明确数据安全组织架构与责任机制。建立了覆盖党委、董事会、高级管理层、数据安全主责部门归口管理、各业务部门配合的组织架构，明确岗位职责和工作机制。

二是制定并发布分类分级标准。根据《银行保险机构数据安全管理办法》要求，结合《GB/T43697—2024 数据安全技术数据分类分级规则》《JR/T0197 金融数据安全数据安全分类分级指南》，制定《四川银行数据分类分级标准》。将数据划分为核心数据、重要数据、一般数据三个等级。

三是选择具备适配银行业数据分类分级实践的 AI 分类分级工具，核心功能包括：内置金融业预训练模型、可部署于私有云，符合金融数据“不出行”要求、支持信创环境部署、支持通过 API 接口对接数据资产管控平台获取各业务系统元数据，实现数据自动采集。

（二）核心实施：AI 驱动“全流程自动化+人工精准校准”

基于数据管控平台、分类分级工具、AI 模型构建自动化分类分级工作流程、动态管理流程，实现全行数据分类分级管理。



图表 16 AI 分类分级流程

1.数据资产全景梳理

构建数据资产管控平台作为核心枢纽，实现全生命周期的元数据管理：

（1）元数据自动化采集与质量管控

平台整合多源数据采集能力，通过数据库直连、日志解析等方式，自动抓取核心系统、信贷系统、手

机银行等 30 余个业务平台的元数据。

（2）数据分类分级工具联动机制

数据分类分级工具通过 API 接口与数据资产管控平台实时对接，T+1 同步全量元数据，确保工具处理的元数据与业务系统保持一致。

2.智能分级与人工校验

构建“AI 自动判定－人工精准校准－模型持续优化”的闭环体系：

（1）AI 模型智能分级

基于银行业预训练模型，AI 模型通过匹配“业务域+数据类型+影响范围+危害程度”四维特征，自动完成元数据分级。例如：识别“客户身份证号”匹配“客户－个人－个人自然信息－个人基本概况信息”，判定为 3 级；识别“企业营业执照编号”匹配“客户－单位－单位基本信息－单位基本概况”，判定为 1 级。

（2）人工审核与自然语言指令优化

按 20%～30%比例抽样审核，重点覆盖 3 级、4 级数据及 AI 判定模糊的“灰度数据”，如“某区域客户群体消费偏好”，通过系统界面标记偏差项并录入自然语言指令。

分类分级工具将自然语言指令转换为结构化规则，补充至模型训练样本，使 AI 对特殊场景的识别准确率从初始的 80%持续提升至 92%。

3.动态更新机制建立

实现元数据分级的“实时感知、自动调整、全程可溯”：

（1）元数据变更同步

数据资产管控平台实时监测业务系统的元数据变化，每天向分类分级工具推送变更清单，确保工具处理的元数据与业务实际同步。

（2）分级动态调整

分类分级工具接收变更清单后，自动触发重新分级流程：对新增字段直接调用 AI 模型判定；对修改字段重新匹配分级规则，更新等级结果。

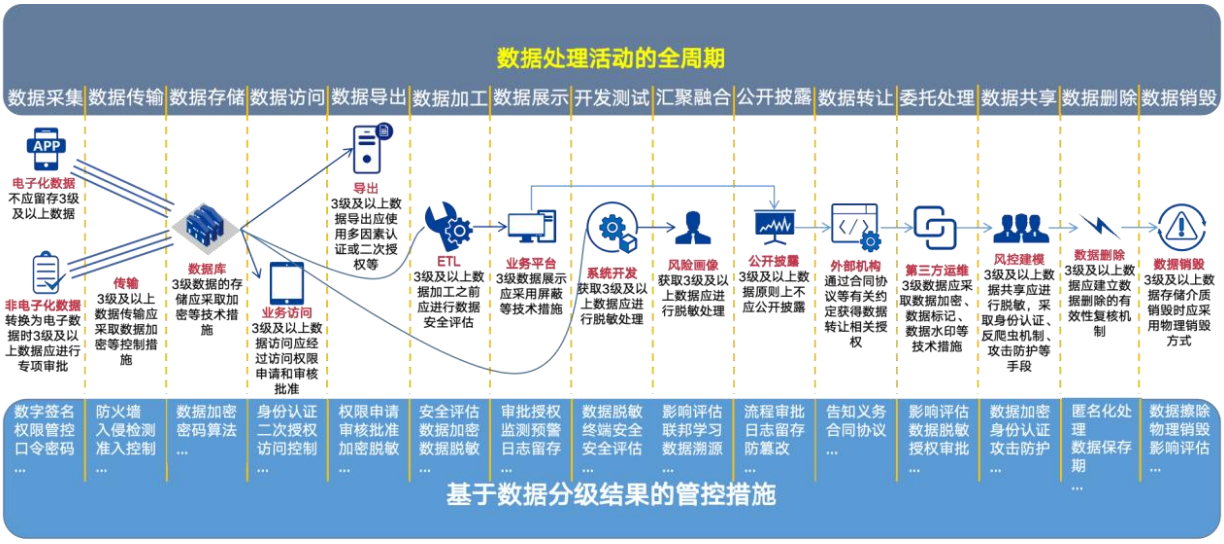
（3）全流程追溯

所有元数据变更记录实时存入审计日志系统，支持监管检查时一键导出，满足“可追溯、可验证”要求。

通过上述流程优化，四川银行实现了数据分类分级从“静态管理”向“动态智能”的升级，既满足《中华人民共和国数据安全法》等法规要求，又为精准营销、风险防控等业务场景提供了安全高效的数据支撑。

（三）落地应用：分级管控与业务场景深度融合

根据数据级别实施“精准防护”，避免“一刀切”式管控：



图表 17 分级结果管控措施

三、成果与效益

一是分类分级风险降低：敏感数据“漏判率”从 45%降低到 2%、“误判率”从 55%降低到 5%。

二是时间成本降低：单系统数据分类分级完成时间从 5～10 天压缩至 1 天，效率提升 80%～90%；动态更新响应时间从人工处理的 3 天缩短至 2 小时。

三是人力成本节约：此前需 10 人团队专职负责分类分级，现仅需 2 人，其中 1 名技术人员维护工具和 1 名业务人员审核结果。

四、经验与启示

（一）关键经验

1.坚持“业务驱动”而非“技术驱动”

分类分级的核心是服务业务发展，而非单纯满足技术指标。始终以“解决业务痛点”为导向：例如针对“小微企业贷款数据”，不仅考虑安全要求，还结合业务部门“快速审批”需求，将非核心字段从 3 级降至 1 级，减少审批环节，同时确保核心字段严格管控。

2.AI 与人工协同是效率与精准的平衡

AI 工具解决“量大、重复”的基础工作，但无法替代业务人员对“灰度数据”的判断。建议保持 20%～30%的人工抽样率，尤其对新业务、新场景数据，需业务人员深度参与。

（二）行业启示

1.中小银行可采用“分步实施”策略

无需一次性投入全量系统，可先聚焦存储重要数据的系统进行试点工作，待流程成熟后再逐步扩展至全业务领域。

2.数据治理基础决定分类分级效果

分类分级依赖规范的元数据管理，建议提前开展数据标准工作，完善数据字典，否则 AI 工具可能因“字段名混乱”导致识别错误。

四川银行的实践表明，数据分类分级不是简单的“安全工程”，而是“合规+安全+业务”的协同体系。通过 AI 技术赋能，不仅能高效满足监管要求，更能释放数据价值，为银行业数字化转型提供安全支撑。

（三）未来展望

未来，四川银行将进一步提升数据安全管理水平。一是以新一代数据安全管理平台为核心，以数据分类分级为基础，联动数据库审计、终端 DLP、邮件 DLP、静态脱敏组件、UEBA 组件，构建全流程闭环管理体系，实现从被动响应到主动预警的转变。二是优化 AI 模型对非结构化数据的处理能力，探索分类分级与数据资产估值的结合，让数据真正成为银行的核心竞争力。三是提升 AI 模型下的人机协作能力，形成“机器效率+专家经验”的协同闭环。最终构建“智能、合规、敏捷”的下一代数据安全治理体系，为数字化转型提供核心支撑。

第十四节　稠州银行 外部数据平台安全合规实践

一、背景介绍

近年来，随着金融科技的快速发展，基于贷前风控评分、贷后管理、交易反欺诈等风控场景，以及精准营销、营销策略优化、客户行为风险分析等银行业务对外部数据的迫切需求，银行机构越来越多地依赖外部数据来提升服务质量和风险管理能力，同时，外部数据的使用也面临数据安全和合规性多方面的新挑战。我行于 2017 年开始外部数据管理平台建设，在实施外部数据整合和应用的过程中，存在数据来源多样、数据传输复杂、数据存储不安全等问题，这些问题不仅影响了银行自身的运营效率，还可能导致客户信息泄露等重大风险，2022 年升级为新一代外部数据管理平台，旨在建立一套“统一管理、高效接入、便捷共享、安全使用、有效监控、合法合规”外部数据管理平台，用于统筹外部数据需求、安全评估、收集引入、数据运维等多项外部数据管理工作。在后续的外部数据管理工作中，2025 年依据金融监管总局最新的《银行保险机构数据安全管理办法》第五十三条关于外部数据交互安全以及其他外部数据采购、数据收集、数据传输、数据存储、数据访问、数据备份、数据使用、数据风险监测、应急响应机制等多项条款的管理要求，全面提升了外部数据的安全合规水平。

二、实施过程

（一）平台建设情况

外部数据管理平台致力于为我行打造稳定高效的底层数据指标服务架构和面向上层业务的数据指标

应用解决方案，能够为智能决策引擎及各业务系统提供强大的数据指标支撑，满足对内外部多源数据的多样化、差异化管理需求，既是实现内部数据资源共享和信息系统协同发展的基础，也是外部数据接入、整合和输出的管控中心。

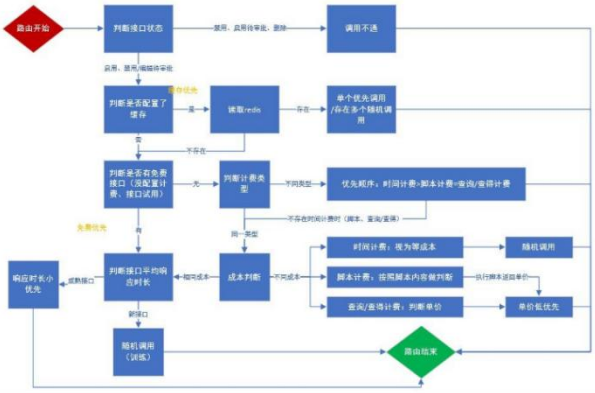
平台提供对数据源的快速接入、接口可视化配置、内外部调用计费、数据融合与衍生、异常监控告警和可视化报表等全流程的数据调用管理；可在前端界面实现数据源接口的直接配置，支持在线测试接口调用，并对指标进行版本管理，跟踪并记录变更历史，支持数据源和指标版本的热切换；平台支持上传脚本或通过内置常见衍生规则在线加工数据，存储原始和衍生数据，沉淀为标准规范的数据资产供其他系统调用，提供强大的数据内部共享能力和大数据差异化实时分析能力，能够实现数据的集中调度与规范化输出。满足办法第五十三条通过集中管理的外联平台或者应用程序接口实施与第三方数据合作的要求，依据“业务必需、最小权限”原则，对接口设计、开发、服务、运行等进行集中安全保护管理。

图表 18 平台管理页面

图表 19 平台数据流程图一

图表 20 平台数据流程图二

图表 21 平台数据流程图三



图表 22 平台数据流程图四

（二）外数合规管理

根据国家金融监督管理总局发布的《银行保险机构数据安全管理办法》，我行结合自身的业务特点，制定了一套详尽的外部数据安全合规政策及操作指南。这些政策全面涵盖了外部数据管理平台中数据从收集、传输、存储、使用到最终销毁的整个生命周期管理过程，清晰地定义了各部门的具体职责和详细的操作流程，从而确保对外部数据实行严格且系统的全生命周期管理。提升了数据安全管理方面的专业水平，预防潜在风险，确保业务的稳健运行。

1.数据来源：

落实办法第二十六条外部数据采购的要求，建立外部数据采购和合作引入机制，对外部数据多个供应商的综合情况进行调研，包括背景、业务资质、信誉等，并询价，筛选拥有个人与企业征信持牌机构的主流数据源，评估数据提供者的安全保障能力及其数据安全风险，通过签订保密协议和数据使用协议，明确双方数据安全责任及义务，对数据来源的真实性和合法性进行调查，明确签约数据项、数据使用授权限制、数据保护措施、数据安全事件通知、合规性与法律义务、终止条款等要求。每年行内需进行供应商综合评估打分，涉及业务使用部门，采购部门与数字金融部门等。

2.数据收集：

按照办法第二十四条，坚持“合法、正当、必要、诚信”原则，明确数据收集和处理的目的、方式、范围、规则、数据来源可追溯。在数据采集过程中，采用数据撞库，对数据进行匹配和验证，匿名化、去标识化处理，保障收集过程的数据安全性。数据联合建模作为一种创新的数据处理方法，能够有效解决数据隐私保护和数据多样性之间的矛盾，采集过程中，我行通过联邦学习、隐私计算等，利用来自不同机构的数据，增加了外部数据的多样性和丰富性，提高了泛化能力。

3.数据传输：

办法第四十四条要求，银行保险机构敏感级及以上数据传输应当采用安全的传输方式，保障数据完整性、保密性、可用性。在数据传输方面，平台通过多项技术支持，确保数据传输过程中的安全。

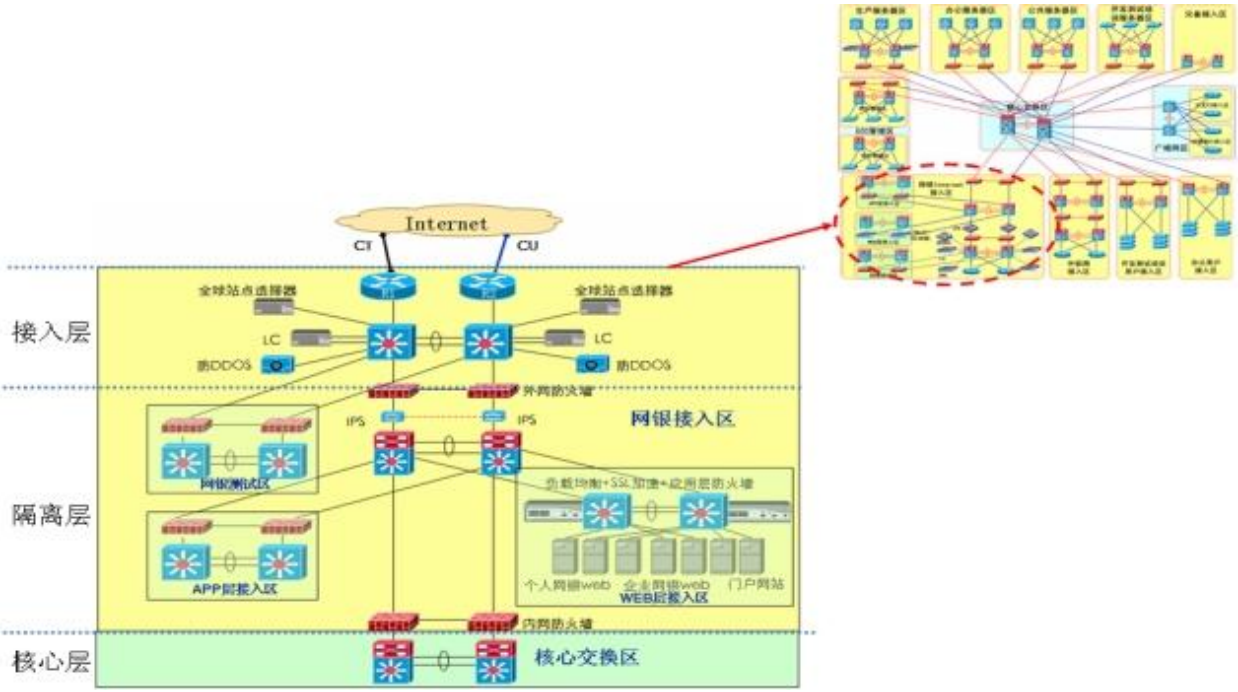
数据加密：传输过程中，与第三方数据源数据交互中，对敏感数据进行加密处理，确保数据在传输过程中的安全性，只有经过授权的用户才能解密数据并访问其原始内容。

数据校验：使用校验码（如 SM3、MD5）确保数据在传输过程中的完整性。

数字签名：使用数字签名技术，确保数据的完整性和真实性。

网络安全防护：加强网络边界防护，部署防火墙、入侵检测系统等网络安全设备，防止外部攻击者通过网络途径获取敏感数据。入侵检测与防御：部署入侵检测系统（IDS）和入侵防御系统（IPS），监控和防御潜在攻击。网银区网络分为接入层、隔离层和核心层。接入层通过两台接入路由器接入不同运营商的 Internet 线路，在接入层部署链路负载均衡和全局负载均衡及防 DDOS 设备，实现不同运营商线路、多数据中心访问网银数据流的负载分担和本地防 DDOS 攻击。网银测试区上联到接入层交换机，提供网银测试服务器的接入。通过双层防火墙异构形成隔离层，隔离层内部的 DMZ 核心交换机下联了 WEB 层接入区和 APP 层接入区。WEB 层接入区接入网银和门户网站 WEB 前置服务器，APP 层接入区接入应用服务器。在

WEB 层接入区部署服务器负载均衡设备、SSL 加速设备和应用层防火墙，提升 WEB 接入性能和网银 WEB 访问的安全性。



图表 23 网络安全防护示意

4.数据存储：

静态数据加密是保护数据隐私和安全的重要手段之一。采用合适的加密技术和最佳实践，可以有效降低数据泄露风险，确保数据在存储状态下的安全。同时，良好的密钥管理和加密策略也是保证加密效果的关键。平台在数据存储时采用 MySQL 数据库静态加密，保护数据安全。满足办法第四十五条的要求，即采取安全存储措施存储数据，数据不得明文存储。

5.数据使用：

在数据使用方面，根据办法第四十三条对数据访问和第二十八条对数据使用的要求，按照“业务必要授权”原则，建立了严格的访问控制系统，制定用户对数据的访问策略，通过身份验证、权限管理和日志审计等手段，进行有效的用户认证、授权管理、行为审计，确保只有授权人员能够访问敏感数据，规范操作行为。按照第三十七条数据备份要求，定期备份数据，以便能够在发生故障时快速恢复平台使用。我行注重用户隐私保护，合规使用用户数据，依据办法中关于个人信息保护的处理原则和告知义务，数据经过客户授权，遵循“合法、正当、必要”原则，履行明确告知义务，尊重用户选择，保护用户隐私。

外部数据分类与标签化：对外部数据进行了详细的分类和标签化管理，区分了不同级别的敏感数据，并根据数据级别设置了不同的访问权限和存储策略。这有助于更精细化地管理和保护数据，避免不必要的风险暴露。

6.数据运维与监控：

定期对外部数据的使用和管理进行审计，确保所有操作符合既定的合规政策和技术标准。办法第六十五条规定，银行保险机构应当对数据安全威胁进行有效监测，实施监督检查。平台建立了内部监督机制，通过不定期抽查和检查，发现并纠正存在的问题。

利用大数据分析技术实时监控数据访问行为，识别异常活动，预防数据泄露。此外，还采用了自动检测和预警潜在的数据安全风险，当第三方数据源出现异常，会第一时间发出预警，通知对应的业务管理部门和技术管理部门，并要求及时处理预警内容，保证生产业务连续性。

（三）外部数据安全应急响应机制

办法第六十八条要求，银行保险机构应当建立数据安全事件应急管理机制。我行构建了一套完整的数据安全事件应急响应流程，一旦发现数据泄露或其他安全事件，能够迅速启动应急预案，采取隔离措施，调查原因，评估影响，修复漏洞，并向相关监管机构报告。通过这种方式，最大限度地减少了安全事件的影响。每年外部数据管理平台将进行一次应急演练，确保所有软硬件和插件均能应急事件处理。

三、成果与效益

外部数据管理平台用于完成全行外部数据的对接工作，年度客户工商数据风铃订阅超过 50 万笔数据预警。外部数据管理平台日常生产运营近 20 家供应商数据源的 100+数据服务，年度超过 3000 万次调用量，为业务部门提供高效稳定的数据服务，保障生产平稳高效运行，助力我行重点产品的顺利投产和应用。通过该平台的建设，实现外部数据管理平台最佳解决方案，建设了一套集统一管理、高效接入、便捷共享、安全使用、智能路由、价值深挖为一体的外部数据管理平台。为银行提供数据开放共享能力和数据分析能力，实现面向服务的综合管理平台，致力于为银行打造稳定底层数据服务架构和面向上层业务的数据解决方案，并为全行风控系统提供必要的数据支持。

平台投入使用后，外部数据相关数据安全合规水平得到了显著提升：

1.数据安全风险降低：数据安全风险降低了 30%，减少了因数据泄露导致的经济损失和声誉损害。

2.供应商合规性提升：合规评分从 80 分提升到了 95 分，达到了行业领先水平，获得了监管部门的认可。

3.业务运营效率提高：业务运营效率提高了 15%，通过自动化工具和流程优化，减少了人工错误和重复工作，提升了整体工作效率。

4.客户满意度提升：客户满意度提升了 10 个百分点，客户对银行的数据安全和隐私保护更加信任，增强了客户黏性。

四、经验与启示

（一）持续监测与改进

数据安全环境不断变化，需要持续监测新的威胁，并及时调整安全策略和技术手段。定期的风险评估和安全审计是必不可少的，可以帮助机构及时发现和解决潜在的安全隐患。

（二）全员参与

数据安全不仅仅是信息科技部门的责任，而是所有员工的义务。定期组织全体员工参加数据安全和合规培训，特别是涉及外部数据管理的相关岗位，确保每位员工都了解并遵守相关规定。培训内容包括数据安全法律法规、数据处理流程、安全工具使用等，提高员工的整体数据安全意识。

（三）强化合作

与其他机构分享成功经验和最佳实践，不仅可以互相学习，还可以共同面对数据安全领域的挑战，提升整个行业的数据安全水平。此外，与外部数据提供商建立长期稳定的合作关系，也是保障数据安全的重要一环。

（四）细化数据管理

对外部数据进行分类和标签化管理，设置不同的访问权限和存储策略，有助于更精细化地管理和保护数据，避免不必要的风险暴露。这不仅能提高数据安全性，还能优化数据使用效率。

将数据安全建设融入外部数据平台系统建设的各个环节，不仅有效地提升了外部数据建设中的数据安全合规水平，也为平台后续的外部数据服务提供了坚实的合规保障。通过在设计、开发、测试和运维等各个阶段实施严格的数据安全策略，确保了平台数据在整个生命周期中的保密性、完整性和可用性。未来，我行将继续深化数据安全合规建设，致力于打造一个更加完善、可靠的数据安全生态系统，进一步探索新兴技术的应用，如人工智能、区块链等，以提高数据加密和防篡改的能力，通过持续的技术创新，保持数据安全和合规性始终处于行业前沿，为客户提供更高效、更安全的服务体验。

第四章　保险机构数据安全合规落地实践案例

第十五节　太平洋保险集团 数据分类分级落地实践

一、背景介绍

（一）公司基本情况

中国太平洋保险集团（以下简称“中国太保”）作为行业领先的综合性保险集团，业务涵盖人寿保险、财产保险、养老保险、健康保险、农业保险及资产管理等多个领域，拥有庞大的客户群体和海量的数据资源。随着数字化转型的加速推进，数据作为新型生产要素，已成为推动社会进步与经济发展的核心驱动力。数据成为太保集团的核心资产之一，对数据的有效管理和安全保护成为公司持续发展的关键。2024 年 9 月，中国太保获得 DCMM 最高等级 5 级认证，成为国内首家通过 DCMM 5 级认证的保险集团。

（二）面临的数据安全挑战与问题

1.技术层面：数据识别与分类难度大。数据来源广、格式多样，结构化、半结构化与非结构化数据特征各异，准确识别需复杂技术。同时，分类分级标准难以精准确定，不同业务对数据敏感度不同，标准制定需兼顾多样性与动态性，而数据重要性随时间、业务和法规变化，要求标准及时更新。此外，技术工具集成与兼容性差，企业系统多样，实现无缝集成和兼容复杂，数据流通时保持分类分级信息准确也面临挑战。

2.管理层面：业务部门重利用效率，安全部门重安全合规，专业差异易导致沟通协同方面产生问题。另外，公司内部数据要素的流通与共享存在壁垒，数据如何在确保安全可控的前提下，充分发挥数据价值，支持业务的发展、融合和创新，是保险业数据分类分级保护面临的难题。

3.外部层面：法律法规和监管要求不断变化，数据的安全等级并非一成不变，需要根据数据的业务属性、重要程度、精度、覆盖程度、可能造成的危害及程度等因素的变化进行动态调整，才能确保数据安全等级的有效性。同时，新技术发展带来挑战，网络安全威胁增加，数据分类分级需考虑安全防护，确保数据安全保密。

二、实施过程

（一）建立数据安全管理体系

1.组织架构：公司建立数据安全责任制，集团总部和各成员机构的党组织、董事会对本机构数据安全工作负主体责任。集团总部和各成员机构的主要负责人为数据安全和个人信息保护第一责任人，分管数据安全的领导为直接责任人。公司数据安全管理遵循集团一体化管控模式和成员机构分级分类管理要求，逐级落实数据安全管理责任。同时，明确各部门在数据安全管理中的职责，按照“谁管业务、谁管业务数据、谁管数据安全”的原则，落实数据安全保护管理要求。

2.制度建设：依据国家法律法规和监管要求，公司制定并持续完善了一系列数据安全管理制度，如《集团数据安全管理办法》《集团数据安全分类分级实施细则》《集团数据防泄漏管理办法》《集团数据安全评估实施方案》等。这些制度明确了数据采集、存储、使用、传输、销毁等全生命周期的安全管理要求，为数据安全流通、高效利用奠定基础。同时，公司将数据安全纳入全面风险管理体系、内控评价体系，定期开展审计、监督检查与评价，督促问题整改和开展问责。

3.安全策略制定：太保集团围绕数据全生命周期的各个环节，制定并实施全方位的数据安全防护策略，确保数据在采集、存储、处理、传输和销毁等生命周期的各个阶段都能得到充分保护。同时，公司通过平台对数据安全授权进行科学合理的管控，实现了系统上的有效权限管理，确保了数据访问的合法性和合规性。

（二）数据分类分级实践

根据《银行保险机构数据安全管理办法》管理要求，公司数据类别分为客户数据、业务数据、经营管理数据、系统运行和安全管理数据四大类。依据数据的重要性和敏感程度，公司将数据分为核心数据、重要数据、一般数据。其中，一般数据细分为敏感数据和其他一般数据。

图表 1 集团数据分类分级目录示例

1.数据分类分级标准制定：结合监管要求和公司业务特点，制定《太保集团数据分类分级标准目录》，涵盖近 500 个保险数据分类分级标准，将数据分为不同的类别和级别，并针对不同级别的数据，推动落实差异化的数据安全保护措施。

2.智能化分类分级工具研发：太保集团自主研发数据安全分类分级自动化工具，该工具能够适配多类型数据库，实现全域系统两百余万字段的分级分类落地与管控。通过智能化手段，将原本单个系统需要 15 人天的工作量减少到 1 人天，大大降低了落地门槛。

3.全流程安全管理：基于数据分类分级结果，太保集团建立了全生命周期的安全管控体系。在数据收

集环节，遵循合法、正当、最小必要原则，明确告知客户数据收集的目的和范围；在数据存储环节，对敏感数据进行加密存储，并采取严格的访问控制措施；在数据使用环节，赋予用户最小操作权限，确保数据使用合规。

（三）技术创新与管理策略

1.技术手段应用：太保集团采用了多种技术手段保障数据安全，如 TLS 加密传输技术、数据防泄漏系统、堡垒机等。同时，通过建设“数据分发管理平台”“数据保护伞”“网络安全险风控护航平台”，显著提升了整体数据安全水平，坚守住了数据安全的底线。

2.数据要素流通体系构建：太保集团创新建立司内数据要素流通体系，明确数据流通的规则、流程和安全措施，打破内部数据壁垒。通过明确的数据分类分级，为数据要素的安全流通提供了规范依据，合理推进数据的共享分析，充分发挥数据价值，支持业务的发展、融合和创新。

3.自研集团智能化统一数据治理平台：集团统一数据治理平台，作为数据分类分级实施落地的核心技术载体，支持全集团各类系统字段级别的数据分类分级的管理、审核及发布等闭环管理，主要功能包括：

（1）数据分类分级参考管理、分类分级标注管理、分类分级标注审批；

（2）通过智能化工具，实现数据分类分级智能标注、自动检核数据分类分级标注问题等，提升分类分级标注效率和准确度；

（3）数据分类分级管理报表。

三、成果与效益

（一）数据安全风险降低

通过数据分类分级和全生命周期安全管控，太保集团对高敏感度数据进行重点保护，有效防范了数据泄露、篡改等安全风险。

（二）数据合规性提升

太保集团严格落实监管总局《银行保险机构数据安全管理办法》和相关法规要求进行数据分类分级，确保了公司的数据管理活动符合合规要求。

（三）业务运营效率提高

智能化分类分级工具的应用，使得数据管理的工作效率大幅提升，单个系统的工作量减少了 90%以上。同时，数据的安全流通为业务创新提供了有力支持，如科技赋能保险扩大行业保障范围，实现了风险减量。

（四）客户满意度提升

太保集团通过数据安全管理，保障了客户的个人信息安全，提升了客户对公司的信任度。同时，通过

科技赋能，为客户提供个性化健康管理等服务，进一步提升了客户满意度。

四、经验与启示

（一）重视数据安全管理体系建设

数据安全管理需要从组织架构、制度建设、技术手段等多方面入手，形成完整的管理体系。太保集团的成功实践表明，明确的职责分工和完善的管理制度是数据安全管理的基础。

（二）智能化工具是提升效率的关键

在数据分类分级工作中，数据量大、复杂度高是普遍存在的问题。太保集团通过自主研发智能化分类分级工具，实现了自动化、高效化的数据管理。这不仅大大减少了人力成本，还提高了分类分级的准确性和一致性。其他机构可以借鉴这种通过技术手段解决复杂问题的思路，积极引入或研发适合自身业务的智能化工具，提升数据管理效率。

（三）全流程安全管理的重要性

数据安全不仅仅是存储和传输环节的安全，而是贯穿数据全生命周期的安全。太保集团在数据采集、存储、使用、共享、销毁等各个环节都制定了严格的安全管理措施，并通过制度和技术手段加以落实。

（四）数据分类分级与业务发展的协同

数据分类分级工作不能脱离业务需求，而应与业务发展紧密结合。太保集团在数据分类分级过程中，注重与业务部门的需求相结合，通过建立数据要素流通体系，打破了数据壁垒，促进了不同级别的数据在公司各部门的安全流通和共享，为业务创新提供了有力支持。

（五）持续改进与创新的必要性

数据安全是一个动态的、不断发展的领域，随着技术的进步和业务的变化，数据安全面临的挑战也在不断变化。太保集团在数据分类分级工作中，及时关注行业动态和监管要求的变化，始终坚持持续改进和创新的理念，建立数据分类分级动态调整机制，不断优化分类分级标准、技术手段和管理流程。

（六）重视数据安全文化建设

数据安全管理不仅仅是技术部门的工作，而是需要全员参与的系统工程。太保集团通过开展数据安全培训、宣传活动等方式，提升了全体员工的数据安全意识，营造了良好的数据安全文化氛围。这种数据安全文化为数据分类分级工作的顺利实施提供了有力支持。

（七）与监管要求紧密结合

太保集团在数据分类分级工作中，以《银行保险机构数据安全管理办法》等监管要求为指引，确保了数据安全管理的合规性。同时，公司应积极参与行业标准的制定和推广，为整个行业的数据安全合规水平提升贡献力量。

五、总结

太保集团的数据分类分级落地实践是金融机构在数据安全管理领域的一次成功探索。通过建立完善的数据安全管理体系、研发智能化工具、实施全流程安全管理、推动数据要素流通等措施，太保集团在提升数据安全管理水平的同时，也为金融业数据安全管理提供了可复制的实践范本。

未来，随着技术的不断进步和业务的持续创新，金融机构的数据安全管理将面临更多的挑战和机遇。太保集团将继续秉持创新、协同、合规的理念，不断优化数据分类分级工作，为行业的数据安全合规水平提升贡献更多力量，同时也为自身的高质量发展筑牢数据安全根基。

第十六节　中国人民保险集团 智能化数据安全运营平台建设

一、背景介绍

中国人民保险集团（以下简称“集团”）旗下拥有 10 多家专业子公司，业务范围覆盖财产险、人身险、再保险、资产管理、不动产投资和另类投资、金融科技等领域。近年来，伴随集团业务发展，系统数量迅速增长，接口与数据表数量呈现迅猛增长趋势。

近年来，在总体国家安全观的指引下，国家网络安全领域法制建设日趋完善，陆续颁布了《中华人民共和国网络安全法》《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》三部基本法，使数据拥有“价值”属性之外，也具备了“法律”属性。随着数据安全法制的完善，监管实践也在有序推进，针对危害网络运行安全、不履行数据安全保护义务、侵犯客户数据安全行为重拳出击，数据安全已正式迈入强监管时代。作为大型国有保险集团，业务运营、系统建设过程中涉及到大量的重要敏感数据，如客户个人信息、保险合同信息、理赔信息、健康医疗信息等。这些数据一旦泄露或被攻击，将会给客户和企业带来极大的损失和影响。

当前集团内各公司存在数据资产规模庞大、资产底数不清、应用场景复杂、资产安全保护需求不明的情况，在数据安全技术体系方面仅是通过分散在各数据中心零散的数据库审计、数据脱敏、数据加密API检测工具实施安全保护，各类工具数据无法关联融合，形成“信息孤岛”，难以全面地实现数据安全风险的监测、预警与处置，亟需建设一套“数据安全集中监测和管控、统一运营”的“数据安全综合管理平台”，通过采集数据安全监控防护数据，利用大数据分析、威胁建模等技术，及时洞察数据生命周期各阶段的安全风险，形成监测预警和处置闭环的运营机制，提升集团数据安全风险管理水平。

在此背景下，本案例通过建设数据安全管理平台，结合《银行保险机构数据安全管理办法》开展运营，

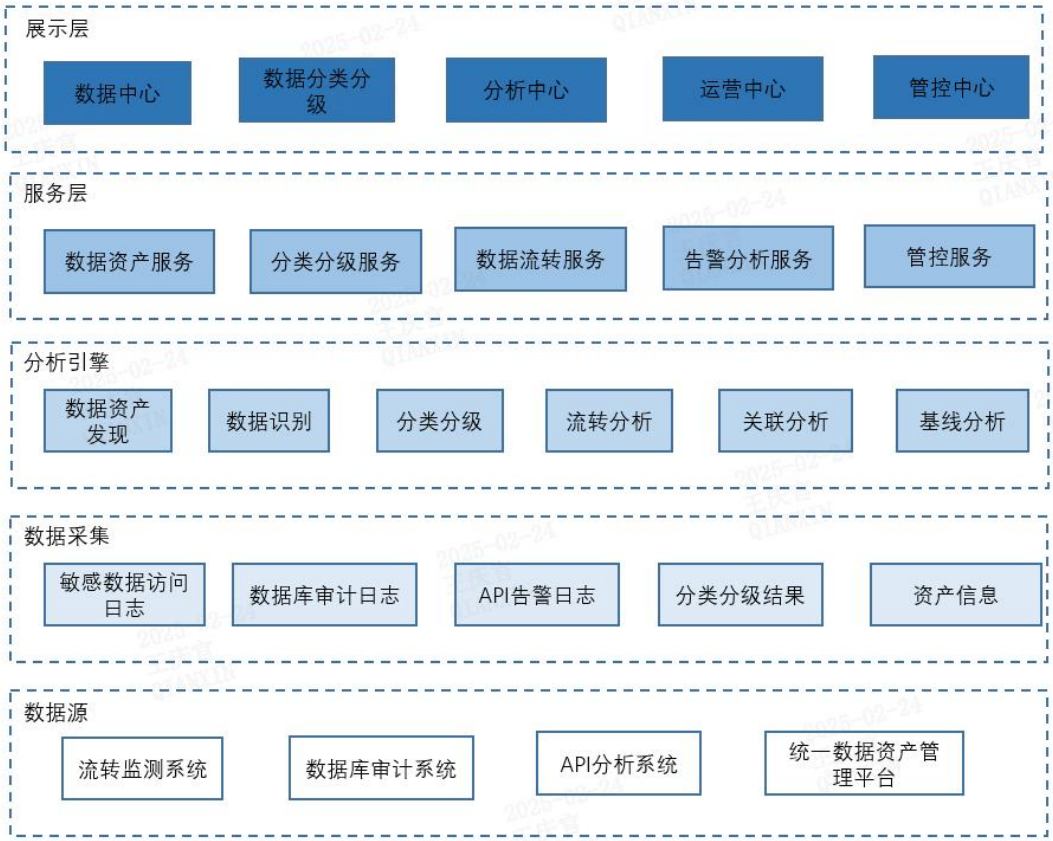
通过对办法第二章到第五章的逐条解析，形成包含账号安全、数据资产安全、数据流动安全等 70+风险场景，为集团提供从数据资产管理、数据流转监测到数据风险分析的全链条数据安全解决方案。助力集团及时发现并处置数据安全风险，保护数据资产免受非法访问和泄露，从而维护企业的声誉和业务连续性。

二、实施过程

本项目通过构建数据安全管理平台实现数据资产管理、数据分类分级、数据流转监测以及数据安全告警分析与响应处置等功能的实现。通过补充部署数据库审计、API 监测、数据流转探针等基础组件，确保数据资产的全面覆盖，并为数据安全管理平台提供丰富的数据源。

最终通过本项目的实施，显著提升集团对数据安全风险的监测、预警与处置能力，降低数据安全事件的发生概率和影响程度。并确保集团的数据安全管理符合《银行保险机构数据安全管理办法》等相关法律法规和行业标准的要求，避免因数据安全违规而引发的法律风险和经济损失。

（一）应用架构设计



图表 2 数据安全管理平台应用架构设计

人保集团数据安全管理平台应用架构如上图所示，数据源层对接是系统对接的外部设备，流量监测主要是通过旁路解析流量产生相关的日志，其输出敏感数据访问日志；数据审计主要对数据库审计流量解析，

产生数据库审计日志；API 分析系统产生 API 告警日志；统一数据资产管理平台主要输出分类分级结果以及资产相关的信息。

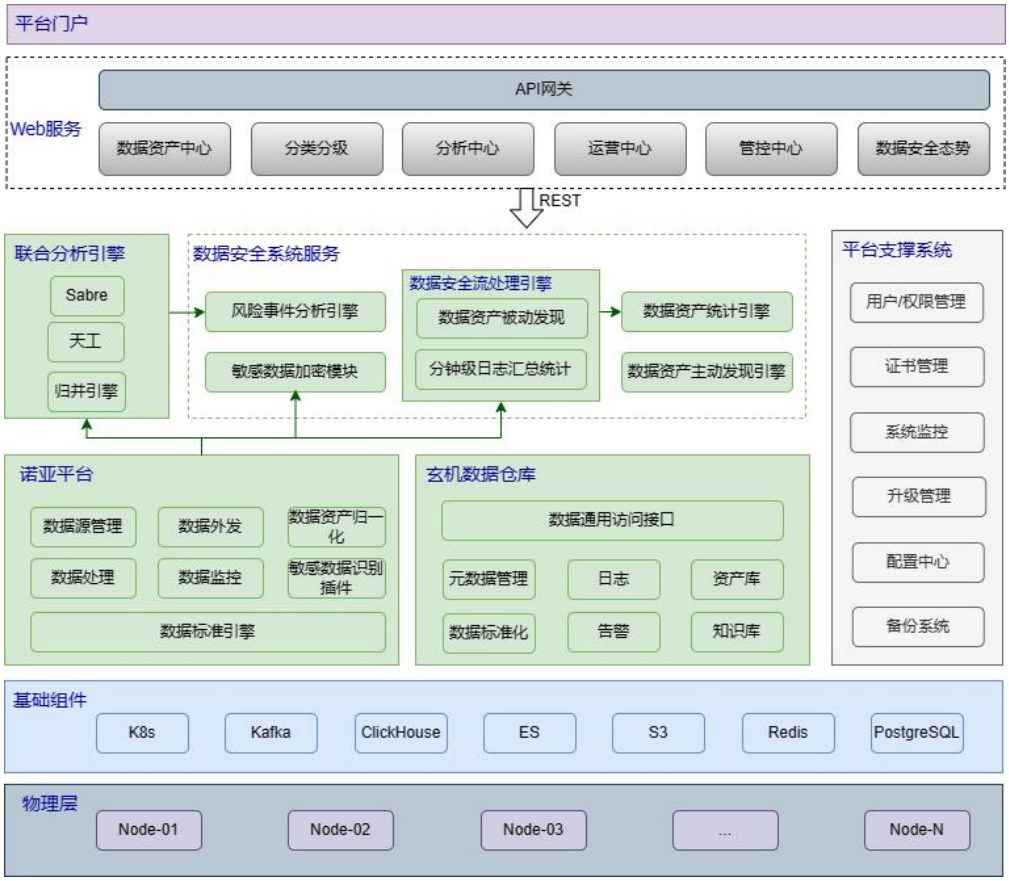
数据采集提供了各种日志接入的能力，可以对日志进行二次加工固化以及标准化，生成高质量的日志。

引擎服务层是产品核心能力，系统共提供了 6 种类型的引擎。数据资产发现引擎主要是自动化发现网络中的数据资产，生成资产列表。数据识别引擎，针对日志或者文件中的数据，进行数据识别，打数据类型标签；分类分级引擎按照策略模板的标准，对元数据进行分类分级；流转分析引擎主要针对数据访问流量日志进行流转路径关联；关联分析和基线分析引擎，主要针对接入的多种日志进行关联分析以及针对数据分析访问行为建立基线，进行基线分析。

服务层主要为展示层提供服务，起到承上启下的作用。

展示层主要包括数据中心，主要针对系统发现的数据资产，应用资产，存储资产和账号资产做可视化展示；分类分级针对元数据信息自动或者手动定级；分析中心按照安全规则通过对日志的分析，产生安全事件和告警，并对告警进行研判处置生成事件或者风险；运营中心针对事件和风险进行处置，并可以联动低位能力针对事件或者风险进行处置；管控中心主要针对接入的设备进行状态监测。

（二）技术架构设计



图表 3 数据安全管理平台技术架构设计

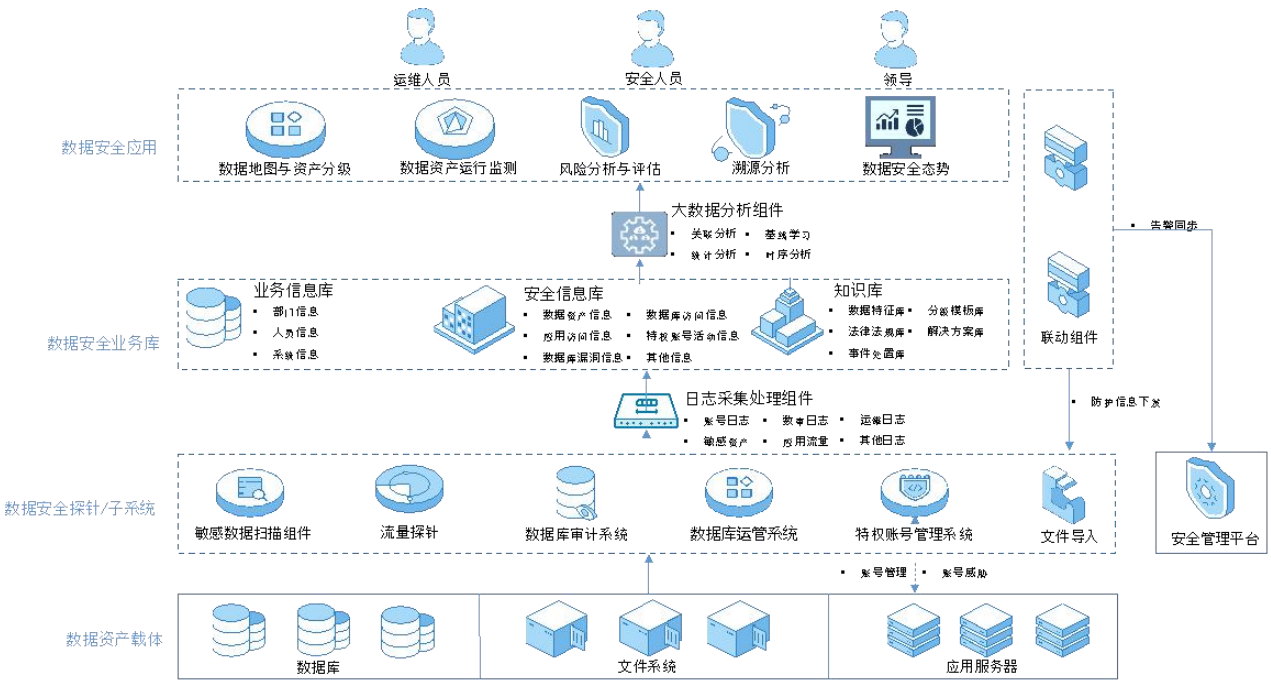
人保集团数据安全管理平台应用基于 Kubernetes 的微服务架构，大数据存储采用 Clickhouse 高性能列存数据库，使用 Kafka 作为消息中间件。

日志通过系统的日志采集功能进入系统，经过日志的过滤，富化操作进入内容解析模块，生成相关的字段信息，经过数据识别模块，对字段进行数据类型和分级打标，后续进入账号解析模块，识别登录接口，或者富化登录账号信息。经过处理后的日志，录入到 Clickhouse 数据库中。

数据资产发现流处理引擎，通过对实时日志的流分析，识别出数据资产的元数据信息，包含敏感数据标签，数据库，表，字段，文件名称，大小等信息。或主动发现数据资产中的元数据信息，数据资产信息写入数据库。

分类分级模块通过读取数据库中的分级模板，对主动发现引擎扫描出的元数据资产信息自动定级，并将信息写入数据库中。分类分级模块生成安全策略，通过自动或者手动的方式下发到数据安全相关设备上。

规则分析引擎通过读取相关的规则配置，通过 Flink 等大数据技术分析收到的原始日志，最终产生告警或事件，并存放到数据库中。平台通过对接工单系统，运营人员可直接联动工单系统进行派单处置，形成告警闭环。



图表 4 数据安全管理平台处理场景

（三）运营方案设计

通过对标《银行保险机构数据安全管理办法》，结合平台能力，将数据安全监测运营分为 5 个步骤：

图表 5 数据安全管理平台运营步骤

1、数据资产盘点

通过对接集团统一数据资产管理平台结合资产梳理调研表盘清家底，识别全量数据资产，完善数管平台“应用系统名称”等元数据；通过资产对比发现暗资产泄漏风险从而在敏感数据泄漏时快速定位关联系统；资产类型包含应用系统、数据接口、数据库、文件服务器等。

2、数据资产暴露面分析

在数据资产盘点基础上，进一步梳理这些资产的服务暴露的范围是否合理，如有误暴露的情况，需要联系责任方进行及时调整。数据资产暴露面分为以下几类：

（1）**程序调用接口：**指业务系统程序间调用，如通信接口、认证接口等，不直接提供业务服务；

（2）**内部接口：**内部业务使用，范围仅限本单位内部，不对外部机构或人员开放；

（3）**外部公众接口：**指对公众开放的业务数据接口，经认证鉴权后可被访问，无明确访问限制；

（4）**外部特定接口：**指对外单位、外部系统的数据接口，通常涉及跨部门共享，第三方业务等，但是有明确的访问限制。

3、数据流转违规监测分析

根据调研到的数据资产情况、资产暴露面情况，结合实际生产环境网络区域划分情况、数据分类分级情况，进一步设计数据违规流转监测策略。场景包括生产区数据流向开发测试区（测试开发使用生产数据）、高等级业务数据流向低等级业务区、互联网违规传输等。

4、数据安全场景化运营分析

数据安全场景化分析的目的在于针对特定业务场景识别和评估数据安全风险，并制定有效的策略来提

升数据安全性。这种分析方法能够更精确地理解数据资产在不同场景下面临的安全威胁，并采取或建立相应的防护措施。通过逐条对照监管要求条例，形成对应的风险监测场景 70+，从而梳理出平台对应的能力要求以及最终的平台价值。

监管要求条款	平台能力对应	体现价值
“重要数据、个人信息向外提供前应脱敏或加密”	字段级敏感识别 + 动态加密联动	即时阻断明文外传，防止违规事件发生
“应及时发现并处置数据安全事件”	秒级告警、SOAR 自动闭环	将风险响应时效从天级缩短至分钟级
“应保留完整审计日志并定期报送”	ClickHouse 存储 + 报表自动生成模块	自动输出监管合规日志与月度安全报告
“应建立数据安全风险基线监测机制”	行为基线建模 + 偏离检测	发现新型或隐藏违规模式，降低漏报概率
“应强化多部门协同处置”	工单系统集成 + IM 通知	一键召集接口负责人、法务及运维三方联动

图表 6 核心能力与监管条款映射举例

场景举例：敏感数据未脱敏外传

检测规则：平台对接数据中心 API 网关的全量流量，在日志清洗层完成时间戳统一、字段范式化及接口画像构建，再由敏感识别模型对 24 类高敏字段进行标注；API 将识别到未脱敏数据信息推送至平台，平台对数据流向进行判断，如数据流向为内网外发至互联网，流处理引擎持续计算脱敏率、基线、偏差三维指标，触发实时告警。

处理流程：一是通过 SOAR 自动下发网关动态加密策略，

二是对接工单系统推送相关告警至业务负责人，由业务负责人确认是否提交例外申请，敏感数据明文外发需提供业务合规性说明及风险评估报告，运营人员对反馈结果进行审核并关闭工单。如在规定时间未提供说明，事件将提级管理。

5、数据安全脆弱性风险分析

脆弱性分析是围绕数据资产开展，属于常态化、基础化的监测范围，通过对脆弱性风险的发现与修复，有效解决数据库、数据接口等自身问题，能够从根本上提升健壮性。为进一步从根本上提升数据库与数据接口的健壮性，将脆弱性风险分析纳入常态化监测，本方案围绕全量数据资产建立 40 余项检测场景，重点覆盖未授权访问、弱认证、过度数据暴露、配置缺陷、权限漂移等五大类风险。通过资产画像、基线对照、异常发现、自动工单、合规复核闭环机制，实现持续发现、精准定位与快速修复能力。

场景举例：同一内部服务 IP（SIP）在 1 小时内累计获取大量身份证号与手机号

检测规则：在数据库审计与 API 流量中实时计算敏感字段取值的去重计数，当单个 SIP 于 60 分钟窗口内去重身份证号>500 且去重手机号>500，即触发批量敏感信息抓取高危告警。

处理流程：关联分析自动比对白名单任务、开发测试工单信息；若无合规授权，则判定为脆弱性利用风险，并即时联动 WAF/网关限速、锁定访问账号并推送工单给系统负责人。事后根据日志回溯确认该接口问题，如缺乏分页限速和加密返回机制，要求研发三日内完成修复。

风险大类	监测样例规则	平台能力亮点
未授权访问	无令牌调用核心 API ≥10 次 /h	动态基线 + 行为白名单校准
弱认证	同账号短时多源地登录 + 密码强度不足	身份图谱 + 异地登录检测
过度数据暴露	返回字段超出接口定义 / 返回明文敏感字段	JSON Diff 引擎 + 字段级标签
配置缺陷	数据库启用弱口令、未启用 SSL	自动化脚本扫描 + CMDB 比对
权限漂移	普通角色调用管理员存储过程 ≥5 次 /h	RBAC 基线建模 + 异常越权检测

图表 7 脆弱性风险监测能力举例

三、成果与效益

项目自实施以来，以全量可视、精准分级、敏捷处置三大能力为牵引，全面提升集团的数据安全治理水平。

在资产纳管方面，依托自动发现引擎与统一数据资产管理平台及 CMDB 对接，实现动态、可追溯的数据资产总账：568 套应用系统、2482 个数据库实例、2960 台文件服务器及 2540 条对外／对内 API 全量纳管，覆盖率由改造前的 27%提升至 100%。同时，基于流量对比与指纹碰撞，额外识别出 112 套暗资产与 486 条遗留接口，为后续治理消除盲区。

数据分类分级方面，人保集团以《银行保险机构数据安全管理办法》为主干、结合行业标准扩展 5 类 46 个分级模型，并通过主动扫描+流量识别双通路自动标注 19.48 万条元数据，覆盖 98.6 %的客户个人敏感信息字段。分类分级结果不仅反向驱动加密、脱敏与水印策略，还与 API 网关、数据库网关联动，实现策略下发自动化率 91%，显著降低人工审批负担。

运营效率方面，ClickHouse+Flink 的实时分析能力将平均发现时间（MTTD）压缩至 14S，通过对接自动工单系统，可实现自动派单与处置结果更新，大幅提升运营效率。

通过以上成果，形成数据安全的统一资产底座、精细分级标签、实时检测响应、自动化运营能力闭环，不但满足最新监管要求，也为数字化业务的持续创新奠定坚实、安全的基础。

四、经验与启示

金融保险行业在数据安全上存在资产盘不清、监管压力大、业务实时性高的共性痛点，本案例给出了一条可落地、可复制的实践路径。

以资产感知为起点的先建账、再建防思路契合金融领域系统多、接口杂、数据散的客观现状；基于自动发现与持续对账机制，解决影子资产隐患，也为后续所有治理动作奠定了可信底座。

其次，将监管条款拆解为可执行的标签、规则和剧本，实现法规即标准，让安全策略随业务变更而自动演化，避免了传统项目合规一次性、事后全手工的困境。

基于 ClickHouse+Flink 的实时计算与 SOAR 的自动编排，将发现、阻断、通报、复核完整闭环压缩到分钟级，实现安全运营与业务节奏同频，确保核心交易稳定。

从落地效果看，平台实施以来资产覆盖率显著提升、高危事件 MTTR 缩短到小时级，并通过量化指标直接映射出运营成本下降与合规通过率提升。更重要的是，整套能力架构采用微服务与标准接口设计，可与银行、券商、互金机构现有的 CMDB、ESB、API 网关快速对接，无需对核心业务系统做深度改造；同时各类引擎可按需启用，支持平台先行的分阶段部署模式。

五、总结

本案例不仅验证数据安全综合管理平台在保险集团场景的可行性，也提供金融行业可普适的实施模板，对正在推进数据合规治理、却苦于工具割裂和运营投入过高的同行业机构而言，本方案具有显著的借鉴与推广价值。

第十七节　泰康保险集团 基于多模型识别与机器学习预警的数据安全系统

一、背景介绍

（一）案例概述

保险业作为金融行业的重要组成部分，在数字化转型中面临着巨大的挑战。为了应对随之而来的数据安全威胁和风险管理问题，泰康保险集团自研打造了基于多模型识别与机器学习预警的数据安全系统-USM 数据安全系统，该系统采用先进的多模型识别技术和机器学习算法，实现了对企业内部及外部威胁大数据的智能化分析和实时风险预警，实现对数据的高效、精准和安全的保护，该案例的实用性在于能够基于保险公司信息安全防控场景，帮助企业降低数据泄露风险、提升数据安全性、提高企业的数据安全管理和防控水平。

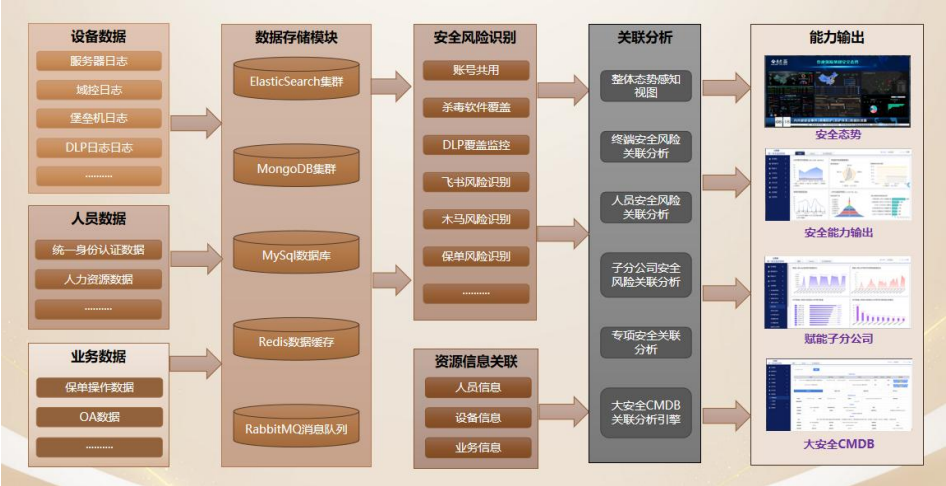
（二）案例背景及意义

在当今数字化时代，数据安全已成为企业面临的重要挑战之一。随着网络技术的不断发展和应用，企业的数据资产越来越丰富，但同时也面临着越来越多的安全风险。因此，如何有效地保护企业的数据安全已经成为每个企业的必修课。为了应对这些问题，我们通过多模型识别与机器学习预警技术，实现数据安全保护与风险管控的双重目标。本案例为保险公司提供了一种高效、智能的数据安全解决方案思路，这不仅是对传统保险信息安全防护机制的革新，更是推动保险企业信息安全数字化转型的重要一步，助力企业提升用户信任度和市场竞争力。

二、实施过程

本系统以业务为驱动、流程为导向、安全为基线，采集汇聚集团相关安全日志，基于用户行为风险模型，利用大数据挖掘分析技术，对接外部瞬息万变的威胁情报，开展安全风险分析，及时预警赋能业务发

展，有效提升了集团及子分公司的整体安全管理水平。以下是系统的整体架构图：



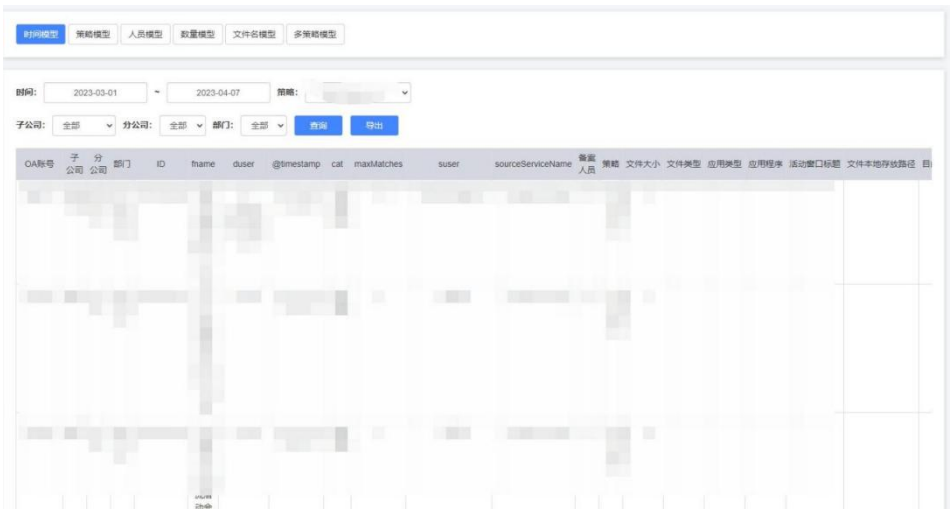
图表 9 系统整体架构图

（一）即时通讯行为安全审计模型

基于即时通讯系统审计日志，建立安全审计场景分析模型，基于此功能，加强对重点敏感岗位的即时通讯文件外发行为进行监控。核心功能有：短时间大量下载转发、非工作时间异常下载转发、手机下载转发敏感文件、敏感岗位人员异常操作、离职人员异常操作、风险数据批量查询。

（二）数据泄露安全分析模型

基于 DLP 原始数据泄露风险数据，结合泰康数据安全工作的具体需求，依托自研的 USM 安全平台，建立了一系列敏感数据识别的模型和策略。对数据泄露风险实现有效降噪，使数据泄露报警降到可排查跟踪的状态。“USM 系统数据泄露安全分析模块实景图”如下：



图表 10 数据泄露安全分析模块实景图

三、成果与效益

该案例创新点主要体现在以下几个方面：

（一）多模型识别技术

基于收集的多种类、大规模、长时段的日志数据，包括即时通信、邮件发送、文件传输等多种类型数据，通过创建并集成“时间模型”“人员模型”“数量模型”“文件模型”“策略模型”等多种先进的数据识别分析模型，实现对异常数据、恶意攻击、违规行为等的精准识别，大幅提高了数据安全保护的准确性和可信度。

（二）机器学习预警能力

系统中引入了机器学习算法，通过对历史数据和实时数据的深度学习和分析，自动识别潜在的数据泄露风险事件，并及时发出预警。

（三）实时监控和响应机制的创新

系统能够实时监控企业的数据安全状况，一旦发现异常情况，能够立即采取相应的响应措施，包括通知相关人员、隔离受影响的系统等，高效协助信息安全人员及时应对风险。

（四）即时通讯公私融合的创新

鉴于市场上移动即时通讯应用普遍缺少安全厂商支持的情况下，基于保险行业数据特征，建立即时通讯应用的安全审计日志规范标准，可基于日志数据快速实现保险公司客户敏感数据异常传输的识别。

（五）事件管理的创新

从多方日志汇聚分析，甄别风险事件，直至事件处置、归档，提供一站式的流程管控体验。

该系统在公司实践应用中，也形成了多项国家发明专利，其中一项专利已授权，另外两项专利已进入实审环节。详细情况见第七章附件。

（六）智能化风险分析

系统在数据安全保护的同时，还能对典型业务场景中存在的潜在安全风险进行分析和评估，为机构提供决策支持和战略指导，提升风险管理水平。

四、经验与启示

通过案例的有效实施，集团可快速实施对重点信息安全风险事件的发现、甄别、定位、分析，并进行快速处理，极大提升了事件处置与安全审计的效率与质量。

（一）高效发现终端敏感文件泄露风险

该系统可以通过技术手段，收集行为数据，建立“时间模型”“人员模型”“数量模型”“文件模型”“策略模型”，从而识别数据泄露风险。通过这种分析，企业能够更加准确地识别数据泄露风险，并采取相应的措施降低数据泄露风险。基于模型有效开展数据泄露风险事件识别工作，发起识别万余次，甄别准确率达 95%，涉及渠道包含邮件、即时通讯软件、网盘、移动介质等。

（二）提高企业数据安全管理效率

借助本系统可以帮助企业建立高效、精准的数据分类及安全分级工作，并持续有效维护。通过系统对不同分级数据的识别，企业可以更加高效地管理存储于系统、终端中的数据，为数据“打标”，确保数据不会被未经授权的人员访问或使用，避免数据泄露、丢失或损坏。通过一段时间模型优化与数据积累系统已完成对保险业各类业务数据标签化，建立千余条敏感数据识别规则。

（三）安全事件处置提效明显

通过系统已实现对终端异常外发、账号共享、堡垒机行为审计、数据库运维操作、敏感数据异常查询、外包人员离场、内网敏感信息暴露等多种类型安全事件的发现、甄别、定位、分析的线上化流程，极大提升事件处理的时效及质量。相较基于日志的人工排查，通过系统实现多模型的筛选，能够较好去除“噪音数据”，真正发现重大安全风险事件。

（四）实现离职人员快速审计

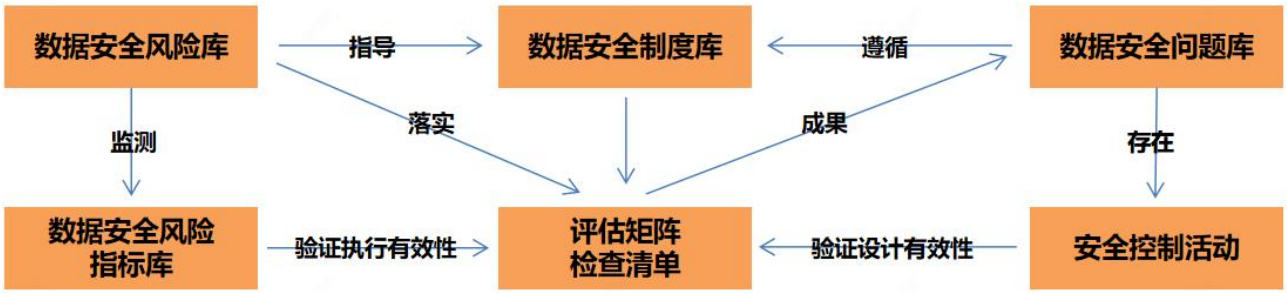
离职人员安全审计之难，主要在于离职信息同步难，审计期间难以有效匡定，执行时间受限于离职流程办理时间等因素影响，往往造成人员办理完离职流程后，才发现重大异常。通过本系统实现自动清理与手工工单流程清单两种预离职人员权限收回数据的快速抓取。通过核心业务系统日志的集中收集，追溯离职前的员工异常行为、实现实时审计敏感数据发送、数据库高敏访问查询、下载数据、同步数据、源代码等行为。一旦研判为可疑行为可第一时间通过系统推送风险提示至离职人员直属领导，确认是否正常。目前通过系统已实现对千余次的离职数据安全审计。

（五）实现基于保单生命周期数据安全跟踪

通过在保险承保、保全、理赔等业务处理系统中埋点，收集客户保单从生效到终止过程中对客户个人隐私信息、保单信息、理赔信息等高敏数据的查询操作记录，并依据查询量级、时间、对端设备，人机识别等数据模型，实现对保险客户数据的防泄露。同时，系统实现了基于业务系统用户权限变化，及历史操作习惯，可快速识别出与岗位不相符的高敏查询操作。

（六）建立保险行业数据安全风险知识库

建立以保险业务为导向的多维度数据安全风险知识库体系架构，对接监管标准变化、间接评估结果、外部舆情及事件、内部制度更新等因素实现可持续迭代。知识库以风险库为中心可扩展至人员信息、资产信息、管理制度、内部控制活动、检查发现、风险事件、检查样本等方面风险知识数据体系架构。同时，基于分类与索引功能，实现评估矩阵与检查清单中用于实操的检查点与上述风险库建立很好的对应关联，对于不同评估对象与目标，灵活配置项目评估矩阵与检查清单，保证所有风险评估与安全检查工作及程序均以风险为导向进行。目前系统已基于监管文件、行业案例、公司历史事件梳理数据安全合规标准库以及数据安全专项库 10 余个，涵盖数据采集、处理、存储、传输、销毁全生命周期，纳入风险项 300 余项。



图表 11 风险知识数据体系架构

五、总结

本案例建立了符合保险行业数据特点的安全数据模型应用平台，并基于开源技术实现了机器学习与 AI+BI 安全场景大数据分析，对安全事件辅助决策技术落地进行了有益的探索。后续案例系统将从以下几个方面进一步加强与优化：

（一）案例应用系统技术栈待需进一步升级，目前系统对于非格式化数据处理还需进一步升级；

（二）在资产与人员维度，建立更多的趋势和关联性的数据分析方法与模型，扩展案例应用系统的服务能力，真正实现对资产安全画像以及对人员的安全画像；

（三）围绕保险服务业态，进一步探索对保险业务场景输出数据安全服务能力，坚定服务保险数字化转型建设。

第十八节　平安人寿 供应商安全管理自动化平台解决方案

一、背景介绍

随着《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》等一系列法律法规及监管规范的要求，我司在数据交互场景上，保障数据安全，实现数据追溯和数据识别，实现后续数据交互真实性审计。建立数据交互安全体系，保障数据在供应商使用场景下的安全合规和可控。

在现代商业环境之下，随着数字化应用技术的广泛应用，整个环境中的个体已经形成了密不可分的业务网络、数据链接、信息互通已经是司空见惯，且也是组织生存密不可分的组成部分，云计算、SAAS、开发外包、业务外包日益盛行，大量的内外系统对接，业务上下游关系，使得整个合作网络和供应链更是显得庞大和诡谲，带来了安全管理上的巨大挑战，特别是在数据安全上面，数据资产的可复制特点带来了比起传统资产如现金、贵金属面临的不一样的风险问题，即难以核实和查证数据的流动轨迹和泄露渠道，供应商的安全漏洞问题也导致了信息系统的整体防护难度越来越大，近年以来越来越多的供应商风险事件也表明了供应商风险会随着业务上下游进行风险扩散，带来快速的风险传导，威胁合作组织的安全情况。供应商信息安全问题增加了安全治理的广度和难度。

二、实施过程

（一）供应商风险评估平台需求与风险分析

结合长期以来对于供应商安全管理的关注，我们总结出来以下四点供应商风险评估的主要挑战。

1、供应商现状了解不足

在供应商准入或者投标环节上，我们往往能看到供应商提供的 ISO27001、等级保护证书，但是实际在后续的合作中，会发现仅凭供应商安全资质无法正确体现信息安全能力真实水平，资质代理严谨程度不一，安全资质仅为投标加分而拿。不能反映其实际安全运营水平。

2、持续监控力度不足

合同约定的年度检查、抽检等方式监控颗粒度不足，信息安全态势瞬息万变，容易遗漏；甚至部分供应商会根据甲方的年度检查进行管理证据的临时生造，只为通过例行检查，并未实际落实证据所代表的管理措施，而由甲方去提升年度检查或者抽检的频次，在人力、资源和配合度方面，也是一个不可达成的想法。

3、评估方式的依赖和成本，不够或难以自动化

传统的安全检查和评估，严重依赖于人工审查，审查范围和细节常因人力资源的问题无法全面覆盖，而且由于审查员个人的经验和风险偏好，多次的抽检往往会得到不甚一致的风险结论，缺乏常态性自动化的方式维持效率和风险偏好的一致性。

4、前后改进效果不清晰

供应商对发现的问题进行跟踪整改之后，也缺乏评估整改前后的效果量化的认知，对于供应商实际安全能力缺乏整体认知，致使一些风险重复发生，屡现不改，或者说因无法合理的量化认知而不清楚风险根本原因，仅能治标，无法治本。

（二）供应商风险评估平台落地建设

基于上述的分析和多年的供应商安全管理的经验，我们思考并搭建了供应商风险评估平台，主要实现以下目的：

1、在供应商入围阶段即启动信息安全评估，联动采购系统，在供应商接受邀标之后，自动获取供应商，避免遗漏，通过平台自动化对供应商进行安全评估，1-2 周内拿到评估结果和报告。

2、对于合作供应商信息安全的持续监控

对于已达成合作的供应商进行持续的安全态势监控，一旦发现安全风险，及时向业务合作商进行披露并触发下一步的安全审计要求来进行风险说明和风险现状的更新。

3、维护供应商风险评估的要素管理

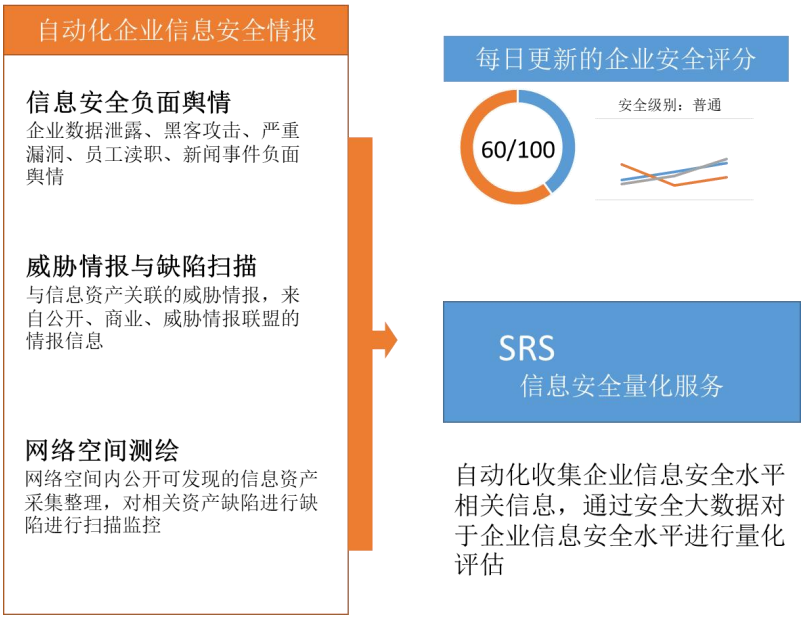
对于风险评估的要素管理上，持续的监控和风险及时的更新需要及时的信息支持。平台将会自动地获取公开材料，结合供应商的调查问卷，实现供应商的安全每次自动评分。

4、供应商资产图谱的自动探索和发现

平台在细节的供应商资产上也实现了图谱的自动探索和发现，及时 而精确的信息，才是正确风险评估的有效支撑。

5、良好的结果呈现

在现代系统应用中，良好的、可视化的结果呈现，甚至有可能决定实际的项目成败，在结果呈现上，必须是直观、通俗的非安全，甚至非风险领域的人员展示风险评估的结果，这样有助于该供应商业务的内部管理方能够清晰认识到安全风险的现状和重要性。



图表 12 平台主要功能描述

三、成果与效益

供应商管理风险管理平台落地以来，不仅解决了供应商现状的了解需求，且保证了对供应商的持续监控。并契合了银保监〔2021〕141 号文《银行保险机构信息科技外包风险监管办法》中的要求，实现对供

应商的分类分级管控、加强信息科技外包风险管控。统筹管理供应商超过 1000+，整体成效上：

（一）对齐了供应商清单，从线下文件管理到线上系统，实现了数据对齐，实时更新，避免了遗漏和错误。

（二）供应商分类分级，能够支持供应商级别的预分级，按照监管要求进行关键基础设施供应商、重要供应商、一般供应商的分级

（三）供应商现状分析，能够从多个渠道自动进行供应商现状整合、包含企业负面新闻、关联资产缺陷等，进行信息安全量化评分，实现每日更新。

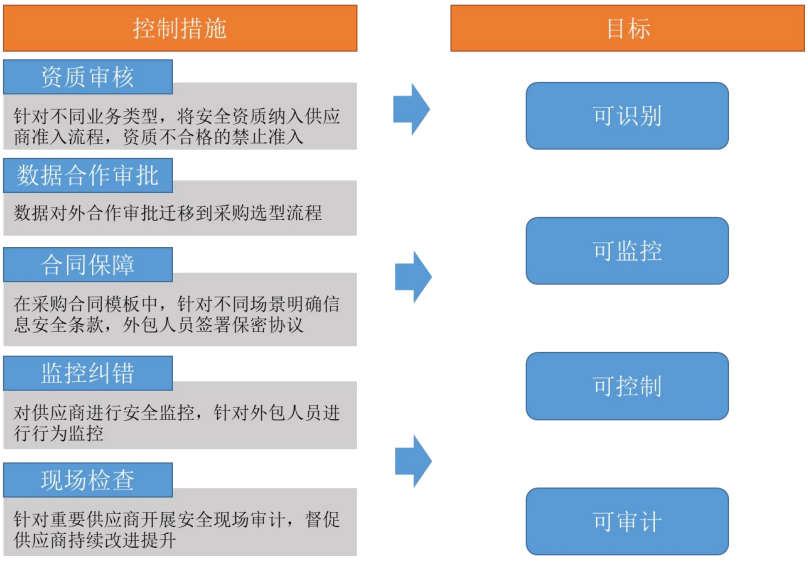
（四）降低供应商抽检成本，从原来平均每个供应商一周的抽检时间，降低为 3 个工作日，有效提升了运营效率。

（五）提升了业务部门安全管理意识，通过供应商下挂的操作，加强了业务部门认知，明确了自身的供应商安全风险管理责任。

四、经验与启示

后续供应商风险评估平台的发展方向，会逐步在威胁情报、网络空 间测绘、合规知识库、自动化缺陷审计四个方面进行持续的自动化 深化，实现线上线下相结合，将内控部门的现场审计、第三方的独立现场审计的报告也整合至一起，进行平台的迭代更新。

在平台建设的过程中，我们也整理出面向供应商管理的控制措施和目标值，在整个过程中，无论是采用自动化平台还是依然采用经验为重的传统方式，希望能给相类似的组织带来一些参考。



图表 13 面向供应商管理的控制措施和目标值

（一）风险可识别

供应商的风险，无论是自身风险还是市场风险，仍需要风险进行识别并量化管理，哪怕初步的量化是基于经验性的，但是在没有更加量化方式下，经验主义仍然是主流并有效的量化评估方式。

（二）风险可监控

供应商的风险必须是一个可持续性监控的方式，这就要求了数据、业务的相对持续性可以保证，哪怕是在合作期之间的间歇期，持续的自动化情报也会给予供应商当前状态的一个持续监控，及时排除不合适的供应商，保证企业的关联业务合作健康。

（三）风险可控制

集中管理风险中，作为甲方企业可控制，可干预的风险管理措施，如内部信息安全管理要求和控制水平，供应链选择风险倾向等。

（四）风险可审计

平台虽提供了供应商自查审计的功能，能够周期性向供应商发送评估邮件进行自评要求和审计结果回传，但是在这之上，独立性的、第三方的供应商安全审计工作仍然是不可缺少的关键组成部分，特别是对于重要级别的供应商。

第五章　咨询机构数据安全合规落地实践案例

第十九节　翰纬科技 银行数据安全治理咨询实践

一、背景介绍

在金融监管环境日益严格的当下，随着《银行保险机构数据安全管理办法》和《中国人民银行业务领域数据安全管理办法》的相继出台，银行业，尤其是中小规模的城市商业银行，正面临着前所未有的数据安全管理挑战。这两个管理办法不仅为银行的数据安全管理提供了全面的指导，也带来了新的挑战和压力。

某银行，作为一家快速发展的城市商业银行，随着业务的扩展，其信息系统和安全建设也在不断升级迭代。为了适应数字化转型的趋势，该银行成立了数字金融部，对数据安全进行归口管理，并设立了数据安全专岗，初步建立了一套数据安全管理办法。尽管在数据安全方面已经取得了一定的进展，但由于数据安全专业人才的匮乏和资源投入的不足，数据安全体系化建设仍显得相对滞后。

在合规建设落地实践中，该银行遇到的问题主要包括：

- 合规理解与执行难度：准确理解总局和人行发布的数据安全管理办法的要求，并将其转化为具体的制度和操作流程，是一项挑战。
- 技术与资源限制：作为一家中小型城商行，技术能力和资源有限，难以全面覆盖两个管理办法中的所有要求。
- 数据安全风险管理：有效识别、评估和管理数据安全风险，确保数据安全，是银行面临的另一个重要问题。

这些问题的存在，使得银行在数据安全合规建设的道路上，需要采取更加有效的措施，以确保数据安全管理的有效性和合规性。基于此，该银行在 2025 年启动了数据安全治理咨询项目，通过实现以下核心目标，以提升银行的数据安全管理水平和合规性：

- 建立健全数据安全合规体系：依据总局和人行数据安全管理办法的要求，构建一个全面覆盖数据安全生命周期的合规体系，确保数据安全管理的有效性和合规性。
- 明确未来三年数据安全治理的目标和实施路径：制定清晰的数据安全治理目标，并规划实施路径，确保目标的实现。
- 建立数据分类分级标准并推广管理模式：制定符合监管要求的数据分类分级标准，并通过试点形成可复制的管理模式，为全行数据安全管理提供标准化支持。

二、实施过程

针对该银行在数据安全合规建设中遇到的问题，项目团队提出了一套综合解决方案，通过引入外部专业咨询机构的力量，建立一个全面、系统且符合未来发展需求的数据安全管理体系。

（一）方案设计原则

- 规范性原则：严格依据数据安全法律法规、金融行业规范及其他相关标准和制度。
- 先进性原则：采用先进的管理和技术方法，具备前瞻性，适应未来数据安全发展的趋势。
- 完整性原则：全面覆盖数据安全涉及的各个层面，确保实施对象覆盖银行所有重要业务、信息系统和数据。
- 合理性原则：制度流程设计立足于该银行的现实情况，确保设计方法合乎逻辑，过程完备详实，结论可信。
- 经济性原则：在满足项目要求的前提下，方案应具有高性价比和经济性，确保资源的合理利用。

（二）方案实施步骤

1. 数据安全现状调研和风险评估：

对总局和人行的数据安全管理办法，逐条进行对照、解读。参照《GB/T 45577-2025 数据安全技术 数据安全风险评估方法》，开展详细的调研和风险评估工作。

领域	子域	细项	《银行保险机构数据安全管理办法》要求	办法解读	对照《中国人民银行业务领域数据安全管理办法》	请填写内该项要求的负责部门或团队	访谈提纲（现场访谈，请提前了解）	请准备并提供以下证明材料
数据安全	第二章 数据安全治理	数据安全治理架构	第九条 银行保险机构应当建立覆盖董（理）事会、高管层、数据安全统筹、数据安全技术保护等部门的数据安全管理组织架构，明确岗位职责和工作机制，落实资源保障。	1、建立覆盖董（理）事会、高管层、数据安全统筹、数据安全技术保护等部门的数据安全管理组织架构 2、明确岗位职责和工作机制 3、落实资源保障	第十一条 数据处理者应当切实履行业务数据安全保护责任，明确业务数据安全保护相关内设部门职责，配备与业务范围和服务规模相适应的数据安全专业人员，细化业务数据安全保护奖惩规程。 面向社会提供产品、服务的数据处理者应当建立便捷的投诉、举报渠道，及时受理并处理业务数据安全有关投诉、举报。 重要数据的处理者应当明确业务数据的安全负责人和管理机构。管理机构应当切实履行法律、行政法规已明确的各项责任。业务数据的安全负责人应当符合法律、行政法规已明确需具备的条件，并确保其能够有效履行数据安全保护义务，有权直接向中国人民银行报告业务数据安全情况。		1、数据安全管理组织架构的建立和运作情况 2、数据安全归口管理部门的职责和日常工作	数据安全组织架构和职责描述
		数据安全责任制	第十条 银行保险机构应当建立数据安全责任制，党委（党组）、董（理）事会对本单位数据安全工作负主体责任。银行保险机构主要负责人为数据安全第一责任人，分管数据安全的高级管理人员为直接责任人，明确各层级负责人的责任，明确违规情形和责任追究事项，落实问责处置机制。	1、建立数据安全责任制 2、明确党委（党组）、董（理）事会对数据安全工作的主体责任 3、明确机构主要负责人为数据安全的第一责任人 4、明确分管数据安全的高级管理人员为直接责任人 5、明确不同层级管理人员在数据安全管理中的责任 6、明确哪些行为或事件被视为违反数据安全管理规定 7、制定责任追究制度，规定在违规情形发生时，如何追究各级责任人的责任 8、落实问责处置机制，用于在违规情形发生时执行责任追究	同上		1、数据安全责任制的建立和运作情况 2、各级责任人的职责分配和执行情况 3、违规情形的界定和责任追究的实施细节	1、数据安全责任制的描述 2、明确数据安全违规事项和处罚机制的文件材料

图 1：对照办法逐条解读、访谈提纲和资料清单（部分示例）

业务部门数据安全情况调查问卷

尊敬的业务部门同事：

您好！为全面了解和提升我行数据安全管理水平，依据《银行保险机构数据安全管理办法》等监管要求中的内容，特开展此次调查。您的意见对我们至关重要，烦请您根据实际情况填写以下问卷，感谢您的支持与配合！

1. 【基本信息】您所在的业务部门是：[ ]
2. 【基本信息】您在部门中的岗位是：[ ]
3. 【数据收集】在日常业务中，您所在部门收集数据的主要渠道有哪些？（可多选）
   - [ ] 线下纸质表格填写
   - [ ] 线上业务系统录入
   - [ ] 客户电话咨询记录
   - [ ] 其他（请注明）_____
4. 【数据收集】您所在部门是否存在从外部机构或平台采集数据的场景？
   - [ ] 是
   - [ ] 否
   - 如果存在，请列举具体从外部采集数据的场景（可多选）：
     - [ ] 从合作机构获取客户信用报告，用于评估客户信用风险
     - [ ] 从第三方数据平台获取行业统计数据，用于市场分析
     - [ ] 其他（请注明）：_____
5. 【数据存储】您所在部门存储的数据主要保存在哪些设备或系统中？（可多选）
   - [ ] 内部服务器
   - [ ] 企业网盘
   - [ ] 个人办公电脑
   - [ ] 移动存储设备（如 U 盘、移动硬盘等）
   - [ ] 其他（请注明）_____
6. 【数据委托处理】您所在部门是否存在委托第三方机构进行数据处理的情况？
   - [ ] 是，存在数据委托处理
   - [ ] 否
   - 如果存在，请列举具体委托处理的场景（可多选）：
     - [ ] 客户数据录入外包
     - [ ] 数据分析外包
     - [ ] 制卡服务外包
     - [ ] 邮寄服务外包
     - [ ] 催收服务外包
     - [ ] 客户服务外包
     - [ ] 其他（请注明）_____

图 2：业务部门调研问卷（部分示例）

银行保险机构数据安全管理办法（金规【2024】24号）			评估发现和整改建议						
办法：章	办法：节	内容	问题发现（存在的差距）	风险描述	风险类型	合规风险等级	整改建议	其他参考依据《中国人民银行业务领域数据安全	整改类型
第三章 数据分类分级	第十六条 （总体要求）	银行保险机构应当制定数据分类分级保护制度，建立数据目录和分类分级规范，动态管理和维护数据目录，采取差异化安全保护措施。	制度中分类分级的标准以及差异化的数据安全保护措施与监管要求不一致，且缺乏对数据目录的动态管理和维护。	银行制度中分类分级标准及保护措施与监管要求不符，且未动态管理数据目录，易致数据保护不到位，面临监管处罚与数据泄露风险。	数据泄露风险、数据篡改风险、数据滥用风险、违法违规处理数据、未有效保障个人信息主体权利、数据不可控风险等	高	1、按照监管要求，修订数据分类分级管理制度，明确数据类型和安全级别的划分标准。 2、建立数据目录，并动态管理和维护，完整准确记录信息系统所存储数据项和对应标识内容。	第二章 业务数据分类分级与总体要求	体系优化（制度流程+技术工具）
	第十七条 （数据分类）	银行保险机构应当对机构业务及经营管理过程中获取、产生的数据进行分类管理，数据类型包括客户数据、业务数据、经营管理数据、系统运行和安全管理数据等。	在制度中虽然有数据分类分级的要求，但数据分类分级的标准，与监管办法存在不一致；实际工作中也尚未开展数据分类分级工作。	数据分类分级标准与监管不符且未实际开展工作，会导致数据安全管理失效，增加数据泄露风险，面临监管处罚和声誉损失。	数据泄露风险、数据篡改风险、数据滥用风险、违法违规处理数据、未有效保障个人信息主体权利、数据不可控风险等	高	1、结合数据治理平台升级项目，落实自动化数据分类分级工作的开展。 2、数据分类：对机构业务及经营管理过程中获取、产生的数据进行分类管理，数据类型包括客户数据、业务数据、经营管理数据、系统运行和安全管理数据等，并准确标识各数据项的个人信息属性、外部收集来源、存储系统清单和关联业务类别，以及数据的敏感性和可用性分类。 3、数据分级：根据数据的重要性和敏感程度，将数据分为核心数据、重要数据、一般数据。其中，一般数据细分为敏感数据和其他一般数据。	第二章 业务数据分类分级与总体要求	体系优化（制度流程+技术工具）

图 3：对发现的问题进行风险识别、分析和评价（部分示例）

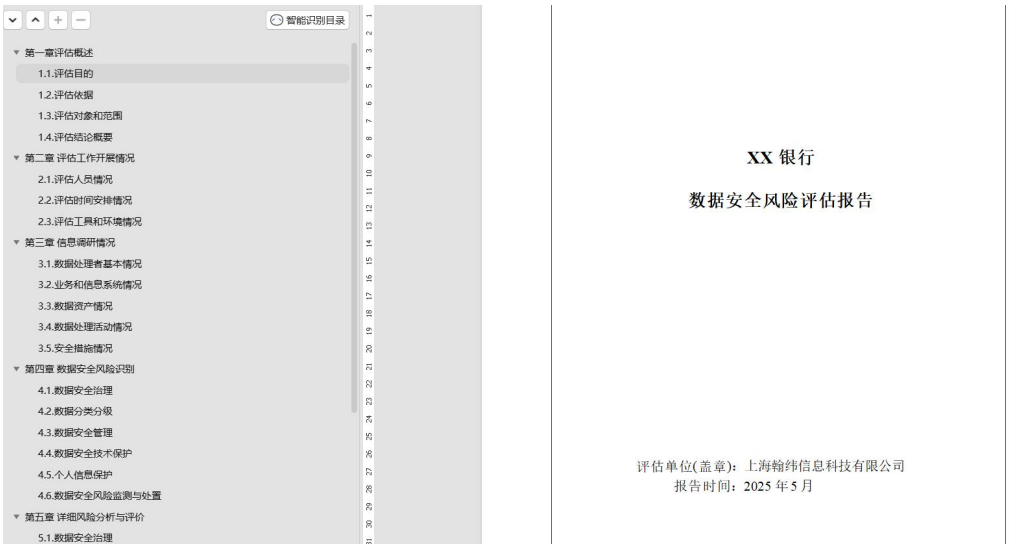


图 4：数据安全风险评估报告（部分示例）

2.数据安全合规制度体系建设：

数据安全管理制度体系可分为四层架构，每一层作为上一层的支撑。第一层是管理总纲，是银行数据安全顶层的方针和策略，应明确数据安全治理的目标和重点；第二层是管理制度，对数据安全管理活动中的各类管理内容建立安全管理制度；第三层是操作流程和规范性文件，是作为制度要求下指导数据安全策略落地的指南；第四层是报告、记录和表单文件，是作为数据安全落地运营过程中产生的执行文件。

以下是在本次项目中编制的数据安全管理制度框架和文件清单：

序号	一级	二级	三级	四级（附在三级文件后面）	涵盖的领域
1	L1-数据安全管理总体策略	L2-01数据安全管理办法	L3-01数据分类分级实施指南	L4-数据目录	数据分类分级
2				L4-数据分类分级标准	
3				L4-数据分类分级变更申请审批表模板	
4			L3-02数据资产管理流程		数据资产管理
5			L3-03数据收集规范		数据收集
6			L3-04数据存储		数据存储
7			L3-05数据传输		数据传输
8			L3-06数据加工管理流程	L4-数据加工需求申请审批表	数据加工
9				L4-数据安全评估报告模板	
10			L3-07人工智能模型开发应用安全管理规范		
11			L3-08模型算法/信息系统数据安全审查流程	L4-模型算法/信息系统数据安全审查报告模板	
12			L3-09数据生产提取操作流程	L4-数据生产提取申请审批表模板	数据提取、使用
13			L3-10数据访问管理流程	L4-数据访问控制矩阵	数据访问权限控制
14				L4-数据访问申请和审批记录	
15			L3-11数据外发安全管理流程	L4-数据外发申请表	数据外发
16			L3-12数据服务规范	L4-数据服务目录	数据服务管理
17			L3-13数据委托处理安全管理流程	L4-数据委托处理合同协议模板	委托处理
18				L4-数据安全评估报告模板	
19				L4-对委托处理者进行尽职调查的报告模板	
20				L4-对委托处理者的数据安全保护能力进行安全评估的报告模板	
21			L3-14数据合作共享安全管理实施细则	L4-数据共享合同协议模板	合作共享
22				L4-数据安全评估报告模板	
23			L3-15数据备份及恢复性测试管理流程	L4-数据备份策略	备份与恢复
24				L4-数据备份恢复性测试计划模板	
25				L4-数据备份恢复性测试报告模板	
26			L3-16数据对外披露安全管理流程		
27			L3-17外部数据采购安全管理流程	L4-外部数据采购和合作引入申请表	数据外部采购
28				L4-合作方尽职调查报告	
29				L4-外部数据处理合作方风险评估报告	
30				L4-与外部数据提供者、外部数据处理者、数据共享的接收方签订的合同模板	
31				L4-外部数据退出申请表	
32			L3-18数据安全风险监测流程		风险监测
33			L3-19数据安全事件管理流程	L4-数据安全事件评估模版	数据安全事件管理
34				L4-数据安全事件应急预案	
35				L4-数据安全事件应急响应培训记录模板	
36				L4-数据安全事件应急演练记录模板	
37				L4-数据安全事件处置报告模板	
38				L4-第三方数据安全事件报告模版	
39			L3-20个人信息保护管理规范	L4-个人信息处理规则（隐私政策）模板	个人信息保护政策
40			L3-21个人信息保护影响评估管理规范	L4-个人信息保护影响评估报告模板	影响评估
41				L4-高风险的个人信息处理活动示例	
42				L4-安全事件可能性等级判定原则	
43				L4-个人权益影响程度判定原则	

图 5：数据安全制度体系文件清单（部分示例）

3. 方案规划：

依据数据安全现状调研和风险评估的结果，结合该银行业务发展战略、目标和需要制定未来三年的数据安全规划。具体来说，该银行依据金监局《银行保险机构数据安全管理办法》的框架搭建了数据安全体系架构，涵盖数据安全治理、数据分类分级、个人信息保护、数据安全管理、数据安全技术和数据安全风险监测与处置等内容，同时也参考了人行数据安全办法和行业标准，识别出未来三年的工作目标和重点任务，指导各方面工作的具体开展。

任务名称	任务目标	任务内容	监管要求
数据分类分级	数据分类分级标准优化	1、融合监管要求和行业标准，优化数据分类分级规则，制定数据分类分级实施指南	
		2、细化数据安全级别的变更场景，并建立动态调整审批机制	《银行保险机构数据安全管理办法》第三章 数据分类分级
	采购数据分类分级工具	采购数据分类分级工具，通过自动化和人工相结合的方式，开展数据分类分级工作	《中国人民银行业务领域数据安全管理办法（征求意见稿）》
	结构化数据分类分级	各信息系统内的数据，每半年组织数据owner对表中字段安全定级确认复核	第二章 数据分类分级
	非结构化数据分类分级	信息系统外数据，制定数据目录，提供定级策略和方法，由各部门自行定级并嵌入业务管理流程中	
	建立企业级数据架构	建立企业级数据架构，统筹开展对全域数据资产登记管理，建立数据资产地图	《银行保险机构数据安全管理办法》第二十一条（数据资产管理）

图 6：数据安全规划任务（部分示例）

4. 数据分类分级试点实施：

在金融行业，人民银行发布了《JR/T 0171-2020 个人金融信息保护技术规范》《JR/T 0197-2020 金融数据安全 数据安全分级指南》《JR/T 0223-2021 金融数据安全 数据生命周期安全规范》《中国人民银行业务领域数据安全管理办法》，为银行数据分类分级工作提供了有力指导，国家金融监督管理总局发布的《银行保险机构数据安全管理办法》也对银行保险机构数据分类分级的相关要求进行明确和强化。

该银行将总局和人行数据分类分级方法进行融合，制定了数据分类分级标准：

- 分类方面：对业务及经营管理过程中获取、产生的数据进行基础分类，包括客户数据、业务数据、经营管理数据、系统运行和安全管理数据等，形成银行的基础数据底账。鉴于《银行保险机构数据安全管理办法》中的数据分类要求只有一级子类，且没有具体各类数据的定义说明和示例。在实际落地执行的过程中，银行按照总结办法要求，将数据一级子类分为客户数据、业务数据、经营管理数据、系统运行和安全管理数据，而二级、三级和四级子类则参考人行分级指南中的内容。同时，结合人行数据安全管理办法的要求，基于基础数据底账，从业务关联性、敏感性和可用性等方面进行细化和标识。
- 分级方面：依据数据重要性和敏感程度的不同，数据分为核心数据、重要数据、一般数据。其中，一般数据细分为敏感数据和其他一般数据。

在本次项目中，选定了部分核心业务系统作为试点，开展手工和自动化结合的数据分类分级工作。以下是通过手工方式，依据总局和人行的标准，对部分客户数据进行分类分级的结果示例：

编号	字段名	依据总局标准			依据人行标准										
		数据类别	数据级别	说明	一级子类	二级子类	三级子类	四级子类	是否为个人信息	是否为外部收集产生	存储该数据项的信息系统清单	关联的业务类别	敏感性分类	可用性分类	数据级别
1	法人机构	客户	一般数据-其他一般	对应单位的法人机构信息	客户	单位	单位基本信息	单位基本概况					2		一般数据
2	机构编号	客户	一般数据-其他一般	具体规则生成编号，属于单位基础属性	客户	单位	单位基本信息	单位基本概况					2		一般数据
3	客户编号	客户	一般数据-其他一般	单位唯一标识符，基础属性信息	客户	单位	单位基本信息	单位基本概况					2		一般数据
4	客户名称	客户	一般数据-其他一般	单位的名称信息	客户	单位	单位基本信息	单位基本概况					2		一般数据
5	客户类型	客户	一般数据-其他一般	分类单位类型的属性	客户	单位	单位基本信息	单位基本概况					2		一般数据

图 7：数据分类分级结果（部分示例）

同时，利用数据治理平台的分类分级功能，该银行根据监管要求预设了分类分级标准，实现了数据的自动化分类分级。并由数据安全管理团队与业务部门协作，对自动化分类分级的结果进行了人工复核，并对分类分级规则进行了调整与优化，在这个过程中显著提高了分类分级工作的准确性，并形成了可复制且高效的管理模式，为全行数据

安全管理提供了标准化支持，并确保了模式的持续迭代与改进。

三、成果与效益

本项目自实施以来，为该银行带来了显著的成果与效益：

1. **合规性提升：**建立了与《银行保险机构数据安全管理办法》和《中国人民银行业务领域数据安全管理办法》相符合的数据安全合规体系，极大降低了合规风险，确保了银行业务的合法合规运行。

2. **风险管理强化：**通过全面的风险评估和管理，有效地识别、评估和管理数据安全风险，提高了对潜在威胁的应对能力，减少了安全事件的发生。

3. **管理效率提高：**数据分类分级的实施和自动化工具的应用，提高了数据管理的效率，优化了数据处理流程，加快了业务响应速度。

4. **员工能力增强：**系统的员工培训和意识提升活动，使得员工对数据安全有了更深入的理解，提高了他们的专业技能，为银行培养了一批数据安全管理的专业人才。

5. **客户信任增加：**数据安全治理的加强，增强了客户对银行的信任，有助于提升客户满意度和忠诚度，为银行赢得了良好的市场声誉。

6. **业务创新支持：**健全的数据安全管理体系为银行的数字化转型和业务创新提供了坚实的基础，支持银行在激烈的市场竞争中保持领先地位。

四、经验与启示

在项目实施过程中积累了宝贵的经验，获得了重要的启示：

1. **高层支持至关重要：**高层管理的支持是项目成功的关键，它确保了项目获得必要的资源和关注，推动了项目的顺利实施。

2. **跨部门协作是关键：**数据安全治理需要跨部门的紧密协作，有助于确保数据安全管理的全面性和有效性，实现从技术、管理、业务等多个维度的综合考量。

3. **持续优化是必然：**数据安全管理体系需要不断地进行评估和优化，以适应不断变化的安全环境和监管要求，保持体系的活力和有效性。

4. **员工培训是基础：**定期的员工培训和意识提升活动对于建立数据安全文化和提升员工能力至关重要，是提升整体数据安全管理水平的基础。

5. **技术与流程的结合是提升效率的关键：**技术措施和流程管理的结合是提高数据安全管理效率的关键，两者相辅相成，共同构建了高效的数据安全管理体系。

通过吸取这些经验与启示，该银行不仅在当前项目中取得了成功，也为未来在数据安全领域的持续发展和创新奠定了坚实的基础。

第六章　培训机构数据安全合规落地实践案例

第二十节　合规社 银行数据安全全员能力体系建设实践

一、背景介绍

在《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》以及《银行保险机构数据安全管理办法》（以下简称《总局办法》）全面落地的大环境下，A 银行像众多金融机构一样，面临着数据安全合规的挑战。数据安全是银行稳健运营的重要基石，关乎客户权益保护、业务连续性以及市场声誉。要有效应对这些挑战，需要从技术、管理以及人员素养等多方面入手，其中提升人员的数据安全技能及素养是筑牢数据安全根基的重要一环。

以往那种统一模式的培训方式，往往难以满足不同岗位人员的个性化需求，培训效果也并不理想。因此，我们为 A 银行量身定制了一套分层分级、紧贴实战的数据安全培训方案。方案的核心是精准匹配不同角色的职责，充分考虑银行内部不同人员在数据安全工作中的角色定位与职责差异，提供针对性的培训内容。

在具体实施中，我们依据《中华人民共和国数据安全法》及《总局办法》对人员培训的要求，结合 A 银行的组织架构与岗位职责，分析数据安全人员的能力要求，构建了相应的能力框架。通过这一过程，明确各层级人员在数据安全中的关键作用，为制定精准的培训内容提供了依据。通过分层分级的培训，助力每个岗位的人员都能获得与其职责相匹配的知识和技能。

同时，我们注重培训的实操性与效果转化。通过案例分析和模拟演练，让学员在实践中加深对数据安全知识的理解，提升应对实际问题的能力。本案例精准施教的培训模式，不仅提高了培训效果，还为 A 银行构建了实效性的全员数据安全能力体系，为银行的数字化转型和业务发展提供了有力支持。

二、实施过程

在着手推进 A 银行数据安全培训项目之际，项目组深入研读了相关法律法规，包括法律、行政法规、部门规章及重要标准中涉及金融机构数据安全培训的具体条款。如，《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《网络数据安全管理条例》以及《银行保险机构数据安全管理办法》等法规从不同角度强调了数据安全培训的重要性，明确要求金融机构建立健全数据安全培训体系，定期对从业人员进行数据安全教育和培训，提升员工的数据安全保护意识与技能。《中国人民银行业务领域数据安全管理办法》《金融数据安全 数据生命周期安全规范》（JR/T 0223-2021）更是细化了培训的具体要求，包括培训计划的制定、培训频次、培训内容的涵盖范围以及培训效果的评估等。

表 1：法规标准对数据培训的要求

法律/标准	具体规定
《中华人民共和国个人信息保护法》	**第五十一条** 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失： …… （四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训； ……
《中华人民共和国数据安全法》	**第二十条** 国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。 **第二十七条** 开展数据处理活动应当依照法律、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。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。
1.1.1.《网络数据安全管理条例》	第四条 国家鼓励网络数据在各行业、各领域的创新应用，加强网络数据安全防护能力建设，支持网络数据相关技术、产品、服务创新，开展网络数据安全宣传教育和人才培养，促进网络数据开发利用和产业发展。 第三十条 重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。网络数据安全管理机构应当履行下列网络数据安全保护责任： …… （二）定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件； …… 掌握有关主管部门规定的特定种类、规模的重要数据的网络数据处理者，应当对网络数据安全负责人和关键岗位的人员进行安全背景审查，加强相关人员培训。审查时，可以申请公安机关、国家安全机关协助。
1.1.2.《银行保险机构数据安全管理办法》	**第十一条** 银行保险机构应当指定数据安全归口管理部门，作为本机构负责数据安全工作的主责部门。其主要职责包括： …… （五）组织开展数据安全宣贯培训，提升员工数据安全保护意识与技能； 第十五条 银行保险机构应当建立良好的数据安全文化，开展全员数据安全教育和培训，提高数据安全保护意识和水平，形成全员共同维护数据安全和促进发展的良好环境。 **第六十八条** 银行保险机构应当建立数据安全事件应急管理机制，建立机构内部协调联动机制，建立服务提供商、第三方合作机构数据安全事件的报告机制，及时处置风险隐患及安全事件。 （一）制定数据安全事件应急预案，定期开展应急响应培训和应急演练。 …… **第七十八条** 中国银行业协会、中国保险行业协会等行业社团组织应当通过宣传、培训、自律、协调、服务等方式，协助引导会员单位提高数据安全管理水平。

1.1.3.《中国人民银行业务领域数据安全管理办法》	**第十三条** 数据处理者应当根据岗位分工，制定业务数据安全年度培训计划，每年组织业务数据处理活动参与人员开展相关教育培训。培训内容应当包括与业务数据安全相关的制度标准、风险防范常识、岗位责任、保护措施和事件应急处置要求。 **第四十二条** 重要数据的处理者应当自行或者委托第三方评估机构，每年对业务数据开展一次风险评估，……，风险评估报告还应当包含与存储重要数据信息系统相关的人员培训与日常管理情况，……。 **第四十九条** 数据处理者未履行本办法规定的数据安全保护义务，有下列情形之一的，中国人民银行及其分支机构依照《中华人民共和国数据安全法》第四十五条予以处罚： …… （二）未依照法律、行政法规对应规定，组织开展业务数据安全教育培训的。 ……
《金融数据安全 数据生命周期安全规范》（JR/T 0223-2021）	**8.3 人员管理** 金融业机构对数据安全管理相关人员进行管理，具体要求如下： b） 在人员培训和教育方面，应制定数据安全相关岗位人员的安全专项培训计划，并至少满足以下要求： 1）按照培训计划定期开展数据安全意识教育与培训，培训内容包括但不限于国家有关法律法规、行业规章制度、技术标准，以及金融业机构内部数据安全有关制度与管理规程等内容，并对培训结果进行评价、记录和归档。 2）对密切接触高安全等级数据的人员定期开展数据安全意识教育和培训，培养办公数据定期删除意识，并定期开展数据删除自查工作。 3）每年至少对数据安全管理专职与关键岗位人员进行 1 次数据安全专项培训。 4）至少每年 1 次或在隐私政策发生重大变化时，对数据安全关键岗位上的人员开展专业化培训和考核，确保人员熟练掌握隐私政策和相关规程。

与此同时，项目组细致梳理了监管机构对未开展数据安全培训而采取的处罚措施。虽然目前公开渠道中少见针对银行因未开展数据安全培训而受到处罚的案例，但这并不意味着此类问题不存在，可能是因为相关信息尚未被广泛披露。实际上，因未落实数据安全培训而导致的处罚案例在其他行业时有发生。例如，2023 年，某某房地产公司数据安全意识淡薄，未建立数据安全管理制度和操作规程，未对员工开展数据安全教育培训，未对采集到的居民个人信息采取加密措施，被公安局处以警告并对直接责任人员处罚款的行政处罚。2024 年，重庆某科技公司未组织开展网络数据安全教育培训，同时未采取必要的技术和其他措施确保网络数据安全，导致大量数据泄露，情节严重，被属地网信办要求责令限期改正，并给予行政警告，处 10 万元罚款的行政处罚。

表 2：未开展数据安全教育培训被处罚案例

时间	案例通报
2023 年 4 月	“湘潭某公司未落实数据安全管理制度，未开展数据安全教育培训，且未对系统采取相应的技术防范措施，致使系统接口存在任意文件上传漏洞等数据安全隐患，大量个人信息、单位信息存在泄露风险。湘潭县公安局根据《数据安全法》相关规定，县公安局依法对该单位予以行政警告处罚，要求其切实履行主体责任，及时清理处置数据安全隐患。”

2023 年 5 月	“邵阳市某置业公司数据安全意识淡薄，未建立健全全流程数据安全管理制度，未开展数据安全教育培训，未采取相应的技术措施和其它必要措施保障公司的数据安全，导致该公司开发楼盘的所有业主信息被本公司工作人员多次贩卖。隆回县公安局根据《数据安全法》第二十七条、第四十五条第一款之规定，给予该公司警告，并责令限期改正。”
2023 年 5 月	“太湖县某房地产公司数据安全意识淡薄，未建立数据安全管理制度和操作规程，未对员工开展数据安全教育培训，未对采集到的居民个人信息采取加密措施。太湖县公安局对该公司未履行数据安全保护义务的违法行为，依法处以警告并对直接责任人员处罚款人民币 1 万元的行政处罚。”
2023 年 7 月	“重庆某科技公司因业务开展，收集、存储、处理的网络数据量较大，但未按法律法规要求建立健全全流程网络数据安全管理制度，未组织开展网络数据安全教育培训，未采取相应的技术措施和其他必要措施，保障网络数据安全等数据安全保护义务，且存在数据库数据泄露的情形。 重庆市网信办依据《数据安全法》第二十七条、第二十九条、第四十五条之规定，对该公司作出责令限期改正，给予行政警告，并处 10 万元罚款的行政处罚。”
2024 年 3 月	“重庆某科技公司运营的某 OA 信息系统由于未履行网络数据安全保护义务，导致大量数据泄露，情节严重。作为网络数据处理者，该公司未按法律规定建立完善的全流程网络数据安全管理制度，也未组织开展网络数据安全教育培训，同时未采取必要的技术和其他措施确保网络数据安全。重庆市网信办依据《数据安全法》第二十七条、第二十九条、第四十五条之规定，重庆网信办对该公司作出责令限期改正，给予行政警告，并处 10 万元罚款的行政处罚。”

案例虽发生在其他行业，但其警示意义不容忽视。数据安全培训不仅是合规的必要条件，更是金融机构防范风险、维护客户权益的关键所在。未落实数据安全培训可能导致机构面临监管处罚，情节严重时，相关责任人也可能受到法律责任追究。

在培训需求分析阶段，项目组依据《总局办法》的要求，结合 A 银行的组织架构和岗位职责，对不同层级人员的数据安全能力要求进行了深入分析。

1.构建 A 银行完整的数据安全知识架构和能力框架

组上组重点梳理了管理层、数据安全专职岗位与关键岗位人员以及全员的能力要求，明确了各层级在数据安全中的关键作用，为后续的课程设计和培训实施提供了科学依据。

（1）管理层作为银行整体数据安全战略的制定者和推动者，需要对数据安全监管要求有深入的理解，以便更好地指导银行整体数据安全战略的制定和实施。管理层还需制定并推动实施数据安全战略，使数据安全与银行整体战略相契合。因此，管理层要了解数据安全的整体态势，掌握行业动态和最新趋势，明确监管的要求及法律责任，保障银行在数据安全方面的资源投入和保障措施到位。此外，管理层要监督数据安全管理体系的执行情况，指导数据安全关键岗位人员的工作，推进数据安全措施的有效落实。

（2）数据安全专职与关键岗位人员是数据安全管理的核心执行者，承担着具体的数据安全操作和管理任务。在本次培训项目中，重点分析其能力要求，包括数据安全管理、数据合规、数据安全技术、数据出境管理以及个人信息保护等多项专业能力及问题解决等 5 项通用能力。《总局办法》将个人信息保护列

为专章，进一步凸显了个人信息保护在数据安全中的重要性。因此，数据安全能力的构建中涵盖了个人信息保护能力。从业人员需要熟悉个人信息保护法规，并能够实施有效的隐私保护措施。同时，随着数据跨境流动的增加，数据出境管理也成为数据安全的重要组成部分。从业人员需要了解并遵守数据跨境传输的法规要求，保障数据出境的合规性。

图 8：数据安全从业人员能力框架

（4）全员聚焦“意识与底线”，全员需聚焦于数据安全意识的提升，这是维护数据安全的基础。员工应熟悉并严格遵守数据安全操作流程，在日常业务中正确合规地处理客户数据。同时，员工需提升对数据安全重要性的认识，增强防范数据泄露和滥用的意识。树立牢固的数据安全意识，明确数据安全的底线，减少因疏忽导致的数据安全事件。

表 3：银行数据安全从业人员能力框架

能力框架	关键能力项	细分能力	能力描述
专业技能	数据安全管理能力——数据安全管理体系构建与执行能力	数据资产识别与分类分级	能够识别组织内的数据资产，了解数据的来源、内容、存储位置和使用情况，并根据数据的重要性和敏感程度进行分类和分级。
		数据安全管理体系构建	构建适应组织特点的数据安全政策、流程和程序，建立专门的数据安全团队，并进行有效的人员管理。
		数据全生命周期管理	管理数据的创建、存储、使用、共享、备份和销毁等阶段，采取相应安全措施，防止数据滥用、丢失或泄露。
		数据安全风险评估	定期进行数据安全风险评估，识别潜在的安全威胁和漏洞，提出并实施风险缓解措施。
	数据合规能力——数据安全法规理解与应用能力	法规理解与适应	熟悉国内外数据安全法律法规，保障数据处理活动符合法规要求。
		标准遵循	了解并遵循相关数据安全标准，包括数据安全重要国家标准及相关金融行业标准。
		合规流程执行	依照合规流程进行数据收集、存储、使用和销毁等操作。

		合规风险识别与处理	识别和处理可能的合规风险，如数据泄露、非法使用数据等，采取预防措施避免问题再次发生。
	数据安全技术能力——数据安全技术应用与创新能力	数据安全工程规划设计	掌握数据安全架构的规划设计和建设实施技术。
		数据安全技术开发与运维	数据加密、访问控制、风险管理、日志分析。
		数据安全监测与应急处置	持续监控数据安全状态，及时发现并应对安全事件。
		数据备份及恢复	负责数据备份和恢复操作，在数据在发生故障或安全事件时能够快速恢复。
		数据加密以及访问控制	掌握数据加密技术，使敏感数据在存储和传输过程中的安全性；实施和管理访问控制机制。
	个人信息保护能力——个人信息保护法规理解与实践能力	个人信息合规能力	熟悉国内外个人信息保护法律法规，在个人信息的收集、存储、使用、共享、跨境传输等环节严格遵守法律要求。
		个人信息安全能力	具备从技术、管理和运营层面全方位保障个人信息安全的能力，在个人信息在收集、存储、传输和使用过程中的安全性。
	数据出境管理能力——数据出境法规理解与合规操作能力	数据出境合规能力	熟悉国内外数据跨境传输的法律法规以及相关国际条约和协议，能够进行数据出境前的合规性审查。
		数据出境安全能力	具备数据出境过程中的安全技术与管理能力，建立数据出境后的持续监控机制，及时发现并应对潜在的安全风险。
通用技能	问题解决能力	问题解决能力	能够解决各种复杂的、未知的问题。
	协作与团队工作能力	协作与团队工作能力	能够跨部门和多角色进行有效地沟通和合作。
	沟通能力	沟通能力	能够与技术团队、管理层、客户、合作伙伴等不同利益相关者进行有效沟通。
	适应性和学习能力	适应性和学习能力	具备高度的适应性和持续学习的能力，能够适应数据安全领域的快速变化，不断提升技术能力和知识。
	伦理责任感	伦理责任感	具备强烈的伦理责任感，严格遵守法律、规定和标准，尊重隐私，保护数据安全。

2.建立多形式、多维度、差异化的培训体系

在课程设计阶段，项目组针对 A 银行不同层级人员的职责特点和工作需求，设计了系统化的分层培训方案。对高管层重点开展数据安全战略规划和治理框架培训，通过集中授课和专题研讨，提升决策层的合规意识和战略规划能力；对数据安全专职及关键岗位人员强化全流程管理能力培养，通过法规解读、案例分析和实战演练相结合的方式，系统提升数据分类分级、风险管理和应急处置等专业能力；面向全行员工则侧重基础安全意识和操作规范培训，采用集中授课、视频微课和模拟演练等多种形式，筑牢数据安全防线。整个培训体系注重理论与实践相结合，通过典型案例分析和实操演练，确保培训内容可落地、见实效。

表 4:A 银行数据安全分层培训对象

培训对象	核心课程模块	培训形式及时长	培训目标
管理层 （战略决策层） ——高管、部门总监、分支机构负责人	1.《数据安全法规与金融监管要求》 2.《〈总局办法〉解读》 3.《数据安全战略规划与治理框架》 4.《数据安全态势分析与核心发展趋势》 5.《银行数据安全治理及个人信息保护实践》 6.《数据安全风险与金融行业案例剖析》	**1.培训形式：** 集中培训+专题研讨会+同业参访交流 **2.培训时长：** 2 天集中培训+1 天参访交流及专题研讨	1.充分认识银行数据安全工作的重要性 2. 明确数据安全治理责任 3.制定合规战略与资源投入决策
数据安全专职及关键岗位 （执行层） ——数据安全归口部门、数据管理部门、科技部、风控部、法务部、合规部、审计部、运营部等部门关键岗位人员	1.《数据安全法规与金融监管要求》 2.《〈总局办法〉解读》 3.《金融数据安全重要标准》 4.《金融业数据安全治理体系及实践》 5.《银行数据生命周期风险管理》 6.《银行保险机构分类分级要求及实践》 7.《数据安全技术及应用场景》 8.《数据安全事件应急处置与沟通协调》 9.《第三方数据合作管理流程》 10.《数据安全审计要点》 11.《个人信息保护合规要点分析》 12.《数据出境监管架构与重点法律问题》	**1.培训形式：** 集中培训+案例研讨（数据分类分级、数据目录梳理等）+演练实战（风险评估、数据案例风险事件应急等） **2.培训时长：** 4 天线下集中培训+1 天演练实战及案例研讨	1.具备建立全流程数据安全管控机制能力 2.具备协调资源落实数据安全合规要求 3.学会主导数据安全风险识别与整改的相关知识
全员 （基础层） ——全行员工（含柜员、客户经理、后勤支持、外包人员等）	1.《数据安全红线意识》 2.《办公环境物理安全规范》 3. 《社交工程防御技巧》 4.《电信网络诈骗案件与数据安全》	**1.培训形式：** 集中培训+视频微课+意识宣贯活动（通过网络安全宣传周/消费者权益保护周钓鱼邮件模拟、厅堂） **2.培训时长：** 线下集中培训 1 天+定期活动宣贯+视频微课（5 小时）	1. 树立“人人有责”数据安全意识 2. 规避常见办公场景数据安全风险 3. 严守客户个人信息保护红线 4. 实现全员数据合规行为覆盖

三、成果与效益

本培训体系通过科学分层设计，系统性地提升了银行组织整体和员工个体的数据安全能力，为数字化转型提供了坚实的人才保障。该体系不仅构建了从战略决策到业务执行的全链条数据安全能力架构，使数据安全要求能够贯穿银行经营管理各环节，更通过针对性的能力培养方案，有效弥合了各层级人员在数据安全认知与执行上的断层，培育出一支既精通业务又具备安全意识的复合型人才队伍。对 A 银行而言，这

种分层递进的能力培养模式，不仅使高层管理者具备战略视野和决策能力，还使基层员工掌握必要的安全操作技能。全员的数据安全意识得到显著提升，数据安全要求转化为全员的自觉行动，为银行业务创新发展构筑了可靠的安全屏障。

为深化培训体系的应用效果，项目组建议 A 银行采取“内外兼修”的实施路径：

对内，特别建议 A 银行从三个维度固化培训成果：一是建立常态化复训机制，将核心课程纳入年度培训计划，针对管理层每半年开展监管政策更新研讨，关键岗位每季度组织案例复盘，全员每年完成安全知识刷新；二是配套考核激励机制，将数据安全履职情况与管理层绩效考核、关键岗位晋升评定、全员年度评优直接挂钩；三是构建岗位能力认证体系，开发数据安全专业序列任职资格标准，实现“培训—认证—上岗”的闭环管理。通过这些措施，培训效果得以持续转化为 A 银行的实际防控能力，推动数据安全真正内化为组织的核心竞争力。

对外，可构建客户端数据安全教育体系，建议银行：

1.在客户办理业务时嵌入数据安全提示，如在开户环节增加个人信息保护告知视频；

2.定期推送防诈骗安全资讯，通过手机银行APP和短信发送因数据安全意识缺失引发的典型诈骗案例；

3.在营业网点设置互动式数据安全教育专区，帮助客户识别常见风险；

4.针对企业端客户开展专项数据安全培训，提升其配合银行做好数据保护的意识和能力。

这种内外联动的安全能力建设模式，既能巩固银行内部培训成效，又能有效提升客户群体的整体数据安全素养，共同构建更加安全可靠的金融生态环境。

四、经验与启示

1.分层分级是核心

银行数据安全培训必须摒弃“一刀切”。高管层需聚焦责任、战略与决策；数据安全专职及关键岗位人员须掌握与其工作直接相关的、可落地的操作规范与风险应对技能；全体员工则重在建立基本意识和行为底线。精准定位才能有效赋能。

2.紧扣法规与场景是关键

培训内容须深度结合《银行保险机构数据安全管理办法》等核心法规的具体要求，并紧密嵌入学员的真实工作场景。脱离法规谈安全是空谈，脱离场景讲操作是无效。

3.意识培养需润物无声

数据全员意识的提升是一个持续过程，需要结合线上便捷学习与线下生动活泼，利用多元化的、贴近员工的方式（如微课、竞赛、快闪、宣传物料）进行常态化渗透。

4.数据安全培训是一个持续的过程

新的数据安全威胁、技术和策略不断出现。因此，数据安全培训应该是一个持续的过程，不仅包括定期的课程，还应该包括不断地学习和更新。对组织方来说需要设立一些机制，以便数据安全人员能够随时获取最新的信息和知识。

第七章　技术厂商数据安全合规落地实践案例

第二十一节　奇安信 银行敏感数据流转管控实践

一、背景介绍

某银行数字化转型后，跨部门、跨区域、跨机构共享用数日益旺盛，在保障数据要素发挥价值的同时，数据泄露、滥用、非授权访问等问题引起的数据安全风险，已成为数据安全防控的重要一环，用数行为不透明、数据泄露溯源难等问题日趋突出。

合规压力大：《银行保险机构数据安全管理办法》等法规要求严格，如敏感级及以上数据的操作需进行日志记录且核心数据操作日志及其备份数据保存时间不低于三年等，银行面临较大的合规压力，一旦违规将面临严重处罚。

数据泄露风险高：银行拥有海量的客户敏感信息，如账户信息、身份证号、联系方式等，这些数据极具价值，容易成为不法分子攻击的目标，一旦泄露将对客户和银行造成巨大损失。

缺乏有效的数据保护手段：在数据流转过程中，如 web 业务应用及 API 接口的数据交互中，难以对敏感数据进行精准识别、实时监测和有效防护，无法满足动态数据保护的需求。

内部人员操作风险：银行内部员工可能因误操作、违规操作或恶意行为导致数据泄露或被篡改，如非法访问敏感数据、非授权使用高危指令等，传统的安全措施难以对内部人员的操作进行细粒度的管控和审计。

数据共享与协作风险：在与第三方机构进行数据共享和协作时，难以确保数据的安全性和合规性，存在数据被滥用、泄露等风险，同时对数据泄露后的溯源和责任界定也较为困难。

审计追溯难度大：当发生数据安全事件时，传统的审计手段难以快速、准确地追溯数据泄露的源头和路径，无法有效界定责任主体，给事后稽核和事件调查带来很大困难。

银行期望构建“数据驱动安全”主动防护体系，实现体系化的数据安全监测响应和溯源机制。在数据流转过程中，具备对敏感数据发现、监测、管控、审计、溯源的安全能力，提高数据安全主动防御能力。各用数场景实现事前可识别、事中可控制、事后可追溯的全链路管理，实现数据全生命周期安全的“硬管控”。

（一）技术需求

1.动态数据保护：对于行里的 web 业务应用及 API 接口，提供实名访问控制，敏感数据拦截、动态脱敏、网页水印和文档水印策略，进行数据流转保护。——业务访问场景下，识别数据流转，并提供数据保护。

2.数据流转风险监测：对于行里的 web 业务应用及 API 接口，数据流转审计及异常调用数据行为的发现，异常用数事件溯源。——基于流转数据的审计日志，进行异常行为分析告警，溯源。

（二）管理需求

满足合规要求：符合《银行保险机构数据安全管理办法》规定，第四十三条：敏感级及以上数据的操作应当进行日志记录，包含操作时间、用户标识、行为类型等，核心数据操作日志机器备份数据保存时间不低于三年。——-零业务改造，满足合规要求

运行需求：

能够对数据安全网关统一集中管理，实现网关管理、监测、策略、补丁等集中下发，统一升级维护。

二、实施过程

结合银行现状及数据安全管理办法要求，本项目通过数据安全网关方案解决用户访问业务应用环节的数据保护需求。基于数据安全网关代理技术，对流量数据进行敏感数据发现、采集、改写，用来对应用系统间的数据流转进行监测管控，通过实名授权访问，按需分配访问权限，并记录访问详情人员在应用上的数据行为（数据查阅、下载、转发、拷贝、加工等）监测管控。结合数据分类分级、“RBAC”权限管控模式、实现敏感数据拦截、动态脱敏、水印和告警等防护。网关日志汇总至 BAAS 进行用户行为的异常分析监测，日志留存汇总溯源。

（一）数据安全网关 SWG

1.深度检测，敏感数据流转可视

基于 web 流量的检测，深度解析还原各业务流转内容，内置通用个人信息规则库及多个行业敏感信息库，并支持自定义复合规则补齐场景化检测要求。记录业务数据流出、梳理业务接口，并基于内容进行标签和分级分类，实现真实业务场景下的数据流转监控。

2.基于用户身份的访问控制

对接用户识别体系、结合业务登录账号、结合上下游 IP 白名单等多种方式识别来访主体身份；

通过安全源 IP 对象分配访问业务范围；

通过目的域名对象，为来访主体分配访问业务范围；

通过对数据包的控制，防止大文件违规下载；

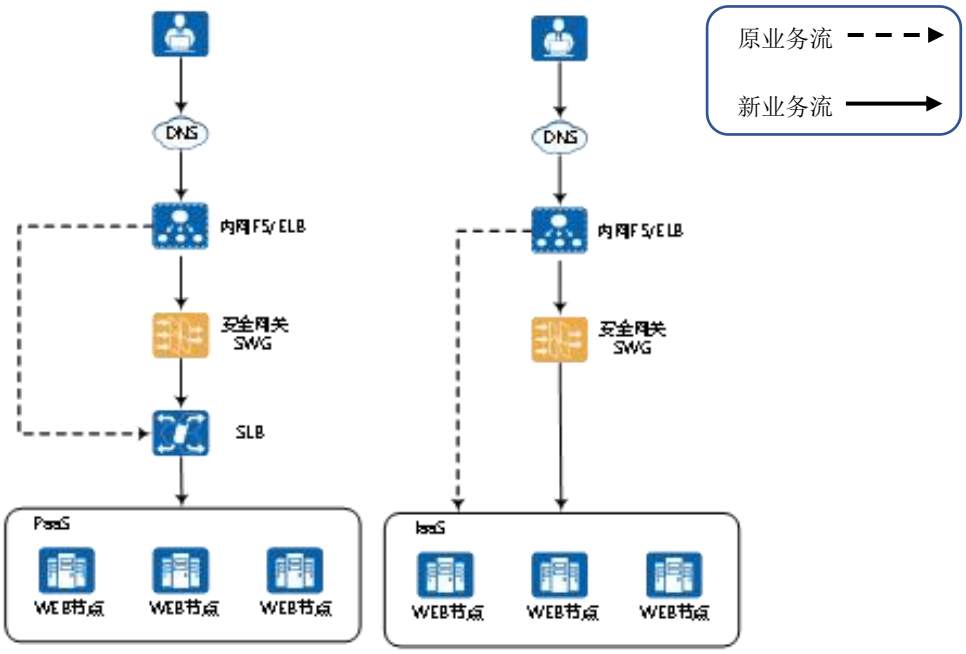
事中保护，最小化分级授权

基于反向代理接入业务，对用户无感知，业务零改造。通过业务访问行为事中的内容检测，并结合人员身份和角色的授权，实时发现风险，并执行对应的管控措施。

3.灵活管控，提供多种管理措施

提供敏感数据检测及拦截能力；提供遮蔽、仿真、随机、哈希、可逆等多种动态脱敏方案实现网页和 API 内容的脱敏；提供网页水印、文档水印、图片水印等能力防止拍照截屏等数据泄露，并基于水印码实现溯源能力。

数据安全网关部署架构：



数据安全网关一期部署 315 台，涉及业务 18+个；对接行内监控平台。

数据安全网关 SWG 完全适配行内云上部署环境（F5、ELB 负载场景），与业务节点同数据中心部署，满足双中心高可用架构要求。

（二）BAAS 行为分析系统

作为上层分析平台，汇聚所有 SWG 日志进行数据分析。

1.业务系统全面梳理

通过规则化的命名和识别业务系统、业务接口，进行便捷的配置管理，自动识别并建立完整的资产列表，实时检测并归类可视化展示。

2.应用接口分级管理

内置敏感信息规则、安全规则、行为接口规则，并根据银行业务特性提供自定义接口规则，业务审计策略基于特定规则对业务系统进行扫描，标记不同敏感级别。

3.敏感数据流转分析

基于检测规则对报文和文件中的信息做检测，发现潜在的安全风险及敏感信息泄露风险。检测结果可作为后续安全加固或流量封堵处置的参考条件。

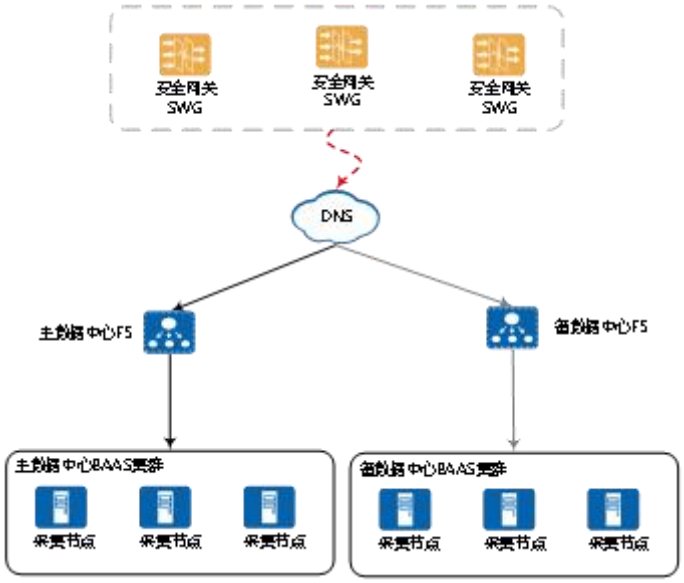
4.异常行为访问分析

基于检测规则对报文和文件中的信息做检测，发现潜在的安全风险及敏感信息泄露风险。检测结果可作为后续安全加固或流量封堵处置的参考条件。

5.风险用户事件追溯

提供更完整、更全面地记录业务网络行为日志。还原业务系统接口报文并记录详细完整的报文信息，包含：请求头、请求体、响应头、响应体和关联文件。

BAAS 部署架构：



客户主备数据中心部署各一套，每套 7 节点集群高可用；

DNS 域名解析正常解析到主数据中心的 BAAS 集群，所有 SWG 节点发送的日志均存储在主 BAAS 集群上；

当主 BAAS 集群出现故障时，由 DNS 切换解析到备数据中心，当前主备 BAAS 集群不能同步数据。

（三）业务系统接入

一期试点共接入 30 个业务系统，对包括姓名、证件号码、联系电话、住址、卡账号等各类敏感信息自动识别，各类业务接入后运行稳定，功能满足各业务系统需求；方案优势：

1.分布式&高性能数据分析引擎

搭载流式检测引擎，具备 CEP 关联分析能力，预置检测规则，支持灵活的自定义规则配置；可实现对互联网访问行为进行实时检测，快速感知异常行为，及时告警处置；

行为分析引擎，支持个人基线和群组基线评价分析，通过构建群组分析，可以跨越单个用户或实体的局限；通过对比群组，便于异常检测；组合基线分析和群组分析，可以构成完整的上下文环境，提高对行为异常评价的准确度；

2.内容检测－全面覆盖&深度检测

依托产品内置策略或主体自定义规则，实现敏感数据自动化分类，帮助企业从全局了解各级各类敏感数据；支持敏感数据实时监控、异常告警能帮助企业精准掌控敏感数据类型、访问时间途径等安全问题；

支持海量数据中快速定位敏感数据的存储与分布，为企业数据溯源、异常分析、优化数据安全措施提供支持。

三、成果与效益

1.零业务改造，流量网关轻落地部署；

2.全方位智能敏感识别，立体化数据安全防护；

3.动态数据保护，拦截、动脱、水印；

4.业务连续保障，集群、降级、熔断；

5.构建日志实时入湖架构，打造安全监测标准模型；

6.建成数据安全溯源机制，提升风险应对处置效能；

7. 虚拟化部署、多款国产化硬件；

四、经验与启示

1.聚焦细分场景需求，针对安全痛点制定个性化解决方案

2.深入业务，安全为业务服务。

第二十二节　明朝万达 广西农商联合银行数据防泄漏体系建设实践

一、背景介绍

《银行保险机构数据安全管理办法》第四十二条：在数据全生命周期内采取有效的访问控制管理措施，对于不同区域流转和共享中的数据，应当实施同等水平的安全防护措施。第六十五条：银行保险机构应当对数据安全威胁进行有效监测，实施监督检查，主动评估风险，防止数据篡改、破坏、泄露、非法利用等安全事件发生。监测内容包括：（二）内部人员异常访问、使用数据；（四）敏感级及以上数据在不同区域的异常流动；（五）移动存储介质的异常使用；

针对上述《办法》的具体要求，本案例通过融合网络 DLP 与终端 DLP 技术，在广西农商联合银行成功落地实施，显著提升了数据安全管控与风险监测能力。

内部数据泄露是机构信息安全的主要风险来源。无论出于故意还是疏忽，员工的不当操作都可能导致敏感信息外泄。研究表明，大多数数据泄露事件均与内部人员（包括已离职员工）相关。以银行业为例，办公终端中存储着客户信息、财务数据、个人隐私、商业秘密、科研成果及内部机密文件等，一旦因系统漏洞或管理疏漏而泄露，后果将不堪设想。

目前，广西农商联合银行内部网络采用“数据中心—市县机构—营业网点”的二级三层架构，划分为业务网、开发网、办公互联网等多个区域。信息流通主要依赖数据中心至县级机构及市县机构至营业网点

的两级通信链路，带宽分别为 50Mbps 和 2–20Mbps。

本项目将部署终端 DLP 系统，实现对敏感数据的集中管控，并辅以网络 DLP 对重点区域流量进行实时分析，精准识别与定位敏感信息。通过构建覆盖数据创建、存储、使用、传输、销毁全生命周期的防泄漏体系，有效防范因用户操作不当引发的数据泄露风险。

二、实施过程

广西农商联合银行将数据安全关口前移至源头，由科技部门率先开展数据分类分级工作，并据此制定全行统一的数据安全管理制度，再分阶段向各业务条线推广。针对敏感数据的外发、共享与流转环节，银行同步建设“一体化数据防泄漏平台”，对数据使用行为进行实时监测与风险预警，确保各网络区域在业务开展过程中既能合规使用数据，又能防止泄漏。具体方案设计如下：

（一）设计原则

计算机终端与网络传输是办公及生产活动中不可或缺的信息载体与数据通道。然而，现有办公终端管理软件在日益复杂的安全挑战面前已显乏力，难以满足当前严苛的管控需求：

（1）对终端、业务系统与外部之间的信息交互缺乏精准监测与有效防护；

（2）无法实现安全策略的联动管理及审计数据的关联分析，整体防护效能受限。

为进一步提升全行办公终端统一管控与网络数据防泄漏能力，项目遵循以下设计原则：

（1）平台化改造：对办公终端数据安全管理系统及网络数据防泄漏系统进行平台级升级，采用分布式部署、分组管理模式。

（2）策略联动：打通终端安全策略与网络数据安全策略，实现联动处置，为后续安全集中管控奠定基础。

（3）分类分级：以数据分类分级制度为核心，配套流程管控，为数据安全提供持续支撑。

最终形成“终端数据安全管理一体化、网络数据防泄漏一体化、安全态势可视化”的闭环运营体系，构建终端与网络数据安全协同的一体化安全运营能力。

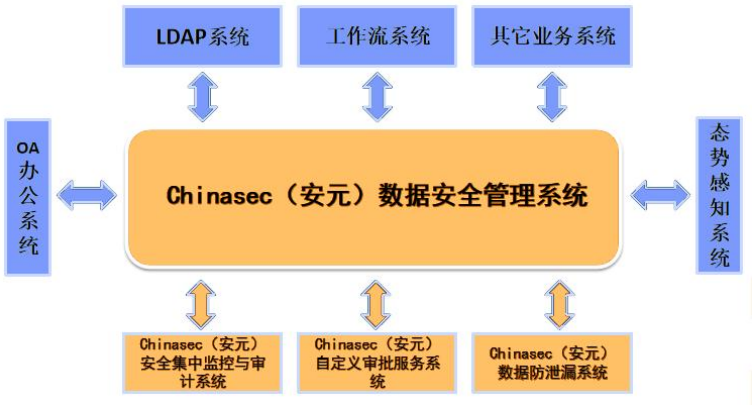


图 9：Chinasec（安元）数据安全管理系统

（二）建设方案

（1）在用户内网核心位置部署“数据安全管理平台”。平台由运维管理子系统与业务处理子系统组成，均采用高可用集群方式部署，确保性能与连续性。

（2）平台支持分级部署：在业务网、互联网、开发网分别接入终端数据防泄漏（DLP）客户端，实现跨网段终端的统一策略下发与状态监控。

（3）所有办公 PC 在安装 DLP 客户端后自动注册至数据安全管理平台，由平台进行集中配置、升级、日志收集与行为审计。

（4）平台内独立部署智能内容语义识别引擎，集成非结构化文档解析、智慧模型自动训练及特征规则提取功能，可对海量样本进行聚类、分类与敏感特征识别，为策略优化提供持续学习能力。

（5）在内网各关键区域旁路部署网络防泄漏设备，通过镜像流量实时检测网络层数据泄露风险，并将日志统一汇总至数据安全管理平台，与终端告警联动分析，形成“端－网”协同的安全事件闭环。

数据安全管理任务包括用户管理、终端管理、敏感规则制定、策略分发、日志收集及报表查询，均通过统一的数据安全管理平台集中完成。平台无缝整合终端数据防泄漏系统、网络防泄漏设备及智能内容语义识别系统，实现各安全组件的协同运行与高效管理。

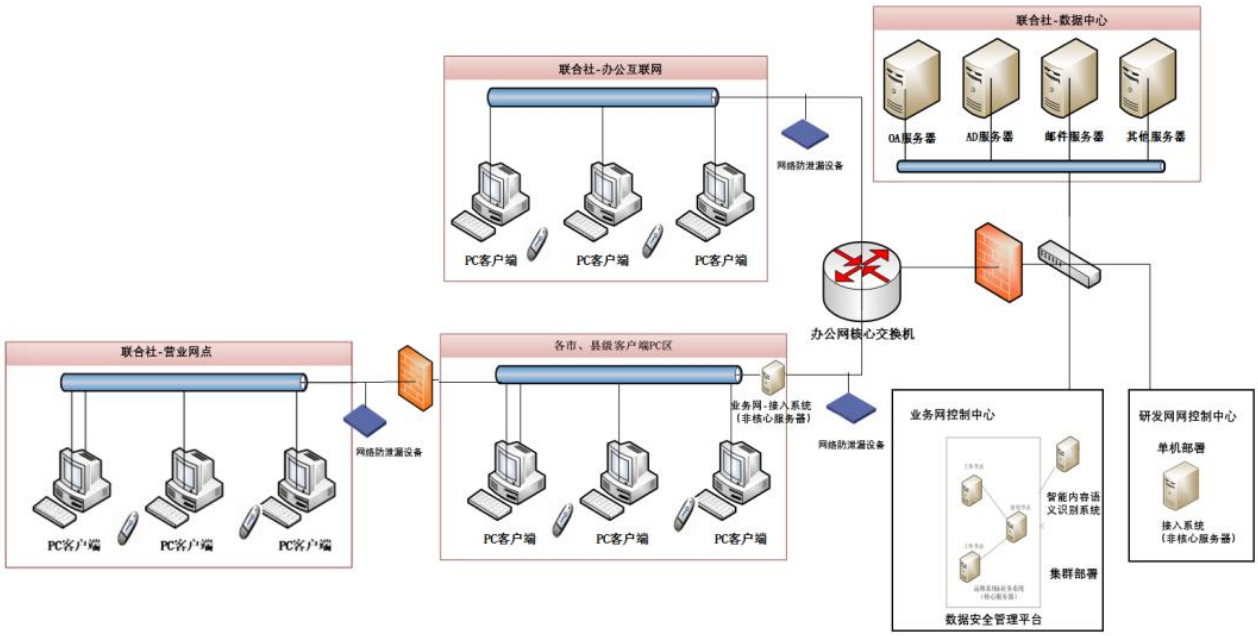


图 10：数据安全管理平台协同运行示意图

三、成果与效益

（一）成果展示

基于统一的数据安全保护体系，可取得以下应用效果：

（1）统一集中的安全管控

将行内的各机构的办公终端和业务网数据进行集中式监测，通过一个平台进行数据汇总，进而实现数据安全的统一、集中管理与防护，让安全体系的建设不再分散、复杂。

（2）敏感数据的分级分类防护

根据国家相关法律法规要求，数据安全保护体系基于应用场景的不同，为敏感数据进行分级分类，并在此基础上提供与之契合的综合防护解决方案，在有效应对各类安全风险的同时，实现了敏感数据的分级保护。

通过敏感数据分类分级的实现，结合全盘扫描技术，可实现对办公终端历史数据的分类分级加密保护，解决了数据防泄漏安全防护的历史遗留难题。

（3）边界的数据安全防护

单位内数据文档的加密应用，可使数据文档在单位内的透明使用，通过其他方式从边界外流的数据无法使用。通过文档水印的应用、U 盘的管控以及邮件数据的自动分类分级识别防护，对单位内办公环境的网络边界、终端边界进行了全方位的数据防泄漏保护。同时通过网络数据防泄漏产品进行补充筛查，及时告警。

（4）实现敏感数据的全生命周期管理

从敏感数据的产生、落地存储，到交互流转、使用外发，以及事后的监管审计追溯，体系均提供了完整的立体式解决方案，且各个阶段的防护与管控层层递进、环环相扣，有机结合为统一的防护体系，实现了敏感数据的全生命周期管理。

（5）全面的审计审批制度

通过办公终端数据防泄漏方案的建设实现了单位内办公环境的数据防泄漏安全保护：对终端人员的日常办公的数据文档的操作、使用、交互有详细的日志记录；对外发的敏感数据有告警、审批、阻断的全面监管；对合规离网的单位内敏感数据有详细的审批审计流程，保证了数据的正确合规使用。全面的审批审计制度实现了单位内可信环境内数据文档的可管、可控，保证了单位内敏感数据的安全。

（6）促进员工安全意识的提高与管理的优化

文档水印的应用使得单位内办公终端在进行文档操作时，可清晰地看到水印内容，提醒终端人员需要保护数据安全。同时，系统强大的日志审计、报表分析功能，从维度和粒度上均为监管、追溯机制的落地实行奠定了坚实的基础并提供了有效依据，从而有利于规范员工对敏感数据的使用行为，促进员工安全意识的提高与安全管理的优化。

（二）经济效益

经过探索与实践，该成果已经运用于广西农商联合银行，有效保护监测了敏感数据泄露行为，一体化安全建设，减少了之前在行内和各分支机构投入的大量人员成本，为行内减少人员成本。其次，良好的数据安全保障，也能够减少因数据泄露导致的监管与司法的隐性风险。

（三）社会效益

（1）提高了敏感数据泄露防护能力

通过建设和推广，不仅提高自身敏感数据泄露行为分析监测和处置能力，还为金融行业敏感数据泄露防护能力的整体提升提供了很好的标杆示范作用，填补了传统加密技术安全风险的不确定性。

（2）推动了企业敏感数据保护措施的不断完善赋能行业

金融行业为等保重点保护以及关基身份，敏感数据泄露行为分析监测与处置能力是很好的开始，知道短板，就能查漏补缺，不断完善企业敏感数据保护措施，为数据资源可视、可管、可控，促进数据有序流动保驾护航。让数据赋能千行百业，充分发挥数据生产要素的价值，推动数字化转型，提升国家的综合竞争力。

（3）增加企业公信力强化企业社会责任树立社会正能量

通过建设，行内可以很好地开展数据安全工作，确保数据安全，预防敏感数据泄露事件发展，增加用户的认可，用实际行动践行《中华人民共和国数据安全法》等法律法规的要求，为社会尤其拥有大量敏感数据的企业树立了正向的榜样。

四、经验与启示

（一）统一顶层设计，避免碎片化：建立覆盖“数据全生命周期”的制度体系：数据分级分类、权限管理、数据脱敏、数据共享等，形成一体化的防护，避免建设孤岛。

（二）建立资产一张表：完成多家下属机构的资产梳理，结合“数据流视角”和“业务流视角”，动态识别风险点。

（三）完善数据安全事件处理机制：建立数据安全运营小组，实现风险态势实时监测，及时同步安全风险，构建闭环处理流程。

（四）不定期数据安全培训：建立不定期培训、意识宣传机制，针对不同岗位（管理者、业务人员、开发人员、IT 运维等）定制安全培训内容。

第二十三节　绿盟科技 银行数据防泄漏体系建设实践

一、背景介绍

数据安全是金融行业的生命线。它直接保障客户资金与敏感信息，是维系信任的基石。一旦泄露，将威胁金融系统稳定。同时，数据安全是合规硬性要求，也是支撑风控决策、业务运行和科技创新的前提。金融机构必须将其视为核心建设任务，构建全方位防护体系。本项目为绿盟科技助力某大型银行构建数据泄露防护体系的典型实践案例。为确保项目高效推进且贴合实际需求，项目采用 “整体规划、分期落地”的科学策略，一期工程聚焦终端数据防泄露建设，旨在筑牢终端这一数据交互的前沿阵地；二期则进一步

拓展至服务器数据防泄露领域，实现数据防护的全方位覆盖。本案例将围绕项目需求痛点、建设方案、实施成效为主线展开阐述，以期为行业提供可借鉴的实践经验。需求痛点如下：

（一）传统终端 DLP 技术局限

若将银行数据安全域比作一张渔网，敏感数据便被这张渔网层层保护，但数据泄露风险犹如渔网漏洞随时可能发生。传统终端 DLP 产品多聚焦于事中事后监控审计，在漏洞出现后才部署监控机制，记录数据泄露轨迹，属于传统补救式防护。因此，传统终端 DLP 无法从根源上解决数据泄露问题，难以满足银行对数据安全的高标准要求。

与此同时，当前市场上的终端 DLP 产品同质化现象严重，功能大多集中于基础监测与管控，缺乏针对银行业务场景的“适配性”，无法满足该行终端数据安全防护的深层次需求、个性化需求。

（二）行方数据安全管理机制仍有提升空间

在本次终端数据安全治理前，该行已建立相对完善的数据安全制度体系，但制度规范与实际落地执行之间仍存在一定差距。由于未能筛选出适配业务场景的终端数据泄露防护产品，不得不依赖人工方式开展数据安全治理工作，这导致治理效率、效果欠佳。同时，该银行机构针对敏感数据管理，在满足监管合规及日常安全管理方面也面临挑战。

二、实施过程

基于对该银行机构需求痛点的分析，协助该银行机构开展敏感数据安全专项整治工作，通过建立健全数据安全制度体系，构建终端信息保护闭环，全面提升终端数据安全防护能力。项目由行方科技部门牵头，协同消保等部门，联合建设并推广终端数据防泄露（DLP）系统。依托该系统，组织开展客户个人敏感数据集中整治行动。对办公终端文件实施“全方位、无死角”扫描，清理大量非必要文件，在全行范围内开展了全面的终端数据安全风险“歼灭战”。

（一）制度完善

在制度完善方面，行方针对多项数据安全相关制度发布与修订，具体包括：

（1）依据《中华人民共和国民法典》《中华人民共和国网络安全法》等法律法规、监管相关要求、行内相关制度及《个人金融信息保护技术规范》等国家标准制定该行数据安全管理办法，旨在加强数据保护与安全保障；

（2）制定针对办公终端个人敏感数据管理机制，其制定源于巩固个人敏感数据集中整治成效、实现新增数据常态化管控的需求，依据相关整治通知及策略；

（3）根据《中华人民共和国个人信息保护法》《数据出境安全评估办法》等法律法规、监管要求、行内相关管理办法及多项行业标准修订了个人信息保护实施细则，以加强个人客户信息管理与安全保障。

（二）关联考核

辅助行方完善终端数据安全制度体系，并将数据安全管理工作纳入相关考核体系，以考核为导向，推动各部门及员工重视数据安全，确保各项制度和措施落到实处。

（三）工具落地

成功实现对全行数十万台 PC 终端的数据防泄露统筹管理，其核心功能包括敏感数据扫描、外发数据管控及重要数据加密保护：

图 11：数据防泄露核心功能示例

- **敏感数据扫描：**覆盖个人敏感信息（银行卡号、身份证号、手机号等）与对公敏感数据（税务登记证、中国统一社会信用代码、组织机构代码、营业执照编号、对公结算账户账号等），确保各类敏感数据都能被精准识别。
- **外发渠道管控：**对打印、光盘刻录、USB 拷贝等数据外发通道实施精准管控，实现重要敏感信息外发禁止，从源头阻断敏感数据外泄的途径。
- **加密保护机制：**采用半透明加密技术，用户可通过客户端右键 “敏感数据处理” 导出功能，主动对扫描结果进行权限化加密保护。未采用强制加密模式，原因是敏感数据经扫描后已按“应删尽删”原则处理，违规存储现象得到根本遏制，无需“一刀切”式强制加密，在保障安全的同时兼顾了用户的办公效率。

除此之外，系统支持文件变动监控、误报处理、扫描结果复用、客户端打包、多模式扫描、终端分组管理、加密授权、扫描进度统计、全员处理情况跟踪及多维度统计分析，为机构级与部门级数据安全员提供统计报表导出功能，强化管理可视化，使数据安全管理工作更加直观、高效。

（四）部署方案

终端数据泄露防护系统服务端采用分级部署架构，设置全行总控管理中心，并在总行机关、各分行、海外分支机构设立分控管理中心，覆盖生产环境、办公环境及灰度测试环境，确保银行各个业务场景下的数据都能得到有效防护。

通过接口与该行 综合办公平台、统一安全认证平台实现联动，通过增量同步机制更新组织架构信息并实现单点认证功能，提升系统的安全性和用户使用的便捷性。

客户端软件部署于终端电脑，依据安全策略实施终端防护。项目覆盖该行总行、全国分支机构，终端点数规模数十万，采用“先试点后推广”的分步实施策略，通过终端安全软件完成客户端批量推送安装，确保客户端部署工作有序、高效进行，最大限度减少对业务的影响。

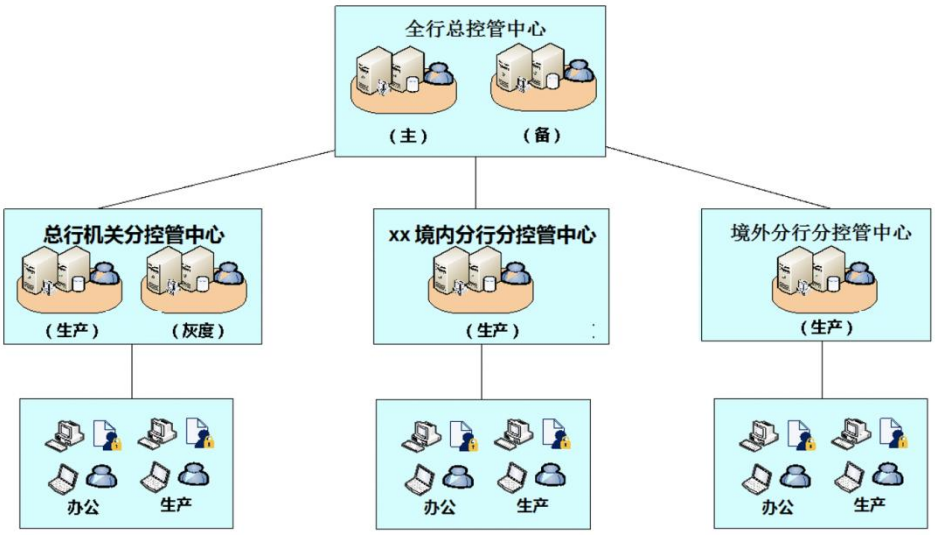


图 12：终端数据泄露防护系统部署示例

三、成果与效益

（一）数据泄露风险全面压降

（1）依托终端数据防泄露系统，结合业务场景与安全需求，在全行建立敏感数据“扫描—通报—核实—清理”常态化闭环管理机制，推动数据安全责任从管理员独担向全员共担转变，革新终端数据防泄露系统应用模式，支撑常态化安全检查开展，实现终端数据安全风险长效管控。

（2）经专项建设工作，涉敏文件压降率取得显著成果，个人客户信息泄露风险得到全面遏制。对确需留存的少量文件，实施“管理+技术”双重管控，严格执行两级主管审批制度，采用加密或等效技术保护措施，确保留存文件的安全性。

（二）健全数据泄露防护体系

（1）随着终端数据安全治理成效显现，内部测试服务器的数据安全风险逐渐凸显，服务器侧数据泄露防护纳入建设重点。通过服务器 DLP 系统补全服务器内数据的全生命周期安全管控。

（2）调试人员申请的测试服务器资源归还至资源池前，需通过系统完成敏感数据扫描并上报结果；调试人员依据扫描报告清理敏感文件，经核验确认清理完成后，测试服务器方可回归资源池供后续申请使用。这一机制从源头上确保了测试服务器在资源流转过程中的数据安全，健全了行内整体数据泄露防护体系建设。

（三）案例优势

（1）采用分布式集群部署模式，保障系统高可用性与稳定性，确保在大规模终端和复杂网络环境下，系统能够持续、稳定地运行；

（2）融合外发管控与加密审批流程，为多场景数据安全使用提供决策支撑，使数据在不同业务场景下的使用都能得到有效的安全保障；

（3）内置行业通用规则库，支持数据有效性校验，实现含校验规则数据零误报，提高了敏感数据识别的准确性，减少了误报对工作的干扰；

（4）通过扫描结果复用、增量扫描、非工作时间扫描、多模匹配等优化方案，大幅提升处理效率，减少系统资源占用，降低对用户办公的影响，实现了安全与效率的平衡；

（5）实现商业秘密信息与保密信息在管理端的隔离管控，按角色分配任务下发、敏感事件处理结果查看及督导权限，确保信息管理的安全性和规范性；

（6）提供扫描结果查询与关键参数统计功能，助力管理者实时掌握数据变化与敏感数据整体态势，为数据安全决策提供有力支持。

（四）案例效果

（1）敏感数据扫描发现后，用户可便捷执行删除、加密等处理操作，提高了数据处理的效率和便捷性；

（2）处理结果实时上报，便于数据安全员全程查阅与督导，实现了对数据处理过程的有效监管；

（3）支持敏感数据多维度统计分析，为考核制度制定与敏感数据整体管控提供数据支撑，使管理工作更加科学、精准；

（4）对暂无法删除的文件实现合规加密留存，并实时掌握加密文件整体情况，确保了留存文件的安全性和可管理性；

（5）与提数平台协同联动，实现提数数据落地终端即加密受控，从数据产生的源头进行安全防护；

（6）经大范围部署及常态化扫描、考核机制运行，全行数十万台终端中，个人敏感信息、对公信息、保密信息等实现 “应删尽删”，仅少量文件经合规加密留存，有效降低了数据泄露风险；

（7）服务器 DLP 上线后，显著提升该行敏感数据治理的全面性与深度，实现了终端与服务器数据安

全防护的无缝衔接。

四、经验与启示

终端 DLP 与服务器 DLP 工具通过“管理+技术”融合模式落地应用，有效助力该银行完成数据治理任务，解决了以往制度落地成本高、执行难度大的问题。

“该体系的落地有效改变了行内数据安全治理模式，实现了从管理员独担责任到全员共同参与的转型。”行方评价不仅充分印证了该数据泄露防护体系在实践中的核心价值与显著成效，更为行业内其他金融机构的数据安全体系建设提供了可复制、可推广的宝贵实践范本，为金融行业数据安全治理的优化升级注入了实践动能。

第二十四节　联软科技 终端敏感数据识别与处置流程的技术创新与合规实践

一、背景介绍

为规范银行业保险业数据处理活动，保障数据安全、金融安全，促进数据合理开发利用，保护个人、组织的合法权益，维护国家安全和社会公共利益，金融监管总局制定了《银行保险机构数据安全管理办法》，其中第四十五条和第四十六条主要针对银行保险机构敏感级及以上数据的安全存储和处置作出了规定。

第四十五条　银行保险机构应当对敏感级及以上数据采取安全存储措施，防止勒索病毒、木马后门等攻击。个人身份鉴别数据不得明文存储、传输和展示。敏感级及以上数据应当实施数据容灾备份，定期进行数据可恢复性验证。

第四十六条　敏感级及以上数据达到使用或者保存期限后，应当采取技术措施及时删除或者销毁，确保数据不可恢复。终端和移动存储介质内的敏感级及以上数据应当采取技术保护措施，确保受控安全访问，介质报废或者重用时，其存储空间数据应当完全清除并不可恢复。

因此，在员工日常办公时，要加强敏感数据的安全加密存储，强化个人身份鉴别数据的保护，采取技术措施及时清理过期数据，加强终端和移动存储介质管理，同时能够防范特定网络攻击。

本案例聚焦江苏江南农村商业银行股份有限公司在严格落实国家金融监督管理总局《银行保险机构数据安全管理办法》过程中，在终端敏感数据识别与处置流程中，呈现的技术创新与合规实践。通过构建全面、高效且创新的数据安全管理体系，江南农村商业银行致力于实现对终端敏感数据的精准识别、妥善处置以及全生命周期的严密保护。这一实践不仅展现了江南农村商业银行在数据安全合规建设方面的创新思维与积极行动，更为整个银行保险行业在数据安全管理领域提供了极具参考价值的成功范例。

（一）机构基本情况

江苏江南农村商业银行股份有限公司经国务院同意、原中国银监会批准，江苏省常州市辖内的 5 家农村中小金融机构（武进农村商业银行、溧阳农村合作银行、常州市区农村信用合作联社、常州市新北区农村信用合作联社、金坛市农村信用合作联社）合并发起设立了江苏江南农村商业银行股份有限公司，是全国首家地市级股份制农村商业银行。自 2009 年成立以来，业务不断拓展，已覆盖多个地区。在数字化转型浪潮中，江南农村商业银行积极拥抱变革，其业务的数字化程度日益加深，终端设备数量众多，涵盖了员工办公终端、自助服务终端以及客户使用的移动终端等。这些终端中存储着海量的敏感数据，如客户的个人身份信息、账户信息、交易记录等，数据安全保护的重要性愈发凸显。

（二）面临的数据安全挑战与问题

1. 严格的合规要求：

《银行保险机构数据安全管理办法》明确规定，银行保险机构必须构建覆盖数据全生命周期和各类应用场景的安全保护机制，尤其对终端敏感数据的识别、分类分级和保护措施提出了极高要求。江南农村商业银行需要确保自身的数据安全管理体系全面符合监管规定，避免因违规而面临处罚。

2. 复杂的安全威胁：

当前网络安全形势严峻，恶意软件窃取、网络钓鱼、黑客攻击等手段层出不穷，终端作为数据产生、传输与使用的关键节点，极易成为攻击目标，面临着敏感数据泄露的巨大风险。例如，一些不法分子通过发送带有恶意链接的邮件或短信，诱使员工点击，从而获取终端中的敏感数据。

3. 广泛的数据分布：

由于江南农村商业银行业务范围广、终端设备数量庞大且分散，导致敏感数据分布广泛，难以实现统一、高效的管理和监控。部分终端中的敏感数据可能长期未被发现和妥善处置，存在较大的安全隐患。

4. 有待提高的员工安全意识：

部分员工对敏感数据的安全重要性认识不足，缺乏必要的数据安全保护知识和技能。在日常工作中，存在随意存储、传输敏感数据的行为，如通过公共邮箱发送包含客户敏感信息的文件，增加了数据泄露的风险。

二、实施过程

（一）制定敏感规则

江南农村商业银行组织专业团队对各类敏感数据进行深入分析，结合自身业务特点和监管要求，制定了详细的第一轮敏感规则扫描策略。例如，对于个人信息，采用行匹配模式，每一行同时匹配身份证号 + 银行卡号、身份证号 + 手机号、姓名 + 手机号等组合，当一个文档包含一定数量（如 5 条）个人信息时，视为敏感文件。在实施过程中，不断根据实际扫描结果和业务需求对敏感规则进行优化和迭代，确保规则的准确性和有效性。

（二）确定扫描策略与范围

扫描策略方面，江南农村商业银行采用一次性扫描与定期扫描相结合的方式。在项目试点初期，执行一次性全盘扫描，快速摸清终端敏感数据的整体情况。在日常运营中，每月定期执行全盘敏感扫描，确保及时发现新产生的敏感数据。扫描范围覆盖所有终端设备的全盘存储，仅排除系统目录，以确保全面且精准地识别敏感数据。扫描的文件类型涵盖文档类（如 doc、docx、txt 等）、表格类（xls、xlsx 等）、文本类、PDF 类、压缩包等常见格式，确保各类可能包含敏感数据的文件都能被有效扫描。

（三）应用多种技术手段

1. 敏感数据发现与分析：

江南农村商业银行引入先进的敏感数据发现与分析技术，采用联软数据防泄露系统和文件安全防护系统。通过关键字匹配、正则表达式、文件智能聚类等多种方式，对终端文件进行深度扫描和分析，精准识别敏感数据。在试点阶段，对部分终端进行扫描，发现了以前未发现的敏感文件，为后续的处置工作提供了明确目标。

2. 透明加解密技术：

江南农村商业银行对重要的业务数据及敏感文件实施数据隔离存储技术。通过下发安全虚拟磁盘策略，对扫描出的敏感文件进行隔离加密存储。在隔离加密的安全虚拟磁盘受控环境中，员工可正常使用加密文件，无需额外复杂操作，不影响工作效率；但当文件被非法拷出受控环境时，将无法打开，有效防止了敏感数据的泄露。

3. 安全 U 盘管控：

在安全 U 盘管理方面，江南农村商业银行优化管理流程，遵循最小可用原则。严格控制安全 U 盘的数量和外发权限，建立完善的安全 U 盘管理流程。对外发操作开启基于敏感等级的审批流程，只有经过授权的人员才能进行敏感数据外发操作，并且详细记录外发日志，以便后续追溯和审计，确保敏感数据外发全程可控。

4. 终端行为审计与控制：

为全面监控终端行为，江南农村商业银行部署了终端行为审计与控制系统。该系统能够对终端的文件读写等行为进行实时审计和管控。例如基于关键字进行识别和管控，一旦发现敏感数据传输行为，立即进行阻断并发出警报。

（四）完善管理策略

1. 员工培训与意识提升：

江南农村商业银行高度重视员工数据安全意识的培养，组织开展了一系列数据安全风险与合规意识培训活动。邀请行业专家进行授课，分享最新的数据安全案例和防范措施，让员工深入了解敏感文件发现与处置的重要性，增强员工对合规要求的理解，提升员工的数据安全意识和操作技能，促使员工积极主动地

参与到数据安全管理工作中。

2. 分级审批与权限管理：

实施严格的敏感文件外发权限管控与分级审批机制。在权限设置上，明确规定仅部门负责人或高级管理人员具备敏感文件外发的申请权限，普通员工无此权限，从源头遏制非必要的外发操作风险。在审批流程上，针对敏感文件外发实行多人审批制度，确保每一笔外发申请都经过多重审核把关，通过权限与审批的双重约束，强化敏感文件外发环节的安全管控，避免因权限滥用或审批疏漏导致的数据泄露风险。

3. 自动处置与定期扫描：

制定完善的自动处置计划，建立敏感文件安全虚拟磁盘策略。对于未及时处置的敏感文件，系统自动将其进行删除，防止敏感文件继续在终端中存在风险。同时，定期执行全盘敏感扫描，每月按时对所有终端进行扫描，及时发现新产生的敏感数据，并按照既定流程进行处理，确保敏感数据始终处于可控状态。

三、成果与效益

（一）数据安全风险显著降低

通过实施上述全面且创新的终端敏感数据识别与处置流程，江南农村商业银行有效发现和处理了大量敏感文件，极大地降低了数据泄露风险。在试点阶段，对扫描出的敏感文件，及时进行了加密、隔离或删除等处置措施，消除了潜在的数据安全隐患。终端行为审计与控制措施的实施，及时发现和阻止了多起异常行为，有效防范了内部人员故意或无意泄露数据的风险。

（二）数据合规性大幅提升

江南农村商业银行严格遵循《银行保险机构数据安全管理办法》的要求，通过精准的敏感数据识别与妥善处置，完成了敏感数据的分类分级和全方位保护，确保自身的数据安全管理完全符合监管要求。在多次监管检查中，江南农村商业银行的数据安全管理工作得到了监管部门的高度认可。通过定期扫描和合规检查，及时发现和整改数据安全隐患，数据合规性水平得到了显著提升，为机构的合规运营提供了坚实保障。

（三）业务运营效率有效提高

透明加解密技术的应用，在保障数据安全的同时，实现了安全与效率的平衡。员工在日常办公中，无需额外复杂操作即可正常使用加密文件，工作效率未受影响。安全 U 盘审批流程的优化，在确保数据安全的前提下，简化了合法外发操作的流程，提高了业务数据交换的效率。

（四）量化指标展示成效

1. 敏感终端占比大幅降低：

在试点阶段，对部分终端进行扫描时发现，存在敏感信息的终端数量较多；经过一段时间的治理后，

这一占比已下降至 10% 以下，降幅十分显著。

2. 员工自主处置敏感文件：

通过工具扫描、处置审计、现场检查发现，员工的终端敏感文件数下降，除了系统自动保护敏感数据之外，90%以上的员工能够从了解安全风险、到理解合规要求、再到参与敏感文件处置，全方位加强了员工和部门的数据安全意识。

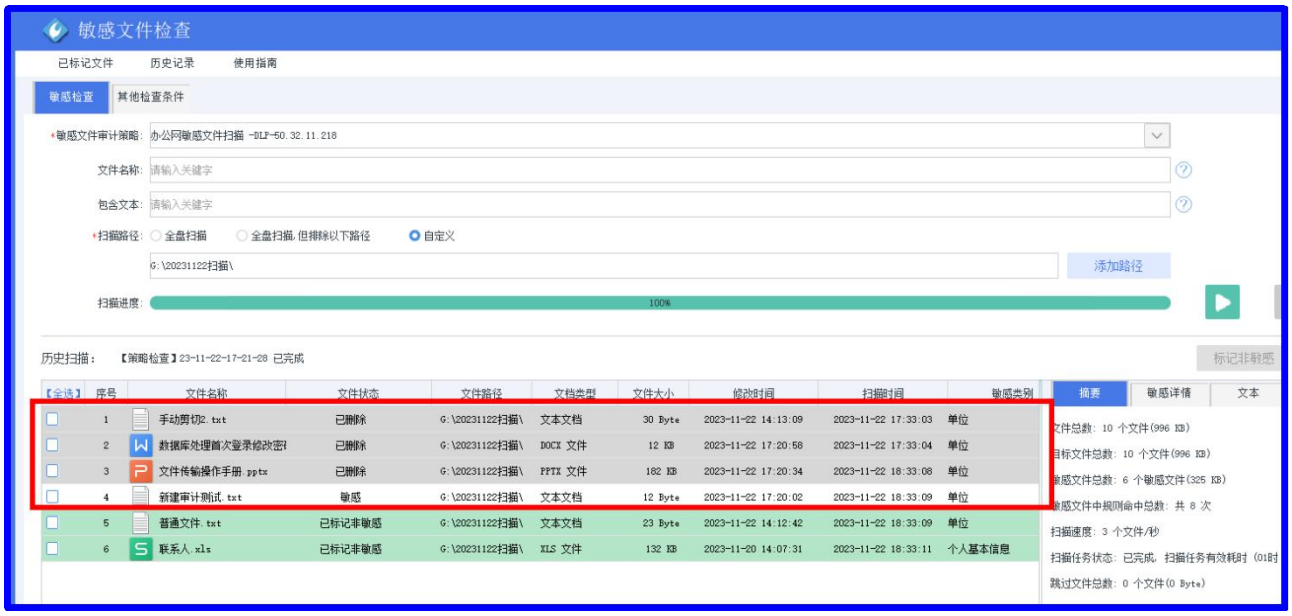


图 13：敏感文件处置功能示例

四、经验与启示

（一）技术与管理深度融合是关键

数据安全管理需要技术手段和管理策略紧密结合，相互支撑。仅依靠技术手段，无法完全解决人为因素带来的风险；仅依靠管理策略，难以应对复杂多变的技术威胁。江南农村商业银行在实践中，将先进的技术手段如敏感数据发现系统、透明加解密技术等与完善的管理策略如员工培训、分级审批制度等有机结合，构建了全面的数据安全防护体系。其他银行保险机构在进行数据安全管理时，也应注重技术与管理的深度融合，根据自身业务特点和风险状况，制定合适的技术和管理方案。

（二）持续优化与迭代是保障

敏感数据管理是一个动态、持续的过程，随着业务的发展、技术的更新以及监管要求的变化，需要不断优化敏感规则、技术手段和管理策略。江南农村商业银行在实施过程中，定期对敏感规则进行评估和优化，根据新出现的安全威胁和业务需求，及时调整技术手段和管理措施。银行保险机构应建立持续优化与迭代的机制，定期对数据安全管理体系进行评估和改进，确保其有效性和适应性。

（三）员工参与是重要环节

员工是数据安全管理的重要参与者，提高员工的数据安全意识和操作技能，能够有效降低人为因素导致的数据泄露风险。江南农村商业银行通过开展丰富多样的培训活动，增强员工对数据安全的重视程度，让员工积极参与到数据安全管理工作中。其他机构应加强员工培训，营造良好的数据安全文化氛围，使员工自觉遵守数据安全规定，从源头上防范数据安全风险。

（四）合规与发展相辅相成

在满足监管合规要求的同时，应充分认识到数据安全管理对业务发展的促进作用。江南农村商业银行通过加强数据安全管理，提升了客户对江南农村商业银行的信任度，为业务创新和拓展提供了有力支持。银行保险机构应将合规要求融入业务发展战略中，以合规促发展，实现合规与发展的良性互动。

（五）行业合作与借鉴意义重大

关注行业最佳实践，积极与同行交流合作，借鉴先进的技术和管理经验，能够快速提升自身的数据安全管理水平。江南农村商业银行在实践过程中，不断探索和创新，形成了自身独特的经验。行业内机构应加强合作与交流，共同分享数据安全管理的经验和成果，推动整个银行保险行业数据安全合规水平的提升。

本案例详细阐述了江南农村商业银行在终端敏感数据识别与处置流程方面的技术创新与合规实践。通过自主创新与积极探索，江南农村商业银行构建了全面、高效的数据安全管理体系，有效应对了数据安全挑战，提升了数据合规性和业务运营效率。案例中的经验与启示为银行保险行业同仁提供了宝贵的参考，有助于推动整个行业在数据安全管理领域不断进步，更好地保障金融数据安全，促进金融行业的稳健发展。

第八章　银行保险机构数据安全合规实践的趋势展望

第二十五节　行业未来数据安全合规发展趋势预测与展望

一、**短期趋势（2025-2027 年）：**

（一）头部机构——“流程化收官、数字化起跑、智能化突破”

- 流程化：董事会－数据安全归口－业务－科技－风险审计的“五层闭环”责任链全部跑通，制度模板完成版本冻结，进入持续优化阶段。
- 数字化：数据目录、策略下发、异常告警全部接入数据安全管理平台，实现“风险可视化、策略可编排、审计可回滚”。
- 智能化：AI 驱动的异常检测（UEBA+大模型）在头部机构落地，平均误报率大幅降低，MTTD 缩短至分钟级。

（二）中小机构——“补短板、打基础”

- 重点仍是制度化和流程化建设：优先完成数据分类分级、数据应用场景和数据生命周期管理、应急演练三项“及格线”任务。

二、**中长期趋势（2028 年 及以后）：**

（一）监管底线常态化

- 《办法》成为行业“最低水位线”，检查方式从“年度大考”变为“日常巡检+随机飞检”。
- 监管机构通过 API 直连接口实时抽查策略合规度，违规即触发快速整改窗口。

（二）管控颗粒度“因场景而异”

- 机构将按业务敏感度（实时交易、批量分析、AI 训练、跨境共享）进一步细化加密强度、脱敏算法、访问频控。
- 形成“一张策略地图”：同一份数据在风控场景用同态加密，在营销场景用差分隐私，在监管报送场景用可控水印。

（三）安全与业务平衡点显性化

- 建立可量化的“合规 ROI”：通过减少罚款、诉讼、品牌损失以及提升数据资产流通效率，反向评估安全投入产出。
- 出现“安全即服务（Sec-as-a-Business）”模式：大型机构把成熟的安全能力组件化输出，中小机构按需订阅，实现“安全成本业务化”。

短期看，头部机构“数字化+智能化”领跑，中小机构“制度+流程”补课；中长期看，《办法》只是底线，真正的竞争在于“场景化颗粒度”与“安全－业务平衡杠杆”的精算能力。

第二十六节　对银行保险机构未来数据安全合规建设的方向指引与行动建议

一、顶层设计：把“合规底线”升级为“治理基线”

（一）董事会承担最终责任，主要负责人是第一责任人，分管负责人是直接责任人。

（二）明确数据安全归口管理部门，赋予横向协调权，建立“业务－数据－安全”三位一体责任制。

（三）将数据安全风险纳入全面风险管理体系，与信用风险、市场风险并列考核，形成“一票否决”机制。

二、数据资产：先“摸清家底”，再“动态保鲜”

（一）建立企业级数据架构，数月内完成全域数据资产登记，形成可视化的“数据资产地图”。

（二）统一使用“核心－重要－一般（敏感/其他）”四级分级标准，配套“内部判定表”解决口径冲突。

（三）每季度执行一次“PDCA 循环”复审，业务变更、系统上线、监管新规触发即时复核。

三、技术体系：从“工具堆”到“统一底座”

（一）建立“数据安全运营平台（DSOP）”，把加密、脱敏、DLP、UEBA 纳管为“服务化组件”。

（二）敏感级及以上系统须通过“三同步”验收：同步规划、同步建设、同步使用；测试环境必须脱敏隔离。

（三）大数据平台实施高可用、多活架构，敏感级数据采用“同城双活+异地灾备”模式，半年演练一次可恢复性。

四、风险监测与应急：7×24 小时“在线闭环”

（一）日志集中化：所有敏感级数据操作日志实时汇聚，留存≥12 个月，支持秒级检索。

（二）告警分级：建立“红橙黄蓝”四色风险雷达，红色事件及时升级至高管群。

（三）应急演练：每半年开展一次数据泄露桌面推演，每季度执行一次模拟攻击回滚，演练报告报送监管备案。

五、成本与人才：轻量化投入，复合型人才

（一）中小机构优先采用“合规 SaaS”订阅，90 天完成轻量级改造，TCO 明显降低。

（二）建立“监管－专业机构－企业”联合培养基地，CDSP、CISP-DSO、CISP-DSG 纳入职称评定，2026 年底前补齐人才缺口。

（三）引入“合规数字员工”自动执行分级打标、日志审计、告警初筛，释放初级岗位人力。

附 录

附录 A 参编机构介绍

一、平安银行股份有限公司

平安银行是中国的一家全国性股份制商业银行，成立于 1987 年，总部位于广东省深圳市。作为中国改革开放后首批成立的股份制商业银行之一，平安银行以其创新的金融服务和高效的运营模式，在中国银行业中占据重要地位。

平安银行坚持以 “中国最卓越、全球领先的智能化零售银行” 为战略目标，坚持 “零售做强、对公做精、同业做专” 战略方针，持续升级零售、对公、资金同业业务经营策略，实现金融高质量发展。平安银行的核心业务包括公司银行、零售银行和金融市场业务。在零售业务方面，平安银行以信用卡、个人理财、消费金融等为主要发展方向，致力于为个人客户提供全面的金融服务。同时，平安银行在供应链金融、贸易融资等领域具有较强的市场竞争力，为企业客户提供个性化的金融解决方案。

平安银行作为中国平安集团的重要成员，充分利用集团的综合金融优势，推动“金融+科技”战略，积极布局数字化转型。通过人工智能、大数据、区块链等技术的应用，平安银行不断提升服务效率和客户体验，打造智能化银行。平安银行以其创新的业务模式、强大的科技实力和国际化视野，正在不断巩固其在中国银行业的领先地位，并致力于为客户提供更加优质、多元的金融服务。

二、华夏银行股份有限公司

华夏银行成立于 1992 年 10 月，是首钢总公司（现已更名为：首钢集团有限公司）独资组建成立的全国性商业银行，是全国唯一一家由制造业企业发起的股份制商业银行。1995 年 3 月，实行股份制改造；2003 年 9 月，首次公开发行股票并上市交易（股票代码：600015），成为全国第五家上市银行；在全国 120 个地级以上城市设立了 44 家一级分行、78 家二级分行，营业网点总数达近千家，形成了“立足经济中心城市，辐射全国”的机构体系，跻身全国系统重要性银行。在 2025 年 7 月公布的英国《银行家》全球 1000 家银行排名中，华夏银行按一级资本排名全球第 47 位。

近年来，在党中央、国务院和北京市委、市政府的领导，华夏银行秉承“服务新时代、建设新华夏”主题，恪守“可持续 更美好”品牌理念，保持战略的坚定性和策略的灵活性，以综合金融服务巩固对公业务基础地位，着力提升数字化和零售业务发展新动能，着力打造绿色金融和财富管理发展新特色，着力建设京津冀、长三角、粤港澳区域发展新高地，加快建设成为有特色、有质量、有竞争力的全国性股份制商业银行，为推进中国式现代化作出更大贡献！

三、浙商银行股份有限公司

浙商银行是十二家全国性股份制商业银行之一，于 2004 年 8 月 18 日开业，总部设在浙江杭州，系全国第 13 家“A+H”上市银行。开业以来，浙商银行立足浙江，放眼全球，稳健发展，已成为一家基础扎实、效益优良、风控完善的优质商业银行。目前浙商银行已在全国 22 个省（自治区、直辖市）及香港特别行政区，设立了 362 家分支机构，实现了对浙江大本营、长三角、粤港澳大湾区、环渤海、海西地区和部分中西部地区的有效覆盖。在英国《银行家》（The Banker）杂志“2024 年全球银行 1000 强”榜单中，浙商银行按一级资本计位列 84 位。中诚信国际给予浙商银行金融机构评级中最高等级 AAA 主体信用评级。

四、河南农村商业银行股份有限公司

河南农商银行系统是河南省资产规模最大、网点数量最多、服务范围最广的省级地方性银行业金融机构。长期以来，河南农商银行系统坚持支农支小支微市场定位，以金融“活水”润泽“三农”沃土，为河南经济社会发展做出突出贡献，是河南农村金融的主力军。截至 2025 年 3 月末，河南农商银行系统共有 1 家省级农商银行（含郑州、新乡、濮阳、济源 4 家中心支行及其辖内县级支行）和 112 家市县农商银行（农信联社），在岗员工 4.44 万人，营业网点 4233 个，覆盖全省所有市县乡（镇）；资产总额 2.68 万亿元，存款余额 2.32 万亿元，贷款余额 1.34 万亿元，存贷款余额和市场份额均居全省银行业金融机构首位。河南农村商业银行股份有限公司是具有独立法人资格的省管重要骨干企业，全面履行对河南农商银行系统“加强党的领导、规范股权管理、提供行业服务、强化风险管控”职能。

五、南京银行股份有限公司

南京银行成立于 1996 年，于 2007 年在沪市主板成功上市，是全国 20 家系统重要性银行之一，位列英国《银行家》杂志公布的全球 1000 家大银行第 86 位。成立 29 年来，始终坚守“做强做精做出特色，致力于打造国内一流的区域综合金融服务商”的战略愿景。南京银行数字银行管理部成立于 2018 年，以数字力量持续推动南京银行“数字化转型”战略建设，强化数字赋能的同时，筑牢数据安全屏障，以“擦亮数字银行名片，成为一流的区域性数字化赋能标杆”为愿景。

六、四川银行股份有限公司

四川银行成立于 2020 年 11 月 7 日，是以攀枝花市商业银行和凉山州商业银行为基础，引入 28 家投资者，采取新设合并方式设立的四川省首家省级法人城市商业银行。四川银行注册资本金 300 亿元，位居全国城市商业银行前列。

四川银行坚守服务地方经济、服务中小企业、服务城乡居民的市场定位，遵循商业银行经营规律，对标行业先进，注重改革创新，以市场化专业化为导向，以“成为客户体验一流、价值创造能力领先的现代金融企业”为愿景，着力支持四川经济社会发展中的重点领域和薄弱环节，支持培育具有区域特色和比较优势的战略性新兴产业，服务成渝地区双城经济圈建设，成为管理规范、经营稳健的现代商业银行和四川

经济社会发展的金融主力军。

七、浙江稠州商业银行股份有限公司

浙江稠州商业银行股份有限公司初创于 1987 年，起源于全球最大的小商品集散中心——义乌，2006 年成功由城市信用社改建为股份制商业银行。经过 30 多年的发展，目前我行共设有分行（管理部）15 家，并发起设立了浙江稠州金融租赁有限公司及 7 家村镇银行，机构遍布全国 9 省（直辖市），已发展为一家资产总额超 3400 亿元、营业网点 270 余家、员工 7000 余名、跻身全球银行 500 强、中国银行业 100 强的现代化股份制商业银行。

因市场而生，为市场服务。作为一家依托市场经济、民营经济成长起来的“市场银行”，市场化的基因早已融入稠州银行的血脉。面对外部发展环境的深刻变化，我行坚守“服务地方经济，服务小微企业，服务城乡居民”的企业使命，秉承“有传统、有担当、有活力、有力量、有梦想、有温度”的“六有银行”企业精神，以“存款立行、管理优行、科技强行、人才兴行”四大战略为总纲，以建设一家“小专新优强”的特色化本土价值银行为愿景，在普惠小微、乡村振兴、国际业务等领域持续打造服务特色和竞争优势，大力推进全方位普惠、数字化转型、便捷化服务，走出了一条差异化、专业化、特色化的发展道路。

凭借稳健经营与实干创新，我行在英国《银行家》杂志 2024 年“全球银行 1000 强”榜单中列第 379 位，“2024 中国银行业 100 强”第 79 位，获评 2024 年“浙商最信赖金融机构样本”、 2023 年度“最佳品牌建设银行”“最佳服务乡村振兴银行”“浙江省民营企业最满意银行”。同时，我行秉承“源于社会、回馈社会、服务社会”的宗旨，积极践行企业社会责任，荣获长三角慈善之星“爱心单位”、义乌市“慈善楷模奖”、“2023 银行业 ESG 普惠金融奖典范案例”、“2023 年度银行家普惠金融服务创新优秀案例”等荣誉。

未来，我行将牢牢把握党建引领这一关键中心，深刻理解“轻资本”“高质量”两个战略本质，深耕细作“四大战略市场”，在“稳中求进”工作总基调中坚定扛起“服务地方经济，服务小微企业，服务城乡居民”的使命担当，不断进阶实现“特色化本土价值银行”的愿景目标。

八、中国太平洋保险（集团）股份有限公司

中国太平洋保险（集团）股份有限公司，简称“中国太保”，成立于 1991 年 5 月 13 日，是一家综合性保险集团，拥有深厚的行业积淀和广泛的市场影响力。作为中国首家 A+H+G（上海、香港、伦敦）三地上市的保险公司，中国太保以“成为行业高质量发展的引领者”为愿景，做精做深主业，拥有人寿保险、财产保险、养老保险、健康保险、农业保险和资产管理等在内的保险全牌照，为近 1.8 亿客户提供全方位风险保障解决方案、财富规划和资产管理服务。

九、人保信息科技有限公司

人保信息科技有限公司，成立于 2022 年 1 月，定位为人保集团公司科技资源整合管理平台、科技服务能力支撑平台、科技运营共享服务平台以及科技服务价值创造平台，致力于建设成为行业领先的保险科技公司，全面赋能集团主业。人保科技以提供优质、便捷、温暖的科技服务为出发点，统筹管理全集团科

技资源，着力构筑科技基础设施、软件研发、数据监控、资源共享、线上运营、新技术应用等方面行业领先的科技服务能力，加快建设科技新军，全面建成集团公司集中共享、自主可控、安全高效的科技体系，优化资源配置，提升管理能力，提高服务水平，形成科技核心竞争力。

十、泰康保险集团股份有限公司

泰康保险集团股份有限公司成立于 1996 年，总部位于北京，至今已发展成为一家涵盖保险、资管、医养三大核心业务的大健康产业头部企业。自 2018 年始，泰康保险集团连续八年荣登《财富》世界 500 强榜单，2025 年位列第 334 位。

泰康保险集团旗下拥有泰康人寿、泰康养老、泰康在线、泰康资产、泰康之家、泰康医疗、泰康口腔等公司。业务范围全面涵盖人身保险、互联网财险、资产管理、企业年金、职业年金、医疗养老、健康管理、商业不动产等多个领域。截至 2025 年 6 月，泰康管理资产规模超 45000 亿元，核心个人有效客户 6100 万人。自成立至 2025 年 6 月，泰康累计理赔金额超 2055 亿元，累计纳税超 978.1 亿元。

初心不改，创新永续，商业向善。长寿时代百岁人生，健康和养老成为最大的民生，泰康致力成为国家大民生工程核心骨干企业，服务国家战略、服务实体经济、服务民生福祉。在传统寿险的“支付端”和“投资端”二维结构中，加入医养康宁的“服务端”，开创“支付+服务+投资”三端协同的“新寿险”模式，打造最佳最优筹资模式，建设高品质无缝衔接的全生命周期医养康宁服务体系。

十一、平安人寿保险股份有限公司

中国平安人寿保险股份有限公司（以下简称“公司”）成立于 2002 年，是中国平安保险（集团）股份有限公司旗下的重要成员。公司坚持以人民为中心，持续打造创新产品、专业服务和多元化渠道，向客户提供全周期人身保险产品和服务，让客户“省心、省时、又省钱”。公司积极履行保险天职使命，为客户寻找理赔的理由，让每个家庭拥有平安，2024 年全年赔付总件数 523.2 万件，赔付总金额达 419.4 亿元。

公司持续深化“4 渠道+3 产品”战略，全面加强渠道建设，提升业务质量，迈向高质量发展。2024 年，平安寿险及健康险业务新业务价值达成 285.34 亿元，可比口径下同比增长 28.8%。2024 年，平安寿险业务品质持续向好，保单继续率稳步提升，13 个月保单继续率同比上升 3.6 个百分点，25 个月保单继续率同比上升 3.9 个百分点。

多渠道综合实力显著增强。2024 年，代理人渠道深化转型，业绩、产能同比提升，可比口径下代理人渠道新业务价值同比增长 26.5%，人均新业务价值同比大幅增长 43.3%，代理人收入同比提升 5.9%；银保渠道聚焦价值经营，新业务价值同比增长 62.7%，不断扩充优质合作网点，提升经营效能；持续推广社区金融服务经营模式，2024 年存续客户 13 个月保单继续率同比提升 5.7 个百分点，新业务价值同比提升近 300%；下沉渠道持续在七个省份推进销售。

“保险+服务”布局持续深化。产品方面，积极响应保险新“国十条”号召，深耕保障、养老、财富三大市场，积极布局普惠保险，满足客户多元化保险需求。服务方面，依托平安集团医疗养老生态圈，稳步深化医疗健康、居家养老、高品质康养社区三大核心服务。截至 2024 年 12 月末，“保险+医疗健康”

方面，平安寿险健康管理已服务超 2,100 万客户，其中新契约客户使用健康管理服务占比近 79%；“保险+居家养老”方面，居家养老服务覆盖全国 75 个城市，累计超 16 万名客户获得居家养老服务资格；“保险+高品质康养社区”方面，平安康养项目已布局 5 个城市，均陆续进入建设阶段，上海及深圳项目拟于 2025 年下半年正式开业。

百年善业，责任为先。公司坚持“专业创造价值”的核心文化理念，携手各利益相关方，追求经济、社会和环境价值最大化可持续发展。公司将 ESG 核心理念和标准融入公司发展战略和经营管理，积极提升金融服务能力和覆盖广度，在绿色金融、服务实体经济、乡村振兴、志愿服务等方面持续投入，专注创造美好明天。

2024 年，公司获“年度卓越寿险公司”“高质量发展保险公司方舟奖”“年度保险保障品牌奖”“最佳客户体验创新保险公司”“年度杰出 ESG 金融企业”等多项大奖。

十二、上海翰纬信息科技有限公司

上海翰纬信息科技有限公司（简称“翰纬科技”）成立于 2004 年，是一家专注于 IT 全栈的专业咨询服务公司。公司总部位于上海，在北京、广州、深圳、成都设有分支机构，目前拥有员工近百人，其中资深咨询师占比超过 70%，多数来自银行、证券、保险、跨国咨询机构等行业的头部企业，具备丰富的实战经验和跨行业视角。

翰纬科技积极支持双态 IT 用户大会、DCMM 金融行业社区技术委员会的活动，并担任网络空间安全协会个人信息保护专委会的创始成员。

翰纬科技的全栈咨询覆盖科技（开发、测试、运维、安全、信创、AI）、数据（数据安全、数据治理）、风险、审计四大领域，能够为客户提供从顶层设计到落地实施的一条龙服务，帮助客户在数字化转型过程中降本增效、稳健合规。

在数据安全领域，翰纬科技提出并践行“上天入地”咨询策略。“上天”指通过常态化的高层对话机制，与各监管机构保持密切沟通，第一时间掌握最新法规、标准与监管口径，并受邀参与官方组织的数据安全专项培训；“入地”则强调方法论到业务场景的闭环落地。翰纬科技依托自研的数据安全治理框架，已在国内数十家头部金融机构成功实施，帮助客户完成数据分类分级、数据安全风险评估、数据安全管理体系建设与规划等关键任务。

为夯实“上天入地”策略，翰纬科技构建了“方法论研究、同业研究、案例实践、专业团队、生态伙伴”五位一体的实施路径，形成了从监管对齐、方案设计到落地运营的完整闭环。未来，翰纬科技将持续以“让数据更安全，让科技更可信”为使命，助力中国数字经济高质量发展。

十三、数责科技（上海）有限公司

数责科技（旗下公众号“合规社”）定位为数据安全与合规领域的专业服务机构，通过社区建设和人才培养推动行业发展。我们打造一个活跃的数据安全与合规行业社区，促进知识交流与合作，同时提供专业的人才培训服务，帮助企业和个人提升数据安全意识和专业能力。

数据安全合规社区建设

数责科技打造的【数据安全合规社区】在行业内拥有广泛的关注度，原创高质量文章阅读量超千万。社区定期分享数据安全领域的最新趋势、合规案例分析、技术实战经验等内容，为从业者提供丰富的学习资源。此外，通过组织线上线下研讨会等活动，搭建起行业专家与从业者之间的互动桥梁，推动数据安全合规领域的共同发展。

数据安全合规培训服务

课程内容丰富多样，满足不同层次和需求的学员，涵盖法规与标准、技术与实务等多个方面。课程体系包括证书类培训课程，如 ISACA、IAPP、CCRC 等，帮助学员获得专业资质。此外，推出一系列实务类课程，如数据合规实战营、数据安全实战营、AIGC 合规实战营、企业出海合规实战营等，帮助学员掌握数据安全合规的实操技巧。

同时，我们积极探索 AI 智能体等前沿技术，致力于将最新技术应用于数据安全与合规领域，为企业提供更智能、更高效的解决方案。

十四、奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，在人员规模、收入规模和产品覆盖度上均位居行业前列。

中国电子信息产业集团（CEC）于 2019 年 5 月战略入股奇安信，奇安信正式成为网络安全国家队。同年 12 月，奇安信成为北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商。2020 年 7 月 22 日，奇安信在科创板挂牌上市；2021 年奇安信当选北京市首批“隐形冠军”企业；2024 年，荣获“世界互联网大会杰出贡献奖”，全球仅 14 家企业获此殊荣，综合实力得到社会和业界的广泛认可。

奇安信深度参与中国电子“PKS”信创体系，创新地把安全能力植入到飞腾 CPU 和麒麟操作系统里，让安全软件在应用层就能利用 CPU 和操作系统的能力，打破 Wintel 体系对中国的影响。目前正对“PKS”体系进行拓展升级，以更好地保障我国重要信息系统的网络安全。

奇安信一直是国家重大活动保障任务的重要支撑力量。公司多次参与国家重大活动网络安保工作，包括全国两会、70 周年阅兵、“一带一路”峰会等。同时，公司也是实战攻防演习的主力军，攻击能力和防守效果全面领先，屡获国家相关部门和客户的认可及感谢。

“十四五”规划收官冲刺，网络安全需求持续释放。奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，助力实现“十五五”良好开局。

十五、北京明朝万达科技股份有限公司

北京明朝万达科技股份有限公司成立于 2005 年，是中国新一代信息安全技术企业的代表厂商，专注于数据安全、公共安全、云安全、大数据安全及加密应用技术解决方案等服务。公司现有员工 700 余人，

总部设于北京，在上海、广州、成都、西安、贵阳、天津、武汉、南京、无锡、长春等地设有分支机构。凭借在数据安全领域取得的优异成就，明朝万达于 2019 年获得中央网信办背景中网投、国家发改委背景国投创合联合投资，并于 2020 年获得中国电科集团（CETC）战略投资。

十六、绿盟科技集团股份有限公司

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 70 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫、企业等各大行业用户提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。其中，网络安全漏洞扫描系统（RSAS）、抗拒绝服务攻击系统（ADS）、网络入侵防护系统（IDPS）、Web 应用防火墙（WAF）、综合威胁探针（UTS）、安全分析、情报、响应和编排（AIRO）、数据保险箱、风云卫大模型等多款产品获国际权威咨询机构推崇。

绿盟科技是国家重点发展的信息安全企业，拥有包括产品与服务资质在内的多项权威认证。同时，绿盟科技发起成立中国网络安全产业联盟，并作为首届理事长单位，致力于推动中国网络安全产业健康良性的发展。目前绿盟科技拥有员工超过 3000 人，其中研发技术人员近 2000 人，拥有各项专利 546 项、软件著作权 620 项。2024 年公司年营业收入 23.58 亿元，年研发投入 6.08 亿元，是中国网络安全行业的头部企业。

十七、深圳市联软科技股份有限公司

深圳市联软科技股份有限公司（简称：联软科技）以成为“保障中国网络安全的中坚力量”为使命，自 2004 年创立以来，始终专注于网络与信息安全管控领域，致力安全与效率统一，极大改变攻防不平衡。基于“构建可控的互联世界”的愿景，2016 年联软科技提出了“可信数字网络架构 TDNA(Trusted Digital Network Architec-ture)”的理念，并基于 TDNA 架构设计了系列安全产品，形成防勒索、防泄密、数字化安全新基建方案，真正帮助政企行业用户构建强大的网络安全防护体系。

经过联软科技团队 20 年持续耕耘，联软产品与解决方案已在证券、银行、运营商、政府、医卫、军队等行业的 4000 多家用户单位中深度应用，为客户、合作伙伴持续提供及时、有效的专业服务。

十八、江苏江南农村商业银行股份有限公司

江苏江南农村商业银行股份有限公司成立于 2009 年 12 月 31 日，系常州辖内原 5 家农村中小金融机构合并发起设立的全国首家地市级股份制农村商业银行。至 2024 年末，我行在常州本地设立 9 家管理行，异地设立 2 家异地分行、22 家异地支行和分理处，共计 197 家网点，实现常州本土全覆盖，并将服务触角延伸至 7 个地级市。在中国银行业协会发布的“2024 年中国银行业 100 强榜单”中，位列第 50 位，在入围农商行中排名第 8 位。主体长期信用等级保持 AAA。

附录 B 监管处罚案例—涉数据安全及个人信息问题

一、国家金融监督管理总局

序号	当事人名称（姓名、职务）	行政处罚决定书文号	违法行为类型	行政处罚内容	作出行政处罚决定机关名称	作出行政处罚决定日期
1	乾县中银富登村镇银行有限公司	咸金罚决字[2025]1 号	1.敏感数据安全管理不到位。	罚款 30 万元	国家金融监督管理总局咸阳监管分局	2025 年 1 月 21 日
2	邓某（时任乾县中银富登村镇银行有限公司综合管理部负责人）	咸金罚决字[2025]1 号	1.敏感数据安全管理不到位。	警告	国家金融监督管理总局咸阳监管分局	2025 年 1 月 21 日
3	李某（时任乾县中银富登村镇银行有限公司综合管理部财务岗）	咸金罚决字[2025]1 号	1.敏感数据安全管理不到位。	警告	国家金融监督管理总局咸阳监管分局	2025 年 1 月 21 日
4	山西农村商业联合银行股份有限公司	晋金管罚决字〔2024〕83 号	1.数据安全管理较粗放，存在数据泄露风险； 2.对网上银行外包管理不到位导致发生二级网络安全事件。	罚款 60 万元	国家金融监督管理总局山西监管局	2024 年 9 月 19 日
5	交银国际信托有限公司	鄂金监罚决字〔2024〕98 号	1.违规对风险项目进行刚性兑付； 2.贷后管理不尽职，导致信托贷款资金违规流入禁止性领域； 3.数据安全管理粗放存在风险隐患；数据治理体系不健全，监管报送数据存在漏报和错报。	罚款 120 万元	国家金融监督管理总局湖北监管局	2024 年 8 月 1 日
6	中国人民人寿保险股份有限公司宁波市分公司	甬金罚决字〔2024〕78 号	1.业务宣传资料不合规； 2.保险代理人培训不合规； 3.违规收集使用个人信息。	警告，并处罚款合计 32 万元	国家金融监督管理总局宁波监管局	2024 年 7 月 1 日
7	交通银行股份有限公司	金罚决字〔2024〕29 号	1.安全测试存在薄弱环节； 2.运行管理存在漏洞； 3.数据安全管理不足； 4.灾备管理不足。	罚款 160 万元	国家金融监督管理总局	2024 年 6 月 3 日

8	湖北银行股份有限公司	鄂金监罚决字〔2024〕6 号	1.流动资金贷款用途监控不审慎； 2.贷后管理不尽职导致个人贷款资金被挪用； 3.项目贷款管理不尽职，资本金未及时到位； 4.贷款管理不审慎，风险暴露不及时； 5.委托债权投资业务不审慎，形成不良； 6.同业投资业务管理不审慎，形成不良； 7.数据安全管理不到位，存在风险隐患； 8.运维管理不到位，存在风险隐患。	罚款 290 万元	国家金融监督管理总局湖北监管局	2024 年 4 月 12 日
9	国泰世华银行（中国）	沪金罚决字[2025]111 号	1.数据安全管控不足。	罚款 30 万元	上海金融监管局	2024 年 4 月 7 日
10	金某（时任国泰世华中国信息科技与数据治理部安全组组长）	沪金罚决字[2025]110 号	1.数据安全管控不足。	警告	国家金融监督管理总局上海监管局	2025 年 4 月 7 日
11	台州银行股份有限公司	台金罚决字〔2024〕8 号	1.理财业务未专营管理问题未真实整改； 2.账外提取浮动管理费，并通过对部分理财产品进行回补操作，以调节产品收益率； 3.风险隔离不到位，浮动管理费与理财资金混用于投资； 4.向银行员工发放个人经营性贷款； 5.贷款管理不到位，个人信贷资金被挪用于购买理财产品且未及时纠偏； 6.贷款管理不到位，流动资金贷款被挪用于固定资产投资； 7.贷款管理严重不审慎，未对异常现象采取相应控制措施； 8.通过不正当方式吸收存款； 9.客户敏感信息保护不到位。	1.对台州银行股份有限公司罚款 385 万元； 2.对林仙兵警告； 3.对邵成渊警告。	国家金融监督管理总局台州监管分局	2024 年 3 月 27 日
12	华美银行（中国）有限公司	沪金罚决字〔2023〕29 号	1.生产环境安全管控不足； 2.生产数据安全管控不足。	责令整改，并处罚款 60 万元	国家金融监督管理总局上海监管局	2023 年 11 月 2 日

13	仲蔚（时任华美中国信息科技部主管）	沪金罚决字〔2023〕28 号	1.对华美中国生产环境安全管控不足及生产数据安全管控不足负直接管理责任。	警告	国家金融监督管理总局上海监管局	2023 年 11 月 2 日
14	中国银行股份有限公司嘉兴市分 行	嘉银保监罚决字(2023)5 号	1.贷后管理不到位，贷款资金实际用途与约定不符； 2.货后管理不到位，贷款资金挪用于购房； 3.项目资本金管理不到位； 4.固定资产贷款用途管理不到位； 5.贴现资金回流； 6.违规泄露客户信息。 沈晓光是前述违法违规行为一的直接责任人；边俞峰是对前述违法违规行为三、四直接负责的主管人员；周亮、傅劲松是对前述违法违规行为五直接负责的主管人员。	对中国银行股份有限公司嘉兴市分行罚款人民币 210 万元，对沈晓光警告，对边俞峰警告，对周亮警告，对傅劲松警告	中国银保监会嘉兴监管分局	2023 年 7 月 7 日
15	浙江农村商业联合银行股份有限公司	浙银保监罚决字(2023)17 号	1.未按照规定及时清退风险统筹资金； 2.清算资金管理运作不够规范，违规截留清算资金收益； 3.违规使用清算资金垫支费用及固定资产等支出； 4.部分高级管理人员未经任职资格核准或在核准前实际履职； 5.报表填报错误； 6.数据安全管理缺失； 7.系统基础元数据漏报错报； 8.对员工贷款行为管理不力； 9.审计履职有效性不足； 10.对监管履职评价提出的问题未整改到位； 11.漏报部分员工及其近亲属入股社员机构情况。	对浙江农村商业联合银行股份有限公司罚款人民币 380 万元	中国银保监会浙江监管局	2023 年 7 月 6 日
16	金华银行股份有限公司	浙银保监罚决字〔2023〕3 号	1.客户信息保护不审慎。	对金华银行罚款人民币 30 万元	中国银保监会浙江监管局	2023 年 3 月 6 日
17	中国平安人寿保险股份有限公司六盘水中心支公司	六银保监罚决字(2022)9 号	1.案防管理不到位，原职工利用职务便利泄露在业务活动中知悉的投保人、被保险人的个人信息。	罚款十万元	中国银行保险监督管理委员会六盘水监管分局	2022 年 10 月 25 日

18	戴华（中国平安人寿保险股份有限公司六盘水中心支公司）	六银保监罚决字(2022)10 号	1.对中国平安人寿保险股份有限公司六盘水中心支公司案防管理不到位，原职工利用职务便利泄露在业务活动中知悉的投保人、被保险人个人信息行为承担主要领导责任的直接责任人。	警告并罚款二万元	中国银行保险监督管理委员会六盘水监管分局	2022 年 10 月 25 日
19	马青青（中国平安人寿保险股份有限公司六盘水中心支公司）	六银保监罚决字(2022)13 号	1.利用职务便利泄露在业务活动中知悉的投保人、被保险人个人信息行为的直接责任人。	禁止进入保险业三年	中国银行保险监督管理委员会六盘水监管分局	2022 年 10 月 25 日
20	刘某阳（中国平安人寿保险股份有限公司六盘水中心支公司）	六银保监罚决字(2022)12 号	1.利用职务便利泄露在业务活动中知悉的投保人、被保险人个人信息行为的直接责任人。	禁止进入保险业十年	中国银行保险监督管理委员会六盘水监管分局	2022 年 10 月 25 日
21	徐无忌（时任中国太平洋财产保险股份有限公司宁夏分公司电网销业务部总经理）	宁银保监罚决字〔2022〕19 号	1.违反法律规定侵犯公民个人信息。	对时任中国太平洋财产保险股份有限公司宁夏分公司电网销业务部总经理徐无忌予以禁止进入保险业 5 年的行政处罚	宁夏银保监局	2022 年 8 月 18 日
22	樊蓉（时任中国人寿财产保险股份有限公司宁夏分公司银川中心支公司创新电子部经理）、刘璐（原中国人寿财产保险股份有限公司宁夏分公司员工）	宁银保监罚决字〔2022〕18 号	1.违反法律规定侵犯公民个人信息。	对时任中国人寿财产保险股份有限公司宁夏分公司银川中心支公司创新电子部经理樊蓉、原中国人寿财产保险股份有限公司宁夏分公司员工刘璐分别予以禁止进入保险业 5 年的行政处罚	宁夏银保监局	2022 年 8 月 17 日

二、中国人民银行

序号	当事人名称（姓名、职务）	行政处罚决定书文号	违法行为类型	行政处罚内容	作出行政处罚决定机关名称	作出行政处罚决定日期
1	贵州道真农村商业银行股份有限公司	遵银罚决字〔2025〕9号	1.提供虚假的统计资料； 2.未履行有关风险管理措施； 3.未按规定收缴假币； 4.未按照规定对异议信息进行标注； 5.提供个人不良信息，未事先告知信息主体本人； 6.未按规定重新识别客户； 7.与身份不明的客户进行交易。	处警告，并处126.5万元罚款	中国人民银行遵义市分行	2025年8月1日
2	平安银行股份有限公司珠海分行	珠银罚〔2025〕1号	1.个别账户交易监测不到位； 2.部分现金从业人员不具备反假专业能力； 3.未按规定履行对信息主体不良信息报送事先告知义务； 4.违反信用信息安全管理要求。	警告，并处罚款88.625万元	中国人民银行珠海市分行	2025年7月30日
4	安徽霍山农村商业银行股份有限公司	六银罚决字〔2025〕3号	1.未按规定履行向人民银行进行单位账户备案义务； 2.未及时采取有效措施防范和处置计算机病毒事件； 3.应急预案和应急演练场景覆盖不全； 4.未按规定将假币解缴中国人民银行分支机构； 5.提供个人不良信息未事先告知信息主体本人。	警告并处以4.6万元罚款	中国人民银行六安市分行	2025年7月23日
5	浙江平湖工银村镇银行股份有限公司	浙银罚决字〔2025〕48号	1.违反账户管理规定； 2.违反反假货币业务管理规定； 3.违反信用信息采集、提供、查询及相关管理规定； 4.未按规定履行客户身份识别义务； 5.未按规定报送大额交易报告或者可疑交易报告。	警告，并处114.75万元罚款	中国人民银行浙江省分行	2025年7月22日
6	浙江温岭联合村镇银行股份有限公司	浙银罚决字〔2025〕46号	1.违反账户管理规定； 2.违反商户管理规定； 3.违反反假货币业务管理规定； 4.违反信用信息采集、提供、查询及相关管理规定； 5.未按规定报送大额交易报告或者可疑交易报告； 6.与身份不明的客户进行交易。	警告，并处294.5万元罚款	中国人民银行浙江省分行	2025年7月22日

7	浙江诸暨联合村镇银行股份有限公司	浙银罚决字〔2025〕42 号	1.违反账户管理规定； 2.违反商户管理规定； 3.违反反假货币业务管理规定； 4.违反信用信息采集、提供、查询及相关管理规定； 5.与身份不明的客户进行交易。	警告，并处 219 万元罚款	中国人民银行浙江省分行	2025 年 7 月 22 日
8	肥乡县农村信用合作联社	邯银罚决字〔2025〕13 号	1.未按规定报送大额交易报告或者可疑交易报告； 2.与身份不明的客户进行交易； 3.未按规定报送账户开立资料； 4.未按规定报送账户撤销资料； 5.未落实网络安全保护责任； 6.向金融信用信息基础数据库报送个人不良信息未事先告知信息主体本人。	警告、罚款 77.9 万元	中国人民银行邯郸市分行	2025 年 7 月 17 日
9	赣州爱信网络小额贷款有限公司	虔银罚决字〔2025〕17 号	1.违反信用信息采集、提供、查询及相关管理规定。	处罚款人民币 19.5 万元	中国人民银行赣州市分行	2025 年 7 月 16 日
10	人保支付科技（重庆）有限公司	渝银罚决字〔2025〕25 号	1.违反账户管理规定； 2.未按规定履行数据安全保护义务； 3.未按规定履行客户身份识别义务。	警告，通报批评，没收违法所得 3698 元，并处 104 万元罚款	中国人民银行重庆市分行	2025 年 7 月 16 日
11	渤海银行股份有限公司南宁分行	桂银罚决字〔2025〕11 号	1.违反数据安全管理规定； 2.未按规定履行客户身份识别义务。	警告，罚款 32.8 万元	中国人民银行广西壮族自治区分行	2025 年 7 月 15 日
12	滨州农村商业银行股份有限公司	滨银罚决字〔2025〕1 号	1.提供个人不良信息，未事先告知信息主体本人； 2.未按规定履行客户身份识别义务。	罚款 375000 元。	中国人民银行滨州市分行	2025 年 7 月 15 日
13	重庆三峡银行股份有限公司	渝银罚决字〔2025〕28 号	1.违反金融统计管理规定； 2.违反账户管理规定； 3.占压财政存款或资金； 4.违反人民币反假规定； 5.违反信用信息采集、提供、查询相关管理规定； 6.未按规定履行客户身份识别义务； 7.未按规定保存客户身份资料和交易记录； 8.未按规定报送大额交易报告或者可疑交易报告； 9.与身份不明的客户进行交易或者为客户开立匿名账户、假名账户。	警告，并处罚款 559.2 万元	中国人民银行重庆市分行	2025 年 7 月 15 日

14	江苏泰兴农村商业银行股份有限公司	苏银罚决字〔2025〕12 号	1.违反金融统计管理规定； 2.违反账户管理规定； 3.违反银行卡收单管理规定； 4.违反人民币流通管理规定； 5.违反信用信息采集、提供、查询及相关管理规定； 6.未按规定履行客户身份识别义务； 7.与身份不明的客户进行交易。	警告，罚款 249 万元	中国人民银行江苏省分行	2025 年 7 月 14 日
15	江苏紫金农村商业银行股份有限公司	苏银罚决字〔2025〕18 号	1.违反金融统计管理规定； 2.违反账户管理规定； 3.违反特约商户管理规定； 4.违反支付受理终端管理规定； 5.违反反假货币业务管理规定； 6.违反人民币流通管理规定； 7.违反信用信息采集、提供、查询及相关管理规定。	警告，没收违法所得 20.22 元，罚款 240 万元	中国人民银行江苏省分行	2025 年 7 月 14 日
16	姚某（时任江苏紫金农村商业银行股份有限公司普惠金融部总经理）	苏银罚决字〔2025〕20 号	对江苏紫金农村商业银行股份有限公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款 10 万元	中国人民银行江苏省分行	2025 年 7 月 14 日
17	宜兴阳羡村镇银行股份有限公司	苏银罚决字〔2025〕14 号	1.违反金融统计管理规定； 2.未按规定报送账户开立资料； 3.未按规定加强银行非柜面转账管理； 4.违反信用信息采集、提供、查询及相关管理规定； 5.未按规定履行客户身份识别义务。	警告，罚款 54.1 万元	中国人民银行江苏省分行	2025 年 7 月 14 日
18	四川三台农村商业银行股份有限公司	川银罚字【2025】16 号	1.违反账户管理规定； 2.未按规定履行客户身份识别义务； 3.未按规定报送大额交易报告或者可疑交易报告； 4.违反反假货币业务管理规定； 5.占压财政存款或者资金； 6.违反信用信息采集、提供、查询及相关管理规定。	给予警告并罚款 85.42 万元	中国人民银行四川省分行	2025 年 7 月 10 日
19	四川荣县农村商业银行股份有限公司	川银罚字【2025】14 号	1.违反账户管理规定； 2.违反信用信息采集、提供、查询及相关管理规定； 3.未按规定履行客户身份识别义务； 4.未按规定报送大额交易报告或者可疑交易报告。	给予警告并罚款 108.74 万元	中国人民银行四川省分行	2025 年 7 月 9 日

20	江西崇义农村商业银行股份有限公司	虔银罚决字〔2025〕1号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反反假货币业务管理规定； 4.占压财政存款或者资金； 5.违反信用信息采集、提供、查询及相关管理规定； 6.未按规定履行客户身份识别义务。	警告，并处罚款人民币87.725万元	中国人民银行赣州市分行	2025年7月8日
21	南康赣商村镇银行股份有限公司	虔银罚决字〔2025〕4号	1.违反信用信息采集、提供、查询及相关管理规定。	处罚款人民币32万元	中国人民银行赣州市分行	2025年7月8日
22	江西信丰农村商业银行股份有限公司	虔银罚决字〔2025〕5号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反金融科技业务管理规定； 4.违反反假货币业务管理规定； 5.占压财政存款或者资金； 6.违反信用信息采集、提供、查询及相关管理规定； 7.未按规定履行客户身份识别义务。	警告，并处罚款人民币107.225万元	中国人民银行赣州市分行	2025年7月8日
23	江西全南农村商业银行股份有限公司	虔银罚决字〔2025〕8号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反金融科技业务管理规定； 4.违反反假货币业务管理规定； 5.占压财政存款或者资金； 6.违反信用信息采集、提供、查询及相关管理规定； 7.未按规定履行客户身份识别义务。	警告，并处罚款人民币98.675万元	中国人民银行赣州市分行	2025年7月8日
24	江西进贤农村商业银行股份有限公司	赣银罚决字〔2025〕18号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反反假货币业务管理规定； 4.违反人民币流通管理规定； 5.占压财政存款或资金； 6.违反信用信息采集、提供、查询及相关管理规定； 7.未按规定履行客户身份识别义务； 8.与身份不明的客户进行交易。	警告，并处罚款人民币215.46万元	中国人民银行江西省分行	2025年7月8日
25	江西湾里农村商业银行股份有限公司	赣银罚决字〔2025〕22号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反金融科技管理规定； 4.违反反假货币业务管理规定； 5.违反信用信息采集、提供、查询及相关管理规定； 6.未按规定履行客户身份识别义务； 7.与身份不明的客户进行交易。	警告，并处罚款人民币154.84万元	中国人民银行江西省分行	2025年7月8日

26	吉安农村商业银行股份有限公司	赣银罚决字〔2025〕26号	1.违反金融统计相关规定； 2.违反反假货币业务管理规定； 3.占压财政存款或资金； 4.违反信用信息采集、提供、查询及相关管理规定； 5.未按规定履行客户身份识别义务； 6.与身份不明的客户进行交易。	警告，并处罚款人民币231.83万元	中国人民银行江西省分行	2025年7月8日
27	南昌昌东九银村镇银行股份有限公司	赣银罚决字〔2025〕30号	1.违反信用信息采集、提供、查询及相关管理规定。	处罚款人民币8万元	中国人民银行江西省分行	2025年7月8日
28	江西进贤农村商业银行股份有限公司	赣银罚决字〔2025〕18号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反反假货币业务管理规定； 4.违反人民币流通管理规定； 5.占压财政存款或资金； 6.违反信用信息采集、提供、查询及相关管理规定； 7.未按规定履行客户身份识别义务； 8.与身份不明的客户进行交易。	警告，并处罚款人民币215.46万元	中国人民银行江西省分行	2025年7月8日
29	江西湾里农村商业银行股份有限公司	赣银罚决字〔2025〕22号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反金融科技管理规定； 4.违反反假货币业务管理规定； 5.违反信用信息采集、提供、查询及相关管理规定； 6.未按规定履行客户身份识别义务； 7.与身份不明的客户进行交易。	警告，并处罚款人民币154.84万元	中国人民银行江西省分行	2025年7月8日
30	吉安农村商业银行股份有限公司	赣银罚决字〔2025〕26号	1.违反金融统计相关规定； 2.违反反假货币业务管理规定； 3.占压财政存款或资金； 4.违反信用信息采集、提供、查询及相关管理规定； 5.未按规定履行客户身份识别义务； 6.与身份不明的客户进行交易。	警告，并处罚款人民币231.83万元	中国人民银行江西省分行	2025年7月8日
31	南昌昌东九银村镇银行股份有限公司	赣银罚决字〔2025〕30号	1.违反信用信息采集、提供、查询及相关管理规定。	处罚款人民币8万元	中国人民银行江西省分行	2025年7月8日
32	江西崇义农村商业银行股份有限公司	虔银罚决字〔2025〕1号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反反假货币业务管理规定； 4.占压财政存款或者资金； 5.违反信用信息采集、提供、查询及相关管理规定；	警告，并处罚款人民币87.725万元	中国人民银行赣州市分行	2025年7月8日

			6.未按规定履行客户身份识别义务。			
33	南康赣商村镇银行股份有限公司	虔银罚决字〔2025〕4号	1.违反信用信息采集、提供、查询及相关管理规定。	处罚款人民币32万元	中国人民银行赣州市分行	2025年7月8日
34	江西信丰农村商业银行股份有限公司	虔银罚决字〔2025〕5号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反金融科技业务管理规定； 4.违反反假货币业务管理规定； 5.占压财政存款或者资金； 6.违反信用信息采集、提供、查询及相关管理规定； 7.未按规定履行客户身份识别义务。	警告，并处罚款人民币107.225万元	中国人民银行赣州市分行	2025年7月8日
35	江西全南农村商业银行股份有限公司	虔银罚决字〔2025〕8号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反金融科技业务管理规定； 4.违反反假货币业务管理规定； 5.占压财政存款或者资金； 6.违反信用信息采集、提供、查询及相关管理规定； 7.未按规定履行客户身份识别义务。	警告，并处罚款人民币98.675万元	中国人民银行赣州市分行	2025年7月8日
36	景德镇昌江九银村镇银行股份有限公司	景银罚决字〔2025〕1号	1.违反金融统计相关规定； 2.违反金融科技管理相关规定； 3.违反信用信息采集、提供、查询及相关管理规定； 4.违反反假货币业务管理规定。	警告并处罚款人民币33万元	中国人民银行景德镇市分行	2025年7月7日
37	酒泉农村商业银行股份有限公司	酒银罚决字〔2025〕1号	1.未按规定确定网络安全负责人、采取防范计算机病毒的技术措施、健全全流程数据安全管理制度、明确数据安全负责人或管理机构、向行业主管部门定期报送风险评估报告； 2.未按规定履行个人信用信息基础数据库安全管理规定； 3.未按规定履行客户身份识别义务。	警告，罚款23.95万元	中国人民银行酒泉市分行	2025年7月3日
38	山东沂源农村商业银行股份有限公司	淄银罚决字〔2025〕7号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反人民币反假有关规定； 4.违反信用信息采集、提供、查询及相关管理规定； 5.未按规定履行客户身份识别义务； 6.未按规定保存客户身份资料和交易记	警告，罚款1238000元	中国人民银行淄博市分行	2025年7月3日

			录。			
39	长安汽车金融有限公司	渝银罚决字〔2025〕12号	1.违反信用信息采集、提供、查询相关管理规定。	处53万元罚款	中国人民银行重庆市分行	2025年7月3日
40	李某达（时任长安汽车金融有限公司运营服务部征信管理岗工作人员）	渝银罚决字〔2025〕13号	对长安汽车金融有限公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询相关管理规定。	处4.1万元罚款	中国人民银行重庆市分行	2025年7月3日
41	罗某（时任长安汽车金融有限公司运营服务部总经理）	渝银罚决字〔2025〕14号	对长安汽车金融有限公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询相关管理规定。	处4.2万元罚款	中国人民银行重庆市分行	2025年7月3日
42	王某娇（时任长安汽车金融有限公司运营服务部征信管理岗工作人员）	渝银罚决字〔2025〕15号	对长安汽车金融有限公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询相关管理规定。	处4.1万元罚款	中国人民银行重庆市分行	2025年7月3日
43	重庆小雨点小额贷款有限公司	渝银罚决字〔2025〕9号	1.违反信用信息采集、提供、查询相关管理规定。	处249.1万元罚款	中国人民银行重庆市分行	2025年7月3日
44	陈某帆（时任重庆小雨点小额贷款有限公司运营管理部运营管理总监）	渝银罚决字〔2025〕11号	对重庆小雨点小额贷款有限公司以下违法行为负有 责任： 1.违反信用信息采集、提供、查询相关管理规定。	处14.2万元罚款	中国人民银行重庆市分行	2025年7月3日
45	曹某（时任重庆小雨点小额贷款有限公司风控中心首席风控官）	渝银罚决字〔2025〕10号	对重庆小雨点小额贷款有限公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询相关管理规定。	处14.2万元罚款	中国人民银行重庆市分行	2025年7月3日
46	分宜九银村镇银行股份有限公司	余银罚决字〔2025〕1号	1.未按规定报送账户变更、撤销等资料； 2.提供个人不良信息未事先告知信息主体本人； 3.未按规定办理网络安全等级保护定级。	警告并处罚款人民币9万元	中国人民银行新余市分行	2025年7月2日

47	王某（时任浙江德清农村商业银行仙潭路支行企业信用报告查询员）	湖银罚决字〔2025〕3号	对浙江德清农村商业银行以下行为负有责任： 违反信用信息采集、提供、查询及相关管理规定。	处0.5万元罚款	中国人民银行湖州市分行	2025年7月1日
48	博白县农村信用合作联社	玉银罚决字〔2025〕1号	1.提供个人不良信息，未事先告知信息主体本人； 2.未准确报送个人信用信息。	罚款312.78万元	中国人民银行玉林市分行	2025年6月30日
49	山东芝罘齐丰村镇银行股份有限公司	烟银罚决字〔2025〕7号	1.违反账户管理规定； 2.违反人民币反假有关规定； 3.违反信用信息采集、提供、查询及相关管理规定； 4.未按规定履行客户身份识别义务。	警告，罚款390000元。	中国人民银行烟台市分行	2025年6月30日
50	湖北荆州农村商业银行股份有限公司	荆银罚决字[2025]1号	1.违反人民币银行结算账户管理规定； 2.违反网络安全管理规定； 3.违反数据安全管理规定； 4.违反反假货币业务管理规定； 5.占压财政存款或资金； 6.违反国库科目设置和使用规定； 7.违反信用信息采集、提供、查询及相关管理规定； 8.与身份不明的客户进行交易。	警告，罚款38.5万元	中国人民银行荆州市分行	2025年6月27日
51	湖北宜都农村商业银行股份有限公司	宜银罚决字[2025]5号	1.违反人民币银行结算账户管理规定； 2.违反网络安全和数据安全管理规定； 3.违反国库科目设置和使用规定； 4.违反大额交易可疑交易报告管理规定。	警告，罚款23万元	中国人民银行宜昌市分行	2025年6月27日
52	湖北孝感农村商业银行股份有限公司	孝银罚决字〔2025〕3号	1. 违反金融统计管理规定； 2. 违反人民币银行结算账户管理规定； 3. 违反反假货币业务管理规定； 4. 违反国库科目设置和使用规定； 5. 违反信用信息采集、提供、查询及相关管理规定； 6. 与身份不明的客户进行交易。	警告，罚款55万元	中国人民银行孝感市分行	2025年6月26日
53	湖北红安农村商业银行股份有限公司	黄冈银罚决字〔2025〕3号	1.违反金融统计管理相关规定； 2.违反账户管理相关规定； 3.违反网络安全管理相关规定； 4.违反数据安全管理相关规定； 5.违反流通人民币管理相关规定； 6.未按规定履行客户身份识别义务。	警告，并处罚款人民币47.5万元	中国人民银行黄冈市分行	2025年6月26日
54	江西井冈山农村商业银行股份有限公司	吉银罚决字〔2025〕4号	1.提供虚假的或者隐瞒重要事实的统计报表； 2.未按规定报送账户开立资料； 3.与身份不明的客户进行交易；	给予警告，并处罚款人民币92.5万元	中国人民银行吉安市分行	2025年6月26日

			4.集中支付退回业务处理不及时，占压财政资金； 5.提供个人不良信息，未事先告知信息主体本人；			
55	井冈山九银村镇银行有限责任公司	吉银罚决字〔2025〕7号	1.提供虚假的或者隐瞒重要事实的统计报表； 2.提供个人不良信息，未事先告知信息主体本人； 3.未按规定将假币解缴中国人民银行分支机构。	给予警告，并处罚款人民币31.4万元	中国人民银行吉安市分行	2025年6月26日
56	海尔消费金融有限公司	青银罚决字〔2025〕6号	1.违反信用信息采集、提供、查询及相关管理规定。	处罚款25万元	中国人民银行青岛市分行	2025年6月25日
57	山东聊城润昌农村商业银行股份有限公司	聊银罚决字〔2025〕1号	1.违反账户管理规定； 2.违反商户管理规定； 3.占压财政资金； 4.违反信用信息采集、提供、查询及相关管理规定； 5.与身份不明的客户进行交易。	警告，罚款518000元，没收违法所得3306.04元。	中国人民银行聊城市分行	2025年6月25日
58	会宁会师村镇银行有限责任公司	白人银罚决字[2025]1号	1.临时存款账户超期使用； 2.取消账户许可后开立企业基本存款账户未在当日内向人民银行备案； 3.未建立系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全事件应急预案，且未开展相关演练； 4.未建立全流程数据安全管理制度和开展重要数据处理活动风险评估，未向监管机构上报数据处理活动风险评估报告。	警告并处1万元罚款	中国人民银行白银市分行	2025年6月24日
59	广信农村商业银行股份有限公司	饶银罚决字〔2025〕4号	1.提供虚假的或者隐瞒重要事实的统计报表； 2.未按规定报送账户开立资料； 3.办理货币收付、清分业务人员不具备判断和挑剔假币专业能力； 4.发现假币而不收缴； 5.与身份不明的客户进行交易； 6.提供个人不良信息，未事先告知信息主体本人。	给予警告，并处罚款94.88万元	中国人民银行上饶市分行	2025年6月24日
60	奉新九银村镇银行股份有限公司	宜银罚决字〔2025〕1号	1.提供个人不良信息，未事先告知信息主体本人； 2.未按规定采取防范计算机病毒的技术措施。	警告，并处罚款人民币8万元	中国人民银行宜春市分行	2025年6月19日

61	江西奉新农村商业银行股份有限公司	宜银罚决字〔2025〕2号	1.与身份不明的客户进行交易； 2.对外支付残缺、污损人民币； 3.提供个人不良信息，未事先告知信息主体本人； 4.集中支付退回业务处理不及时，占压财政资金； 5.未按规定对关键网络设备提供持续安全维护。	警告，并处罚款人民币41.3万元	中国人民银行宜春市分行	2025年6月19日
62	江西铜鼓农村商业银行股份有限公司	宜银罚决字〔2025〕5号	1.错报单位活期存款统计数据； 2.未按规定重新识别客户身份； 3.未按规定为公众兑换残缺、污损人民币； 4.提供个人不良信息，未事先告知信息主体本人； 5.未按规定留存网络设备核心路由器网络日志不少于六个月。	警告，并处罚款人民币52.45万元	中国人民银行宜春市分行	2025年6月19日
63	河北临西农村商业银行股份有限公司	邢银罚决字〔2025)4号	1.未按规定报送大额交易报告或者可疑交易报告； 2.违反信用信息采集、提供、查询相关管理规定。	罚款53万元	中国人民银行邢台市分行	2025年6月16日
64	上饶农村商业银行股份有限公司	饶银罚决字〔2025〕1号	1.提供虚假的或者隐瞒重要事实的统计报表； 2.未按规定报送账户开立资料； 3.办理货币收付、清分业务人员不具备判断和挑剔假币专业能力； 4.未按规定将假币解缴中国人民银行分支机构； 5.占压财政存款或者资金； 6.与身份不明的客户进行交易； 7.提供个人不良信息，未事先告知信息主体本人。	给予警告，并处罚款96.81万元	中国人民银行上饶市分行	2025年6月13日
65	抚顺银行股份有限公司	辽银罚决字〔2025〕7号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.未按规定落实反电信网络诈骗相关管理规定； 4.未按照规定落实数据安全相关管理规定； 5.违反反假币业务管理规定； 6.违反信用信息采集、提供、查询及相关管理规定； 7.未按规定履行客户身份识别义务； 8.未按规定报送大额交易报告或可疑交易报告。	警告，罚款184.174万元	中国人民银行辽宁省分行	2025年6月12日

66	交通银行股份有限公司辽宁省分行	辽银罚决字〔2025〕12号	1.违反金融统计相关规定； 2.未按规定落实网络安全相关管理规定； 3.未按规定落实数据安全相关管理规定； 4.违反信用信息采集、提供、查询及相关管理规定； 5.未按规定履行客户身份识别义务。	警告，罚款116万元	中国人民银行辽宁省分行	2025年6月12日
67	中国光大银行股份有限公司沈阳分行	辽银罚决字〔2025〕9号	1.违反金融统计相关规定； 2.未按规定落实反电信网络诈骗相关管理规定； 3.未按规定落实网络安全相关管理规定； 4.违反人民币流通管理规定； 5.违反信用信息采集、提供、查询及相关管理规定； 6.未按规定履行客户身份识别义务。	警告，罚款229.15万元	中国人民银行辽宁省分行	2025年6月12日
68	厦门金美信消费金融有限责任公司	厦门银罚决字〔2025〕1号	1.违反信用信息采集、提供、查询及相关管理规定。	处罚款82万元	中国人民银行厦门市分行	2025年6月11日
69	日照岚山农村商业银行股份有限公司	日银罚决字〔2025〕3号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反数据安全管理规定； 4.未按规定履行客户身份识别义务。	警告，罚款820000元	中国人民银行日照市分行	2025年6月10日
70	山西神池农村商业银行股份有限公司	忻银罚决字(2025)3号	1.违反人民币结算账户管理规定； 2.提供虚假的或者隐瞒重要事实的统计报表； 3.未按规定建立全流程数据安全管理制度； 4.未按规定在开展数据处理活动时加强风险监测。	警告，并处罚款人民币262200元	中国人民银行忻州市分行	2025年6月9日
71	广发银行股份有限公司青岛分行	青银罚决字〔2025〕4号	1.违反信用信息采集、提供、查询及相关管理规定； 2.违反反假货币业务管理规定； 3.未按规定履行客户身份识别义务。	警告，并处罚款30.2万元	中国人民银行青岛市分行	2025年6月9日
72	郑州珠江村镇银行股份有限公司	豫银罚决字〔2025〕9号	1.违反金融统计相关规定； 2.违反网络安全管理规定； 3.违反人民币流通管理规定； 4.违反反假货币业务管理规定； 5.违反信用信息采集、提供、查询及相关管理规定； 6.未按规定履行客户身份识别义务。	警告，罚款53.9万元	中国人民银行分行	2025年6月6日
73	陈某全（时任郑州珠江村镇银行股份有限公司合规与风	豫银罚决字〔2025〕11号	对郑州珠江村镇银行股份有限公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款1.3万元	中国人民银行分行	2025年6月6日

	险管理部（原风险管理部）副总经理（主持工作）					
74	青岛农村商业银行股份有限公司	青银罚决字〔2025〕2号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反人民币流通管理规定； 4.违反反假货币业务管理规定； 5.违反信用信息采集、提供、查询及相关管理规定； 6.未按规定履行客户身份识别义务。	警告，并处罚款91.2万元	中国人民银行青岛市分行	2025年6月3日
75	山东郯城农村商业银行股份有限公司	临银罚决字〔2025〕8号	1.违反账户管理规定； 2.违反流通人民币管理规定； 3.违反人民币反假有关规定； 4.违反信用信息采集、提供、查询及相关管理规定； 5.未按规定履行客户身份识别义务。	警告，罚款440000元。	中国人民银行临沂市分行	2025年5月30日
76	山东沂水农村商业银行股份有限公司	临银罚决字〔2025〕10号	1.违反账户管理规定； 2.违反流通人民币管理规定； 3.违反信用信息采集、提供、查询及相关管理规定； 4.未按规定履行客户身份识别义务。	警告，罚款554000元。	中国人民银行临沂市分行	2025年5月30日
77	福建智云融资担保有限责任公司	闽银罚决字〔2025〕9号	1.违反信用信息采集、提供、查询及相关管理规定。	罚款224万元	中国人民银行福建省分行	2025年5月29日
78	陈某花（时任闽侯县农村信用合作联社下属青口信用社主任助理兼客户经理）	闽银罚决字〔2025〕10号	对闽侯县农村信用合作联社以下违法行为负有责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款1万元	中国人民银行福建省分行	2025年5月29日
79	王某（时任福建智云融资担保有限责任公司产品运营总监）	闽银罚决字〔2025〕12号	对福建智云融资担保有限责任公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款9万元	中国人民银行福建省分行	2025年5月29日
80	吴某燕（时任福建智云融资担保有限责任公司业务支持副总监）	闽银罚决字〔2025〕14号	对福建智云融资担保有限责任公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款2万元	中国人民银行福建省分行	2025年5月29日
81	闽侯县农村信用合作联社	闽银罚决字〔2025〕	1.违反信用信息采集、提供、查询及相关管理规定。	罚款5万元	中国人民银行福建省分行	2025年5月29日

		15 号				
82	中国民生银行股份有限公司威海分行	威银罚决字〔2025〕3 号	1.违反金融统计相关规定； 2.违反账户管理规定； 3.违反信用信息采集、提供、查询及相关管理规定； 4.未按规定报送大额交易报告或者可疑交易报告。	警告，罚款685000元。	中国人民银行威海市分行	2025 年 5 月 29 日
83	池州九华农村商业银行股份有限公司	池银罚决字〔2025〕1 号	1.涉农贷款统计有误； 2.单位银行结算账户开立未核准； 3.未按规定办理网络安全等级保护定级工作； 4.未健全全流程数据安全管理制度； 5.未按规定设置“待结算财政款项”科目核算经收的预算收入款项； 6.占压财政存款或者资金； 7.与身份不明的客户进行交易。	警告，并处罚款 54.15 万元人民币	中国人民银行池州市分行	2025 年 5 月 27 日
84	张某（时任重庆海尔小额贷款有限公司数字科技部大数据总监）	渝银罚决字〔2025〕4 号	对重庆海尔小额贷款有限公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询相关管理规定。	处 7.1 万元罚款	中国人民银行重庆市分行	2025 年 5 月 21 日
85	重庆海尔小额贷款有限公司	渝银罚决字〔2025〕3 号	1.违反信用信息采集、提供、查询相关管理规定。	处 48 万元罚款	中国人民银行重庆市分行	2025 年 5 月 21 日
86	海南宜信普惠小额贷款有限公司	琼银罚决字〔2025〕3 号	1.违反信用信息采集、提供、查询及相关管理规定。	罚款 62.5 万元	中国人民银行海南省分行	2025 年 5 月 20 日
87	伍某润（时任海南宜信普惠小额贷款有限公司执行总经理）	琼银罚决字〔2025〕4 号	对海南宜信普惠小额贷款有限公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款 10 万元	中国人民银行海南省分行	2025 年 5 月 20 日
88	遂平中原村镇银行股份有限公司	豫银罚决字〔2025〕6 号	1.违反信用信息采集提供、查询及相关管理规定。	罚款8.4万元	中国人民银行河南省分行	2025 年 5 月 15 日
89	永善县农村信用合作联社	昭银罚决字〔2025〕3 号	1.账户变更后未及时向人民银行报告； 2.违反账户管理规定； 3.违反网络安全管理规定； 4.违反数据安全管理规定； 5.占压财政资金； 6.向金融信用信息基础数据库提供非依法公开的个人不良信息，未事先告知信息主体本人；	警告，并处罚款 71 万元	中国人民银行昭通市分行	2025 年 5 月 15 日

			7.未按照规定处理征信异议； 8.未按照规定履行客户身份识别义务；			
90	睢县农村信用合作联社	商银罚决字〔2025〕1号	1.违反金融统计管理规定； 2.违反人民币银行结算账户管理规定； 3.未按照规定报送可疑交易报告； 4.违反人民币流通管理规定； 5.违反反假货币业务管理规定； 6.违反信用信息采集、提供、查询及相关管理规定； 7.违反网络安全管理规定； 8.违反数据安全管理规定。	警告、罚款64.4万元	中国人民银行商丘市分行	2025年5月14日
91	贾某娜（时任睢县农村信用合作联社信用管理部主任）	商银罚决字〔2025〕3号	对睢县农村信用合作联社以下违法行为负有责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款1.4万元	中国人民银行商丘市分行	2025年5月14日
92	云南汇泽融资租赁有限公司	云银罚决字〔2025〕4号	1.违反信用信息采集、提供、查询相关管理规定。	处10万元罚款	中国人民银行云南省分行	2025年5月14日
93	段某刚（时任云南汇泽融资租赁有限公司风险管理部门负责人）	云银罚决字〔2025〕5号	对云南汇泽融资租赁有限公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询相关管理规定。	处2万元罚款	中国人民银行云南省分行	2025年5月14日
94	三门峡农村商业银行股份有限公司	三银罚决字〔2025〕1号	1.违反金融统计相关规定； 2.违反银行结算账户管理规定； 3.未按规定履行客户身份识别义务； 4.违反反假货币业务管理规定； 5.违反信用信息采集、提供、查询及相关管理规定； 6.违反网络安全管理规定。	警告，罚款55.1万元	中国人民银行三门峡市分行	2025年5月8日
95	威海蓝海银行股份有限公司	威银罚决字〔2025〕1号	1.违反信用信息提供相关管理规定。	罚款209000元。	中国人民银行威海市分行	2025年5月7日
96	中国邮政储蓄银行股份有限公司临高县支行	儋州银罚决字〔2025〕1号	1.违反信用信息采集、提供、查询及相关管理规定。	罚款3.5万元	中国人民银行儋州市分行	2025年5月6日

97	王某川（时任中国邮政储蓄银行股份有限公司临高县支行副行长）	儋州银罚决字〔2025〕2号	对中国邮政储蓄银行股份有限公司临高县支行以下违法行为负有直接责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款0.7万元	中国人民银行儋州市分行	2025年5月6日
98	宝马汽车金融（中国）有限公司	银京罚决字【2025】45号	1.未经同意查询个人信息或企业的信贷信息。	处罚款90.1万元	中国人民银行北京市分行	2025年4月27日
99	*Min（时任宝马汽车金融服务中国区IT总监）	银京罚决字【2025】46号	1.未经同意查询个人信息或企业的信贷信息。	处罚款10万元	中国人民银行北京市分行	2025年4月27日
100	浙江庆元泰隆村镇银行股份有限公司	丽银罚决字〔2025〕1号	1.违反金融统计管理规定； 2.违反支付结算管理规定； 3.违反反假货币业务管理规定； 4.违反信用信息采集、提供、查询及相关管理规定； 5.与身份不明的客户进行交易或者为客户开立匿名账户、假名账户。	警告，并处56.4万元罚款	中国人民银行丽水市分行	2025年4月25日
101	恩施兴福村镇银行股份有限公司	恩银罚决字〔2025〕1号	1.违反信用信息采集、提供、查询及相关管理规定。	罚款人民币2万元	中国人民银行恩施州分行	2025年4月25日
102	广西宾阳农村商业银行股份有限公司	桂银罚决字〔2025〕4号	1.违反反假货币业务管理规定； 2.违反信用信息采集、提供、查询及相关管理规定； 3.未按规定履行客户身份识别义务； 4.未按规定报送可疑交易报告。	罚款人民币83.9万元	中国人民银行恩施州分行	2025年4月18日
103	广西农村商业联合银行股份有限公司	桂银罚决字〔2025〕6号	1.违反信用信息采集、提供、查询及相关管理规定。	罚款人民币23万元	中国人民银行广西壮族自治区分行	2025年4月18日
104	雷某炘（时任广西农村商业联合银行股份有限公司风险管理部风险系统管理室经理）	桂银罚决字〔2025〕7号	对广西农村商业联合银行股份有限公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款4.6万元	中国人民银行广西壮族自治区分行	2025年4月18日
105	广西乐业农村商业银行股份有限公司	百银罚决字〔2025〕1号	1.违反金融统计管理规定； 2.未履行对异常账户、可疑交易的风险监测和相关处置义务； 3.违反账户管理规定； 4.违反人民币反假规定； 5.违反信用信息采集、提供、查询相关管	罚款人民币186.9万元	中国人民银行百色市分行	2025年4月14日

			理规定； 6.未按规定履行客户身份识别义务； 7.与身份不明的客户进行交易。			
106	湖南平江农村商业银行股份有限公司	岳银罚决字〔2025〕3号	1.超过期限向中国人民银行报送账户撤销资料； 2.未履行尽职调查义务； 3.未履行对异常账户、可疑交易的相关处置义务； 4.未按规定收缴假币； 5.相关人员不具备反假专业能力； 6.未按规定将假币解缴中国人民银行分支机构； 7.将经收的预算收入款项转入“待结算财政款项”以外其他科目或账户； 8.占压财政存款或者资金； 9.提供个人不良信息，未事先告知信息主体本人； 10.未按规定履行客户身份识别义务； 11.未采取必要的防计算机病毒技术措施； 12.未采取必要措施保障数据安全； 13.未按规定开展风险评估和报送评估报告。	警告，罚款人民币48.3万元	中国人民银行恩施州分行	2025年4月2日
107	云南景洪农村商业银行股份有限公司	西银罚决字〔2025〕1号	1.违反银行结算账户开立管理规定； 2.违反银行非柜面转账管理规定； 3.未按规定收缴假币； 4.占压财政存款或者资金； 5.违反安全管理要求，征信查询用户调岗离岗未及时停用； 6.违反安全管理要求，征信查询用户未按规定备案； 7.提供个人不良信息，未事先告知信息主体本人。	警告，并处罚款71.5万元	中国人民银行西双版纳州分行	2025年4月2日

108	湖南平江农村商业银行股份有限公司	岳银罚决字〔2025〕3号	1.超过期限向中国人民银行报送账户撤销资料； 2.未履行尽职调查义务； 3.未履行对异常账户、可疑交易的相关处置义务； 4.未按规定收缴假币； 5.相关人员不具备反假专业能力； 6.未按规定将假币解缴中国人民银行分支机构； 7.将经收的预算收入款项转入“待结算财政款项”以外其他科目或账户； 8.占压财政存款或者资金； 9.提供个人不良信息，未事先告知信息主体本人； 10.未按规定履行客户身份识别义务； 11.未采取必要的防计算机病毒技术措施； 12.未采取必要措施保障数据安全； 13.未按规定开展风险评估和报送评估报告。	警告，罚款48.3万元	中国人民银行岳阳市分行	2025年4月2日
109	中国民生银行股份有限公司岳阳分行	岳银罚决字〔2025〕5号	1.提供虚假的统计报表； 2.未制定网络安全事件应急预案； 3.未采取必要的防计算机病毒技术措施； 4.未按照规定开展风险评估和报送评估报告； 5.对外支付残缺、污损人民币。	警告，罚款10.4万元	中国人民银行岳阳市分行	2025年4月2日
110	徐某芳（时任山西沁水农村商业银行股份有限公司信贷管理部经理）	晋市银罚决字〔2025〕12号	1.未经同意查询个人信息（企业）信贷信息。	罚款人民币4万元。	中国人民银行晋城市分行	2025年3月21日
111	王某（时任山西沁水农村商业银行股份有限公司营业部征信查询用户）	晋市银罚决字〔2025〕13号	1.未经同意查询个人信息（企业）信贷信息。	罚款人民币3万元	中国人民银行晋城市分行	2025年3月21日
112	王某（时任山西沁水农村商业银行股份有限公司营业部征信授权用户）	晋市银罚决字〔2025〕14号	1.未经同意查询个人信息（企业）信贷信息。	罚款人民币3万元	中国人民银行晋城市分行	2025年3月21日

113	高平市太行村镇银行股份有限公司	晋市银罚决字〔2025〕1号	1.未按规定向人民银行报送账户撤销资料； 2.与身份不明的客户进行交易； 3.网络安全技术措施不到位； 4.数据处理活动风险监测不到位； 5.数据安全保障措施不到位。	警告，并处罚款人民币26万元	中国人民银行晋城市分行	2025年3月21日
114	广西通盛融资租赁有限公司	桂银罚决字〔2025〕3号	1.违反信用信息采集、提供、查询及相关管理规定。	罚款人民币27万元	中国人民银行广西壮族自治区分行	2025年3月19日
115	王某予（时任广西通盛融资租赁有限公司授信评审部风险经理、征信管理岗牵头人）	桂银罚决字〔2025〕1号	对广西通盛融资租赁有限公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款人民币5.4万元	中国人民银行广西壮族自治区分行	2025年3月19日
116	覃某凤（时任广西通盛融资租赁有限公司授信评审部副总经理（主持工作）、总经理））	桂银罚决字〔2025〕2号	对广西通盛融资租赁有限公司以下违法行为负有责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款人民币5.4万元	中国人民银行广西壮族自治区分行	2025年3月19日
117	大方富民村镇银行股份有限公司	毕银处罚〔2025〕1号	1.提供虚假的或者隐瞒重要事实的统计报表； 2.超过期限或未向中国人民银行报送账户开立资料； 3.未按规定收缴假币； 4.向金融信用信息基础数据库提供个人不良信息，未事先告知信息主体本人； 5.未按规定重新识别客户； 6.未制定内部安全操作规程； 7.未采取有效措施防范计算机病毒、网络攻击和网络侵入； 8.未明确数据安全负责人和管理机构，未落实数据安全保护责任； 9.未及时处置数据安全漏洞风险； 10.未向有关主管部门报送风险评估报告且数据安全管理风险评估报告要素不全。	警告，罚款59.6万元	中国人民银行毕节市分行	2025年3月13日
118	河南许昌许都农村商业银行股份有限公司	许银罚决字〔2025〕1号	1.违反金融统计管理规定； 2.违反银行结算账户管理规定； 3.违反信用信息采集、提供、查询及相关管理规定；	警告，并处罚款人民币62.1万元	中国人民银行许昌市分行	2025年3月10日

			4.未按照规定履行客户身份识别义务。			
119	浙江武义农村商业银行股份有限公司	浙银罚决字〔2025〕23 号	1.违反金融统计管理规定； 2.违反账户管理规定； 3.违反商户管理规定； 4.违反反假货币业务管理规定； 5.违反信用信息采集、提供、查询及相关管理规定； 6.未按规定履行客户身份识别义务； 7.未按规定报送大额交易报告或者可疑交易报告。	警告，处 314 万元罚款	中国人民银行浙江省分行	2025 年 3 月 4 日
120	江西金溪农村商业银行股份有限公司	抚银罚决字〔2025〕1 号	1.违反信用信息采集、提供、查询及相关管理规定。	罚款人民币 13 万元	中国人民银行抚州市分行	2025 年 2 月 28 日
121	虞某峰（时任江西金溪农村商业银行股份有限公司信贷管理部总经理）	抚银罚决字〔2025〕2 号	对江西金溪农村商业银行股份有限公司以下违反行为负有责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款人民币 2 万元	中国人民银行抚州市分行	2025 年 2 月 28 日
122	徐某（时任江西金溪农村商业银行股份有限公司新区支行行长）	抚银罚决字〔2025〕3 号	对江西金溪农村商业银行股份有限公司以下违反行为负有责任： 1.违反信用信息采集、提供、查询及相关管理规定。	罚款人民币 2 万元	中国人民银行抚州市分行	2025 年 2 月 28 日
123	江苏涟水太商村镇银行股份有限公司	淮安银罚决字〔2025〕1 号	1.违反信用信息采集、提供、查询及相关管理规定。	罚款 17.1 万元	中国人民银行淮安市分行	2025 年 2 月 27 日
124	中信银行股份有限公司日照分行	日银罚决字[2025]1 号	1.违反金融统计相关规定； 2.未按规定履行客户身份识别义务； 3.未及时处置数据安全漏洞风险； 4.未制定网络安全事件应急预案。	警告，罚款 540000 元	中国人民银行日照市分行	2025 年 1 月 8 日
125	阿拉善左旗黄河村镇银行股份有限公司	阿银罚决字[2024】04 号	1.违反网络安全、数据安全管理规定； 2.未按规定将假币解缴中国人民银行分支机构； 3.未按规定履行阪忮少客户身份识别义务； 4.违反金融统计管理规定。	警告，并处罚款人民币 94 万元	中国人民银行阿拉善盟分行	2024 年 12 月 16 日
126	贵安新区发展村镇银行股份有限公司	贵银罚决字〔2024〕4 号	1.提供个人不良信息，未事先告知信息主体本人。	罚款 33.65 万元	中国人民银行贵州省分行	2024 年 7 月 23 日

127	河南义马农村商业银行股份有限公司	三银罚决字[2023]3号	1.违反账户管理相关规定； 2.（1）未按规定履行客户身份识别义务；（2）未按规定报送大额交易或可疑交易报告；（3）与身份不明的客户进行交易； 3.违反货币金银管理相关规定； 4.(1)违反消费者金融信息保护管理规定；（2）违反金融消费权益保护管理规定。	警告，罚款46.35 万元	中国人民银行三门峡市分行	2023 年 10 月 23 日
128	中国银行股份有限公司福建省分行	福银罚决字(2023)35号	1.违反个人金融信息保护规定； 2.违反金融消费争议解决的相关规定； 3.涉诈账户管理不到位。	警告，并处罚款 179 万元	中国人民银行福州中心支行	2023 年 6 月 13 日
129	厦门银行股份有限公司	福银罚决字〔2023〕10 号	1.违反个人金融信息保护规定； 2.违反金融营销宣传管理规定； 3.违反信息披露管理规定； 4.违反金融消费者保护内部控制及其他管理规定； 5.未准确报送金融统计数据； 6.银行结算账户未按规定备案； 7.涉诈账户管理不到位； 8.将外包服务机构发展为特约商户； 9.商户实名制落实不到位； 10.个别现金从业人员判断和挑别假币专业能力不足； 11.误收假币未按规定报告； 12.未按规定解缴假币； 13.冠字号码采集、存储不符合规定； 14.延解、占压和挪用收纳的预算收入； 15.国库集中支付退回资金未及时退回国库，占压财政存款或者资金； 16.向金融信用信息基础数据库提供个人不良信息未事先告知信息主体本人； 17.未在规定期限内处理异议，异议处理超期； 18.因系统原因发生未经授权查询个人信用报告； 19.个人征信系统征信管理员用户兼任查询用户； 20.未准确、完整、及时报送个人信用信息； 21.未按规定履行客户身份识别义务； 22.未按规定保存客户交易记录； 23.未按规定报告大额交易和可疑交易报告。	警告，没收违法所得767.17 元，并处罚款764.6 万元。	中国人民银行福州中心支行	2023 年 1 月 16 日

附录 C 电子联合会 DCMM 金融行业社区技术委员会

中国电子信息行业联合会是经民政部注册登记的全国性社会团体，简称电子联合会。2014 年 6 月 28 日在北京成立。会长由工业和信息化部原党组成员、副部长陈肇雄担任，常务副会长由中芯国际集成电路制造有限公司原董事长周子学担任，秘书长由工业和信息化部原运行监测协调局副局长高素梅担任。目前有个人会员 8 名、单位会员 4775 家。

2018 年 3 月，由工信部牵头指导、全国信标委大数据标准工作组组织制定并正式发布了国内首个数据管理领域国家标准《数据管理能力成熟度评估模型》（GB/T 36073-2018）。并委托中国电子信息行业联合会全面负责 DCMM 国家标准在全国范围内的贯标和评估工作。

为有力推动 DCMM 在金融行业的推广和实施工作，由 19 家金融机构及相关企业联合向中国电子信息行业联合会（简称：联合会）发起成立“DCMM 金融行业社区技术委员会（简称：DCMM 金数社）”，经联合会会长办公会研究，于 2024 年 6 月 14 号批复同意筹备。经过前期的筹备工作，在 2024 年 6 月 28 日召开的联合会第二届第五次理事会议上审议通过， DCMM 金数社正式成立！

DCMM 金数社属于联合会分支机构，旨在通过推动金融行业内 DCMM 贯标企业及相关各方更好的交流协作，促进产业合作和创新发展，提升金融机构数据管理及应用水平。 DCMM 金数社致力于成为金融行业最具活跃度和影响力的 DCMM 交流平台！

理事会是全体成员大会闭会期间的日常执行机构，由各理事单位共同选举产生包括理事长、副理事长等人员，与各理事单位委派的联络人共同组成，负责指导秘书处工作。

秘书处设在上海翰纬信息科技有限公司，由秘书长、常务副秘书长以及副秘书长组成，负责理事会、秘书处及社区的日常运营工作 ，包括会议召开、活动组织、联络沟通等，并向理事会汇报。

刘巍 （国家工业信息安全发展研究中心 人工智能所副所长）担任秘书长，左天祖 （上海翰纬信息科技有限公司 创始人）担任常务副秘书长。

为了深入了解与分析我国金融机构当前在数据安全管理方面的实践情况，发现其中的难点和挑战，由 DCMM 金融行业社区指导，双态 IT 论坛、翰纬科技与安全牛共同发起“2024 金融机构数据安全合规建设”问卷调查活动。整体通过对 44 家金融机构的问卷调研，全面评估了金融机构在数据安全组织架构、分类分级、管理、技术、个人信息保护、风险监测等多个关键领域的实践和挑战。并组织行业专家进行《2024 年度金融机构数据安全合规建设调查研究报告》编写工作，报告已于 10 月份正式对外发布。

为促进 DCMM 在金融领域的深入应用与实践，进一步加强行业内外交流与合作。2024 年 9 月 24 日，由工业和信息化部信息技术发展司、中国电子信息行业联合会指导，国家工业信息安全发展研究中心承办，DCMM 金融行业社区技术委员会协办的“金融行业 DCMM 座谈会”在北京召开。会议邀请到相关主管部门及 40 余位来自银行、保险、证券等金融机构的数据管理相关部门负责人参加本次座谈会。

2024 年（第三届）数据治理年会暨博览会于 11 月 17 日-19 日在北京展览馆举办。DCMM 金融行业社区技术委员会特别举办“金融行业分论坛暨 DCMM 金融行业社区技术委员会成立仪式”活动。本次分论坛主题为：以评促建：DCMM 助力金融数据治理效能提升。本次会议邀请到联合会副秘书长，国家工业信息安全发展研究中心总工程师等领导，以及金融机构数据治理相关专家 50 余人参会，会上特别举办了 DCM

M 金融行业社区技术委员会成立仪式。

在中国电子信息行业联合会的支持与指导下，作为 DCMM 金融行业社区技术委员会最重要的年度成果，在 2024 年第三届数据治理年会金融行业分论坛上，DCMM 金融行业社区正式启动《金融行业 DCMM 研究报告（2024）》项目编写工作，邀请来自银行、保险、证券、基金等金融机构的数据治理相关专家共同进行参与编写，本年度报告计划在 2025 年发布。后续，报告计划每年编写一期，旨在全面分析、评估和提升金融行业在数据管理方面的综合能力。

在数字化时代，数据已成为金融机构的核心资产，数据管理的质量直接关系到业务的竞争力和客户体验。数据管理部作为金融机构的“数据中枢”，承担着数据治理、安全保障、价值挖掘等重要职责。2025 年 3 月 15 日，由 ITSS 数据中心运营管理工作组、DCMM 金数社主办的双态 IT 雁栖湖论坛·数据管理主题对话在北京召开，本次对话由 DCMM 金数社区理事长李保旭主持，邀请来自邮储银行、中华财险、泰康养老、北京农商银行等单位的专家参与，话题围绕数据管理在金融机构中的战略地位、数据治理与数据治理提升的关键挑战、数据安全与合规管理的重要性等当下热点问题展开。

2025 年 3 月 28 日，为贯彻落实国家有关高质量数据集开发利用的决策部署，同时考虑贵阳在大数据领域的发展基础和优势，国家工业信息安全发展研究中心联合贵州省大数据发展管理局，在贵阳市召开金融领域高质量数据标注座谈会，DCMM 金数社作为本次会议的承办单位之一。会议邀请了国家金融监督管理总局贵州监管局党委委员、副局长袁震，贵州省大数据发展管理局党组书记、局长，兼任贵州省政府副秘书长朱宗尧，省大数据局党组成员、省信息中心党委书记焦德禄等领导出席，同时 12 家单位参与本次座谈会。

在国家金融监管新政持续深化与落实的背景下，银行及保险机构正面临着数据安全合规建设方面的严峻挑战。为有效应对这一挑战，《银行保险机构数据安全管理办法》应运而生，旨在为金融机构提供一套系统化、全面化的数据安全管理框架。2025 年 5 月 23 日，由 DCMM 金数社区组织召开数据安全专题研讨会，邀请 80 余位来自金融机构的实战专家、顶尖技术服务商以及咨询机构的专业人士，重点讨论银行保险业在数据安全合规方面遇到的十大关键问题，包括但不限于数据分类分级、数据安全评估、数据安全风险监测等。

人工智能技术正以前所未有的深度与广度重塑全球金融业的格局，如何构建一套既能有效驾驭 AI 技术红利，又能前瞻性防范其潜在风险、确保技术应用负责任的监管框架与治理体系已成为金融监管机构和行业共同面临的紧迫课题。2025 年 6 月 27 日，由 DCMM 金数社组织召开金融 AI 监管趋势研讨会，旨在共同深入剖析当前 AI 在金融领域应用面临的核心监管痛点与最新趋势，本次会议邀请到网信办、国家工业信息安全发展研究中心、邮政储蓄银行、光大银行等单位参会。

2025 年 8 月 29 日，在 2025 中国国际大数据产业博览会期间，为聚焦国家数据工作部署，由国家数据局数字科技和基础设施建设司指导，贵州省大数据发展管理局主办，特别开展数据标注系列活动，期间将举办“金融行业数据标注与高质量数据集建设”交流活动，国家工业信息安全发展研究中心、DCMM 金数社等联合承办本次会议，并邀请到贵州大数据局、人民银行贵州分行等单位领导参会，嘉宾主要围绕金融行业数据标准与高质量数据集建设探讨相关政策、技术、产业发展。


数字
安全

版权声明