长沙农村商业银行股份有限公司

大数据平台二期建设采购项目需求

**金融科技部**

**2022年10月**

目 录

[1 引言 1](#_Toc28228)

[1.1 背景 1](#_Toc2985)

[1.2 项目概况 1](#_Toc26558)

[1.3 读者对象 2](#_Toc9381)

[2 总体业务需求 2](#_Toc28841)

[2.1 业务目标 2](#_Toc25058)

[2.2 业务功能需求清单 3](#_Toc13845)

[3 总体技术需求 16](#_Toc2773)

[3.1 系统总体要求 16](#_Toc32190)

[3.2 系统建设反洗钱标准 17](#_Toc25079)

[3.3 系统架构要求 18](#_Toc3360)

[3.4 系统性能要求 19](#_Toc6168)

[3.5 系统兼容性要求 21](#_Toc22022)

[3.6 系统安全要求 22](#_Toc13099)

[3.7 系统部署要求 28](#_Toc1567)

[3.8 系统对接要求 30](#_Toc7377)

[3.9 系统测试需求 32](#_Toc6605)

[3.10 知识转移要求 33](#_Toc20180)

[3.11 知识产权要求 33](#_Toc7745)

1 引言

## 1.1 背景

为积极应对金融科技时代的挑战和机遇，促进《长沙农村商业银行股份有限公司2021-2023年三年金融科技发展规划》（简称“金融科技规划”）的落地实施，加速长沙农村商业银行股份有限公司（以下简称“本行”）数字化转型，通过应用更高效智能的数字化技术工具与解决方案，夯实数字化转型基础，完善全行数字化体系结构；打造数字化核心能力，丰富应用场景、深挖数据价值，将数据智能贯穿到经营管理全流程，实现本行的智能营销、智能投顾、智能风控、智能运营和智能管理，持续推动本行的信息化、数字化、智能化、开放化。

## 1.2 项目概况

遵照全行金融科技发展三年规划和数字化化转型方案，借鉴同业和互联网企业的先进经验，按照“总体规划、分步实施、急用先行、先有后优”的指导原则，计划分三期实施大数据平台及应用建设。

大数据平台一期已完成华为大数据基础平台的搭建、SmartBI、统一调度平台、外部数据管理平台、数据门户平台、大屏展示、数据看板等数据应用部署。一期已接入省联社下发数据及行内系统近300张表，开发了近100张固定报表，若干业务指标，并形成客户、产品、风险三大数据集市，为电子挎包、微贷项目提供了数据支撑。

本次二期项目内容包括丰富数据源，完善省联社下发数据、行内系统数据采集(包含外部数据采购)、下游系统迁移；从落地十大数据标准进行数据治理；完善数据门户平台以及丰富数据集市，为智能营销、智能投顾、智能风控、智能运营、智能管理以及各业务应用系统提供数据支撑等数据应用实施；建设数据补录平台、自助分析等工具平台。

持续完善大数据平台的建设，持续丰富数据源，持续开展数据治理、持续完善数据资产，丰富应用场景、深挖数据价值，将数据智能贯穿到经营管理全流程，实现本行的智能营销、智能投顾、智能风控、智能运营和智能管理，持续推动本行的信息化、数字化、智能化、开放化。

## 1.3 读者对象

长沙农商银行科技项目审批委员会、集中采购管理委员会等相关领导，以及信息技术部相关人员，包括但不限于部门领导、项目经理、开发人员、运维人员或测试人员。

# 2 总体业务需求

## 2.1 业务目标

根据行内《长沙农村商业银行股份有限公司2021-2023年三年金融科技发展规划》和《长沙农村商业银行股份有限公司2021-2023年数字化转型方案》，通过引进业内领先的大数据基础平台和应用软件，统一接入外部数据，实现行内、外数据资源的集中及整合，构建全行统一的数据标准，完善数据体系结构，自主掌握大数据关键技术，加速大数据资源的开发利用、深挖数据价值，将数据决策化贯穿到经营管理全流程，建设智慧银行，提升核心竞争力。

（一）建设大数据基础设施，完善全行数据体系结构

为落实本行数据中台架构规划，建设大数据平台，在集成省联社下发数据、行内系统数据、外部采购数据的基础上，实现更广泛的结构化、半结构化、非结构化数据集中采集、存储、加工、分析和应用，极大地丰富本行的信息资源，形成本行统一的基础数据体系，为经营管理的各类数据应用提供支撑。

（二）丰富数据应用场景，支撑全行经营管理创新

搭建数据中台是为数据应用提供通用服务，数据应用才是关键。大数据平台提供高性能可扩展的分布式计算引擎，通过数据挖掘、计量分析和机器学习等手段，对丰富的大数据资源进行开发应用，并将数据决策化过程应用到营销、投顾、风控、运营、管理等活动。

（三）培养数据人才队伍，提升本行核心竞争力

本行需培养自己的数据人才队伍，以推进全行的数据化转型，开展数据治理、管理数据资产、推广数据应用等。结合大数据平台项目建设，同步建立起一支拥有数据运营人才、高端建模人才、数据应用开发人才、数据安全人才等全方位的数据人才队伍，具备自主运营、开发应用、数据建模的能力，以更好推动业务创新，提升本行核心竞争力。

## **2.2 业务功能需求清单**

**2.2.1.丰富数据源**

**2.2.1.1.省联社下发数据**

完成省联社16个应用系统下发的150张表的接入大数据平台。

**2.2.1.2.行内系统数据**

全面分析并接入行内系统50张的数据，经过数据清洗转换并存储到大数据平台。

**2.2.1.3.外部数据**

全行统一采购并接入外部数据，实现数据库同步、文件导入、第三方系统接口直连（专线或互联网方式）等方式的数据采集功能，并将数据清洗转换存储到大数据平台。主要包括：天眼查的企业外部数据、政务数据的个人和企业数据、省市公积金数据、百行征信、电力数据等外部数据。

**2.2.2.数据治理**

**2.2.2.1.落地十大数据标准**

根据本行金融活动领域和标准属性,本行标准体系中将数据标准分为人员标准、机构标准、产品标准、客户标准、渠道标准、协议标准、事件标准、财务标准、公共标准、指标标准共十大主题，本次项目需要完成1000个数据标准的落地。每一主题的标准包括术语和定义、主题分类、主题信息性分类、主题信息项等。主题分类按照不同层级进行划分，具体划分至哪个层级依据主题的属性而定；信息项分类则通常由信息项大类及信息项子类构成。

**2.2.2.2.数据校验**

完善现有的数据校验规则，数据质量校验分为以下5部分，准确性、完整性、一致性、规范性、唯一性。本次项目补充100个相关校验规则。

**2.2.2.2.1.准确性**

准确性：表现在数据与目标特征之间的差异程序

1、数据的值域约束，即数据的取值应该其值域范围内（具有业务意义的连续范围）【数据值域约束】

2、数据的规则约束，是指业务上、技术上对于不用数据项间的相互校验关系，可以是等值校验，也可以为不等值校验【数据规则约束】如：合同到期日应大于开始日期

3、代码数据存在于代码列表【代码取值约束】

**2.2.2.2.2.完整性**

完整性：表现在数据的缺失程序

1、数据无值，即NULL【非空约束】

2、数据虽有值，但期值为无意义的空格或特殊字符【非法值约束】

3、记录缺失，即目标表中的记录数少于原系统中的记录数【记录缺失】

**2.2.2.2.2.一致性**

一致性：表现确保数据在数据仓库、应用场景中保持一致。

1、数据引用约束，即通常所说的参考完整性(数据引用约束)主外键。

2、同一个数据项在系统间或系统内部，该数据项的信息保持一致(数据流转约束)数据同步如：账户中的客户编号在客户信息中不存在，则说明不符合数据质量一致性标准。

**2.2.2.2.4.唯一性**

唯一性：表现是保证在一个字段或者一组字段里的数据与表中其他行的数据相比是唯一的。

主键唯一性约束，是指一个唯一标识智能属于一个个体。

**2.2.2.2.5.规范性**

规范性：表现是数据格式的规范程序

1、数据长度要求：即对数据长度的约束【长度约束】

2、数据精度要求：即对数据精度的约束【精度约束】

3、数据格式要求：即对数据中各位取值的约束，如日期的格式【格式约束】

**2.2.3.数据应用实施**

**2.2.3.1.数据门户平台**

数据门户平台，提供体验良好的数据查询、分析的交互式服务门户。支持在线查询、各类固定报表展示、审计分析、业务查询、经营分析等，支持多种查询方式灵活查询、低延时响应。

**2.2.3.1.1.首页改版**

打造面向数据用户统一的一站式服务门户，支持快速开发应用，数据查询检索，挖掘数据价值，降低数据使用的门槛，帮忙业务人员自主完成数据分析，更快地相应用户需求，需要对现有的门户进行改版。

**2.2.3.1.2.统一搜索功能**

统一搜索门户功能，利用搜索引擎和中文语义处理技术，集成内部结构数据，实现数据的统一搜索和聚合分析。可以按照报表、指标维度，输入关键字，按规则检索相应维度的数据源，反馈命中结果。 例如：输入指标名称反馈指标定义、指标值、同业值、监管规定等；而输入企业名称或身份证号可自动识别为客户搜索，反馈客户信息。其中门户体内搜索在门户内完成，体外搜索（包括行内系统和外部数据库）可通过接口传参的形式完成。

**2.2.3.1.3.报表监控日志**

实现用户操作查询报表、看板等日志的收集信息，通过对用户的统计分析，能让我们对用户行为有非常直观的了解，方便后续做行为分析。

**2.2.3.1.4.报表开发**

完成零售类每旬贷款数据、零售考核月报表，全行经营日报等共涉及报表数据7张，4张通用查询“固定报表”、3张监管报表优化需求等不少于15张报表的开发工作。

**2.2.3.2.数据集市开发**

大数据平台一期已完成建设面向客户、产品、风险主题的数据集市，构建全行统一的客户信息视图，为电子挎包、小微信贷平台等系统提供数据支撑。

**2.2.3.2.1.完善客户数据集市**

通过完善客户画像，打造高效率运营体系，提高管理和营销团队的执行力，快速识别低风险、优质客户，规避和预先识别风险。我们给用户画像打标签分类为两大类，基础类标签和个性化标签。标签通过不同的角度去定义和刻画一个用户，来满足不同的业务营销需求。以标签体系为基础，打造客户全景视图，全方位展现客户信息，对客户情况一目了然。

客户集市包括客户基本信息、客户产品信息、客户销售信息、客户价值信息、客户行为信息及外部数据信息等，预估涉及12张表的模型设计工作，为建立统一完整的客户视图提供数据支撑，同时客户信息整合是银行经营管理与信贷风险管控的基石。

**2.2.3.2.2.建设审计数据集市**

随着金融科技的快速发展，商业银行业务创新、业务管理、风险管控、内部控制等工作中对于行内外的数据需求日益增多，但由于行内系统建设等历史原因造成的大量缺失数据和错误数据，需求考虑不周导致的数据质量问题，出现系统间数据不一致，当前数据无法满足各种业务创新和风险管理等使用情况，同事还有操作人员在操作过程中的错误或不严谨，导致的数据问题，如电话号码和手机号码录入错误等。全行系统及系统间数据缺乏统一规划及有效数据字典，造成在数据应用中，出现查不了、差不实、查不通、查不全、查不上、查不清等问题。

针对我行目前的数据现状，我行需要赋予内审更大的职责，对内部审计提出了更高的要求。在现有审计资源条件下，淡出依靠传统的审计方式和手工作业模式，难以保障审计监督所必须的广度和深度。为了对行内各类业务和控制进行独立评价，以确定是否遵循工人的方针和程序，是否符合规定和标准，是否有效和经济地使用资源，是否在实现行内目标，迫切需要启动审计集市的建设。

审计集市按照业务分类,1）客户；2）渠道；3）授信；4）审批；5）合同；6）担保；7）押品；8）放款；9）计息；10）回收；11）不良；12）财务；13）费用；14）流水（内外部账户）；15）员工关系；16）业务（密码、开销户等）；17）理财；18）绩效，根据源系统的表，进行相关主题数据的归并和拆分的工作，而后由开发人员根据源系统表模型设计说明书,在行内大数据平台的基础上，进行审计业务宽表整合，预估新建6个主题，涉及10张表的模型设计工作。

**2.2.3.3.应用系统消费数据**

**2.2.3.3.1.网格化营销系统**

运用数字化、信息化手段，以街道、社区、村社、商圈、园区等为区域范围，以客户为管理内容，以网格管理员为责任人，通过网格化营销信息平台，实现上下联动、资源共享，为辖区内的农民、居民、商户、中小企业主提供主动、高效、有针对性的金融服务。通过认真细致的网格化营销工作，促进各项零售业务发展，有效防范风险，提升客户满意度，增强普惠金融工作成效。

网格化营销系统建设需求，分为三个阶段，主要涉及到客户、产品集市完善和补充。

一阶段有10个主题：对私客户基本信息、对私客户联系信息、对私客户签约信息、对私客户标签、对私客户业务统计表、对私客户经理业务统计表、对私客户机构业务统计信息表、客户授信统计表、客户经理授信统计表、机构授信统计表。

二阶段有9个主题：产品基本信息、对私客户管户关系、对公客户基本信息、对公客户联系信息表、对公客户签约信息、对公客户标签、对公客户业务统计表、对公客户经理业务统计表、对公客户机构业务统计信息表。

**2.2.3.3.2.智能金融服务平台**

智能金融服务平台通过营销应用功能和工具引擎实现对各类名单制营销、事件式营销、场景式营销服务的支持，在以客户为中心的营销服务运营理念指引下，结合客户标签数据、客户行为采集数据、客户基础指标数据的支持，配合员工对客户渠道、客户接触渠道、广告投放渠道、第三方合作渠道的营销执行，为不同特征的营销客群提供差异化的营销服务运营体系。

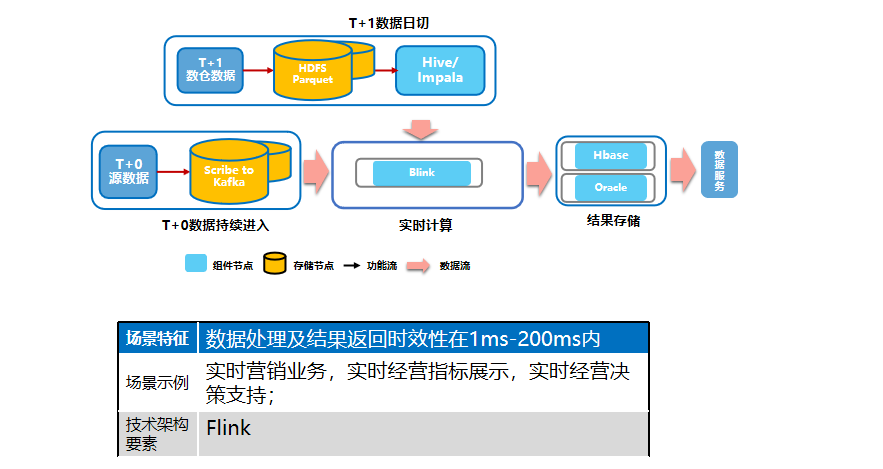
**2.2.3.3.2.1.提供接口服务**

大数据平台提供6个数据接口并且配合业务提供相关取数验证工作，为保证数据时效性对作业调度进行相应的改造。

**2.2.3.3.2.1.提供标签服务**

大数据平台本次提供客户画像相关的150个标签服务，具体标签内容见附件：基础客户标签。

**2.2.3.3.2.1.实施实时数仓**

几乎所有行业都有实时精准营销的需求，通过系统生成用户画像，在营销时通过条件组合筛选用户，快速提取目标群体，对数据时效性要求很高，需要构建全行级实时数仓，支持行内系统的实时数据的需求。

**2.2.3.3.3.产品定价系统**

**2.2.3.3.3.1.一阶段**

资产负债产品定价系统旨在通过建设系统实现管理机制建设、业务规则管理、存贷款定价测算、定价授权与审批、后评价及统计分析等目标。本次大数据平台需要提供57个数据接口给产品定价系统。

**2.2.3.3.3.2.二阶段**

大数据平台定位为全行统一的数据资源中心，总体目标是建设成强有力的数据中枢，规范全行批量数据处理的架构，提高供数的效率；建立统一的应用支持基础框架，支持各种分析型应用的开发；为业务的持续发展提供基础支撑。但是由于一些系统在建设时早于大数据平台，很多数据来源并未依赖于大数据平台，基于整体规划，需要完成这些系统的迁移工作，迁移策略为分阶段迁移，本次迁移系统为：产品定价系统，迁移目前的11个接口数据到大数据平台，由大数据平台完成11个接口的对接工作。

**2.2.3.3.4.长沙快贷**

该项目是通过对消费贷产品全流程风控体系的搭建，进一步完善行内现有的贷前、贷中和贷后的风险管控体系，全面提升行内自主风控能力；其次是对新的小微经营贷产品提供申请信用评级模型和专家策略，辅助行方搭建小微经营贷贷前风险管理体系。其数据支撑主要为征信数据入仓和实时供数。

**2.2.3.3.5.信用卡神俱乐部需求**

为更好地整合全行信用卡条线资源配置，打造信用卡营销队伍培养体系，推进信用卡业务高质量发展，拟借鉴互联网“游戏化”升级闯关式设计理念推出我行信用卡“卡神”俱乐部。采取“积分制+任务制”形式，以个人积分划分段位，针对不同段位配置不同的资源支持和奖励，同时配置专项任务包，提供专项奖励。积分从年初开始累计计算，年末清零。获取积分需坚持风控优先、合规操作的基本原则，对个人名下不良高于全行平均水平的人员，取消评优评先资格；对于与中介合作、索拿卡要或存在其他违规行为的员工，取消所有资源配置，按行内相关规定处置。

**2.2.3.3.6.普惠金融信息共享平台**

**2.2.3.3.6.1.客户风险报告**

个人客户风险报告：根据身份证号查询出该客户的行内基本信息、资产情况、授信情况以及人行征信信息、第三方百行征信、电力数据信息生成客户的风险报告。

对公客户风险报告：根据企业统一信用代码或名称查询出该客户的行内基本信息、资产情况、授信情况以及人行征信信息，并结合企业外部数据生成对公客户的风险报告。

**2.2.3.3.6.2.数据接口服务**

大数据平台负责整合普惠金融信息共享平台需要的上游数据，如：美好乡村、网格化平台、小微信贷平台等走访或业务开展所采集的客户信息，并整合外部数据后，按照普惠金融客户数据标准提供数据接口给普惠金融共享服务平台。

**2.2.3.3.6.3.报表开发**

3张普惠金融数据报表开发。

**2.2.3.3.7.数字零售信贷管理平台**

1.基于行内的历史数据、外部数据和贷后数据等情况，对策略中变量、规则、模型进行分析、设计和优化，包含信用卡、贷款信息及外部数据

2.存款及贷款都有的账户，关联贷后信息及基本信息进行分析。

**2.2.4.工具平台**

**2.2.4.1.数据补录平台**

数据补录平台为帮助我行进行数据补录，提高数据完整性；减少手工补录，提高工作效率及数据质量；减少各个部门的重复补录情况；提供历史数据抽取，补录部分字段功能。

补录系统可以作为一个数据源，提供数据。它可以为各系统提供更为明细的数据以及确定各个业务数据系统中比较含糊不定数据,也可以为满足应用集市和应用系统的数据要求提供数据，特别是应用集市，如监管报表集市、风险集市等。

补录数据主要有以下几种应用场景：

（1）数据完全缺失，需要从无到有地进行数据补录。中间操作包括：新增记录、修改记录、删除记录，数据检验，提交数据，审核数据，数据汇总等。

（2）数据已经部分存在，但是不完整，需要对个别记录或者字段进行修改补充。中间操作包括：修改记录，数据检验，提交数据，审核数据，数据汇总等。

（3）分布式录入。录入任务需要多个人协作完成，比如各个分行或者机构分别录入，录入后由指定人员进行提交、审核。这种方式通常需要录入后进行：补录、检验、提交、核查、审核、汇总、处理的操作。

（4）非分布式录入。录入任务不需要多个人协作完成。

**数据补录平台的基本原则**

（1）为保证补录数据质量，需要系统提供一定的检验规则，辅助补录人员补录数据正确。

（2）为监控补录数据质量，需要系统提供数据提交、检验和审核服务，提高数据准确性。

（3）补录审核原则：补录和审核分离。

（4）数据汇总原则：汇总层次按核心机构层次进行，部分任务需注意有补录，但不参与汇总情况存在。

（5）任务自动推送功能：系统根据业务提供的规则，推送本月需执行的相关任务。

（6）权限分配管理原则：除人员信息外，补录任务、审核任务都由各分行业务管理员进行统一分配

**数据补录平台的基本功能**

数据补录流程处理要求：从数据补录→提交→审核→入库，再到数据经过汇总等，直至数据展示给各级监管人员使用，其全程都由业务人员操作，不需科技干涉。

数据接口：与数据交换平台互联，实时获取源业务系统的数据，并在完成数据补录后回传给大数据平台，并支持识别补录标记增量回传。

数据采集：支持新增报表格式的采集表，定义对应的数据表名称和字段名称；发布后可新增数据项，如果下游系统不需要使用新增的数据项，则下游系统无需改造。

数据补录：铺底数据需按照业务规则明确主键，并按照主键进行回写，除补录字段以外，还需展示所有辅助判断的业务属性，可控制只有补录字段可编辑。

其它功能特点：支持单条录入和批量录入；支持数据留痕，对数据的修改、更新操作，以及记录补录人员及时间等信息进行完整记录，以便事后追踪；支持数据限时补录，数据定时锁定后执行数据批量；支持工作流配置，对数据补录进行复核操作；需要记录补录前和补录后的数据，方便进行差异比较。

**2.2.4.2.推广自助分析工具**

**2.2.4.2.1.背景介绍**

随着信息化技术的进一步发展，各种新技术的呈现，且我行积累的海量数据已经成为重要数据资产，如何使用数据资产成为业务发展的重要突破点。基于行内的大量数据，用其预测业务发展趋势，已成为行内业务、技术各部门关注的话题。结合我行的实际情况，很多部门还停留在日常数据提取，工具使用程度不够、数据使用场景不够丰富等阶段。为快速提升我行自助式分析工具的使用能力，释放部分科技人力资源，培养我行业务人员使用数据的习惯，规范全行数据服务出口。

**2.2.4.2.2.项目目标**

通过自助分析工具，在对自助分析服务做好底层支持工作的同时，对业务部门进行数据赋能，优化与提升数据使用能力。规划和实施相关基础工作，建立符合我行实际情况的宽表及模型，并在日常工作中给予业务部门相关的技术支持及业务支持。通过与业务部门的访谈，为数据使用需求旺盛的几个部门制定专题分析方案并落地实施，在技术输出的基础上，解决数据使用难、不会用的问题。自助分析服务以自助分析工具为基础，通过构建自助分析查询模型，在满足业务用数的同时，减少科技人员临时数据提取工作量，提高数据使用效率，提升各部门数据自主分析能力。

**2.2.4.2.2.项目内容**

自助分析的关键是构建标准化的数据模型。本次计划建设贷款主题、存款主题、信用卡主题、理财主题等业务主题数据进行分析，形成主题域数据分析包，按权限开放给相关数据分析人员使用。

**2.2.4.3.大数据平台扩容**

大数据平台一期采购了华为FusionInsight平台，共采购了720vcpu的节点授权。目前已部署3台管理节点、6台数据节点，剩余160vcpu授权。

为满足智能金融服务平台提出了实时数据需求，拟将批处理和实时数据分开部署，需独立部署3台实时数据节点（一期建设时剩余2个节点授权未使用），需要在现有基础上增加至少1个节点(80vcup)以满足实时需求。

同时，华为大数据平台的验收时间是2021年8月9日，远程维保1年于2022年8月9日到期。本次项目将续签维保服务以保障平台正常运行并定期进行巡检。

# 3 总体技术需求

## 3.1 系统总体要求

开发过程须充分考虑到先进性要求，包括但不限于以下方面：

（1）系统要具有高效性、开放性、可扩展性、前瞻性、高可用性，保证运行流畅且操作方便；

（2）系统性能要满足处理海量数据和大并发量交易的要求；

（3）系统功能要支持业务需求的快速开发实现；

（4）系统安全性要满足信息系统安全等级保护的相关要求；

（5）系统要保存所有交易数据，保存形式和保存期限要符合招标人数据保存标准；

（6）系统要便于我行或第三方维护，系统相关开发和升级改造文档要齐全；

（7）系统要具有全面整体设计方案和网络及软硬件配置建议方案。

## 3.2 系统建设反洗钱标准

（1）系统对接要求。系统在满足“3.8.1省联社接口”规定动作的基础上，在系统上线前须完成与省联社反洗钱监测分析及数据报送系统、名单监测管理系统的对接，确保系统各类客户、交易信息能无遗漏、准确、完整的接入反洗钱监测分析及数据报送系统；名单监测管理系统能够逐笔、实时调取系统交易，并进行阻断、提示、放行等操作。

（2）信息保存要求。系统各类客户、交易信息等记录保存应至少满足《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》（中国人民银行 中国银行业监管管理委员会 中国证券监督管理委员会 中国保险兼顾管理委员会令〔2007〕第2号）、《金融机构大额交易和可疑交易报告管理办法》（中国人民银行令〔2016〕第3号）中规定的客户、交易信息记录及保存要求，当与客户、交易记录等资料保存相关监管文件变更时，能够及时响应监管变化。

（3）信息保密要求。系统在满足“3.5系统安全要求”的基础上，必须符合反洗钱工作保密要求，严格控制各用户查询、查看、导出数据范围，特别是批量修改、拷贝、下载、对外传递等重要操作的内部审批流程；强化数据管理中的反洗钱信息的去标识化脱敏处理，将可用于恢复识别个人身份的反洗钱信息与去标识化后的脱敏信息分开存储并加强访问和使用的权限管理；加强通过界面展示反洗钱个人身份信息的管理，降低个人反洗钱身份信息在展示环节的泄露风险。当与反洗钱信息安全相关的监管文件变更时，或是与反洗钱信息安全相关系统运行环境、业务模式等发生重大变更时，更够及时响应变化，将反洗钱信息安全风险降低到可接受水平。

（4）业务管控要求。系统应设置灵活的业务管控功能，既包括管控对象的灵活选择，还包括管控手段的灵活配置；完整留存每次业务管控记录，完善留痕化管理；预留接口，以满足后续省联社反洗钱监测分析及数据报送系统的同步管控需求。应确保系统业务管控功能符合反洗钱工作需求，并根据监管及本行需求变更，及时响应变化。

## 3.3 系统架构要求

（1）项目组要提供详细的系统技术方案，内容包括但不限于设计原则、系统集成能力说明、系统稳定可靠性说明、系统安全性说明、系统运行效率的描述、系统管理说明、接口方案、数据整合方案、测试方案、验收方案、上线运行方案、辅助系统需求说明等等，及其他需要关注的内容；要求提供明确的系统版本号及实现方式（B/S或C/S），列出系统具体的模块及功能；

（2）项目组要按照国际标准、国家标准或行业标准，利用先进的软件设计方法论、设计模型和数据模型，进行符合工业标准和金融行业规范的系统开发；

（3）系统架构要分层清晰、健壮高效，能够适应招标人整体架构要求，通讯处理应与业务处理逻辑分离，具有快速的响应速度、良好的并发支持能力和交易完整性的保障机制；

（4）系统架构要具有良好的扩展性和高复用性，采用组件化、参数化、模块化和弹性化设计，保证软件系统架构易于改造和扩展，满足新业务功能的不断扩充，系统扩充保证不影响系统的各种原有功能；

（5）系统设计要充分集成和兼容现有软、硬件环境，符合监管部门的“两地三中心”容灾等要求，不影响我行既有软件、网络和硬件系统的性能和安全；

（6）系统使用的第三方产品，应说明该产品的性能、产地等并给出具体的性能指标说明或不同产品的对比，如并发用户数、稳定性、扩展性等；

（7）系统设计需要支持我行的统一身份认证等；

（8）系统设计需要支持我行的统一用户登录等。

## 3.4 系统性能要求

（1）系统要支持灵活的部署方式，要支持按不同类型的业务、不同的核心服务器等多种方式进行部署；

（2）系统要具有较高的可靠性和持续使用能力，保证全年7×24小时稳定运行，支持同时在线用户峰值不少于【2000】，并发数不低于【500】，登录响应时间不超过【3】秒，一般查询操作响应时间不超过【0.5】秒，复杂查询操作响应时间不超过【3】秒，系统响应时间最长不超过【5】秒。系统设计要按照每年业务量增加【10%】，考虑未来【五】年的发展空间；

（3）在不考虑外部系统耗时和网络延迟时，系统平均交易响应时间（系统自收到业务请求至处理完毕返回所须的平均时间）要小于300毫秒，在交易并发峰值情况下，系统平均交易响应时间要小于500毫秒；

（4）在满足交易响应时间要求的前提下，系统的实时联机业务所能提供的并发交易数量（同一时刻由系统处理的交易数量）峰值要大于100笔/秒，满足招标人未来5至10年内的业务发展需要；

（5）在满足交易响应时间和并发交易数量的前提下，系统的交易成功率（成功交易数占总交易数的比例）要达到99.99%，保证系统的稳定运行；

（6）在满足交易响应时间和并发交易数量的前提下，系统的交易正确率（处理和数据完全正确的交易数占成功交易数的比例）要达到100%；

（7）为了保证系统能够正常、稳定运行，系统在业务最高峰时的推荐配置计算资源占用率（CPU占用率和内存占用率）要小于60%；

（8）项目组要提供性能压力测试计划和验收标准，以及测试方案、环境、工具和调试策略（相应的报告文档），并负责完成压力测试，确保系统满足上述性能容量要求。

## 3.5 系统兼容性要求

（1）项目组要充分利用我行的现有软硬件及网络基础环境，根据应用和数据的性能、安全、存储等各方面要求，规划设计整个系统运行所需的软硬件及网络环境方案；

（2）系统要符合我行的现有软硬件基础环境（包括但不限于服务器、操作系统、数据库、中间件等）使用标准，具备开放性、通用性、标准性的特点，要使用业界主流产品，并支持和兼容国产化；

（3）系统web端需要兼容主流浏览器，如chrome、IE、firefox等；

（4）系统的移动端需要兼容移动端的主流浏览器，系统的移动端需要兼容IOS、安卓手机操作系统；

（5）系统支持的服务器要包括IBM、HP等小型机和PC Server及国产化同类产品，如不支持应由项目组确保兼容性；

（6）系统支持的操作系统要包括AIX、HP-UX、Linux等操作系统及国产化同类产品，如不支持应由项目组确保兼容性；

（7）系统支持的数据库要包括Oracle、DB2、Mysql等主流数据库及国产化同类产品，以及CDH、华为FusionInsight等大数据平台，如不支持应由项目组确保兼容性；

（8）系统支持的中间件要包括WAS、WebLogic、Tomcat等中间件及国产化同类产品，如不支持应由项目组确保兼容性。

## 3.6 系统安全要求

#### **3.6.1 身份鉴别**

1. 系统鉴别机制。应根据系统所处的环境，确定系统身份鉴别的强度要求，如：除了那些特定设为“公开”的内容以外，对所有的网页和资源的访问，必须在后端服务上执行标准的、通用的身份验证过程；用户认证通过后，如果在一定时间内（例如20分钟）无操作，用户需要进行确认性重认证；当用户连续鉴别错误次数超过阈值时（例如五次），将该用户锁定；每次鉴别都使用安全的验证码；在执行关键操作以前，对用户再次进行身份验证；对于重要的信息系统，推荐采用双因素认证方式；所有验证在服务端进行，验证问题的答案不能以任何形式返回客户端中（如图片验证码答案、短信验证码、验证问题答案等）；验证结果及下一步跳转操作由服务端直接进行；用户账号的上一次使用信息(成功或失败)应当在下一次成功登录时向用户报告；只有当所有的数据输入以后，才进行用户身份鉴别数据的验证。
2. 鉴别失败处理。在采取鉴别机制时，根据风险和用户的方便性，确定在鉴别处理失败时，允许鉴别失败的次数和提示的鉴别失败原因。（身份鉴别的失败提示信息应当避免过于明确。比如:可以使用“用户名和/或密码错误”，而不要使用“用户名错误”或者“密码错误”。）
3. 鉴别时采用的口令。输入的密码应当在用户的屏幕上模糊显示；用户的口令在存储、传输过程中必须是以密文方式存在；用户的口令必须以HTTP POST方式提交；用HTTPS协议来加密通道、认证服务端；对于采用静态口令认证技术的系统，口令长度至少8位，并至少包括数字、小写字母、大写字母和特殊符号中的三种类型；帐号口令的生存期不长于90天（不包括外部客户的账户口令）；最近使用过的口令不能使用，且密码在被更改前应当至少使用了一天，以阻止密码重用攻击；如果系统管理着凭证的存储，应当保证只保存了通过使用强加密单向哈希算法得到的密码，并且只有应用程序具有对保存密码和密钥的表/文件的写权限。
4. 密码重设/更改。密码重设和更改操作需要类似于账户创建和身份验证的同样控制等级；当使用初始密码时，强制修改初始密码；当再次使用临时密码时，强制修改临时密码；当密码重新设置时，通知用户；如果使用基于短信的重设，短信验证码应当有一个短暂的有效期（例如3分钟）。

#### **3.6.2 会话管理**

1. 注销。注销功能应当完全终止相关的会话或连接；注销功能应当可用于所有受身份验证保护的网页；在平衡的风险和业务功能需求的基础上，设置一个尽量短的会话超时时间。通常情况下，应当不超过几个小时（例如3小时）；如果一个会话在登录以前就建立，在成功登录以后，关闭该会话并创建一个新的会话。
2. 会话标识符。在任何重新身份验证过程中建立一个新的会话标识符；不要在 URL、错误信息或日志中暴露会话标识符；通过在每个请求或每个会话中使用强随机令牌或参数，为高度敏感或关键的操作提供标准的会话管理；生成一个新的会话标识符并周期性地使旧会话标识符失效(这可以缓解那些原标识符被获得 的特定会话劫持情况)；不允许同一用户 ID 的并发登录。

#### **3.6.3 访问控制**

1. 应用系统访问策略。需要考虑对应用系统的访问控制，从时间、IP地址、端口和用户角色来进行访问控制；对于需要通过外网访问的系统，则需要考虑采取防火墙技术，对于特别重要的运行在内网的系统，也需要考虑采取防火墙技术进行隔离。
2. 业务访问控制策略。需要从业务角度出发，从时间和用户安全属性（如用户身份、角色、安全级别等）允许或拒绝业务操作；支持权限控制，控制用户可以访问的业务种类、业务数据字段和其他资源；访问方式限定，可以指定用户业务数据能够执行的操作。如：读、写、删除、创建等；访问系统中非常重要的数据时，应采取多重身份认证方式；对关键数据进行加密，只有拥有密钥的用户才能解密访问。
3. 角色安全属性的管理。充分考虑权限控制，设定不同用户角色的权限来限制用户的访问权限和操作范围，在授权时应实现角色分离，如:一个帐号不能同时具有审计员和管理员两种角色。

#### **3.6.4 信息交换安全**

1. 外部系统连接必须要有身份验证检查；
2. 外部系统连接身份验证信息加密传输；
3. 用户密码加密传输；
4. 其它重要数据加密传输。

#### **3.6.5 交易安全**

1. 明确哪些交易需要实现抗抵赖性；
2. 明确系统中交易完整性、机密性、可用性要求；
3. 明确对各类交易的审计要求。

#### **3.6.6 数据安全**

1. 存储数据的保密性。确定系统存储中需要保密的数据以及应该采取的保密措施。
2. 传输数据的保密性。确定传输过程中的需要保密的数据以及应该采取的措施。
3. 存储数据的完整性。确定系统存储中需要保证完整性的数据以及应该采取的保密措施。
4. 传输数据的完整性。确定传输过程中的需要保证完整性的数据以及应该采取的措施。
5. 处理数据的完整性。确定是否需要采取措施来保证处理数据的完整性，如果需要，采取何种措施，需要考虑的要素包括交易过程完整性等。
6. 系统参数及代码的完整性。根据系统参数及代码的重要性，确定系统中需要保证完整性的系统参数及代码，以及需要采取的相应措施。
7. 安全导入导出。数据导入导出时，根据风险，确定是否有安全性要求，以及应该采取的安全措施。
8. 敏感信息展示。敏感信息展示时,如果是展示在Web页面上,应在后端服务器上进行敏感字段的脱敏处理。
9. 剩余信息保护。确定系统中是否存在特别敏感的信息，是否需要进行剩余信息保护。
10. 隐秘。确定系统是否有隐秘功能要求，即哪些信息可以被收集, 存储以及这些信息可以被谁泄露和泄露给谁。需要考虑的要素包括：与用户身份有关的安全上下文的设计、安全上下文与用户名（或身份）对应表的设计、用户授权等。

#### **3.6.7 组件配置**

1. 版本安全。确保框架或部件采用了当前的最新稳定版本。
2. 必要功能。移除所有不需要的功能和文件。
3. 测试代码。在部署前，移除测试代码。
4. HTTP。明确应用程序采用哪种 HTTP 方法:GET 或 POST，以及是否需要在应用程序不同网页中以不同的方式进行处理；禁用不需要的 HTTP 方法，比如 WebDAV 扩展；移除在 HTTP 相应报头中有关应用程序框架的无关信息。

#### **3.6.8 文件上传安全**

1. 身份校验。在允许上传一个文档以前进行身份验证。
2. 合法性校验。只允许上传满足业务需要的相关文档类型（采用白名单方式）；通过检查文件报头信息，验证上传文档是否是所期待的类型。只验证文件类型扩展是不够的。
3. 隐藏文件路径。进行文件保存时,成功上传的文件需要进行随机化重命名,禁止给客户端返回保存的路径信息。例如使用随机数改写文件名和文件路径。
4. 文件访问设置。进行文件下载时,应以二进制形式下载,建议不提供直接访问(防止木马文件直接执行)。
5. 存储环境设置。关闭在文件上传目录的运行权限。

#### **3.6.9 密码支持**

确定所采取的密码或口令强度、密码算法和密钥机制。

#### **3.6.10 输入、输出合法性检测**

1. 输入合法性检测。确定系统是否有输入合法性检测要求，合法性检查机制、检查范围等；输入合法性检查机制适用于所有的数据输入；检查范围包括数据的类型、长度、格式和范围等；对于多层架构的系统，在客户端和服务器端都应做彻底的合法性检查。
2. 输出合法性检测。程序输出数据校验。

#### **3.6.11 异常处理和日志**

1. 异常处理。确定系统发生异常时的处理要求，如非结构化异常处理、部分结构化异常处理、完全结构化异常处理等；不要在错误响应中泄露敏感信息，包括:系统的详细信息、会话标识符或者帐号信息。
2. 日志。不要在日志中保存敏感信息，包括:不必要的系统详细信息、会话标识符或密码。

#### **3.6.12 备份与故障恢复**

1. 备份。确定系统备份范围（对关键或全部数据进行备份）、备份策略、备份过程中的安全性等。
2. 故障恢复。确定系统故障恢复的方式及能力、故障恢复的时效性、故障恢复过程中的安全性。

#### **3.6.13 抗抵赖与安全审计**

1. 操作记录。对用户登录进行记录，记录内容包括但不限于用户登录使用的帐号、登录是否成功、登录时间和登录终端；记录用户对系统的操作，包括但不限于以下内容：帐号创建、删除和权限修改，口令修改，读取和修改系统配置，重要业务操作等，日志记录中需要包含用户帐号，操作时间，操作内容以及操作结果；对日志文件的读取、修改和删除操作进行权限控制。
2. 记录存储。应确定日志存储能力（大小）、日志安全性（完整性、保密性等）、日志可用性（故障恢复等）。

#### **3.6.14 安全管理**

1. 安全功能的管理。确定安全功能管理的范围与能力、安全管理模式（比如采用集中式管理，分布式管理或两者结合）、针对管理员自身的管理权限，对管理员进行授权管理等。
2. 安全属性的管理。确定安全属性管理的范围、安全管理模式（比如采用集中式管理，分布式管理或两者结合）、针对管理员自身的管理权限，对管理员进行授权管理等。
3. 安全功能数据的管理。确定安全功能数据管理范围（时钟、系统配置参数、安全功能配置参数、审计信息等）与能力、安全管理模式（比如采用集中式管理，分布式管理或两者结合）、针对管理员自身的管理权限，对管理员进行授权管理等。

#### **3.6.15法律法规特定要求**

对于特殊的涉密系统，按照国家相关法律法规进行设定。

## 3.7 系统部署要求

（1）项目组要提供详细的实施方案，包括但不限于项目管理、项目组成员及职责、分期实施计划、应用上线部署实施方案、数据库实施方案、备份接入实施方案、应急预案、系统日常维护方案等，系统安装、调试、试运行到验收期间的工作进度、发现的问题及解决方法均要记录在工作日志上，经项目负责人签字后各自保留一份；

（2）系统部署方式需支持虚拟化部署或容器化部署，对性能有特殊需求，如需部署在物理服务器之上，至少在上线前4个月提出需求。

（3）项目组要明确系统容灾等级，RTO、RPO指标。提供数据容量规划咨询，设计系统数据备份和恢复策略，定期对应急预案进行演练；

（4）项目组要承担软件部署规划、结构设计、系统所有的开发（包括由于需求变更导致的开发）、测试、故障诊断、完善工作。部署生产环境、功能测试环境和性能测试环境，针对性能测试结果，进行现场调优工作（如系统调优、中间件调优、数据库调优等）；软件的功能开发及测试要根据需求变更进行调整，系统开发测试过程要遵循《IT系统开发代码规范与安全标准》和《IT系统测试标准》；

（5）项目组负责协调、配合系统设备及相关软硬件的安装调试工作，物理服务器部署需支持主流x86服务器品牌型号，如华为、浪潮、HPE、联想等，虚拟化部署需支持主流虚拟化平台，如VMWARE、华为云等，操作系统需支持主流linux平台，如RedHat Linux、CentOS、Ubuntu、SUSE等，解决发现的质量及性能等有关问题，并根据实际环境进行适配；

（6）在系统建设全过程加强对各类科技风险的防范，严格按照相关监管部门风险管理的相关要求进行系统建设，全过程各环节的风险能有效控制，按照最小权限进行部署；

（7）项目组要签署保密协议并严格执行保密协议，保证针对项目实施涉及技术资料及内部信息不外泄。

## 3.8 系统对接要求

**3.8.1省联社接口**

1. 我行使用湖南省农村信用社联合社（以下简称“湖南省联社”）核心系统，项目组要负责对接湖南省联社相关系统，配合相关业务对接工作，支持与其相关系统之间的数据交换等；
2. 系统接口规范要满足省联社对我行系统的有效、无缝接入，要具有对软件系统运行的监控测试手段，能够有效支持与其它相关系统之间的数据交换；
3. 系统接口规范要该满足对数据一致性的要求，即在任何异常和故障情况下，一个交易对数据库的所有更新或是全部完成，或是没有执行，不能有中间结果，保证交易的完整性；
4. 在系统升级时，能提供最大程度上的软、硬件投资保护；
5. 确保交易的快速开发过程的质量和效率；
6. 系统上线运行后，项目组要按照我行的需求开发必需的接口供其他系统使用，直到满足验收要求。

**3.8.2行内接口**

（1）项目组要负责对接我行内部的相关系统，如jira、git、运维一体化平台等，配合相关业务对接工作，支持与其相关系统之间的数据交换等；

（2）系统接口规范要满足系统对我行系统的有效、无缝接入，要具有对软件系统运行的监控测试手段，能够有效支持与其它相关系统之间的数据交换；

（3）系统接口规范要该满足对数据一致性的要求，即在任何异常和故障情况下，一个交易对数据库的所有更新或是全部完成，或是没有执行，不能有中间结果，保证交易的完整性；

（4）在系统升级时，能提供最大程度上的软、硬件投资保护；

（5）确保交易的快速开发过程的质量和效率；

（6）系统上线运行后，项目组要按照我行的需求开发必需的接口供其他系统使用，直到满足验收要求。

**3.8.3外部接口**

（1）项目组要负责对接外部接口（外部采购的接口或外部提供的接口），配合相关业务对接工作，支持与其相关系统之间的数据交换等；

（2）系统接口规范要满足系统对外部接口的有效、无缝接入，要具有对软件系统运行的监控测试手段，能够有效支持与其它相关系统之间的数据交换；

（3）系统接口规范要该满足对数据一致性的要求，即在任何异常和故障情况下，一个交易对数据库的所有更新或是全部完成，或是没有执行，不能有中间结果，保证交易的完整性；

（4）在系统升级时，能提供最大程度上的软、硬件投资保护；

（5）确保交易的快速开发过程的质量和效率；

（6）系统上线运行后，项目组要按照我行的需求开发必需的接口供其他系统使用，直到满足验收要求。

## 3.9 系统测试需求

|  |  |  |  |
| --- | --- | --- | --- |
| **测试大类** | **解释** | **测试细类** | **是否进行** |
| 系统测试 | 对已经集成好的软件系统进行彻底的测试，以验证软件系统的正确性和性能等能满足其规约所指定的要求，检查软件的行为和输出是否正确并非一项简单的任务，它被称为测试的“先知者问题”。因此，系统测试应该对照测试计划进行，其输入、输出和其他动态运行行为应该与软件规约对比。 | 功能测试 | 是 |
| 性能测试 | 是 |
| 随机测试 |  |
| 验收测试 | 验收测试旨在想软件的购买者展示该软件系统是否满足其用户的需求。它的测试数据通常是系统测试的测试数据的子集。 | 验收测试： | 是 |
| 回归测试 | 回归测试是在软件的维护阶段，对软件进行修改之后进行的测试。其目的是检验对软件进行的修改是否正确。这里，修改的正确性有两重含义：一是所作的修改达到了预定目的，如测试得到改正，能够适应新的运行环境等等；二是不影响软件的其他功能的正确性。 | 回归测试 | 是 |
| Alpha测试 | 在系统开发接近完成是对应用系统的测试：测试后，仍然会有少量的设计变更。这种测试一般由最终用户或其他人员完成，不能由程序员或测试员完成。 | Alpha测试 | 是 |
| Beta测试 | 当开发和测试根本完成时所作的测试，而最终的错误和问题需要在最终发行前找到。这种测试一般由最终用户或其他人员完成，不能由程序员或测试员完成。 | Beta测试 | 是 |

## 3.10 知识转移要求

（1）项目组要确保在系统开发和建设中所提供的培训是全面而系统的，培训的主要对象是系统的使用者和技术支持人员；

（2）对相关人员的培训要为我行认为需要的所有培训（包括但不限于系统业务使用培训、技术运维培训、建模培训等），每项培训的受培训人员不少于十人，培训时间不少于三天；

（3）培训要保证技术人员掌握系统的设计思想、整体架构，具备独立的应用开发以及系统运维和管理能力，保证技术人员全面掌握系统开发和维护方法且能够独立操作。

## 3.11 知识产权要求

在项目实施期间，项目组要通过培训、研讨等方式，提升项目管理及运用能力。

项目组须提供本项目所涉资料包括但不限于：

（1）约定提供的部分源代码：包括但不限于客户化定制源代码、二次开发源代码等，提供的源代码要保证代码的完整性；

（2）所有说明文档：包括但不限于需求规格说明书、设计说明书（包括系统架构设计、概要设计、详细设计）、数据库设计说明书、测试计划、测试用例（SIT）、测试报告、系统安装手册、用户操作手册、系统维护手册（包含系统监控部分）、系统切换演练方案、上线方案等；

（3）相关工具：包括但不限于开发工具、编译工具、部署工具等，我行根据以上提交的文档可以独立完成环境的搭建，并通过源码验证（可通过源码编译产生平台执行程序）；

（4）本项目产品须严格按照最终合同中约定的license授权许可；

（5）与本项目有关的其他资料。

项目组提交的部分源代码、文档、工具、授权码或授权文件（若有）需经验收通过，且本项目部分源代码、文档、授权码或授权文件（若有）等必须在指定期限内全部提交。

知识产权要求包含以下内容：

1. 核心技术文档；
2. 部分源代码；
3. 系统开发所需的全部文档资料；
4. 系统实施过程中形成的各类文档。

项目组需提交一套可保存的、并容易查阅的中文文档，文档要求以纸质和电子格式提供，文档内容包括但不仅限于：

1. 定制化源代码注释及说明文档；
2. 项目实施工作说明书；
3. 需求说明书；
4. 整体实施架构设计说明书；
5. 概要设计、详细设计说明书；
6. 数据库设计说明书；
7. 操作使用手册、安装手册、维护手册；
8. 测试计划、测试用例、测试报告；
9. 数据移植方案、对外接口方案、上线方案说明；
10. 命名规范、软件质量管理标准、信息安全规范、编程规范、应用接口规范等；
11. 业务流程文档；
12. 模型开发相关资料和文档；
13. 培训相关资料和文档。

对于项目实施阶段目标设定的文档交付物，将作为本阶段工作完成的标志之一。对于文档交付物的描述要包含但不限于：各个阶段名称、阶段目标、交付物描述、形式（即文件、演示文稿、软件系统等）、建议的接受标准、阶段负责人等。

项目组要提供“知识产权要求”中的所有资料和文档并通过审核。