长沙农村商业银行股份有限公司

数字化内控平台（一期）建设采购项目

业务需求书

**内审部**

**2023年03月**

**目 录**

[1 引言 1](#_Toc14567)

[1.1 背景与目标 1](#_Toc22044)

[1.2 项目概况 2](#_Toc8976)

[1.2.1 同业情况 2](#_Toc21862)

[1.2.2 系统内情况 2](#_Toc7681)

[1.3 读者对象 3](#_Toc25547)

[2 总体业务需求 3](#_Toc14416)

[2.1 业务目标 3](#_Toc31494)

[2.2 项目范围及局限性 4](#_Toc7237)

[2.3 平台建设设计及框架 4](#_Toc15828)

[2.4 业务功能需求 5](#_Toc17653)

[2.4.1 主要业务功能概述 5](#_Toc14615)

[2.4.1.1风控模型管理 5](#_Toc6482)

[2.4.1.2监测预警 6](#_Toc30508)

[2.4.1.3风险地图 6](#_Toc1203)

[2.4.1.4机构/员工画像 6](#_Toc16077)

[2.4.1.5项目管理 7](#_Toc8350)

[2.4.1.6整改督导 7](#_Toc25149)

[2.4.1.7内控智库 7](#_Toc25050)

[2.4.2 机构用户和角色 7](#_Toc26763)

[2.4.3 业务功能清单 8](#_Toc2830)

[2.5 渠道支持 13](#_Toc27182)

[2.6 系统关联需求 13](#_Toc31109)

[3 总体技术需求 16](#_Toc844)

[3.1系统总体要求 16](#_Toc17604)

[3.2 系统建设反洗钱标准 17](#_Toc4453)

[3.3 系统架构要求 18](#_Toc12308)

[3.4 系统性能要求 19](#_Toc24385)

[3.5 系统兼容性要求 20](#_Toc9529)

[3.6 系统安全要求 21](#_Toc14666)

[3.6.1 身份鉴别 21](#_Toc27101)

[3.6.2 会话管理 23](#_Toc30139)

[3.6.3 访问控制 23](#_Toc3467)

[3.6.4 信息交换安全 24](#_Toc5966)

[3.6.5 交易安全 24](#_Toc15391)

[3.6.7 数据安全 24](#_Toc9804)

[3.6.8 组件配置 25](#_Toc16664)

[3.6.9 文件上传安全 26](#_Toc31533)

[3.6.10 密码支持 26](#_Toc10807)

[3.6.11 输入、输出合法性检测 26](#_Toc20265)

[3.6.12 异常处理和日志 27](#_Toc11339)

[3.6.13 备份与故障恢复 27](#_Toc19055)

[3.6.14 抗抵赖与安全审计 27](#_Toc17175)

[3.6.15 安全管理 28](#_Toc17619)

[3.6.16 法律法规特定要求 28](#_Toc3510)

[3.7 系统部署要求 28](#_Toc21813)

[3.8 系统对接要求 29](#_Toc13043)

[3.8.1 省联社接口 29](#_Toc27895)

[3.8.2 行内接口 31](#_Toc13665)

[3.8.3 外部接口 33](#_Toc26674)

[3.9系统测试需求 34](#_Toc7485)

[3.10 知识转移要求 35](#_Toc146)

[3.11 知识产权要求 36](#_Toc20066)

# 

# 1 引言

## 1.1 背景与目标

随着长沙农村商业银行（以下简称“我行”）各项业务的飞速发展及信息化建设的不断深入，创新性金融产品和金融服务不断涌现，业务数据和业务流程复杂程度不断提高，交易信息和管理信息不断膨胀。业务的长足发展和数据的迅猛膨胀给内部控制带来了新的挑战，各种风险不断增加，传统的内部控制手段已明显不适应进一步的发展要求，内控对象的信息化要求内控手段必须信息化，否则，内部控制跟不上业务发展的要求，内部控制的缺失或滞后将为业务的稳健发展带来巨大的风险隐患。

基于以上背景，我行有必要根据业务发展的需要，依托我行大数据平台，建立一套涵盖内审、风险合规、业务管理等三道内部控制防线的数字化内控平台，实现全行内控管理信息化。数字化内控平台建设分两个阶段实施：第一阶段，通过建立一个覆盖内部控制各项业务的数据集市，融合行内外数据，构建一套集数据查询分析、风控模型应用、项目管理、内控成果运用、整改督导等功能于一身的数字化内审模块，以风险为导向，以科技为支撑，依靠大数据分析，实现非现场数据分析与现场检查的有机结合，实现对违规问题和风险隐患的精确定位、精准打击，同时为各项业务经营和制度完善提供数据参考，从总体上提高审计工作的效率和效能，促进审计工作信息化、标准化、效率化；第二阶段，以制度为切入点，以问题为中心，聚焦业务管理条线、合规风险条线在检查作业、问题管理方面的规范化、标准化建设，建立全行问题库，同时依托大数据平台，不断建设和完善符合我行实际的风控模型，向业务前台、风险中台、审计后台输出高质量的管理数据及分析结果，建立合规风险监测、预警、评估（包括合规风险视图、合规风险画像等）体系，构建全行统一的数字化内控平台。本次项目主要建设第一阶段，即建立数字化内控平台内审模块。

## 1.2 项目概况

### 1.2.1 同业情况

经调研，国内具有一定规模的股份制银行、农村商业银行绝大部分建立了审计系统或类似平台，湖南省内长沙银行、华融湘江银行、三湘银行等具有独立法人属性的银行都建立了相关系统，其中大型股份制商业银行在十几年前就开始设计和使用审计系统。近年来，随着审计系统相关产品的不断迭代和成熟、各类业务数据及关联数据日益膨胀和扩充，传统的审计手段难以适应信息数据化的审计需求，审计系统在中小银行得到了日益普及，近3年来开始使用或迭代审计系统的农信机构包括安徽、甘肃、湖北、山东、四川、黑龙江等农信机构及东莞、江阴、大连、杭州、南海等地的农村商业银行，审计系统作为各家银行审计工作的重要审计手段及审计作业管理工具，为发挥审计监督、评价方面的作用提供了重要助力。

### 1.2.2 系统内情况

湖南省农村信用联社2019年10月上线了审计管理信息系统，为我行近3年的各项全面审计、专项审计提供了重要的审计线索，对降低我行审计成本、提高审计质量、提升审计效率、扩充审计覆盖面发挥了重要作用。但由于省联社审计系统非我行自主建设和运维，业务需求面向全省，存在数据来源不全（未包括我行自建系统数据及外部采购数据）、不能及时响应我行个性化审计需求（审计画像、风险地图等）、关键节点运行效率不高（省联社项目优先、全省运行压力等）等问题。基于此，在我行建立大数据平台的情况下建立一套自主控制的数字化内控平台，集中、整合行内外数据资源，实现符合我行个性化风控需求的大数据分析模型、机构/员工画像、风险地图、内控智库等功能，将作为省联社审计系统的有益补充，进一步释放审计潜能，快速、有效的响应我行各项审计需求，推动我行审计向“风险导向、数据驱动”的智慧型审计转变。

## 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，包括计划财务部、法律合规部、风险管理部、金融科技部、内审部等项目建设管理相关人员，参与系统招标相关厂商。

# 2 总体业务需求

## 2.1 业务目标

数字化内控平台第一阶段在充分考虑我行大数据平台系统架构及特点的情况下，整合省联社数据、我行自建业务系统数据及行外数据，实现资源共享和合理利用；提供灵活高效的数据查询服务，并对数据进行初步分析；建立风险监测和查证模型，提高审计工作的广度和深度；同时实现风险自动预警，及早化解行内金融风险；实现对审计日常工作和风险内控所发现的问题和风险状况进行分析，以多样化的形式进行展现，帮助及时调整审计工作重心和内控策略，真正实现以风险为导向的审计监督、评价作用；同时也为行内经营和制度完善提供数据参考；规范检查工作流程，实现项目管理、作业登记管理、整改督导管理的全流程管理模式，提高风控工作效率和质量。

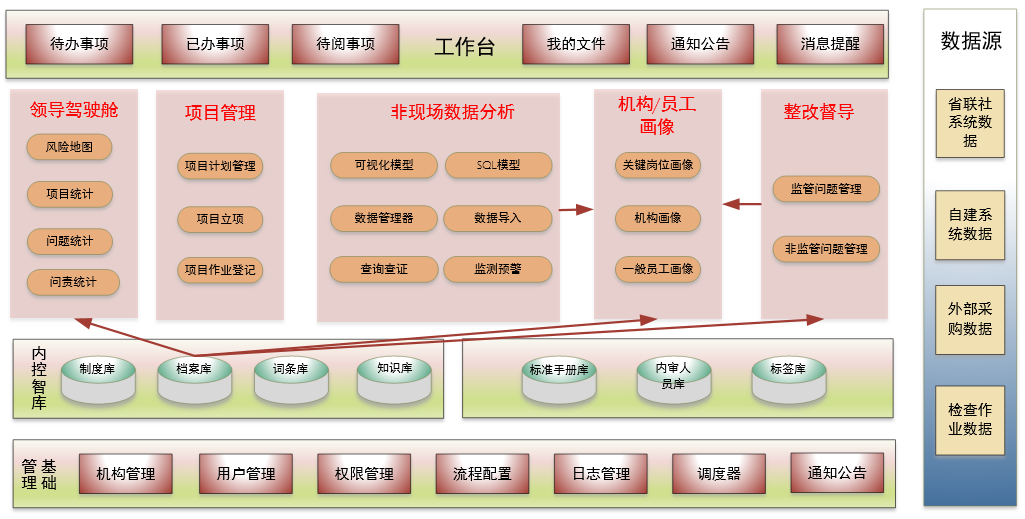
## 2.2 项目范围及局限性

数字化内控平台第一阶段覆盖我行审计主要业务，包括非现场数据分析、现场检查、审计成果运用、整改督导以及资料库等功能范畴。

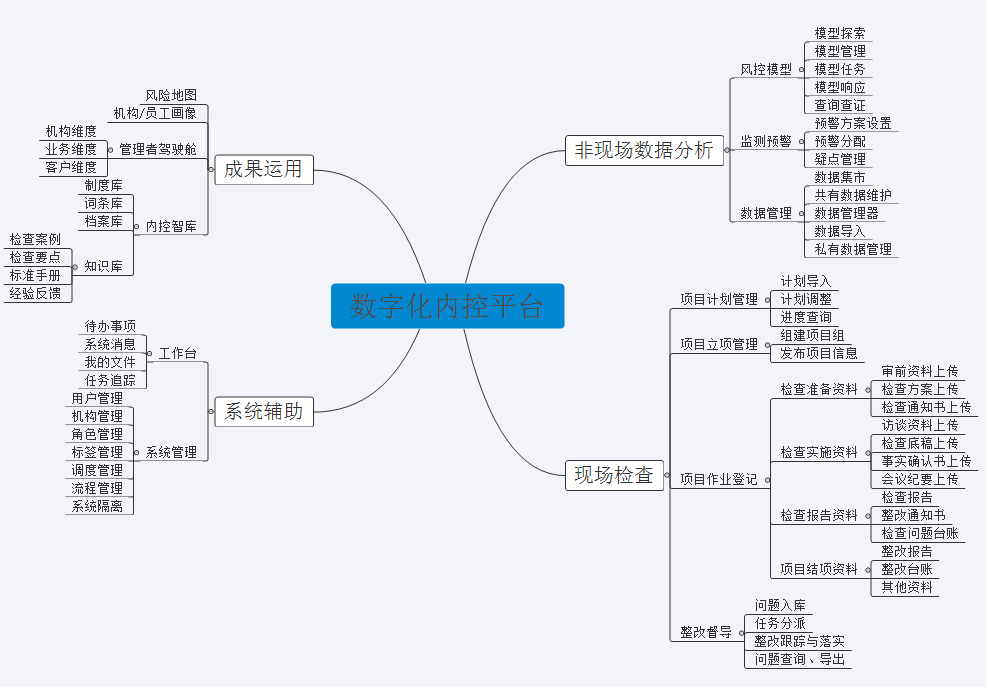
## 2.3 平台建设设计及框架

本次项目功能性需求包括核心功能业务需求和一般功能业务需求，其中核心功能业务需求包括机构/员工画像、风控模型、风险地图、监测预警、整改督导、项目管理等功能，一般功能业务需求包括内控智库、数据管理、工作台管理、系统管理、调度管理、档案管理、制度库、问题词条管理、日志管理等流程性功能和辅助性功能。

平台建设框架如下：



平台功能思维导图如下：



## 2.4 业务功能需求

### 2.4.1 主要业务功能概述

#### 2.4.1.1风控模型管理

风控模型是指通过可视化模型编辑工具进行模型编制及数据分析的过程，包括模型探索、模型管理、模型响应、模型任务等功能模块，是非现场数据分析的重要工具，数据来源包括省联社数据、我行自建系统数据、外部采购数据等。本次风控模型建设将充分考虑省联社审计模型，对于我行在日常工作中经常用到的或者认为可用性高的模型要移植到本平台（100个模型），在此基础上，要充分运用我行自建系统数据和外部采购数据，既要对已有模型进行拓展和优化，也要创建符合我行特色业务需求的风控模型（100个模型），重点包括信用卡管理、票据业务、员工行为等，为现场检查作业和其他检查应用提供高质量的数据线索。

#### 2.4.1.2监测预警

该功能模块实现对关注对象状态和行为的持续监测和风险预警，监测预警平台根据提供的数据分析工具建立风险剖析或风险监测模型，可以按日、周、月、季度、半年、年等固定运行频率或设定的频率对业务数据进行监测和预警。通过模型结果或指标的周期性推送，及时发现风险隐患，督促支行或业务部门及时采取控制措施，迅速发现、传递和处置系统预警信息，从而逐步建立动态监测、早期预警、持续改进的风险管理机制。该功能模块主要包括风险预警方案、预警信息分配、疑点管理3个细分模块组成。

#### 2.4.1.3风险地图

风险地图以图形化的表现形式，对我行主要风险点的整体分布及当前状态实现直观化的全景展现，该功能模块要从风险点数量、风险问题金额、风险严重程度等维度构建科学合理的风险权值体系，要分别以机构单位、业务领域为对象构建机构风险地图和业务领域风险地图，展现形式要简洁、直观、清晰、形象。

#### 2.4.1.4机构/员工画像

该模块要通过采集数据、构建标签体系、确定画像场景、画像呈现等过程对被关注对象进行画像，包括对关键岗位人员的画像、一般员工画像、机构画像，来实现对审计对象或审计业务丰富的、立体化的描述。机构/员工画像功能可在经济责任审计、全面审计、员工风险排查等场景进行应用。机构/员工画像的呈现形式包括标准化审计报告、重点可疑数据分析表、雷达图、知识图谱等多种方式展示，通过横向、纵向的对比，从不同角度进行分析、以多种形式展现结果，突出业务问题本质。

#### 2.4.1.5项目管理

该模块实现对检查项目计划管理、检查项目立项管理及检查作业登记管理，是现场检查作业全流程管理的重要辅助工具。其中检查作业登记管理支持通过标准化的格式模板自动对检查数据进行结构化转变，也支持对原有的历史检查成果资料进行手工录入并完成数据结构化处理，能根据检查数据的密级和重要性，提供设置审阅、编辑、增加、删除等用户权限管理功能，该功能是对历史检查成果进行统计分析的数据基础。

#### 2.4.1.6整改督导

通过该功能实现检查问题在线全流程化管理，包括推送或录入问题清单、被检查单位反馈流程、整改反馈确认流程、实时更新整改状态及问责情况、整改情况统计等，该功能支持通过OA系统进行消息推送和处理。同时，支持其他业务部门使用该功能模块。

#### 2.4.1.7内控智库

内控智库是内控管理的文档管理中心，包括制度库、知识库、词条库、档案库等4个功能模块。各项档案资料能根据数据的密级和重要性，设置审阅、编辑、增加、删除等用户权限管理。另外，制度库支持与我行办公OA系统进行对接，实现制度的定期更新。

### 2.4.2 机构用户和角色

（1）机构和用户。

系统用户基本架构为二级，第一层级为总行，设置系统管理员及操作员等，可进行参数管理、系统配置、角色管理、用户管理、被审计单位管理、现场检查、非现场数据分析等；第二层级为一级支行，设置操作员，可查询一级支行辖内审计问题统计信息，反馈整改情况等。

（2）角色及权限

涉及总行及一级支行全体用户，相关权限根据工作职责进行设置和分配，一般包括系统管理员、非现场业务操作员、现场管理员、模型编辑员、预警管理员、整改督导员、档案管理员等。

### 2.4.3 业务功能清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 一级模块 | 二级模块 | 大项 | 细项 | 功能说明 |
| 1 | 现场检查 | 项目计划管理 | 计划导入 |  | 年度审计计划由检查部门内部进行线下制定，制定完毕的计划由计划管理员导入至内控平台。 |
| 2 | 计划调整 |  | 针对已导入且审核通过的年度审计计划进行调整，包括调增、调减和调整实施团队等功能。项目一旦进入立项环节，将不允许再进行调整。 |
| 3 | 进度查询 |  | 以项目列表和进度条的形式展示项目进度，跟踪项目的执行情况。 |
| 4 | 项目立项管理 | 组建项目组 |  | 项目立项组建项目组成员，上传项目方案、实施时间等项目信息。 |
| 5 | 发布项目信息 |  | 发布项目信息，项目组成员查阅项目信息进行确认。 |
| 6 | 作业登记管理 | 检查前准备资料上传 | 检查准备资料上传 | 审前资料包括非现场数据分析的抽样数据、内控模型产出的可疑数据、其他途径收集的疑点信息等。 |
| 7 | 检查方案上传 | 通过本环节可以上传项目的检查方案，系统需支持在线编辑功能。 |
| 8 | 检查通知书上传 | 通过本环节可以上传项目的检查通知书。 |
| 9 | 实施资料上传 | 访谈资料上传 | 审计过程中产生的访谈资料通过本环节上传，支持数据结构化处理。 |
| 10 | 检查底稿上传 | 项目成员检查产生的工作过程记录，检查组成员可通过本环节上传。 |
| 11 | 事实确认书上传 | 项目成员检查产生的事实确认书，检查组成员可通过本环节上传。 |
| 12 | 会议纪要上传 | 项目成员检查产生的会议纪要，检查组成员可通过本环节上传。 |
| 13 | 检查报告资料上传 | 检查报告 | 编辑确定的检查报告正式稿，检查组成员可通过本环节上传。 |
| 14 | 整改通知书 | 编辑确定的整改通知书，检查组成员可通过本环节上传。 |
| 15 | 检查问题台账 | 编辑确定的检查问题台账，检查组成员可通过本环节导入和维护，支持数据结构化处理。 |
| 16 | 项目结项资料上传 | 整改资料上传 | 被检查的单位反馈的检查整改报告及整改台账，可通过本环节上传。 |
| 17 | 其他材料上传 | 检查计过程中产生的其他材料，可通过本环节上传。 |
| 18 | 整改督导 | 问题入库 |  | 将现场检查、非现场检查和其他渠道发现的问题纳入问题库集中管理，支持手工新建或导入子功能。 |
| 19 | 任务分派 |  | 系统将问题分派至整改机构指定人员，支持转派功能。 |
| 20 | 整改跟踪与落实 |  | 整改机构收到系统分派的问题跟踪任务后，处理人逐笔录入问题的整改情况各字段详情，并上传佐证资料，经逐级审核后更新问题库。 |
| 21 | 问题查询、导出 |  | 根据需要，多维度查询问题库，支持导出与推送查询结果。 |
| 22 | 非现场数据分析 | 风控模型 | 模型探索 |  | 模型探索通过可视化建模平台，业务人员能够将模型思路转化为风控模型，包括模型新建、模型编辑、模型查询、模型共享、模型另存、模型删除、模型执行、模型提交上线等功能。 |
| 23 | 模型管理 |  | 模型管理主要针对模型管理员对已上线的模型进行标签维护、下线、另存、权限分配、角色划分等操作以及查询功能。 |
| 24 | 模型任务 |  | 模型任务是检查人员根据检查需要灵活定制模型任务，可以根据需要选择多个模型批量运行和设置需要执行的机构以及日期范围。 |
| 25 | 模型响应 |  | 模型响应是业务人员针对具体检查项目或检查思路需要建模以满足相关检查需求而向建模人员提供建模需求，建模人员据此完成模型建设并提供模型数据的过程。 |
| 26 | 模型组合查询 |  | 对共同被审计对象或共同审计目的，形成组合模型，设置模型或模型结果权重分值，进行多角度触发，提高审计精准性。 |
| 27 | 模型落表 |  | 模型落表：支持将探索的模型进行落表处理，落表的内容包括但不限于指定运行的频率、运行的时间范围规则、机构代码规则等；落表的模型支持被系统调用执行。 |
| 28 | 查询查证 |  | 因后台数据结构复杂且逻辑关联等影响，需对业务人员常用的固定查询，可通过查证开发平台进行研发配置，发布上线后业务人员可以直接进行查询使用。 |
| 29 | 监测预警 | 预警方案设置 |  | 为了实现对关注对象状态和行为的持续监测和风险预警，监测预警平台根据提供的数据分析工具建立风险剖析或风险监测模型，可以按日、周、月、季度、半年、年等固定运行频率或设定的频率对业务数据进行监测和预警。 |
| 30 | 预警分配 |  | 监测预警支持自动及手动分配预警信息两种模式，预警信息分配策略可根据行内需要自行设定为按模型、机构、业务类型、岗位、角色等多种策略，也可通过手动分配方式分配给指定人员。 |
| 31 | 疑点管理 |  | 针对监测预警或模型任务推送的疑点数据，系统支持在线进行疑点管理，包括疑点分配、疑点核查、疑点认定等环节，根据不同的疑点数据情况，可以有内审部或被审计单位进行疑点核查和认定。 |
| 32 | 数据管理 | 数据集市 |  | 数据集市是对接内控平台的内控审计数据集市，在数据集市上建立数据集市用户和空间，用于加工信贷、财务费用等数据宽表、落地风险模型结果等。 |
| 33 | 共有数据维护 |  | 规范数据集市的数据管理、数据接入、数据使用的标准，提供前台可配置的数据表及字段的维护功能，包括数据表的基本信息、标签分类，字段基本信息和字段的特殊属性等。 |
| 34 | 数据管理器 |  | 数据管理器中可以查询已经接入内控平台的业务系统数据表及个人私有数据表。同时，可以通过“通用查询”功能，查询数据表的数据。 |
| 35 | 数据导入 |  | 数据导入是提供前台页面导入业务数据文件的功能，支持可按模板导入，包括：新增、追加、覆盖等方式。支持EXCEL、CSV、TXT文本等格式的文件导入。 |
| 36 | 私有数据管理 |  | 私有数据是指通过“数据导入”模块导入的数据表，这部分数据只有导入人可见，看不到其他用户的数据，所以只能由用户本人管理维护自己的私有数据。 |
| 37 | 审计成果运用 | 风险地图 |  |  | 风险地图以图形化的表现形式，对我行主要风险点的整体分布及当前状态实现直观化的全景展现，该功能模块要从风险点数量、风险问题金额、风险严重程度等维度构建科学合理的风险权值体系，要分别以机构单位、业务领域为对象构建机构风险地图和业务领域风险地图，展现形式要简洁、直观、清晰、形象。 |
| 38 | 机构/员工画像 |  |  | 该模块要通过采集数据、构建标签体系、确定画像场景、画像呈现等过程对被关注进行画像，包括对关键岗位人员的画像、一般员工画像、机构画像，来实现对检查对象或审计业务丰富的、立体化的描述。内控画像功能可在经济责任审计、全面审计、员工风险排查等场景进行应用。机构/员工画像的呈现形式包括标准化审计报告、重点可疑数据分析表、雷达图、知识图谱等多种方式展示，通过横向、纵向的对比，从不同角度进行分析、以多种形式展现结果，突出业务问题本质。 |
| 39 | 统计分析 |  |  | 该模块用风险视图的形式向行内管理层展示预警信息核查处置的结果及风险发展趋势，并按照机构、业务条线等主题进行分类展现，管理层可以对关注重点点击相应主题进一步了解，页面可逐级展示明细结果。该模块用来从检查年度、被检查机构、项目名称、检查业务领域、检查人员、内控模型使用情况等不同维度统计检查项目开展情况及问题发现情况。 |
| 40 | 内控智库 | 制度库 |  | 本模块包括行内制度、行外制度，提供各类制度的新增、删除、查看、下载等功能。其中行内制度模块支持对接我行OA系统，实现对我行制度进行定期更新。 |
| 41 | 词条库 |  | 词条是根据将各个历史检查项目的问题进行汇总、分类整理、归纳总结而形成的，以便对问题进行规范化表达。该功能模块包括词条的增加、编辑、查看、查询、删除、作废、审核审批、启用、导入导出等功能。 |
| 42 | 档案库 |  | 档案库是内控审计条线工作的电子档案管理中心，包括用来归集和整理各类专项审计、经济责任审计、突击检查等审计项目及重要工作总结、重要会议资料、部门管理行政资料等综合性档案等。支持根据数据的密级和重要性，设置审阅、编辑、增加、删除等用户权限管理。 |
| 43 | 知识库 |  | 知识库包括审计案例、标准手册、经验反馈、外部监管数据等4个子模块。系统提供知识库具体内容的增加、在线编辑、删除、上传及下载等功能。 |
| 44 | 系统辅助 | 工作台 | 待办事项 |  | 系统中提交的申请都集中在待办事项中由审批人进行审批，显示最新需处理的审批个数和累计已办理的审批数。 |
| 45 | 系统消息 |  | 在工作台模块，支持查看并操作我的消息，工作台——系统消息——执行相应操作。 |
| 46 | 我的文件 |  | 在工作台模块，申请导出文件默认存储在后台服务器指定目录中，必须经过审批通过后，才允许到我的文件下载附件至本地，若不需要该文件支持删除后台数据文件功能。 |
| 47 | 任务追踪 |  | 用户提交模型或任务运行后，为便于用户查看任务的运行进度，在工作台的任务跟踪栏位进行显示。对于执行完毕的模型或者任务，可点击直接查看结果，对于失败的任务，可以查看错误信息。 |
| 48 | 系统管理 | 用户管理 |  | 对人员的信息维护，包括内控部相关人员、被检查单位的人员。操作有：用户编辑、分配角色、分配空间等功能。 |
| 49 | 机构管理 |  | 包括检查机构和被检查机构的新增、修改、删除、撤销操作，机构之间以树状结构表示其归属关系。 |
| 50 | 角色管理 |  | 角色管理包括领导角色和系统角色，主要控制功能模块的操作权限，支持一个用户可以拥有多个角色。支持角色的增加、删除、编辑、分配资源及清除互斥角色功能。 |
| 51 | 标签管理 |  | 标签管理，支持对系统中数据表、模型等模块的标签进行灵活配置，如：业务种类、模型类型、信息系统、风险等级等，支持树状或列表，支持单选或多选。 |
| 52 | 调度管理 |  | 调度管理，提供模型批量运行、监测预警、数据处理加载等任务的监控、调度及日志查看等功能。 |
| 53 | 日志管理 |  | 包含用户在系统所有操作日志，包括系统日志、应用日志、跑批日志、错误日志、反馈日志、用户登录、注销和日常操作日志等，支持对所有日志记录进行查询、分析和导出。 |
| 54 | 流程管理 |  | 流程管理，实现对系统中涉及的审核审批等事项进行灵活配置，并配置相关审批角色。 |
| 55 | 系统隔离 |  | 系统隔离，通过指定热键或虚拟账号实现对系统特定功能模块进行隐藏，可以选择隐藏哪些功能模块，哪些不隐藏，用来特殊情况下的外部展示。 |

## 2.5 渠道支持

支持PC端。

## 2.6 系统关联需求

数字化内控平台的核心功能是在我行大数据平台的基础上建设一个完整标准的数据集市，覆盖内控各项业务数据，为各项风控模型及场景应用提供数据基础。从涉及业务角度划分，系统取数范围主要包括但不限于授信、运营、财务、票据、人力、绩效等，涉及系统包括但不限于核心业务系统、信贷管理系统、财务管理系统、总账系统、借记卡系统、客户关系系统、人力资源管理系统、大数据平台、业绩计量系统、资金转移定价系统（FTP）、费控系统、OA系统、内容管理平台、红绿灯积分管理系统、信用卡账户管理系统、日志平台、运维平台、全栈监控平台、自动化建模工具、数据脱敏工具、知识图谱、短信平台、统一消息平台、统一用户平台、ESB系统、行内注册配置中心等。从数据来源的角度划分，包括省联社业务系统、我行自建系统以及第三方外部数据（司法、工商、征信、民政等）。详细具体的数据需求需要待详细设计阶段确定，部分关联系统描述情况如下：

**关联系统描述**

（1）核心业务系统、信贷管理系统、财务管理系统、总账系统、借记卡系统、客户关系系统等：该系列系统由省联社开发并管理。

（2）人力资源管理系统：全行员工管理、薪酬管理、绩效管理、招聘管理系统。

（3）大数据平台：全行统一的数据分析、挖掘、处理平台。

（4）业绩计量系统：关键业务指标考核管理，为全行员工绩效管理提供依据。

（5）资金转移定价系统(FTP)：用于为行内资金转移提供内部定价机制。

（6）费控系统：全行费用管理系统。

（7）OA系统：人员组织管理及流程化办公管理。

（8）内容管理平台：全行统一音影、图像等内容存储平台。

（9）红绿灯积分管理系统：全行员工及支行违规积分管理系统。

（10）信用卡账户管理系统：全行信用卡客户账户查询、统计管理系统。

(11)日志平台：全行系统日志管理平台。

(12)运维平台：全行系统应用、配置制品管理及自动化发布平台。

(13)全栈监控平台：全行系统应用监控平台。

(14)自动化建模工具：端到端、可解释的交互式机器学习建模平台。

(15)数据脱敏工具：数据脱敏工具。

(16)知识图谱：全行构建的知识图谱。

(17)短信平台：全行短信发送、管理平台。

(18)统一用户平台：全行机构、人员的统一管理平台。

(19)ESB系统：企业服务总线。

(20)注册配置中心：行内统一的Nacos注册中心及Apollo配置中心。

（21）其他合作系统，根据业务实际情况补充。

**关联功能描述**

（1）核心业务系统、信贷管理系统、财务管理系统、总账系统、借记卡系统、客户关系系统：为系统提供核心业务数据来源，对接以保障数据实时更新。

（2）人力资源管理系统：提供员工基本信息、工作简历、绩效薪酬、年度评价等数据。

（3）大数据平台：审计集市数据由大数据平台T+1供数，由大数据平台统一加工和处理，供数据应用系统使用,大数据平台原则上只提供原始数据，由内审平台主要进行数据加工和开发工作，大数据平台提供支持。

（4）业绩计量系统：提供员工业绩数据。

（5）资金转移定价系统(FTP)：提供内部资金转移定价数据。

（6）费控系统：提供费用报销、预算管理等费用数据。

（7）OA系统：对接OA员工信息及组织架构、规章制度等。

（8）内容管理平台：各项目整理音影、图像等内容，由内容管理平台提供统一的接口或格式要求，进行对接。

（9）红绿灯积分管理系统：提供全行员工及支行违规数据信息。

（10）信用卡账户管理系统：提供全行信用卡客户账户流水信息。

(11)日志平台：将系统日志纳入到日志平台统一管理。

(12)运维平台：将制品纳入管理，对接自动化发布及批量任务管理。

(13)全栈监控平台：将系统纳入到平台进行应用的全栈监控。

(14)自动化建模工具：对接自动化建模工具便于后续开展数据模型开发。

(15)数据脱敏工具：对接数据脱敏工具便于后续开展数据模型开发。

(16)知识图谱：对接知识图谱便于后续开展数据模型开发。

(17)短信平台：全行短信发送、管理平台。

(18)统一用户平台：全行机构、人员的统一管理平台。

(19)ESB系统：接入ESB实现内部系统之间调用、本系统接口发布及文件在ESB文传平台上的传输。

(20)注册配置中心：将系统服务的注册及配置纳入到注册配置中心统一管理。

（21）其他关联系统，根据审计业务实际情况补充。

详细信息待详细设计阶段完善。

# 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【5000】，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，批处理时间不超过【3】小时。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、Microsoft edge，以及省联社统一建设的行内专用浏览器等；

（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X86 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、MySQL、DB2、Informix等主流数据库及国产化同类产品，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。

（9）系统支持IPv4/IPv6双栈运行。

## 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。

### 3.6.7 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。

### 3.6.8 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。

### 3.6.9 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。

### 3.6.10 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。

### 3.6.11 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。

### 3.6.12 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。

### 3.6.13 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。

### 3.6.14 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）。

### 3.6.15 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。系统需要满足用户端和管理端应用功能分离的安全要求。

（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。

### 3.6.16 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）我行自建系统通过直连行内ESB系统并按照相关接口规范进行对接，再通过行内ESB系统来调用省联社相关系统的交易接口。新系统接入行内ESB需提供：《业务需求说明书》、《软件需求规格说明书、《长沙农商服务治理\_XX系统\_系统接入申请单模板》、《长沙农商ESB外围系统\_XXX系统\_接口需求VX.X.X模板》、《长沙农商服务治理\_XX系统\_服务水平协议模板》、其他能够辅助服务治理人员理解业务流程、明确功能系统功能定位的材料（无则可不提供）。存量统接入行内ESB需提供：《长沙农商服务治理\_XX系统\_系统接入申请单模板》、《长沙农商ESB外围系统\_XXX系统\_接口需求VX.X.X模板》《长沙农商服务治理\_XX系统\_服务水平协议模板》、或者架构设计、概要设计、业务需求文档、其他能够辅助服务治理人员理解业务流程、明确功能系统功能定位的材料（无则可不提供）。消费系统接入行内ESB需提供如下文档：《长沙农商服务治理\_XX系统\_服务消费申请单模板》。

（3）对接行内ESB接口开发规范：服务方法的定义需要明确具体的实现方法、方式，关键控制节点，使用场景和限制，关键输入输出要素等。各个接入ESB系统则要按照ESB提供的《长沙农商服务治理\_字段映射\_XX系统\_VX.X.X》文档进行开发。

对接行内ESB技术规范要求：微服务平台集成模式为框架模式或边车模式；通讯协议为http1.1的POST模式；报文编码统一采用UTF-8；报文长度限制不超过100KB。

（4）对接行内ESB时，报文总体分为两个主要部分，包括系统和应用报文头，内容报文体。响应码分为2种：成功码统一返回“000000”； 异常返回码采用三段编码，两段用“-”分割，第一段：用于标识信息源，第二段：用于返回信息的定向，确定返回处理大方向，第三段：系统内部对错误码的进一步细分。(考虑到与现有系统返回码的兼容性，系统也可直接使用现有系统的返回码，不足6位的左补“0”)。特殊字符处理原则：当前后端系统在自己组的JSON报文时，需要对这些特殊字符进行转换。

（5）系统接口规范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；

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；

在系统升级时，能提供最大程度上的软、硬件投资保护；

确保交易的快速开发过程的质量和效率；

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

项目组要负责对接我行内部的相关系统，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；

我行ESB系统是全行IT应用架构中服务访问、应用系统集成的核心枢纽，系统与在与行内ESB系统对接时，需满足ESB系统相关要求。新系统接入行内ESB需提供：《业务需求说明书》、《软件需求规格说明书、《长沙农商服务治理\_XX系统\_系统接入申请单模板》、《长沙农商ESB外围系统\_XXX系统\_接口需求VX.X.X模板》、《长沙农商服务治理\_XX系统\_服务水平协议模板》、其他能够辅助服务治理人员理解业务流程、明确功能系统功能定位的材料（无则可不提供）。存量统接入行内ESB需提供：《长沙农商服务治理\_XX系统\_系统接入申请单模板》、《长沙农商ESB外围系统\_XXX系统\_接口需求VX.X.X模板》《长沙农商服务治理\_XX系统\_服务水平协议模板》、或者架构设计、概要设计、业务需求文档、其他能够辅助服务治理人员理解业务流程、明确功能系统功能定位的材料（无则可不提供）。消费系统接入行内ESB需提供如下文档：《长沙农商服务治理\_XX系统\_服务消费申请单模板》。

对接行内ESB接口开发规范：服务方法的定义需要明确具体的实现方法、方式，关键控制节点，使用场景和限制，关键输入输出要素等。各个接入ESB系统则要按照ESB提供的《长沙农商服务治理\_字段映射\_XX系统\_VX.X.X》文档进行开发。

对接行内ESB技术规范要求：微服务平台集成模式为框架模式或边车模式；通讯协议为http1.1的POST模式；报文编码统一采用UTF-8；报文长度限制不超过100KB。

对接行内ESB时，报文总体分为两个主要部分，包括系统和应用报文头，内容报文体。响应码分为2种：成功码统一返回“000000”； 异常返回码采用三段编码，两段用“-”分割，第一段：用于标识信息源，第二段：用于返回信息的定向，确定返回处理大方向，第三段：系统内部对错误码的进一步细分。(考虑到与现有系统返回码的兼容性，系统也可直接使用现有系统的返回码，不足6位的左补“0”)。特殊字符处理原则：当前后端系统在自己组的JSON报文时，需要对这些特殊字符进行转换。

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；

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；

在系统升级时，能提供最大程度上的软、硬件投资保护；

确保交易的快速开发过程的质量和效率；

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 |  |
| 性能测试 |  |
| 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： |  |
| 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 |  |
| 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 |  |
| 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 |  |

## 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、源代码使用与二次开发培训等），每项培训的受培训人员不少于三人，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、整体架构及源代码，具备独立的系统设计、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）约定提供的全部源代码：包括但不限于本项目开发平台源代码、本项目软件产品源代码、客户化定制源代码、二次开发源代码、所有非编译后的底层源代码等，源代码类型包括但不限于平台级、应用级、中间件级源代码，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）本项目产品须不得有任何时间期限、容量、用户数量、功能等其它限制的license授权许可。

（5）与本项目有关的其他资料。

项目组提交的所有源代码、文档、工具、授权码或授权文件（若有）需经验收通过，且本项目所有源代码、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）源代码（包括但不限于平台级、应用级、中间件源代码）、开发及相关培训；

（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）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）二次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。