基金公司数据安全管理标准研究

【摘要】随着金融科技快速发展，数据已成为公募基金公司的核心资产与关键风险点。软件系统作为业务运营的重要载体，其开发过程中存在大量数据安全风险，传统“事后防护”模式难以应对日益复杂的合规与技术挑战。本课题系统梳理了国内外数据安全法规与行业实践，以及对21家基金公司的调研分析，总结当前行业数据安全管理体系在软件开发“事中”环节存在过程性标准缺失的问题，提出将数据安全要求“左移”并深度嵌入软件开发生命周期的管理框架，构建了涵盖立项、需求、设计、开发、测试、上线等阶段的数据安全闭环管控流程，提炼出数据安全基线，并在试点项目中验证了“基线+流程嵌入”模式的有效性。课题证明该体系有助于公募基金公司实现从数据安全“被动合规”向“主动治理”的转变，为行业在数字化转型中构建内生数据安全能力提供了可操作的路径与方法支撑。

关键词：数据安全；软件开发生命周期；安全左移；数据分类分级；安全基线

目录

一、研究背景及方法

（一）研究背景及目的

近年来，随着我国金融科技的迅速发展，数据已成为公募基金公司最核心的生产要素与战略资产。从产品设计、投资决策、交易执行到风险控制及客户服务，基金公司的各项业务均高度依赖于数据的高效采集、安全传输、合规存储和深度分析。与此同时，各类软件系统构成了基金公司业务运营与金融创新的重要基础设施，其开发活动贯穿了企业信息化建设与数字化转型的全过程，成为数据生成、处理与流转的核心场景。在此背景下，软件开发生命周期（以下简称“SDLC”，Software Development Life Cycle）中潜藏的数据安全风险日益突出。与单一来源或单一业务环节的风险相比，这些风险更为复杂、隐蔽且难以控制，已成为影响公募基金行业乃至整个金融系统稳健运行与合规发展的关键挑战之一。

数据安全问题的紧迫性不仅体现在理论层面，更在近年频发的数据安全事件中得到印证。金融行业作为数据密集型行业，已成为数据泄露的重灾区。据统计，2023 年仅银行业的数据泄露事件就高达 4293 起。这些事件不仅给机构带来巨大的经济损失，更严重损害了客户信任和市场信心。例如，2025 年某公募基金就发生了因内部权限管控失效和敏感数据流转未脱敏，

导致的数据泄露信息安全事故。另一案例发生在2023年，某企业微信服务商在为多家银行提供服务时，未经授权私自调用超过600万条包含客户姓名、身份证号、银行卡号等高度敏感信息的会话存档数据用于模型训练。这一事件不仅暴露出机构在第三方合作和软件供应链管理中存在风险敞口，也揭示了在软件开发与集成过程中普遍存在的数据安全责任边界不清、监控机制缺失等问题。这些案例充分说明，若在软件开发流程的早期阶段缺乏系统化的安全设计与过程控制，极易在后续的测试、上线乃至运维阶段埋下数据泄露、权限滥用和非授权访问的严重隐患，构成重大的合规与声誉风险。

为应对日益严峻的内外安全挑战，国家正加速推进数据安全治理法律体系的系统化建设。继《中华人民共和国网络安全法》（以下简称“《网络安全法》”）《中华人民共和国数据安全法》（以下简称“《数据安全法》”）《中华人民共和国个人信息保护法》（以下简称“《个人信息保护法》）”和《关键信息基础设施安全保护条例》之后，国务院于2024年9月正式颁布了我国首部网络数据安全领域的行政法规——《网络数据安全管理条例》（国务院令第790号），该条例已于2025年1月1日起施行，为数据全生命周期管理提供了更高层级的法律依据。与此同时，金融监管机构也在持续强化行业监管与

标准建设：国家金融监督管理总局于2024年12月发布《银行保险机构数据安全管理办法》，中国人民银行于2025年5月发布《中国人民银行业务领域数据安全管理办法》，这两份重要文件与此前已实施的国家标准GB/T 43697-2024《数据安全技术 数据分类分级规则》共同塑造了金融行业数据安全监管的新格局，对数据分类分级、风险评估、技术防护以及软件开发、测试、运维的各个环节提出了明确要求。

然而，现行监管框架与企业实践，仍更多地侧重于数据安全治理的宏观框架、机构层面的责任划分以及事后评估与合规检查，对于软件开发这一核心“生产环节”，如何在事中进行有效控制，目前仍缺乏一套具体、可操作的标准化实施指南。基金公司普遍采用的外包开发、敏捷迭代、微服务架构等灵活高效的开发模式，使得安全责任主体分散、数据交互接口复杂、攻击暴露面增大，传统的“边界防护”和“事后审计”模式已难以为继。因此，如何将数据安全要求“左移”至软件开发流程的早期阶段，实现安全与开发的深度融合，构建一套贯穿软件开发全生命周期的“内建式”而非“附加式”的数据安全管理体系，已成为公募基金公司在严监管和高风险环境下亟须解决的核心课题。

本课题的目的在于： 一是系统梳理并深入解读国内外最新的数据安全法规、金融行业监管要求及国际最佳实践，明确公募基金公司在软件开发生命周期中的数据安全风险点与核心合规义务。 二是致力于构建一套模型化、流程化的软件开发数据安全管理框架，将数据分类分级、威胁建模、安全设计、数据脱敏、环境隔离等安全要求系统性地嵌入立项、需求到设计、开发、测试、上线的各个阶段，以形成可操作、可评估、可持续优化的闭环管理体系。 三是通过行业调研，总结数据安全管理在软件开发流程中的落地经验与共性痛点，进而从制度、技术、流程与组织层面提出切实可行的改进建议。 四是探索标准化路径，旨在为制定《公募基金公司软件开发流程中的数据安全管理实施指南》提供理论与方法支撑，推动行业标准的形成，最终助力基金行业在数字化转型浪潮中，实现安全、合规与效率的和谐统一。

（二）研究思路及方法

本课题以问题导向和体系化构建为核心思路，力求在现有政策与行业实践的基础上，形成一套可应用、可推广的基金公司软件开发数据安全管理框架。研究整体遵循“宏观治理—中观体系—微观落地”的逻辑展开，既注重政策法规与监管趋势的

纵向分析，也关注基金公司实际运行过程中的横向比较与经验提炼。

1.文献分析法

系统梳理国内外关于数据安全、信息技术治理和个人信息保护的法规、政策和标准，明确金融行业数据安全管理的总体脉络与监管趋势。重点参考《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》以及欧盟《通用数据保护条例（GDPR）》、美国 NIST 系列标准（如 SP 800-218）等，比较不同法域下的数据安全监管理念与治理框架，分析其在制度逻辑、实施路径及风险控制重点上的差异，为本课题建立理论与制度基础。

2.比较研究法

在文献研究的基础上，横向对比分析国内外金融机构在软件开发生命周期（SDLC）中实施数据安全管控的先进做法与成熟经验。重点比较不同监管体系下的“安全左移”策略，例如欧盟 GDPR 第 25 条“默认及内嵌式数据保护”的落地实践、美国 NIST 安全软件开发框架（SSDF）的应用模式，在自动化测试、威胁建模、测试数据管理等方面的具体差异，以及我国

当前以分级分类、事前审批为特征的监管框架。通过比较，识别我国基金行业在数据安全过程管控中的短板与改进方向。

3.问卷调研法

面向公募基金公司开展问卷调查与访谈研究，了解行业机构在软件开发全流程中落实数据安全管理的现状、难点与需求。调研内容包括开发立项安全审查、需求阶段数据脱敏设计、代码审查与漏洞扫描、测试环境隔离与访问控制、上线前安全验收等方面，旨在识别基金公司在制度执行与技术实现之间的脱节问题，提炼出公募基金行业面临的共性风险与核心痛点，增强本课题的现实针对性。

4.流程建模法

依据软件工程管理理论，结合瀑布模型与敏捷开发模型的特征，将数据安全要求系统性嵌入软件开发生命周期（SDLC）各阶段，构建“安全左移”的流程框架。该框架以立项阶段的安全评估为起点，通过需求分析阶段的敏感数据识别、设计阶段的安全架构控制、开发阶段的安全编码规范、测试阶段的漏洞管理与验证机制，以及上线阶段的安全验收与持续监测，形成贯穿系统开发全流程的安全管理闭环。通过此方法，将安全责任明确到岗位，将安全措施转化为可执行的工作流程。

5.案例归纳与对策分析

基于案例归纳与对策分析，对实证研究与建模成果进行梳理，提炼行业共性问题与典型解决路径。从组织管理、技术防控与制度执行三个维度提出针对性对策，涵盖数据分级分类、权限控制、开发外包管理，以及安全审计机制等方面。同时，结合监管要求，提出推动行业统一标准建设和监管协同的政策建议，确保研究成果既具有实践可操作性，又能为行业标准化提供参考。

通过上述多维度研究方法的综合运用，本课题在理论上旨在完善公募基金行业的数据安全治理体系，在实践上为基金公司建立可执行、可评估、可持续改进的软件开发数据安全管理体系提供支撑。研究成果将为行业监管、机构合规及标准化制定提供系统化的理论依据与操作路径。

二、国内外数据安全管理整体背景

本章系统梳理国内外数据安全管理的政策法规、监管机制及标准体系，旨在为后续分析公募基金公司软件开发流程中的数据安全问题并构建针对性管控体系，提供宏观背景与理论参照。目前，全球主要经济体均已在法律、监管及行业标准层面

建立了较为成熟的数据安全管理框架，这些框架展示出一些共性特点，主要包括：以风险为导向建立数据分类分级制度，以全生命周期为核心确立安全治理要求，并通过强化监管协同和标准化建设提升数据安全治理的可操作性。

国外先行实践更强调将安全控制“前置化”和“内嵌”于业务流程与系统设计中，相比之下我国的数据安全管理体系虽已基本成型，但在具体实施中，仍存在偏重事后评估与合规检查、对软件开发这一核心“事中”环节的过程管控标准不足等问题。基于此，本章将首先介绍国外主要经济体的数据安全管理体系，随后深入分析国内最新的监管与标准框架现状，并在此基础上总结出现有体系的局限性，论证将安全控制“左移”至软件开发流程的必要性。

（一）国外数据安全管理相关情况

1. 欧盟：以 GDPR 为核心的“设计即安全”体系

欧盟是全球最早建立系统性数据保护法律体系的地区。其核心法规《通用数据保护条例》（以下简称“GDPR”，General Data Protection Regulation）自 2018 年正式实施以来，确立了个人数据保护的基本原则与监管体系。GDPR 适用于所有在欧盟境内处理个人数据的组织，无论数据处理者或控制者是否设立在欧

盟境内。该条例由各成员国的数据保护机构（Data Protection Authority）执行，欧洲数据保护委员会（以下简称“EDPB”）负责统一协调，形成“中央协调+属地执法”的分层监管体系。

GDPR 的核心原则包括合法性、公平性、透明性、目的限制、数据最小化、准确性、存储期限限制和完整性保护。其中第 25 条提出“默认及内嵌式数据保护”（Data Protection by Design and by Default），要求在业务系统与技术设计阶段即嵌入隐私保护机制，该条款从根本上改变了数据安全的传统思路，它强制要求数据控制者在确定处理方式（如设计新软件系统）之初，就必须实施假名化、数据最小化等技术和组织措施，将数据保护原则融入处理过程本身。这意味着，安全不再是开发完成后的“附加项”，而是软件架构和功能的“原生属性”。GDPR 还引入数据保护影响评估（DPIA）制度，要求高风险数据处理活动在实施前进行风险评估和报告，确保监管机构事前知悉潜在风险并可进行干预。

为落实这一原则，挪威数据保护局等监管机构给出了具体实施指南，将软件开发中的“数据保护设计”分解为七个关键活动：

(1) 培训（Training）：确保开发团队充分理解法规要求和安全风险。

(2) 需求（Requirements）：在项目需求阶段就明确数据保护和信息安全要求，并开展数据保护影响评估（DPIA）。

(3) 设计（Design）：在系统架构设计中应用数据最小化、隐藏、分离、聚合等隐私增强技术（PETs），并开展威胁建模。

(4) 编码（Coding）：使用经批准的安全框架和工具，进行静态代码分析，避免在日志中记录个人数据。

(5) 测试（Testing）：使用合成数据（Synthetic Data）而非真实数据进行测试，并开展全面的安全测试（如渗透测试、模糊测试）。

(6) 发布（Release）：制定并演练事件响应计划，进行最终安全审查。

(7) 维护（Maintenance）：持续运行事件响应计划，并定期进行安全审计和测试。

这一系列活动构成了“安全左移”的完整实践闭环，确保数据保护贯穿于 SDLC 的始终。

总体而言，欧盟体系具有高标准、强约束和统一执行的特征，对全球数据安全治理具有示范作用。其核心监管思路是通过制度设计，确保数据处理活动全过程的安全与合规，从而将数据安全治理纳入组织运营的日常管理之中。

2. 美国：NIST 框架与行业法规并行的实践导向体系

美国的数据安全管理体系采用“联邦行业立法、州级通用立法与国家技术标准”并行的架构，这一体系实践指导性强，尤其在技术框架层面为全球提供了重要参考。金融领域主要适用《格拉姆—里奇—布莱利法案》（Gramm－Leach－Bliley Act，GLBA），由联邦贸易委员会及货币监理署等部门负责执行。在其他行业，美国还实施了《健康保险可携性与责任法案》（HIPAA）、《儿童在线隐私保护法》（COPPA）及《加州消费者隐私法案》（CCPA）等多部专项法律，形成“行业分立、地方补充”的制度格局。

在国家技术标准层面，美国国家标准与技术研究院（以下简称“NIST”）发布的系列标准构成了信息安全管理的事实标杆。其中，NIST SP 800-218《安全软件开发框架》（Secure Software Development Framework）为组织提供了一套高级别的安全软件开发实践核心集合。SSDF 并非强制标准，但它为软件生产者遵循美国总统行政令 14028《改善国家网络安全》提供了指引。该框架将安全实践分为四大核心组：

(1) 准备组织（Prepare the Organization）：定义安全需求，建立安全开发环境。

(2) 保护软件（Protect the Software）：保护代码不被篡改，并提供软件物料清单（SBOM）。

(3) 生产良好安全的软件（Produce Well-Secured Software）：从安全设计、安全编码到安全测试，确保软件产品的内生安全。

(4) 响应漏洞（Respond to Vulnerabilities）：建立漏洞识别、评估、修复和分析的闭环流程。

在金融行业法规层面，《格拉姆-里奇-布莱利法案》（Gramm-Leach-Bliley Act, GLBA）及其下的《保障规则》（Safeguards Rule）对金融机构提出了具体要求。2023 年更新的《保障规则》明确强化了对软件开发和测试过程的管控，要求金融机构必须实施应用程序安全评估，对自研或使用的第三方应用程序进行安全评估；同时，机构还需要进行持续监控或定期测试，若无法实现持续监控，则必须执行年度渗透测试和每六个月一次的漏洞评估；此外，该规则还强化了访问控制和加密要求，规定机构需对存储和传输中的客户信息进行加密，并对所有访问人员实施多因素认证（MFA）。这些规定将安全测试、漏洞评估等软件开发生命周期中的关键活动从“建议”变为了“强制”，推动了金融机构将安全融入日常开发运维流程。

3. 日本：以 APPI 为基础的自律与监管结合体系

日本的体系采用监管与自律相结合的模式，其特点在于监管机构提供指导方针，同时积极鼓励行业协会制定自律规则。日本的数据保护制度以《个人信息保护法》（以下简称“APPI”，Act on the Protection of Personal Information）为基础，最初于 2003 年颁布，经过 2015 年和 2020 年的两次重大修订后，形成了较为完善的个人数据保护体系。2022 年修订版 APPI 正式生效后，进一步强化了跨境数据传输监管与安全保障义务。该法要求个人信息处理者在处理过程中采取必要的技术与组织措施，防止数据泄露、篡改或滥用。日本个人信息保护委员会（Personal Information Protection Commission）为中央独立监管机构，负责发布实施细则、指导方针及执法监督。

APPI 要求企业在个人信息的收集、存储、使用、传输及销毁全过程中实施分级管理，并建立安全管理计划和内部控制机制。APPI 第 23 条要求企业采取“必要和适当的措施”来管理个人数据安全。在软件开发和系统建设领域，这一原则被延伸应用于对外包供应商的管理。日本个人信息保护委员会的指南明确要求，企业在将包含个人数据的处理任务外包时，必须对供应商进行充分的监督，确保其具备同等的安全管理能力。在涉及系统开发和技术外包时，日本法律实践对责任边界有清晰

地界定。企业需在合同中明确规定供应商的数据安全义务、审计权利、事件通知机制以及数据返还/销毁要求。特别是对于涉及个人数据跨境传输的开发项目（例如使用离岸开发中心），APPI 要求必须获得数据主体的明确同意，或确保接收方所在国具有与日本同等的数据保护水平，或接收方自身已建立符合 APPI 标准的保护体系。此外，日本金融服务厅（FSA）发布的《金融部门网络安全指南》进一步强调，金融机构应对核心系统的开发和运营外包进行严格的风险评估和持续监督，管理层需为网络安全分配适当资源，并从被动防御转向主动预防。

4. 韩国的相关规制情况

韩国自 2011 年实施《个人信息保护法》（Personal Information Protection Act），经过多次修订，已成为亚洲地区最严格的数据保护法律之一。PIPA 确立了获取同意、最小收集、用途限定、保存期限控制及安全保障义务等基本原则。根据该法第 29 条，个人信息控制者在处理信息时必须采取必要的技术和管理措施，以防止数据丢失、泄漏或篡改。个人信息保护委员会（以下简称“PIPC”）作为中央监管机构，负责统一监管、制定安全措施标准指南，并实施处罚。指南对内部管理制度、访问控制、日志记录、加密和恶意程序防护等提出了细致要求。

韩国监管体系展现出高度一致性和强制约束力。PIPC 定期

发布检查计划，对金融机构、通信企业和大型平台实施合规审查。违规行为除行政罚款外，还可能面临刑事责任。韩国的制度设计与执行机制实现了数据安全治理的闭环管理，即通过明确责任主体、制定技术规范和建立处罚机制，形成从制度到执行的全链条监管体系。

5. 印度的相关规制情况

印度的数据保护制度长期以来以《信息技术法案》（2000年）及其附属规则为主要依托。2023 年《数字个人数据保护法案》（以下简称“ DPDP”，Digital Personal Data Protection Act）的通过，标志着其正式建立起全国统一的个人数据保护法律框架。该法以“数据受托人”（Data Fiduciary）为核心监管对象，要求组织在数据处理活动中取得同意、遵循目的限制原则并采取适当的安全保障措施。DPDP 法案确立了数据泄露通报义务，并授权设立印度数据保护委员会（Data Protection Board of India）作为独立监管机构。该法案借鉴了 GDPR 的诸多原则，以“数据受托人”（Data Fiduciary）为核心监管对象，要求其在处理个人数据时履行获取同意、目的限制和采取合理安全保障措施等义务。法案同样规定了数据泄露的通报义务。目前，印度正在制定该法案的详细实施细则和行业标准。在此之前，印度金融机构普遍参考 ISO/IEC 27001、NIST 网络安全框架等国际标

准来构建其内部的信息安全和软件开发安全控制体系。总体来看，印度正处于从分散的信息技术法案监管向综合性数据保护体系转型的关键阶段，其监管框架正加速向国际主流标准看齐。

（二）国内数据安全管理相关情况

我国已初步构建起以《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》“三驾马车”为核心，以部门规章、国家标准和行业规范为支撑的多层次数据安全管理体系。2024 至 2025 年间，随着一系列重磅法规和标准的密集出台与实施，我国数据安全监管进入了全面深化和体系化建设的新阶段。

1. 国家顶层设计：《网络数据安全管理条例》的统领作用

《网络数据安全管理条例》（国务院令第 790 号，2025 年 1 月 1 日施行）是我国首部网络数据安全领域的行政法规，是对上位数据安全三大法的全面细化和重要补充，具有承上启下的关键作用。

该条例在软件开发和系统建设层面提出了多项原则性要求，如条例规范了网络数据的“处理”包括收集、存储、使用、加工、传输、提供、公开等，明确了全生命周期管理各个环节，将软件开发的全过程纳入了监管范围。另外，第五条明确要求

对网络数据实行分类分级保护，这是后续所有差异化安全措施的基础。在第二十二条明确处理“金融账户”等敏感个人信息时需取得个人单独同意，说明了对敏感个人信息保护的要求，这一条例直接关系到金融软件的功能设计。条例还在第四十八条明确了各行业主管部门（包括金融监管部门）的数据安全监督管理职责，为金融监管机构出台更细化的行业规定提供了上位法律依据。

《GB/T 43697-2024 数据安全技术 数据分类分级规则》（2024 年 10 月 1 日实施）作为我国首个数据分类分级的推荐性国家标准，与金融监管机构的“核心、重要、一般”的三级分类法完全对齐，并给出了数据分类分级的通用规则、流程和方法，为金融机构在软件开发、需求分析阶段进行数据识别、分类和定级提供了权威的方法论依据，是落实差异化保护策略不可或缺的技术前提。

2. 金融行业监管：新规下的精细化管控

我国金融行业的数据安全管理实行多部门协同监管体系，中国证券监督管理委员会、中国人民银行和国家金融监督管理总局各司其职、各负其责、相互配合、齐抓共管，共同履行监管职责。按照中金办的协调工作要求，各部门都应当就重要数据管理进行分级的保密管理以及应对处理数据的系统故障的报

告机制。各监管部门根据行业特性制定了相应的数据安全管理办法和配套制度，共同构成金融领域数据安全治理的制度基础。总体来看，当前监管要求呈现出治理结构体系化、技术措施精细化与风险评估制度化的特征，而在具体监管重点上，各部门又各有侧重。

(1) 中国证券监督管理委员会的相关规制情况

证监会对于信息技术的监管体系以《证券期货业网络和信息安全管理办法》（证监会令第 218 号）和《证券基金经营机构信息技术管理办法》（证监会令第 152 号）为核心，有效承接了《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》《中华人民共和国网络安全法》等上位法要求，构建了证券期货行业对于数据安全领域的监管框架。于 2023 年正式施行的《证券期货业网络和信息安全管理办法》，对投资者个人信息全生命周期保护要求作出了系统性规范，强调数据处理各环节的安全合规措施，要求机构建立统一信息安全管理体系、实施系统分级保护、完善应急响应机制。《证券基金经营机构信息技术管理办法》则从信息系统治理视角，对系统开发、测试、运维及外包管理等环节提出了综合性要求，强调应在系统设计阶段嵌入安全控制，强化变更管理与测试审查机制，确保信息系统运行的安全、稳定与可控。另外，该办法还在数据

治理章节对机构在“数据全生命周期”安全管理提出了管理要求，为数据保护提供了方向性要求。

在数据安全行业标准层面，《证券期货业信息安全标准规划（2023-2025）》统筹规划了数据安全技术、分类分级、传输存储、脱敏技术等多维度标准制定路径。其中，标志性的工作成果是国家标准《证券期货业数据安全风险防控 数据分类分级指引》（GB/T 42775-2023）于 2023 年正式实施，该标准由 2018 年发布的《证券期货业数据分类分级指引》修订而来，确立了基于重要性和敏感性的多维度风险评估方法体系，可供证券期货业制定数据管理、数据安全防护等相关标准时进行参考。此外，全国金融标准化技术委员会证券分技术委员会（以下简称“证标委”）近年持续发布数据标准、数据模型等数据相关系列标准（如《证券期货业数据标准属性框架》《证券期货业数据模型》），并推进数据管理能力成熟度评估等重要标准制定（如《证券期货业数据管理能力成熟度评估规范》），标志着证券期货行业数据安全管理从制度要求向技术评估标准化的纵深延伸。

(2) 中国人民银行的相关规制情况

人民银行在银行业数据安全管理中承担总体统筹与标准协调职责，通过规章建设和标准制定，构建了较为完善的制度体

系。2025 年 5 月发布的《中国人民银行业务领域数据安全管理办法》（中国人民银行令〔2025〕3 号）是近年金融监管体系的一项重要制度创新，标志着我国金融数据安全监管进入了一个新阶段。该办法的革新性在于构建了一个全链条、分级化的管理范式。其核心是确立了“谁处理、谁负责”的责任模式，强制要求金融机构建立覆盖数据全生命周期的安全治理体系，从采集、传输直至最终删除的每一环节均需落实安全保障。在操作层面，办法展现了清晰的监管逻辑：在数据分级层面，通过建立“核心、重要、一般”三级分类，实现了保护资源的精准配置，避免了“一刀切”的管理僵局；在技术防护层面，办法体现出对高敏感数据的重点关切，明确要求采取加密、脱敏、环境隔离等具体技术手段，特别是在测试数据管理、敏感数据访问控制及 API 接口安全等方面，提出了极具操作性的合规要求；在风险管控层面，它将数据安全从静态合规推向动态管理，通过强制要求重要数据处理者进行年度风险评估、应急演练和合规审计，并辅以事件报告与问责机制，形成了一套贯穿事前、事中、事后的持续监督闭环。该办法不仅是一部具体的行为规范，更从治理架构、技术路径和管理流程三个维度，为机构在支付清算、征信、反洗钱等关键业务领域的数据安全管理提供了系统性指引。

在数据安全行业标准层面，全国金融标准化技术委员会（以下简称“金标委”）在人民银行指导下发布了系列数据安全标准，构建了金融数据安全管理的标准体系。《金融数据安全 数据安全分级指南》（JR/T 0197-2020）为金融机构数据安全分级工作提供方法论支撑，明确了数据安全等级划分的目标、原则、要素、规则和定级过程；《金融数据安全 数据生命周期安全规范》系统规范了采集、传输、存储、使用、删除、销毁等各阶段的安全要求，明确各阶段应采取的技术措施和管理措施；《金融数据安全 风险评估指南》则为机构建立常态化风险评估机制提供标准化参考，有助于系统识别数据安全风险并制定针对性应对措施。此外，金标委还配套发布了数据交换安全规范、敏感数据识别指南等配套标准。这些标准与人民银行的制度框架形成相互支撑，强调建立全流程安全责任链条和持续改进机制。

(3) 国家金融监督管理总局的规制情况

金融监管总局在银行保险领域的数据安全监管中承担主要职责，通过发布规章和推动标准建设，已建立起较为完善的监管体系。2024 年 12 月发布并施行的《银行保险机构数据安全管理办法》（金规〔2024〕24 号）在银行与保险领域建立了系统的数据安全制度框架。该办法的显著特征在于，它从公司治

理的高度明确了数据安全的责任链条。它强制要求机构设立数据安全管理委员会或类似机制，并清晰划分了董事会（承担最终责任）、高级管理层（负责组织实施）与监事会的职责，从而将数据安全从技术层面提升至机构战略与治理的核心。在具体管理要求上，办法展现了与人民银行规制框架的协同性，并发展了具有行业特色的实施细则。一是通过建立“核心、重要、一般”三级数据分类体系，并与人民银行标准保持衔接，确保了监管的一致性。同时，要求机构编制数据目录，实现数据资产的清晰化与可视化管控。二是办法强调构建体系化的技术防护能力，要求依据数据级别采取差异化的加密、脱敏、访问控制等措施。它特别针对行业常见的开发测试场景，明确要求测试环境与生产系统隔离，并原则上禁止未经脱敏的敏感数据流入测试环境，精准地封堵了这一高风险漏洞。三是办法专设“个人信息保护”章节，强化了对金融消费者权益的保障。在风险管控上，它建立了贯穿事前、事中、事后的持续监管机制，从定期风险评估、应急预案制定到明确的事件报告时限，形成了一套完整的风险监测与处置闭环。办法不仅是一部合规检查清单，更从治理结构、流程控制与技术实施三个维度，为银行保险机构建立常态化的数据安全内控机制提供了系统性指引。

金标委在银行保险领域发布了与上述规章配套的标准文件，

二者共同构建了银行保险领域的数据安全标准体系。通过法律规章与标准化建设的结合，银行保险领域初步建立起覆盖制度管理、技术保护、风险监测与应急响应的综合性数据安全保障体系。

证监会、人民银行和金监总局分别从证券基金期货、银行及保险领域出发，形成了相互衔接、各有侧重的金融数据安全监管体系。三者在制度层面均强调数据分类分级管理、全生命周期保护、风险评估机制和应急响应机制，但各自监管重心存在差异：

- 证监会更注重信息技术与个人信息保护的结合，强调对系统开发的全流程安全管控。信息技术管理办法对软件开发、测试、运维等环节提出明确要求，证标委持续推进行业标准建设，形成了较为完善的证券期货业数据安全标准体系。
- 人民银行强调制度与治理体系的建设，突出数据安全责任链条和合规审计要求。业务领域数据安全管理办法对数据处理各环节提出细致的技术保护要求，特别是对高敏感性数据项的加密、脱敏和访问控制提供可操作指引，为软件开发过程中的数据保护提供规范依据。
- 金监总局侧重突出风险防控与应急响应，强化数据安全

事件的监测与处置。银行保险机构数据安全管理办法对测试环境与生产环境的隔离、测试数据的脱敏处理等软件开发关键环节提出明确要求，直接针对开发测试过程中的数据安全风险。

随着金融标准体系的不断完善和监管部门规章的持续更新，数据安全监管的行业标准化程度正在逐步提高，为金融机构落实全流程数据安全治理提供了可执行的规范依据。然而，现有体系对软件开发流程中“事中”环节的数据安全管理尚缺乏系统性、可操作性的过程标准，导致机构在实际执行中更多依赖内部制度与第三方标准进行自我约束。这种以合规审查为核心的监管模式在保障总体安全的同时，过度依赖评估与报告可能削弱事中监控的有效性，影响数据管理效率和创新能力。因此，在未来的制度建设中，应在维持现有合规要求完整性的基础上，进一步强化对开发与测试等事中环节的过程性管理标准，推动监管重心从“结果合规”向“过程安全”转变，从而真正将数据安全要求嵌入软件开发生命周期的每一个环节。

3. 《GB／T 37988-2019 信息安全技术 数据安全能力成熟度模型》

《GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型》（以下简称“DSMM”）是全国信息安全标准化技术委员

会发布的国家标准，为组织建立数据安全能力评估与改进提供了方法论支撑。该标准以数据全生命周期为主线，覆盖采集、传输、存储、处理、交换与销毁等环节，并从组织建设、制度流程、技术工具与人员能力四个维度，定义了非正式执行、计划跟踪、充分定义、量化控制、持续优化的五级成熟度模型，强调从“制度存在”到“持续优化”的渐进式能力建设。

DSMM 在金融行业广泛应用，各经营机构在合规审计和自评中普遍参考该标准，以衡量自身数据安全管理体系的完善程度。通过成熟度等级划分，该标准帮助组织有效识别数据安全管理的薄弱环节，制定改进路径，逐步提升数据安全能力。

然而，DSMM 的适用重心在于能力评估与过程改进，并不直接规范软件开发生命周期中的数据使用与保护操作，更多关注组织的数据安全管理成熟度而非具体技术实施细节。因此，在研发与测试环节，机构往往需要结合 ISO/IEC 27001 信息安全管理体系、ISO/IEC 27701 隐私信息管理体系、NIST SP 800-53 安全和隐私控制、NIST SP 800-64 软件开发生命周期安全考虑等国际标准，通过引入测试数据保护、数据最小化原则与环境隔离机制来完善内部控制。

（三）现有体系局限性与“安全左移”的必要性分析

尽管我国已构建起了层次分明、要求严格的数据安全管理体系，但通过与国际最佳实践的对比，并结合国内频发的数据安全事件，可以发现现有体系在“事中”管控环节仍存在一定的局限性，这也凸显了将数据安全控制全面“左移”至软件开发流程的紧迫性和必要性。

1. 现有体系的局限性：侧重“事后评估”与“宏观治理”，缺乏“事中过程”管控标准

当前，无论是《网络数据安全管理条例》还是各部门数据安全管理办法，其对于数据安全监管的核心逻辑更侧重于明确治理架构与责任、强调分类分级与目录管理、规范数据处理活动、侧重风险评估与审计。这些要求对于构建数据安全的宏观治理框架至关重要，但它们本质上更偏向于一种“结果导向”或“事后评估”的监管模式，即监管机构关注的是“是否建立了制度”“是否提交了评估报告”“系统最终是否通过了等级保护测评”。然而，对于如何将这些宏观的安全要求转化为安全、可靠、合规的软件代码和系统功能，即在软件开发这一核心“事中”环节，缺乏一套如 NIST SSDF 或挪威 DPA 指南那样细致、可操作的过程性标准。

这种局限性直接导致了经营机构在实践中的普遍痛点：一方面，业务和开发团队面对“原则上”“应当”等宏观要求时，

不知如何在代码层面具体落地；另一方面，安全和合规团队由于缺乏开发过程的可见性和介入手段，只能在系统上线前进行“黑盒”测试或在事后进行审计，难以从源头上消除风险。近年来多起网络安全事件的根源正是软件开发过程中的权限设计缺陷、测试数据管理不当等“事中”管控缺失，而非机构没有数据安全制度或未做过风险评估。

2. 对比国际实践：“安全左移”是弥补“事中管控”短板的必然选择

与国内偏重治理框架的模式不同，国际上的实践更强调“内建于过程”的安全理念。欧盟 GDPR 的“设计即安全”，其本质是法律层面的“安全左移”，强制要求在构思新系统（即需求和设计阶段）的初始阶段，就必须将数据保护作为其核心功能之一来统筹考虑。美国 NIST SSDF 更是一部纯粹的“操作手册”，它不预设任何技术或工具，而是提供了一套从准备、设计、编码、测试到响应的完整“安全生产流程”，其核心价值在于过程管理。

这些国际实践清晰地指明，只有将安全活动（如威胁建模、安全编码、自动化扫描、数据脱敏）深度嵌入到开发团队日常使用的持续集成/持续部署流水线中，才能从根本上高效地、低成本地从源头控制安全风险。这种“安全左移”的 DevSecOps

模式，正是弥补我国当前监管体系中“事中过程管控”上不足的有效实践路径。

综上所述，本章的分析为后续章节的研究构建了清晰的逻辑起点。正因现有体系侧重于宏观治理和事后评估，而对软件开发这一核心“事中”环节缺乏具体的过程管控标准，才导致了数据安全风险在系统“出生”时就被不断引入，并最终演变为实际的安全事件。因此，为了解决公募基金公司在数据安全领域的实际困境，后续章节将以此为切入点展开：

第三章 将通过行业调研，进一步验证上述局限性在公募基金行业的具体表现和痛点。

第四章 将聚焦于构建一套覆盖软件开发生命周期全流程的、可操作的数据安全管理框架和实施体系，以弥补“事中管控”的空白。

第五章 将探讨该体系在公募基金公司的具体落地应用策略，并最终形成《公募基金公司软件开发流程中的数据安全管理实施指南》的核心内容。

通过这样的逻辑递进，本课题旨在为行业提供一个从“为什么”到“是什么”再到“怎么做”的完整解决方案。

三、基金公司数据安全管理现状调研

（一）基金公司数据安全管理工作现状

1. 调研目的

课题组通过分析数据安全监管要求的相关条款，基于数据安全管理、数据安全保护和数据安全运维三大数据安全评估领域，设计了对基金公司数据安全管理工作情况的调研问卷，对行业内基金公司开展数据安全现状评估及差距分析，旨在结合基金公司数据安全现状，识别当前基金公司在数据安全工作中存在的通用问题，总结行业在数据安全管理中的整改方向，为建设数据安全管理标准体系提供有效输入。

2. 调研问卷设计

课题组以《GBT 37988-2019 信息安全技术 数据安全能力成熟度模型》为基础，结合近年来国家及金融行业已发布的相关法律法规、政策文件和技术标准，包括《数据安全法》《个人信息保护法》《金融数据安全 数据生命周期安全规范》《证券期货业数据安全管理与保护指引》等共计 15 份相关制度要求，系统梳理了基金公司在数据安全管理中应遵循的基本要求和合规要点。在此基础上，课题组归纳整理出一套适用于基金公司的《数据安全风险评估矩阵》，涵盖数据安全管理、数据

安全保护、数据安全运维3个一级领域，组织架构建设、制度体系建设、技术管理、人员管理、合作管理、配合监督管理、数据资产管理、数据生命周期安全保护、技术保护体系、网络安全防护、边界管控、访问控制、安全监测、安全审计、安全评估、应急响应与事件处置16个二级领域，共计100个评估控制目标。

课题组以问卷形式将《数据安全风险评估矩阵》发送给25家大中小型各规模、各类基金公司进行填写，广泛收集行业数据安全管理现状情况。同时，课题组还通过现场访谈与线上交流相结合的方式，深入调研基金公司业务人员和管理人员对数据安全的认知水平、管理意识以及在日常工作中的实践情况。访谈过程中，重点识别了当前业务流程中存在的数据安全风险点、典型问题及应对措施。

3. 调研结果

课题组根据评分规则对每家基金公司二级领域的数据安全能力现状进行评分，根据平均分判定基金公司数据安全评估结果（见表1、表2）。

一级	总分	平均分
S1 数据安全管理评估	19	85.46
S2 数据安全保护评估	40	84.70
S3 数据安全运维评估	41	79.97
总分	**100**	**82.90476**

表 1 问卷结果（一级领域）

二级	总分	平均分
S1-1 组织架构建设	5	76.67
S1-2 制度体系建设	4	85.91
S1-3 技术管理	2	77.38
S1-4 人员管理	4	95.83
S1-5 合作管理	3	92.86
S1-6 配合监督管理	1	80.95
S2-1 数据资产管理	2	78.41
S2-2 数据生命周期安全保护	38	80.98
S3-1 技术保护体系	4	72.62
S3-2 网络安全防护	1	88.10
S3-3 边界管控	5	87.14
S3-4 访问控制	9	90.74
S3-5 安全监测	4	59.52
S3-6 安全审计	8	76.79
S3-7 安全评估	3	70.63
S3-8 应急响应与事件处置	7	83.33
总分	**100**	**82.90476**

表 2 问卷结果（二级领域）

根据回收到的 21 份有效问卷调研结果，可以看出目前行业多数基金公司在数据安全管理方面处于发展阶段，其中数据安全管理组织架构已初步建立，人员管理已相对完善，但仍缺少数据安全管理的中长期规划，且数据安全管理制度体系建设不够完善，数据全生命周期安全技术保护实施细则和操作流程有欠缺。在数据安全保护方面处于发展阶段，多数公司在数据采集、传输、存储、使用、删除、销毁各环节均采取了一定保护措施，但数据资产梳理和分级分类工作不完善，且尚未发布数据生命周期安全保护纲领性制度，也未建立数据生命周期安

全保护基线。在数据安全运维方面处于初始阶段，多数公司未基于数据维度开展体系化安全能力建设并形成常态化、集中化、规范化的数据安全运营体系；同时，缺少长效的数据安全专项评估及审计活动，未建立数据安全应急管理和演练机制。

综上，虽然所调研的基金公司不能代表行业整体情况，但总的来说，基金公司在数据安全领域仍处于发展阶段。对比部分银行、券商的数据安全管理实践，其已建立相对完备的数据安全组织架构体系，形成决策、管理、执行、监督四位一体的组织架构，在日常数据安全工作协同和推进中形成数据安全柔性团队，落实各部门所辖领域数据安全管理职责；在基础支撑方面，数据分类分级作为保障数据全生命周期的安全管控前提条件，头部银行、券商已开展专项梳理工作，通过全域数据资产盘点与整合，构建企业级数据资产目录，再通过自动化工具+人工实现安全分级打标工作，从而推动安全措施布控落地；在数据全生命周期管控方面，其多以数据安全管理平台框架为指导，以重点业务场景为切入，逐步引入数据安全专项技术工具并深度融合网络安全基础防护能力，结合数据全生命周期安全控制基线，落实数据安全管控措施，并通过数据安全持续运营工作不断优化整体数据安全防护措施。

（二）调研发现问题及应对

课题组通过本次问卷调研，对21家基金公司的有效问卷结果进行系统分析后发现，当前基金行业在数据安全管理方面整体处于从“初步建设”向“规范发展”过渡的关键阶段。

深入剖析其管理现状可发现，当前行业的数据安全工作仍存在明显的结构性短板和系统性不足。在管理体系层面，行业机构普遍缺乏中长期战略规划，数据安全工作多以应对监管检查或响应突发事件为导向，呈现出“被动响应、零散推进”的特点；制度体系建设尚不完善，尚未发布覆盖全生命周期的纲领性管理制度，也未建立统一的数据安全保护基线和实施细则，导致不同系统、不同业务之间的安全标准不一、执行落地存在偏差。在数据治理基础方面，数据资产梳理不全面，分类分级工作推进缓慢或流于形式，直接影响了差异化安全策略的制定与实施。在运维保障机制上，整体仍处于初始阶段，尚未构建基于数据维度的体系化安全运营能力，缺乏常态化的风险评估、合规审计和持续监控机制；同时，绝大多数机构尚未建立数据安全事件应急管理机制，也未开展过实战化应急演练，事件响应与处置能力薄弱。

上述问题的背后，反映出一个深层次的共性矛盾：当前的数据安全管理重心过度集中在“运行阶段”的技术加固与事后补救，而忽视了在信息系统规划、设计、开发等前端环节植入

安全要求。大量安全隐患实际上是在系统建设初期就已埋下，例如系统需求未明确数据安全级别，架构设计未考虑最小权限原则，开发过程中未实施代码安全审计，测试环境直接使用未脱敏的生产数据等。这些问题一旦随系统上线进入生产环境，后续整改成本高、影响范围大，且难以彻底根除。由此可见，仅依靠后期运维手段已无法满足日益复杂的数据安全挑战。若要实现从“被动防御”到“主动防控”的转变，必须从根本上重构安全管理逻辑，推动数据安全管控向前延伸、关口前移。

因此，本章研究得出核心结论：基金公司亟须将数据安全考量“左移”，深度融入信息系统开发生命周期的全过程。具体而言，应在项目立项阶段识别数据处理场景与安全等级，在需求分析阶段明确数据访问规则与保护目标，在系统设计阶段嵌入加密、脱敏、审计等安全控制，在开发测试阶段落实代码安全检测与敏感数据隔离，并在上线评审中设置数据安全专项准入门槛。通过此方法能实现数据安全要求与业务系统的同步规划、同步建设、同步交付，真正构建起覆盖“规划—开发—运行”全链条、贯穿“制度—技术—人员”全要素的数据安全治理体系，为行业在数字化转型背景下实现数据要素的安全高效利用提供坚实支撑。

四、系统数据安全管控试点落地方法论

安全软件开发生命周期（以下简称“S-SDLC”，Secure Software Development Life Cycle）是一个帮助开发人员构建更安全的软件和解决安全合规要求的同时降低开发成本的软件开发过程。自 2004 年起，微软将 S-SDLC 作为全公司的计划和强制政策，S-SDLC 的核心理念就是将安全考虑集成在软件开发全生命周期（见下图 1），从要求阶段、设计阶段、实施阶段、验证阶段直至发布阶段。这一过程通过在每个阶段增加相应的安全活动来减少软件中的漏洞数量，并将安全缺陷降到最低程度，确保每一环节交付到下一环节的产品都是安全可控的。

图 1 生命周期

S-SDLC 不仅仅是一个流程或工具，它代表了一种按时间分程的思想方法，在软件工程领域内形成了一种原则。该模型帮助开发人员构建高安全性的软件，取得了巨大的成功。特别是在当前数据安全越来越受到重视的大背景下，如何从源头控制数据安全问题的发生，把数据安全问题融入到整个软件开发

生命周期中，已成为数据安全行业内的共识。

为了有效管理和保护数据，越来越多的企业选择将数据安全管理纳入软件开发生命周期的全过程。为此，许多组织借鉴了研发安全运维一体化（以下简称“DevSecOps”，Development Security Operations）的理念，结合传统的瀑布模型（见下图 2），，将数据安全从管理层面、流程层面、控制点层面及软件自动化层面，以体系化的思路来试点落地软件开发过程的数据安全。

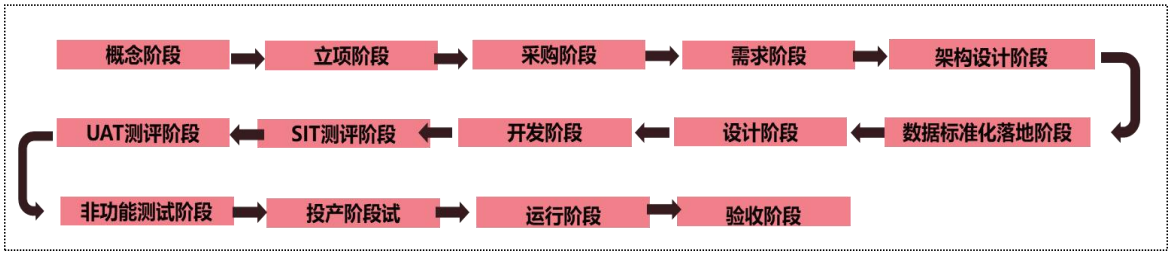


图 2 瀑布模型

基金行业高度依赖合规性、数据完整性与金融安全，系统通常涉及客户资产、交易结算和监管报送等关键功能，对安全缺陷的容忍度极低。S-SDLC 从需求、设计、编码到测试、部署各阶段嵌入安全控制，强调“安全左移”和全生命周期治理，契合金融行业强监管、重审计的特点。相比之下，DevSecOps 虽然在持续集成/交付中集成自动化安全检测，提升响应速度，但其敏捷性和自动化前提依赖成熟的安全基础设施和文化，在传统基金公司中落地难度较大。因此，以 S-SDLC 为框架，逐步融入 DevSecOps 的自动化与协作理念，通过“稳中求进”的

方式，逐步提升安全交付效率与响应能力，最终可以实现安全、合规、敏捷与可靠的有机统一。

课题组采用“基线化”+“工程化”+“技术化”理念，以法律法规、行业标准、实践指南为切入点，综合梳理数据安全相关监管条款及现状调研过程中产生的相关管理要求，提炼并形成数据安全控制基线，嵌入业务原有生产流程并在早期介入风险管理，降低业务数据安全风险。

在提炼过程中，核心关注合规要求、内部数据全生命周期管理相关的办法、条例、规定、细则，以及行业最佳实践，系统性地关联映射至控制目标及重要程序，从而形成适用于基金公司数据安全基线知识库的标准化方法。

通过标准化基线生成方法及数据全生命周期试点所需关注的重点数据安全管控措施，将其嵌入鑫元基金现有流程中，从项目及需求的创建开始，将数据安全控制要求与现有整体安全等级进行融合评定，在安全分析阶段融入数据安全基线对应的需求、设计、测试、运营等要求，从而形成数据安全管理闭环。

在试点过程中，课题组将核心关注整体流转是否通畅、各环节干系人是否清晰掌握相关技能、安全管控措施自动化比例

等内容，通过试点过程优化并提炼出推广流程。

五、系统数据安全管控试点落地步骤

（一）系统数据安全试点落地基线编制

鑫元基金以“数据生命周期安全技术控制要求知识库”为蓝本，同时参考数据安全典型处罚案例、优秀同业实践，并结合本行应用系统实际情况，最终编制出**15**条系统数据安全试点落地基线。

1. 编制步骤

(1) 遴选与裁剪

由于监管要求数量庞大，且多数为推荐性金融行业标准，在系统实践落地中无法也无必要将全量监管要求纳入系统安全开发生命周期中，因此需要对知识库中的数据安全控制要求进行遴选与裁剪，具体步骤如下：

① 监管处罚案例映射：将前期梳理的数据安全典型处罚案例与知识库中的数据安全控制要求进行映射，遴选出能够被映射的数据安全控制要求，并将其作为系统数据安全试点落地基线底稿；

② 不适用领域裁剪：将部分系统不适用领域进行裁剪，

例如：内部无线网络传输、物理介质传输、数据销毁等。

③ 非必要要求裁剪：部分监管要求涉及“优先…”“推荐…”措辞，考虑监管要求的落地难易程度，将此类要求进行裁剪；

④ 优秀同业对标：通过调研同业以及母公司数据安全实践情况，将已普遍满足的数据安全实践与知识库中的数据安全控制要求进行映射，遴选出能够被映射的数据安全控制要求，并将其作为系统数据安全试点落地基线底稿。

(2) 外规内化

经过遴选与裁剪后，课题组得到15条系统数据安全试点落地基线底稿。随后结合鑫元基金实际情况，对监管要求原文措辞进行优化，将系统数据安全试点落地基线底稿转化为适用于本地的、可供系统设计及开发人员参考的基线要求。优化方式包括但不限于对重点术语进行释义、对重要场景给出场景示例等。最终，形成系统数据安全管控试点落地基线。

2. 基线构成

数据安全基线横向可分为数据生命周期、生命周期细分场景、基线要求、适用级别、目的说明等方面，部分解释及示例如下。

(1) 数据生命周期：分为收集、传输、存储、使用、删除、销毁及全生命周期共七个领域；

(2) 生命周期细分场景：针对生命周期各阶段进行进一步细分，便于在后期落地时快速区分具体适用的控制项。例如：采集可分为“采集通用要求”和“从个人客户处采集”两种细分场景。对于外部数据采集场景，需要考虑“采集通用要求”；对于从个人客户处采集数据的场景，则两种细分场景均需考虑；

(3) 基线要求：系统必须满足数据安全底线要求；

(4) 适用级别：根据基线知识库，确定各控制点适用的数据级别，便于后续快速筛选各级别数据对应的控制要求。

编号	数据生命周期	基线要求	细分场景	适用级别
1	数据收集	收集投资者个人信息数据前，应以显著方式、清晰易懂的语言明确告知数据收集和处理的目的、方式、种类、保存期限，并获得投资者的明示同意。	收集数据前，系统界面应向客户展示单独的隐私政策协议，且以显著方式、清晰易懂的语言明确数据收集和处理的目的、方式、范围、规则、存储期限，并提供勾选框或签字栏获得投资者的授权同意。	所有
2	数据收集	从外部机构信息系统采集3级及以上数据时，应对数据提供方身份进行认证。	从外部机构（如企业客户、外部数据供应商等）信息系统收集3级及以上数据时，应对数据提供方身份通过静态口令、数字证书、动态口令等进行认证。	3级及以上数据

3	数据收集	从投资者处采集个人身份鉴别信息时，应对传输过程进行加密。	对从投资者个人信息主体采集的个人身份鉴别信息数据使用安全的加密算法进行加密。	3 级及以上数据
4	数据收集	面向投资者使用的 APP、WEB 等客户端相关业务完成后，不应留存投资者个人敏感信息（身份证号、手机号码、中文详细地址、中文姓名）、3 级及以上数据，并及时对缓存进行清理。	APP、WEB 等客户端相关业务完成后投资者个人敏感信息（身份证号、手机号码、中文详细地址、中文姓名）、3 级及以上数据至本地，可设计无痕模式，相关业务结束后，APP 及 WEB 需及时对缓存进行清理，因业务所需临时留存时需要进行本地数据加密。	3 级及以上数据
5	数据传输	互联网服务区应用系统与外部（含投资者或外部机构）数据传输时，应采用数字签名、时间戳、摘要、消息认证码等方式，确保数据的完整性和抗抵赖性。	互联网服务区应用系统与外部（含投资者或外部机构）数据传输过程中，应用系统应采用以下组合方式实现数据完整性和抗抵赖性： 1）数字签名：RSA、DSA、ECDSA； 2）时间戳：UTC 时间戳、Unix 时间戳； 3）消息认证码：HMAC； 4）摘要：SHA-2； 5）加密：AES-256,、RSA-2048 及以上。	所有
6	数据传输	互联网服务区应用系统与外部（含投资者或外部机构）数据传输过程使用的加密算法，不应使用 MD5、DES-CBC、SHA1 等已被证实为不安全的算法。	经营机构应当遵循国家密码管理部门和行业相关规定，使用符合要求的密码算法、产品和服务，禁止使用 MDS、DES-CBC、SHA1 等不安全的算法。	所有
7	数据存储	对于互联网应用系统，应对个人身份鉴别数据使用密码算法进行字段级加密存储。	对于互联网应用系统，应对个人身份鉴别数据使用密码算法进行字段级加密存储，加密应在系统实现，确保数据存储时状态为密文。	所有

8	数据使用	2级及以上的数据访问应进行身份认证，对访问者实名认证，将数据访问权限与实际访问者的身份或角色进行关联，防止数据的非授权访问。	2级及以上的数据访问应对访问者实名认证，可采用RBAC（Role-Based Access Control基于角色的访问控制）模型，将数据访问权限与实际访问者的身份或角色进行关联，防止数据的非授权访问。	2级及以上数据
9	数据使用	投资者个人敏感信息（身份证号、手机号码、中文详细地址、中文姓名）、3级以上数据从应用系统界面导出操作前应使用多因素认证或二次授权机制，应使用加密、脱敏等技术手段防止数据泄漏、并将操作执行的网络地址限制在有限范围内。	投资者个人敏感信息（身份证号、手机号码、中文详细地址、中文姓名）、3级以上数据的导出操作，应具备以下技术措施： （1）多因素认证或二次授权：多因素认证手段如要求用户同时使用静态口令，令牌设备或验证码进行身份验证；二次授权为要求数据访问者在进行身份验证后再次进行授权，以确保数据访问者的身份和授权的准确性。 （2）加密或脱敏：加密如AES、SM2、SM4；可配合数据脱敏系统使用，或采用泛化、抑制、扰乱、有损脱敏技术等； （3）通过设置IP地址白名单，将操作执行的网络地址限制在有限的范围内。	3级及以上数据
10	数据使用	互联网应用系统界面展示投资者个人敏感信息（身份证号、手机号码、中文详细地址、中文姓名）、3级以上数据后，应及时将展示数据从本地缓存中清除。	互联网应用系统对投资者个人敏感信息（身份证号、手机号码、中文详细地址、中文姓名）、3级以上数据展示后，应及时将展示数据从本地缓存中清除。	3级及以上数据
11	数据使用	应用系统涉及投资者个人敏感信息（身份证号、手机号码、中文详细地址、中文姓名）、3级以上数据界面展示对应后台管理及客户经理业务处理时，应采取数字水印等措施，标识信息系统当前数据使用账号、时间等信息；批量展示需脱敏。	应用系统后台管理及客户经理业务处理涉及投资者个人敏感信息（身份证号、手机号码、中文详细地址、中文姓名）、3级以上数据展示，应当实现： （1）数字水印：标识信息系统当前数据使用账号、时间等信息； （2）批量展示应脱敏：脱敏手	3级及以上数据

			段包括泛化、抑制、扰乱、有损等，脱敏可配合数据脱敏系统使用。	
12	数据使用	投资者个人敏感信息（身份证号、手机号码、中文详细地址、中文姓名）、3 级以上数据应当经授权并实施脱敏处理后才能用于开发测试，确需不经脱敏处理即用于开发测试的，数据处理者应当履行内部审批手续。	投资者个人敏感信息（身份证号、手机号码、中文详细地址、中文姓名）、3 级以上数据应当经授权并实施脱敏处理后才能用于开发测试，脱敏手段包括：泛化、抑制、扰乱、有损等，脱敏可配合数据脱敏系统使用。	3 级及以上数据
13	数据使用	在应用系统对外公开数据时，应采取有效技术（如网页防篡改）措施，保障公开数据不被篡改。	在应用系统对外公开数据时，应采取有效技术（如网页防篡改）措施，保障公开数据不被篡改。除了网页防篡改，也可采用其他防护方式防止公开数据不被篡改： （1）一般网络安全防护：防火墙、IDS/IPS； （2）数字签名技术：对公开数据使用数字签名技术，并建立数字证书管理机制，对数字签名进行有效管理，保证其可信度和安全性； （3）数据备份与恢复：建立完善的数据备份与恢复机制，定期对公开的重要数据进行备份，并存储在安全可靠的地方，以防止数据被恶意篡改时，可以及时恢复到最近的备份状态。	所有
14	数据使用	将投资者个人敏感信息（身份证号、手机号码、中文详细地址、中文姓名）共享或委托给第三方机构进行处理时应事先采用数据脱敏等技术防止数据泄露。3 级以上数据原则上不应共享或委托给第三方机构处理。	将投资者个人敏感信息（身份证号、手机号码、中文详细地址、中文姓名）数据共享或委托给第三方机构进行处理时应事先采用数据脱敏等技术防止数据泄露，除了数据脱敏以外还可以采用加密协议（例如 TLS/SSL）来保护数据在传输过程中的安全。确保与数据库服务器、网站和其他金融系统的	所有

			通信都经过加密。	
15	数据使用	应用系统应当建立统一的日志规范，明确数据处理活动日志应当完整记录的溯源所需信息，应用系统应当委托保存数据处理活动日志至少六个月、2 级及以上数据访问及操作过程应留存相关操作日志，操作日志应至少包含明确的主题、客体、操作时间、具体操作类型、操作结果等。	数据访问及操作过程日志一般被定义为记录在数据系统、网络应用或其他信息技术资源上的一系列事件和操作的详细记录。这些事件和操作包括但不限于用户访问、数据读取、数据写入、系统配置更改、错误和异常事件等； 为了保证数据在使用过程中的安全性，针对 2 级及以上的数据操作应留存至少六个月的操作日志，而操作日志的内容至少包含明确的主体、客体、操作时间、具体操作类型、操作结果等。	2 级及以上数据

表 3 鑫元基金数据安全基线示例

（二）在安全软件开发生命周期中嵌入数据安全管控

在本环节，课题组主要通过修订系统建设阶段管理文档，在系统安全软件开发生命周期中嵌入数据安全基线，系统建设阶段与相应的数据安全管控嵌入说明如下表 4 所示。

序号	系统建设阶段	数据安全管控嵌入	嵌入说明
1	概念阶段	否	/

2	立项阶段	是	《技术可行性分析报告》新增数据安全要求落地可行性分析章节。
3	采购阶段	否	/
4	需求阶段	是	通过场景关联出安全需求、安全设计、安全测试文档。
5	架构设计阶段	是	新增《数据安全评审项清单》，包含系统基线对应关注项，在系统架构设计评审会进行卡点核实清单内容。
6	设计阶段	是	1）通过《安全设计用例》提供指导； 2）数据库设计阶段，梳理数据库表设计，形成初步的数据字典清单后利用自动化工具进行分类分级。
7	数据标准化落地阶段	否	/
8	开发阶段	是	新增源代码审计工具（待建设），供开发过程持续验证基线满足情况。
9	SIT 测评阶段	否	/
10	UAT 测评阶段	否	/
11	非功能测试阶段	是	新增数据安全相关人工检核用例，配合进行闭环测试验证。
12	投产阶段	是	《上线评审表》新增数据安全基线要求符合评审内容。
13	试运行阶段	否	/
14	验收阶段	是	1）《项目验收报告》新增数据安全部门批准章节内容； 2）《项目后评价评分表》修订数据安全评价要点及调查问卷。

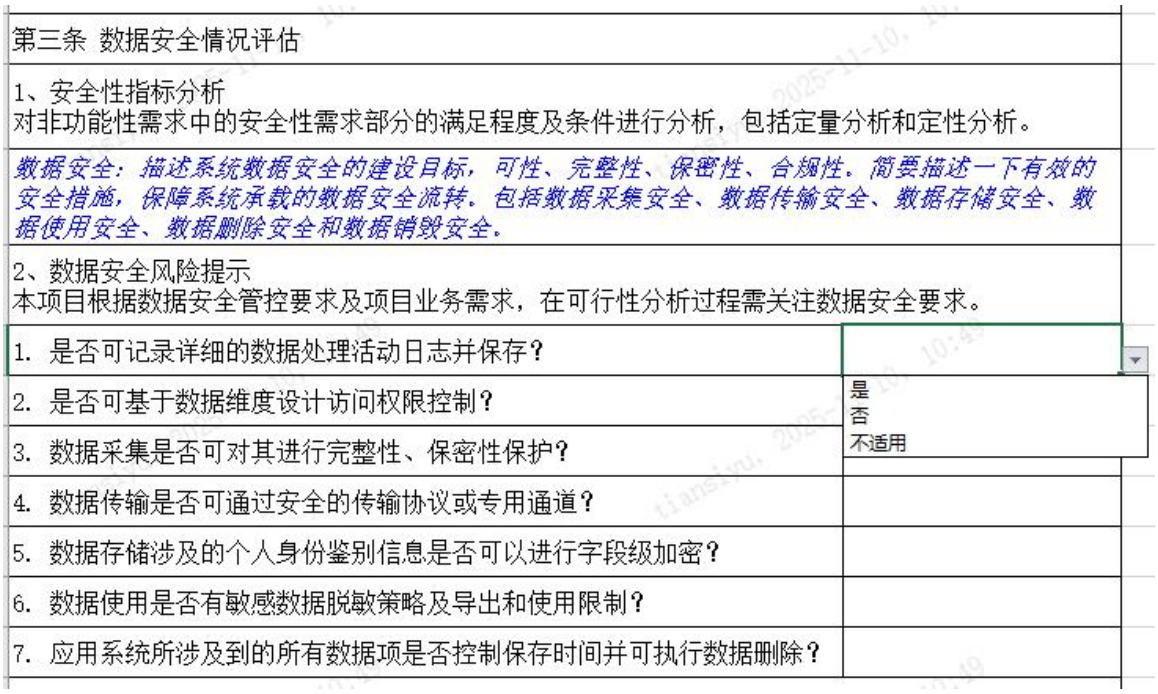
表 4 管控嵌入说明

1. 立项阶段

技术可行性是对立项阶段进行数据安全管控的重要一环。课题组通过将数据安全要求嵌入系统技术可行性环节中，对系

统所涉及的数据安全技术要求、数据安全技术资源等进行研究与评估，可以确定系统的数据安全要求在技术上是否可行。技术可行性评估有助于确定系统所需的数据安全技术方案、数据安全技术支持以及技术人员等是否能够满足系统的实施需求。

课题组对鑫元基金《技术可行性分析报告模板》（图 3）进行修订，主要包括以下两部分内容：一是在“安全性指标分析”中完善数据安全指标内容，将数据全生命周期安全融入数据安全指标分析中；二是新增“数据安全要求落地可行性分析”章节，在可行性分析过程中增加对数据安全要求的分析。



第三条 数据安全情况评估
1、安全性指标分析 对非功能性需求中的安全性需求部分的满足程度及条件进行分析，包括定量分析和定性分析。
数据安全：描述系统数据安全的建设目标，可性、完整性、保密性、合规性。简要描述一下有效的安全措施，保障系统承载的数据安全流转。包括数据采集安全、数据传输安全、数据存储安全、数据使用安全、数据删除安全和数据销毁安全。
2、数据安全风险提示 本项目根据数据安全管控要求及项目业务需求，在可行性分析过程需关注数据安全要求。

1. 是否可记录详细的数据处理活动日志并保存？	
2. 是否可基于数据维度设计访问权限控制？	
3. 数据采集是否可对其进行完整性、保密性保护？	
4. 数据传输是否可通过安全的传输协议或专用通道？	
5. 数据存储涉及的个人身份鉴别信息是否可以进行字段级加密？	
6. 数据使用是否有敏感数据脱敏策略及导出和使用限制？	
7. 应用系统所涉及到的所有数据项是否控制保存时间并可执行数据删除？	

是
否
不适用

图 3 《技术可行性分析报告模板》节选

2. 需求阶段

在需求阶段，开发人员根据《软件需求规格说明书》中“安全性”要求，以线下问卷形式（见下表 5），通过实际使用场景关联出数据安全需求。

ID	场景分类	问题
1	基础信息	系统提供服务的对象是谁？
2	基础信息	用户访问系统的途径有哪些？
3	基础信息	开发的应用类型是？
4	基础信息	系统是否涉及客户敏感信息？
5	系统对接	系统与行外第三方平台对接用途包含哪些？
6	基础信息	系统使用人员有哪些？
7	基础信息	系统的数据类型有哪些？
8	部署安全	是否使用云环境？

表 5 数据安全需求线下问卷

在需求阶段考虑数据安全要求具有重要意义，其通过把数据安全管控要求前移，实现系统的数据安全管控内生化，减少系统上线的防护和运维成本。

针对安全需求，课题组为基线要求逐一编写安全需求，生成《数据安全需求文档》，示例如下：

需求编号	安全需求	采用	补充
1	收集个人信息主体数据前，应以显著方式、清晰易懂	是	

	的语言明确数据收集和处理的目的、方式、处理的数据种类、保存期限，并须获得客户的明示同意。		

需求详解：

1. 收集数据前，系统界面应向客户展示单独的隐私政策协议，且以显著方式、清晰易懂的语言明确数据收集和处理的目的、方式、范围、规则、存储期限，并提供勾选框或签字栏获得客户的授权同意。

3. 架构设计阶段

在架构设计阶段，课题组在原有评审基础上新增《数据安全评审项清单》（表 6），在“系统架构设计评审会”时根据清单项进行卡点评审。评审内容包含系统基线对应关注项，包括数据处理活动日志要求、数据采集相关要求、数据传输相关要求、数据存储相关要求、数据使用相关要求、数据删除相关要求以及数据销毁相关要求。

序号	子序号	安全架构评审项	评审项说明
一、通用要求	1.1	系统是否留存数据处理活动日志并至少保存六个月？	应用系统应对数据处理活动过程留存相关日志，日志应至少包含明确的主体、客体、操作时间、具体操作类型、操作结果等，并至少保存六个月。 数据处理活动包括：采集、传输、存储、使用（访问、导出、加工、展示、开发测试、汇聚融合、公开披露、数据转让、委托处理、数据共享等）、删除、销毁。
二、数据采集	2.1	系统从外部采集数据时，是否具备技术手段确保真实性、保密性与合规性？	真实性：应用系统从外部机构信息系统采集 3 级及以上数据时，应对数据提供方身份进行认证（如通过静态口令、数字证书、动态口令，核实发送方的身份，确保对方为预期的、可信任的实体）； 保密性：从个人金融信息主体采集个人身份鉴别信息时应进行数据加密（如 AES-256、RSA-2048、SM2、SM4 加密）； 合规性：应用系统收集个人金融信息主体数据前，应以显著方式、清晰易懂的语言明确数据收集和处理的目的、方式、处理的数据种类、保存期限，并获得客户的明示同意。

三、数据传输	3.1	系统传输数据时，是否具备技术手段确保真实性、保密性、完整性和抗抵赖性？	真实性：对于与行内应用系统通信（包括 API 接口形式、批量文件传输形式等）的情况，应用系统应对行内系统进行身份认证，如通过静态口令、数字证书、动态口令； 保密性：若应用系统为 DMZ 区系统，在与外部（含金融客户或外部机构）数据传输时，应使用安全的加密算法（如 AES-256、RSA-2048、SM2、SM4 加密），不应使用 MD5、DES-CBC、SHA1 等不安全的算法； 完整性：若应用系统为 DMZ 区系统，在与外部（含金融客户或外部机构）数据传输时，应采用数字签名、摘要、消息认证码等方式确保数据传输的完整性。 抗抵赖性：若应用系统为 DMZ 区系统，在与外部（含金融客户或外部机构）数据传输时，应采用数字签名、时间戳等方式确保数据传输的抗抵赖性。
四、数据存储	4.1	系统存储个人身份鉴别数据时，是否采用字段级加密存储？	若应用系统为互联网应用系统，应对个人身份鉴别信息采用字段级加密（如 AES-256、RSA-2048、SM2、SM4 加密）存储。
五、数据使用	5.1	在相关业务完成后，是否未留存重点敏感数据（身份证号、手机号码、中文详细地址、中文姓名）、3 级及以上数据，并能够及时对缓存进行清理？	面向个人金融信息主体使用的 APP、WEB 等客户端相关业务完成后不应留存重点敏感数据（身份证号、手机号码、中文详细地址、中文姓名）、3 级及以上数据，并及时对缓存进行清理。
	5.2	系统访问、导出、展示、公开数据时，是否具备技术手段防止数据泄露？	访问：2 级及以上的数据访问应进行身份认证，对访问者实名认证，将数据访问权限与实际访问者的身份或角色进行关联，防止数据的非授权访问； 导出：应用系统针对重点敏感数据（身份证号、手机号码、中文详细地址、中文姓名）、3 级及以上数据从应用系统界面导出操作，操作前应使用多因素认证或二次授权机制，应使用加

			密、脱敏等技术手段防止数据泄露，并将操作执行的网络地址限制在有限的范围内； 展示：应用系统涉及重点敏感数据（身份证号、手机号码、中文详细地址、中文姓名）、3 级及以上数据展示且对应后台管理及客户经理业务处理时，应采取数字水印等措施，标识信息系统当前数据使用账号、时间等信息；批量展示时应脱敏。互联网应用系统界面展示重点敏感数据（身份证号、手机号码、中文详细地址、中文姓名）、3 级及以上数据后，应及时将展示数据从本地缓存中清除。 公开（对外）：应用系统对外公开数据时，应采取有效技术(如网页防篡改)措施，保障公开数据不被篡改。
	5.3	系统对数据进行汇聚融合时，是否已采用技术措施防止数据泄露？	应用系统涉及与第三方机构合作进行汇聚融合时，应采用技术手段如多方安全计算、联邦学习、数据加密等技术降低数据泄露、窃取等风险；应用系统汇聚融合不应用于 3 级数据。 （1）汇聚融合：指金融业机构因提供金融产品和服务、开展经营管理等活动，在机构内部不同部门之间或本机构与外部机构之间，进行多源或多主体的数据汇集、整合等产生数据的过程。 （2）多方安全计算：通过参与方准备、密钥交换、数据加密、协商计算协议、协同计算的步骤实现该技术。 （3）联邦学习：通过客户端数据准备、中心服务器建立、模型下载和更新、聚合操作、模型再下载和本地训练的步骤实现该技术。 （4）数据加密：如 AES-256、RSA-2048、SM2、SM4 加密。
	5.4	系统数据共享或委托给第三方机构进行处理时，是否已采取技术措施防止数据泄露？	针对重点敏感数据（身份证号、手机号码、中文详细地址、中文姓名）共享或委托给第三方机构进行处理，应用系统应事先采用数据脱敏等技术防止数据泄露，3 级及以上数据原则上不应共享或委托给第三方机构处理。 委托处理：指金融业机构因金融产品或服务的需要，在不改变该数据相关权利和义务的前提下，将数据委托给第三方机构进行处理，并获取处理结果的过程。 共享：指金融数据在不同机构之间进行分享，包含与行业主管部门的数据分享，各方均承担该数据相关权利和义务的过程。

表 6 《数据安全评审项清单》

4. 设计阶段

在设计阶段，课题组根据数据安全基线要求逐一编写安全设计要求，生成《数据安全设计文档》，示例如下。安全设计示例以 Java 语言为主，旨在为安全开发人员提供一套可参考、可扩展的数据安全设计文件。

安全需求	收集个人信息主体数据前，应以显著方式、清晰易懂的语言明确数据收集和处理的目的、方式、处理的数据种类、保存期限，并须获得客户的明示同意。

安全设计：在设计和实现这个功能时，建议考虑几个关键因素：前端界面、后端处理和数据存储。以下是一个简单的示例，展示了如何使用 HTML、JavaScript 和 Node.js 来实现这个功能。

前端（HTML）：

```
<!DOCTYPE html>
<html>
<head>
    <title>收集客户数据</title>
</head>
<body>
    <h1>收集客户数据</h1>
    <p>我们想要收集您的数据以提供更好的服务。请在下方勾选以表示您同意。</p>
    <form id="dataCollectionForm">
        <input type="checkbox" id="consentCheckbox"> 我同意收集我的数据。</input>
        <input type="submit" value="提交">
    </form>

    <script src="script.js"></script>
</body>
</html>
```

前端（JavaScript）：

在 script.js 文件中，我们添加事件监听器以处理表单提交。如果用户没有勾选同意框，我们将阻止表单提交。

```
document.getElementById('dataCollectionForm').addEventListener('submit', function(event) {
    if (!document.getElementById('consentCheckbox').checked) {
        alert('您必须同意收集您的数据才能继续。');
        event.preventDefault(); // 阻止表单提交
```

```
    }
});
```

后端（Node.js）：

假设使用 Express 框架，后端代码可能如下。此示例只是简单地处理，并未包含实际的数据存储逻辑。在实际应用中，需要将数据存储在数据库中，并确保遵循适当的数据保护和隐私法规，如《个人信息保护法》。

```
const express = require('express');
const app = express();
const bodyParser = require('body-parser');

app.use(bodyParser.json()); // for parsing application/json
app.use(bodyParser.urlencoded({ extended: true })); // for parsing application/x-www-form-urlencoded

app.post('/collectData', function(req, res) {
    const data = req.body; // 这里假设你的数据作为 JSON 对象发送到服务器
    // 在实际应用中，你应该在这里添加代码来存储数据，并确保遵循适当的数据保护和隐私法规。
    res.sendStatus(200); // 成功的 HTTP 响应码
});

app.listen(3000, function() {
    console.log('Server is running on port 3000');
});
```

这只是一个基本的示例，需要根据具体需求和环境进行修改和扩展。

5. 开发阶段

在开发阶段新增源代码审计工具，将涵盖代码安全性（包含部分数据安全基线）和编码规范，供开发过程持续验证数据安全基线满足情况。

6. 测试阶段

在测试阶段，课题组根据数据安全基线要求逐一编写安全测试要求，生成《数据安全测试用例》，示例如下：

安全需求	收集个人信息主体数据前，应以显著方式、清晰易懂的语言明确数据收集和处理的目的、方式、处理的数据种类、保存期限，并须获得客户的明示同意。

安全测试用例：

测试用例名称：客户授权同意验证

难易程度：中

用例等级：高

是否工具化：人工

测试目的：验证收集客户数据前，是否获得用户授权。

测试条件：1.系统已部署并可正常运行。

执行步骤：

1.打开应用程序或网站。

2.尝试进行操作，系统开始收集用户数据。

3.检查是否有任何地方提示用户阅读隐私政策等收集使用规则，并提供勾选框供客户进行授权同意。

测试结果：通过

7. 投产阶段

在投产阶段，课题组在鑫元基金系统上线评审表中新增数据安全基线要求符合评审内容（图 4），包含源代码审计、安全测试验证、数据安全设计及开发三方面数据安全基线投产前的核实方向。

七、数据安全部门审批			
数据安全测试结果（接入互联网系统需有）	□无数据安全隐患和问题 □存在数据安全隐患和问题（选择此项时请说明原因）		
数据架构部经理	（签字）	日期	年 月 日

图 4 系统上线评审表节选

8. 验收阶段

在验收阶段，课题组在鑫元基金项目验收报告、项目后评

价评分表两份文件中嵌入数据安全要求，旨在验收过程中确认系统是否遵循系统数据安全管理，同时将数据安全作为项目后评价评分要点，评估系统落地后的数据安全情况。

(1) 在项目验收报告中新增数据安全部门批准章节内容，包含数据安全需求、数据安全设计、数据安全测试三个维度，需提交《XXX 安全需求》《XXX 安全设计》《XXXX 安全测试报告》《XXX 源代码安全缺陷扫描报告》等文件证明。

(2) 在项目后评价评分表（图 5）中修订数据安全评价要点及调查问卷，涵盖数据分级安全保护、上线后数据安全防护效果等评价内容。

信息科技项目后评价评分表

指标分类	二级指标	三级指标	评价要点	评分标准	权重	分值
数据治理要求执行情况		数据安全	评估系统落地后的数据安全情况	5分:评估项目数据安全情况，完全遵循本行数据安全相关要求，结合数据分级要求实现差异化保护。 3分:评估项目数据安全情况，基本遵循本行数据安全相关要求，结合数据分级要求实现基本保护。 1分:评估项目数据安全情况，有违反本行数据安全相关要求的情况存在。	3%	

图 5 信息科技项目后评价评分表

（三）数据安全基线迭代更新

根据系统数据安全管控试点落地情况，鑫元基金将持续完善系统试点落地基线，不断丰富现有基线要求相关细节，使其更加契合现状，同时从数据生命周期安全技术管控要求知识库

中抽取新的管控要求，使系统试点落地基线持续迭代更新，形成可推广的行业实践。

六、研究结论与建议

（一）总体结论

通过上述系统性的研究，课题组认为将数据安全管理要求系统性“左移”并深度嵌入软件开发生命周期，对于公募基金行业而言总体具备充分的必要性与可行性。此举是经营机构应对趋严的监管环境、化解内生安全风险的关键路径，在保障安全与促进创新之间寻求平衡，能够为公募基金行业在数字化转型中构建坚实的数据安全底座。

该体系的必要性主要体现在三个方面：第一，业务内生需求。信息系统已成为基金公司业务运营与创新的核心载体，其开发过程本身就是数据生成、处理与流转的关键场景，在此环节早期缺乏数据安全设计，将为后续阶段埋下数据泄露、权限滥用等严重隐患，行业调研中暴露的“测试数据管理不当”“安全与开发脱节”等问题即为明证。第二，外部合规驱动。国家与监管机构密集出台的数据安全相关法规，对数据处理活动提出了全生命周期高管理要求，传统的“边界防护”与“事后审

计”模式已难以满足更严格的合规需求。第三，发展模式倒逼。公募基金公司普遍采用的外包开发、敏捷迭代等模式，此类模式给机构带来了数据安全责任分散、数据接口复杂等挑战，唯有将安全管控前移至源头的开发环节，才能实现从被动防御到主动治理的根本性转变。

该体系的可行性则建立在五大支柱之上：第一，政策法规有依据。我国已构建起核心的数据安全法律体系，并正在陆续颁布各类数据安全国家标准与行业规范，为数据安全管理的实践提供了明确的制度指引。第二，技术手段有支撑。数据分类分级、动态脱敏、代码安全扫描等关键技术已日益成熟，能为软件开发各阶段提供有效保障工具。第三，实践经验有借鉴。欧盟 GDPR 的“设计即安全”、美国 NIST SSDF 框架以及国内同业的先行实践，已验证了安全内嵌于开发流程的高度可行性。第四，行业基础已具备。根据课题组调研显示，基金公司在组织架构与人员管理方面已打下良好基础，具备了推进体系化建设的初步条件。第五，试点验证已通过。本课题构建的融合数据安全基线与 S-SDLC 的管控框架，在鑫元基金的试点中成功验证了其技术路径与流程的可操作性。

（二）具体结论

通过系统性地研究与实践，本课题得出以下四个层面的具体结论：

1. **在数据安全治理与组织层面，应建立权责清晰的协同机制。**研究结论表明，有效的管理始于明确的组织职责。基金公司需确立由董事会负最终责任、高级管理层组织实施、跨部门（信息技术、合规、业务）协同工作的治理架构，将数据安全职责明确分配到需求、设计、开发、测试等各个具体岗位，解决责任虚化问题。

2. **在流程与管控层面，应构建覆盖软件开发全流程的闭环体系。**课题组成功构建了以“安全左移”为核心的流程框架，系统性地将数据安全要求嵌入从立项到验收全流程的关键环节。通过增加数据安全可行性分析、关联安全需求、引入数据安全评审项进行卡点评审、设置数据安全专项评审等措施，形成了“可操作、可评审、可审计”的管控闭环。

3. **在技术与基线层面，应形成具体可执行的控制标准。**针对宏观要求落地难的问题，课题组通过“遴选与裁剪”“外规内化”等方法，提炼出 15 条核心数据安全基线要求。该基线横向覆盖数据全生命周期场景，并明确了各项基线的适用数据级别与管控层级（系统级/字段级），为开发团队提供了清晰、直接的技术实施指引。

4. 在落地与效能层面，试点已验证模式的有效性。在鑫元基金的落地试点证实，将数据安全基线要求融入现有流程与项目管理文档，能够在不大幅影响开发效率的前提下，实现对数据安全风险的源头管控。该模式确保了数据安全活动与开发活动同步进行，有效降低了系统“带病上线”的风险。

（三）应用与展望

基于本课题的成果与行业发展趋势，课题组对后续应用与深化工作的展望主要包括：

一是在技术发展层面，随着人工智能和自动化技术的快速演进，未来应重点推动数据安全管控工具与持续开发流水线的深度融合，通过智能化的手段实现数据安全需求的自动识别、代码的自动安全审计以及测试数据的智能生成与脱敏等目标，从而全面提升数据安全管控的效率和精准度。

二是标准规范的体系建设将成为行业数据安全管理体系发展的关键支撑。行业监管机构将会与行业协会牵头，以管理框架与控制基线为核心基础，推动数据安全管理行业标准或自律规范的制定，通过统一行业实践标准提供更明确的指导以及更严格的要求。

三是数据安全行业生态的协同共建不断深化。金融科技公司、第三方安全服务商在监管更为明确的要求下积极与行业经营机构战略合作，共同研发更贴合业务场景的数据安全解决方案，并通过建立行业最佳实践共享机制，形成协同共进、良性互动的安全发展生态。

四是经营机构内部的安全能力内化落地见效。基金公司将持续的安全培训与文化建设作为长期系统性工程，全面提升从管理层到一线开发人员的数据安全意识、责任，确保数据安全要求被深刻理解、主动执行并形成行为自觉，从而实现安全能力在组织中的深度内化和持续进化。

七、结语

在数字经济时代，数据安全是公募基金公司发展的基石，而软件开发流程作为数据处理的源头，其安全管理水平一定程度上决定了经营机构整体的数据安全态势。本课题通过系统性的分析、框架构建与实践探索，证实了将数据安全“左移”并内嵌于开发流程兼具必要性与可行性，并为行业提供了一套从治理、流程到技术基线的解决方案。随着国家与行业监管政策的持续完善与技术工具的不断演进，课题组将持续优化该管理框架与控制基线，并积极推动其向行业标准转化，以期助力公

募基金行业在保障安全、合规的前提下，充分释放数据要素价值，实现高质量、可持续的数字化转型。

本课题过程中得到了证监会科技司、证标委秘书处以及证标委 WG21 数据标准专业工作组的指导，得到了多家行业经营机构以及专业技术机构的大力支持。后续，课题组将继续与相关单位保持密切沟通，充分利用本次研究提供的交流平台和研究成果，研制形成行业标准，进一步促进提高证券期货业数据安全管理的标准化和规范化水平。

课题负责人:	杨晓宇	鑫元基金管理有限公司	副总经理、首席信息官兼信息技术部总经理
课题成员:	吴银刚	鑫元基金管理有限公司	数据管理部总经理
	田思雨	鑫元基金管理有限公司	数据治理
	张宇	鑫元基金管理有限公司	数据开发
	步若晨	鑫元基金管理有限公司	数据开发