【数据治理实践】第十期：数据安全管理

前言

上期文章，我们分享了数据目录的重要价值和管理实践，本期我们将围绕数据安全从概念、规范和技术等进行深入介绍。众所周知，随着数字化时代到来，数据驱动业务正成为未来发展创新的主要模式之一，数据也被认为是创造价值的核心资产。与此同时，随着业务互联互通，数据资产正被机构内外不法组织或个人所觊觎，数据安全管理面临严峻考验。

如何避免机构内部贩卖信息、员工离职泄露信息、第三方交易被共享数据等行为发生、防止开发测试过程的敏感数据违规使用等数据风险，金融机构急需从传统抵御网络攻击为中心的安全策略，增加以数据保护为中心的新型策略，才能有效对应《银行业金融机构数据治理指引》（简称“《指引》”）等法律法规的数据安全监管要求。

监管要求

第十八条 银行业金融机构应当制定全面科学有效的数据管理制度，包括但不限于组织管理、部门职责、协调机制、安全管控、系统保障、监督检查和数据质量控制等方面。

第二十四条 银行业金融机构应当建立数据安全策略与标准，依法合规采集、应用数据，依法保护客户隐私，划分数据安全等级，明确访问和拷贝等权限，监控访问和拷贝等行为，完善数据安全技术，定期审计数据安全。

银行业金融机构采集、应用数据涉及到个人信息的，应遵循国家个人信息保护法律法规要求，符合与个人信息安全相关的国家标准。

第二十六条 银行业金融机构应当建立数据应急预案，根据业务影响分析，组织开展应急演练，完善处置流程，保证在系统服务异常以及危机等情景下数据的完整、准确和连续。

——《银行业金融机构数据治理指引》

1. 数据安全治理介绍

1. 1 数据安全治理目标和理念

金融机构围绕“让数据使用更安全”的核心目标，重点关注数据的使用权限和应用场景，建设数据安全管理体系，主要理念如下：

- 数据安全管理不能仅关注单一产品或技术平台，应该覆盖数据所有使用环节和应用场景安全；
- 满足数据安全的基本需求，包括数据保护、数据合规、敏感数据管理等；
- 重视数据分级分类、数据角色授权、数据安全过程场景化管理。
- 为了有效实践数据安全目标和理念，机构必须打造数据安全闭环管理体系，推动数据安全治理体系持续改善。

1. 2 数据安全管理框架

图*1*-数据安全管理框架

1. 3 数据安全与网络安全差异

引入数据安全并非取代网络安全，而是在传统网络安全体系基础上，有效地实现对核心数据的安全管控。数据安全是在网络安全提供的有效边界防御基础上保障数据安全。

差异对比	数据安全	网络安全
目标	以数据安全使用为目标	以网络安全防护，免受攻击为目标
对象	内部人员或准内部人员行为的安全管控为主要对象	以对外部黑客或入侵者防控为主要对象
理念	以数据分级分类为基础，以信息合理、安全流动为目标	以区域隔离、网络安全域划分为目标
技术	以信息使用过程的安全管理和技术支撑	以边界防护为主要安全手段
融合	安全技术和流程深度结合	流程管理与安全技术相对分离

表 *1*-数据安全与网络安全的差异对比

1. 4 数据安全与数据治理差异

差异对比	数据安全	数据治理
发起部门	安全合规部门/业务部门在驱动	数据管理部门/业务部门在驱动
应用目标	让数据使用中更安全，保障数据的安全使用和共享，实质也是保障数据价值	数据驱动商业发展，发挥或发掘企业数据价值
产出内容	通过企业数据分级分类，针对性加强访问安全策略、数据合规安全措施	通过数据的清洗和规范的过程，提升数据质量
资产管理	明确数据分级分类的安全标准，识别敏感数据资产分布，呈现敏感数据资产的访问状况和授权报告	通过元数据管理，赋予数据上下文和含义的参考框架

表 *2*-数据安全治理与数据治理的差异对比

2. 数据安全需求分析

2. 1 数据安全外部监管合规要求

- 《指引》要求金融业机构建立数据安全策略与标准并执行落地，保障机构数据的完整性、准确性和连续性。
- 《中华人民共和国网络安全法》发布及配套陆续出台了《数据出境管理办法》、《个人信息安全管理规范》、《个人隐私数据管理办法》、《大数据安全标准》等相关法律法规，对数据安全有明确合规要求；

- 《国家信息安全等级保护2.0》由公安部牵头推动，要求国境内信息系统进行安全保护等级保护，根据信息系统在国家安全、经济建设、社会生活的重要程度，以及其遭破坏对国家安全、社会秩序、公共利益以及公民、法人和其他组织合法权益的危害程度等因素定级；
- 在国外开展业务，还需了解海外数据安全相关法律法规，如欧盟《通用数据保护条例》（General Data Protection Regulation，简称GDPR）等。
- 更多数据安全法律法规可以参考附件-数据安全法律法规清单。

2.2 数据安全内部管理提升需求

当前许多机构积极开展数字化战略，利用大数据、云计算、人工智能、物联网等技术重塑商业和运营模式。随着数字化深入业务，业务上下游数据流转、汇集、不断创新价值，对数据完整性、保密性和可用性提出更多安全方面的管理提升需求。

3. 数据安全对象识别

3. 1 数据资产安全盘点

数据安全对象的识别一般可以通过数据资产盘点的方式进行。我们建议数据资产的安全盘点要遵循外部法律、法规的合规要求实施，盘点过程中需要特别注意对个人隐私信息和重要数据的定义。数据资产安全盘点的产出是将期望识别的安全对象的关键属性与现有系统字段建立映射，具体的映射过程可以在信息系统的数据字典设计阶段进行。

数据安全对象识别环节的侧重点是数据资产分级分类

- 数据资产分类依据数据来源、内容和用途，数据资产分级按照数据价值、内容敏感程度、影响和分发范围不同，划分相应数据机密级别。
- 经过数据分级分类，识别核心数据资产，投入更多资源精细化管理数据安全，使数据安全在敏捷共享和安全可控之间达到平衡。
- 对于敏感数据资产，按其所有者（部门、系统、管理人员等）进行密级分类，将数据资产分级为公开、内部、敏感、机密等。

4. 数据安全风险评估及消除

数据安全风险评估一般分为“按数据生命周期安全评估”和“按场景化数据安全评估”两种方法。将评估结果输入数据安全风险矩阵，输出风险视图和消除举措。

- 按数据生命周期安全评估是基于数据生命周期各阶段进行风险识别，按数据安全成熟度评估相应差距。
- 按场景化数据安全评估是在数据生命周期各阶段的数据安全细化场景，基于数据资产分级分类的不同安全属性，识别数据安全具体风险点。
- 将数据安全风险评估的风险点输入数据安全风险矩阵，列出各场景的风险消除举措。

4.1 数据生命周期安全评估法

围绕数据生命周期各阶段，明晰相关数据安全过程域的监管法规要求和业务需求，分析对应安全策略，从组织建设、制度流程、技术工具和人力能力角度评估数据安全现状、原则和数据安全控制措施。

图2-数据生命周期安全

阶段风险评估重点：

- 数据采集阶段，数据分级分类、数据采集安全处理、数据源鉴别和记录、数据质量管理；
- 数据传输阶段，数据传输加密、网络可用性管理；
- 数据存储阶段，存储媒体安全、逻辑存储安全、数据备份和恢复；
- 数据处理阶段，数据脱敏、数据分析安全、数据正当使用、数据处理环境安全、数据导入导出安全；
- 数据交换阶段，数据共享安全、数据发布安全、数据接口安全；
- 数据销毁阶段，数据销毁处置、存储媒体销毁处置；
- 在数据通用过程中，加强数据安全策略、组织和人员管理、数据供应链安全、元数据安全、终端数据安全、监控与内部审计、鉴别与访问控制、需求分析、安全事件应急。

4.2 场景化数据安全评估法

围绕数据安全场景，以数据分级分类为核心，根据数据安全合规监管和业务提升要求，评估相应数据访问控制的现状差距、制定数据安全控制措施。

主要场景的风险评估重点：

- 数据访问账号和用户权限管理，通过账号专人专用、账号独立、账号授权审批、最小授权、账号及时回收、行为内部审计、定期账号稽核等方式控制；
- 数据使用过程的访问权限管理，建议批量操作审批、高敏感数据访问审批、批量操作和高敏感数据访问的指定设备、地点、访问过程内部审计记录、开发测试访问模糊化、访问行为定期稽核等方式控制；
- 数据共享（提取）权限管理，通过最小共享和泛化、共享（提取）审批、最小使用范围、责任传递、定期稽核等方式控制；
- 定期权限稽核，主要通过数据安全的合规性检查、操作监管或稽核、数据访问账号和权限的监管与稽核、业务单位和运维的数据访问过程的合法性监管与稽核、日志风险分析与数据安全性测试等方式控制；
- 数据存储管理，通过涉密数据存储的网络区隔、敏感数据存储加密、备份访问管理、存储设备的移动管理、存储设备的销毁管理等方式控制。

4.3 风险差距分析矩阵

将风险评估识别出的数据安全风险，按风险类型归集并输入风险差距分析矩阵，根据数据安全场景，进行数据流的用户隐私、机构机密和合规威胁的现状差距分析。输出风险消除举措、保护技术和管控行为，形成风险分析统一视图。

表3-风险差距分析矩阵

风险矩阵实施步骤：

- 建立风险差距矩阵，明确数据流的业务目的、涉及系统和业务流程的数据安全、保密和合规要求；
- 执行安全威胁建模，识别数据流的机密数据所需跨越的信任边界，应对数据安全性、策略、流程或实施要求的可能变化；
- 分析数据安全风险，针对现有数据安全的保护控制、技术和行为进行风险 / 差距分析，识别现有保护措施未能解决的威胁，评估相关风险；
- 确定风险消除措施，列出使各项风险达到可接受水平所需额外控制措施、技术和活动，评估每项风险成本 / 收益，决定是否以及如何降低、转移确定风险；
- 评估消除措施有效性，如存在不可接受风险，审查前述结果并重新启动整个风险评估周期。

5. 数据安全管理规划

在系统化评估数据资产的机密性，完整性和可用性，识别风险消除举措足以将风险降低到可接受水平后，据此进行数据安全管理规划：

5. 1 建全安全组织

基于数据治理组织构架，在合规或IT部门成立专业化数据安全团队，通过与数据治理组织的协同配合，保证能长期持续执行数据安全管理工作。制定数据安全的决策机制，界定部门和角色（受众）职责和权限，使数据安全任务有的放矢。灵活设计该组织的结构、规模和形式，协同多方部门积极参与数据安全管理过程。

5. 2 制定制度规范

建立整体方针政策，加强数据资产分级分类和管控，划分敏感数据使用部门和人员角色，限定角色的数据使用场景，制定场景对应制度规范、操作标准和模板，推动执行落地。

5. 3 建立技术架构

规划数据安全技术架构，保护计算单元、存储设备、操作系统、应用程序和网络边界各层免

受恶意软件、黑客入侵和内部人员窃取等威胁:

- 信息基础设施层保护，如认证机制、数据和资源访问控制、用户账户管理，身份管理系统等;
- 应用数据层保护，整个数据生命周期内正确分类和保护存储于数据库、文档管理系统、文件服务器等的敏感数据;
- 内部审计监控层，合规管控系统、监控与自动化内部审计验证系统和数据访问控制是否有效。

6. 持续改善

通过行为管理、内部审计稽核和闭环管理等措施，推进数据安全管理体系的不断优化，推动数据安全的持续改善。

6. 1 行为管控

结合数据流相关的业务流程，加强数据在访问、运维、传输、存储、销毁各环节的数据安全保护举措:

- 及时梳理和更新数据资产清单，增加/修改核心数据资产信息及安全访问角色;
- 监控数据安全指标，加强敏感数据的用户访问行为管控;
- 主动响应最新合规需求，新增或移除数据安全管控策略;
- 当业务模式或组织结构发生变化，及时调整敏感数据的访问权限和行为方式;
- 建全高效数据安全组织结构，调整和持续执行数据安全策略和规范。

6. 2 内部审计稽核

对过程化主要场景，如开发测试、数据运维、数据分析、应用访问、特权访问等，引入量化内部审计手段和稽查工具定期内部审计和稽核。

- 合规性检测，确保数据安全政策有效执行;
- 对操作过程数据安全进行监管和稽查;
- 监管和稽查数据访问账号和用户权限;
- 加强业务单位和运维部门的数据访问过程合法性监管和稽查;
- 运用大数据自动分析日志，发现潜在异常行为;

- 采用渗透测试等技术开展数据安全测试。

6.3 闭环管理

闭环管理数据安全，及时根据政策合规与制度规范提升需求，滚动修订数据安全的制度、流程、标准，保障数据安全的规划、计划、实施、运行、监督的全程管控，持续提升机构的数据安全能力。

结语

数据安全是企业稳健经营的重要因素，近些年从监管趋势上也不难看出，国家对数据安全管控的重视。在长期的数据治理过程中，我们建议企业通过识别和整改数据安全风险及问题，逐步完善权限管理和数据安全评估等管控流程，严格执行数据日志内部审计和安全备份等制度，建立数据管理应急机制，通过提升安全团队专业化能力来逐步构建企业的数据安全文化，助推企业数据资产价值的不断提升。

附录-数据安全相关法律法规清单

- 《中华人民共和国网络安全法》
- 《银行业金融机构数据治理指引》
- 《中国银保监会办公厅关于开展银行业和保险业网络安全专项治理工作的通知》
- 《APP违法违规收集使用个人信息自评估指南》
- 《电信和互联网行业提升网络数据安全保护能力专项行动方案》
- 《电信和互联网用户个人信息保护规定》
- 《儿童个人信息网络保护规定》
- 《法人金融机构洗钱和恐怖融资风险管理指引（试行）》
- 《个人信息保护技术指引》
- 《个人信息出境安全评估办法（征求意见稿）》
- 《个人信息和重要数据出境安全评估办法（征求意见稿）》
- 《关键信息基础设施安全保护条例（征求意见稿）》
- 《关于金融机构进一步做好客户个人金融信息保护工作的通知》
- 《关于银行业金融机构做好个人金融信息保护工作的通知》

- 《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》
- 《互联网个人信息安全保护指南》
- 《互联网用户账号名称管理规定》
- 《金融机构大额交易和可疑交易报告管理办法》
- 《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》
- 《数据安全管理办法（征求意见稿）》
- 《银行业金融机构监管数据标准化规范》
- 《中华人民共和国密码法》