兴化农商银行聚焦五个维度 做好客户信息保护审计



江苏兴化农商银行开展客户信息保护全生命周期专项审计,通过多维度核查排查出中小银行普遍存在的共性风险点,配套形成全链条闭环整改方案。

当前,中小银行客户信息保护工作普遍面临资源投入、治理模式与技术支撑层面的结构性短板,不少机构难以兼顾业务发展与数据安全管控,在实际操作中容易出现管控盲区。如何结合自身业务实际与风险控制水平,精准识别管理薄弱环节、推动问题闭环整改,最终实现审计环节“推动风险最小化、合规效益最大化”的目标,是行业内普遍关注的现实议题。

对此,兴化农商银行在内部开展客户信息保护专项审计,结合自身经营管理实际制定针对性审计方案,通过多维度审计方法体系完成全流程排查,为中小银行落地客户信息保护审计工作提供了可参考的实践样本。

全维度搭建审计框架

该行本次专项审计以客户信息全生命周期为主线,覆盖采集、存储、使用、加工、传输、提供、公开、删除八大核心处理环节,从制度、流程、系统、资料、人员五个维度同步推进排查,全面检验现有客户信息保护控制措施的实际运行有效性,排查体系中存在的漏洞与潜在隐患。

审计过程中综合运用五类标准化审计方法,实现对各环节的无死角核查。一是文档审阅法,审查制度体系。对照客户信息保护相关法律法规与监管要求,逐项核查三方面内容:是否制定并持续迭代客户信息保护相关制度体系;是否建立完善个人客户信息保护组织架构,明确各层级内设部门与相关岗位的管理职责;核查隐私政策、用户授权书、第三方合作协议等核心文本,确认其中采集目的、数据保密、权责划分等内容表述准确清晰。

二是穿行测试法,审查业务流程。一方面模拟客户从开户、日常使用、信息修改到账户注销的全业务生命周期,验证各环节是否符合信息保护技术控制要求与业务操作规范;另一方面模拟客户信息从采集到删除的八大处理活动,核查各阶段操作是否符合管理规定,相关控制措施是否执行到位。

三是渗透测试法,审查系统数据。通过系统渗透测试、数据建模等科技手段,重点核查数据库加密技术应用、访问权限设置、日志留存完整性、对外提供数据管控、数据共享合规性及网络传输安全控制措施等落实情况,防范客户信息被非法获取、违规提供或传输泄露。

四是抽样核查法,审查资料内容。按比例抽取部分客户信息开户材料、日志查询记录、数据修改记录、外部调阅申请资料等,核查相关操作流程是否规范、内容要素是否齐全,确认客户信息录入、修改、调阅等操作均符合制度要求。

五是现场检查法,审查人员执行。现场询问客户信息保护管理部门与业务责任部门相关人员,确认其是否清晰掌握岗位权责,是否熟知个人客户信息保护工作的方针、目标与原则,检验全行对该项工作的重视程度;现场排查员工及外包人员工作场所,核查客户资料保管是否符合规定,是否存在外包人员违规接触客户敏感信息、客户资料易被第三方获取等风险隐患。

审计排查发现典型问题

该行本次专项审计排查出多项行业内中小银行普遍存在的共性风险点,主要集中在六个方面。

一是制度体系建设不完善,部分机构未按监管规定制定数据分类分级制度,风险管理部门未将数据安全纳入全面风险管理体系,且未定期开展数据安全风险评估;

二是信息系统操作账号全生命周期管理不到位,部分业务系统中,转岗或离职人员的操作账号权限未及时调整或注销,违反“业务必需”和“最小权限”的管控原则;

三是客户信息安全影响评估机制缺失,相关责任部门在对客户信息进行加工、汇聚融合前,未按要求开展客户信息安全影响评估,存在后续客户信息泄露、客户合法权益受损的潜在风险;

四是客户信息日常使用操作不规范,部分部门通过网络渠道群发包含客户卡号、身份证号、手机号、住址等敏感隐私信息的文件,信贷客户资料存放管理不合规,客户经理私自留存客户征信报告等敏感影像档案,相关资料易被第三方违规获取;

五是合作业务协议内容存在漏洞,理财、贵金属等代销业务的合作协议文本不完善,未明确约定客户信息处理规则及违约追责条款,缺失数据处理的期限、目的和方式,合作结束后数据返还或删除要求,以及违约后的赔偿责任等核心内容;

六是数据存储介质销毁环节管控缺位,未制定明确的数据存储介质销毁操作规程,未对资料存储介质销毁全过程进行监督管控,相关处置记录不完整。

针对性整改优化措施

针对排查出的各类问题,兴化农商银行结合监管要求与自身实际业务情况,制定了全链条闭环整改方案,明确各环节责任主体与落地要求。

完善制度体系,强化合规基础。客户信息保护管理部门对照《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》等法律法规及监管规定,补充完善数据分类分级相关制度与配套操作流程,保障制度的完备性、及时性与可操作性。

规范账号管理,严控访问权限。人力资源部门应建立岗位变动信息同步机制,及时将员工调岗、离职信息等推送至各相关业务部门,各业务部门应建立常态化系统账号权限清理机制,确保员工岗位变动或离职时,对应操作权限能够及时、准确地调整或收回。

落实影响评估,前置风险防范。客户信息保护管理部门应将客户信息安全影响评估嵌入产品创新、业务拓展、技术应用的全流程中,将评估作为项目立项或上线的前置必要环节,对评估排查发现的高风险点,必须制定并落实有效的风险缓释措施后方可推进相关工作。

加强资料管控,严防信息泄密。信息发布部门应严格执行客户信息“最小必要”原则,强化对外发布信息的多级审核机制,涉及客户敏感信息的文件严禁通过网络渠道群发;客户信息保护管理部门应联合各业务责任部门加大现场检查频次,将客户信息保护纳入常规检查范围,通过定期例会、问题通报、专项培训等方式持续强化员工信息安全意识,提升全员合规操作水平。

优化合作协议,明确权责边界。客户信息保护责任部门应全面梳理、迭代完善代销业务相关协议范本,清晰界定与合作机构在客户信息保护方面的权利义务,在协议中明确数据处理的期限、目的、方式,以及违约后的赔偿责任等关键条款,同步对各类合作类数据处理活动定期开展安全评估,确保合作过程中客户信息保护标准不降低。

规范存储介质销毁机制,杜绝数据残留。数据管理部门应加强对报废设备的全流程处置管理,重点强化存储介质销毁环节管控,明确销毁流程、技术标准与监督要求,建立从介质报废、数据清除、物理销毁到记录归档的全流程闭环管理机制,保障敏感数据彻底、安全销毁。

兴化农商银行本次客户信息保护专项审计,精准击中了中小银行普遍存在的资源不足、管控碎片化、合规边界模糊等共性痛点。它跳出了传统单点排查的零散模式,以客户信息全生命周期八大处理环节为主线,通过文档审阅、穿行测试、渗透测试等五类标准化方法,实现了从制度流程到系统人员的无死角穿透核查,同时配套形成可直接落地的全链条闭环整改方案。这不仅帮助机构补上了数据分类分级、账号权限动态清理、第三方合作权责划分等关键短板,更给资源有限的广大中小银行提供了一套低成本、可复制的客户信息保护审计落地框架,推动行业在业务扩张与数据安全之间找到合规效益最大化的平衡路径。 (通讯员 华平)