长沙农村商业银行股份有限公司

统一用户管理平台项目

业务需求书

**信息技术部**

**2021年07月**

目 录

**1. 引言 1**

1.1. 背景 1

1.2. 项目概况 2

1.3. 读者对象 3

1.4. 定义 3

**2. 总体业务需求 3**

2.1. 业务目标 3

2.2. 项目范围及局限性 4

2.3. 业务功能需求 5

2.4. 报表需求 15

2.5. 标准规范需求 16

2.6. 系统关联需求 16

**3. 总体技术需求 19**

3.1. 系统总体要求 19

3.2. 系统建设反洗钱标准 20

3.3. 系统架构要求 22

3.4. 系统性能要求 23

3.5. 系统兼容性要求 24

3.6. 系统安全要求 25

3.7. 系统部署要求 32

3.8. 系统对接要求 34

3.9. 系统测试需求 38

3.10. 知识转移要求 39

3.11. 知识产权要求 40

#

# **引言**

## **背景**

为了支撑业务的高速发展，长沙农村商业银行股份有限公司（以下简称“本行”）依托于湖南省农村信用联合社的业务系统，以及本行通过自建、采购等模式建设的一系列应用系统，完善了业务支撑体系、实现规范化运作、提升运营效率，但各式各样、纷繁复杂的应用系统也带来一些亟需解决的问题。现有应用系统的形态包括BS、CS、APP、SAAS等形式，用户类型涵盖了行内员工、系统管理员、外包人员、临时用户等，总结起来有以下三方面的问题：

**账号管理难**。因为各应用系统中账号和权限管理是分散的，系统管理员需要在每个系统中创建、维护、注销用户的账号和权限信息，这些工作重复繁琐且出错率高。随着应用系统和员工数量的不断增加，账号管理、权限管理的工作量在直线上升。

**用户体验差**。每个员工需要记住多个应用系统的账号密码，且在登录每个应用系统时都需要输入不同的账号密码，常常因为密码太多而出现忘记密码的情况；并且不同的应用系统依赖的浏览器类型不一样、版本不一样，所以往往需要打开很多种不同的浏览器。

**安全风险大**。首先，各应用系统使用的密码认证方式不一致，容易造成密码泄露和共享，且存在大量使用弱密码的应用系统，密码安全得不到保障；其次，本行员工数量大、用户类型多，账号与权限管理容易出现管理漏洞、造成关键信息泄密；再者，本行缺乏统一的用户行为审计系统，无法全面掌握应用系统操作风险。

因此从减少IT管理成本、提升员工工作效率、提高业务安全性等多方面考虑，有必要建立一套统一用户管理平台，首先对本行的用户身份与权限进行统一治理，在实现业务系统的单点登录与双因素认证，建立集中化的日志审计平台，从而达到应用系统可管理性、易用性、安全性的目标。

## **项目概况**

统一用户管理平台是管控全行用户和业务系统级别的一个统一管控平台，主要包含以下几个方面的功能：

（1）统一身份治理和管理：确定权威数据源，能支持主流的数据源同步方案，针对本行的所有用户进行统一管理。

（2）统一授权管理：用户应用授权决定用户拥有哪些应用的访问权限，无论是通过统一门户访问还是单独访问应用系统，都需要进行权限判断。

（3）统一认证服务：用户认证提供多种（账户名+密码、扫码认证、一键推送、动态口令、人脸识别、短信验证码等）认证方式供客户选择，替代传统的用户名密码认证，实现用户主账号登录统一门户；同时支持CAS、OAuth、OIDC、SAML、JWT等标准单点登录协议，提供SDK和API供应用系统快速集成。

（4）统一审计管理：统一审计可以对管理员行为、用户操作行为、用户认证行为，用户访问行为进行审计，并可以支持对用户业务行为进行风险审计，并通过设置策略自动防控风险。支持日志查询、风险报表、风险预警、二次认证等功能。

（5）统一门户：统一门户是用户使用入口，用户只需通过一次门户认证便可以直接单点登录到其他系统，不需要再进行身份认证，门户上可集成消息代办，用户自助服务等功能。

## **读者对象**

长沙农商银行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。

## **定义**

**IDM**：Identity Manager，身份管理

**IAM**：Identity and Access Management，身份识别与访问管理

**SSO**：Single Sign On，单点登录

# **总体业务需求**

## **业务目标**

本次项目拟通过建设统一用户管理平台，实现对我行应用系统及用户有效的集中管理、认证和授权，并形成统一的用户管理及登录对接规范体系。主要实现以下五点目标：

**统一登录规范**。规划、制定技术标准和规范，包括登录认证标准、账号管理标准，权限分配和访问控制标准、以及安全审计标准等方面安全技术标准，规范各业务系统与统一用户管理平台的对接。

**降低账号风险**。统一用户所有业务系统的登录账号密码，方便用户记忆，减少泄露风险，并可以通过添加多因素认证方式，解决密码认证不安全的问题。

**改善用户体验**。所有业务系统都可以通过统一的门户进行单点登录跳转，用户只需要在门户页面做一次登录就可以访问其所有有权访问的系统，方便用户快速访问应用。

**加强安全管控**。通过建设行内用户安全审计策略体系，实时监测用户对各业务系统的访问状态，及时发现非法访问事件，对系统运行状态实时监控审计，增强系统可维护性，利于出现问题的事后追溯和责任追究。

**减少开发成本**。建立了统一的用户数据源和登录模块后，新开发的业务系统可以直接套用，减少开发成本。

## **项目范围及局限性**

**实现行内统一组织管理**：明确组织的标准数据源，同时支持多维组织架构管理能力，支持多法人机构，构建标准化组织中心，向下游应用供应所需组织数据。

**实现行内统一用户管理**：明确用户的标准数据源，同时支持自建不同用户类型的新用户，包括但不限于：行内用户、第三方用户、游客、系统用户、设备用户等。构建标准化用户中心，支持向下游应用供应所需用户数据。

**打造行内统一认证中心**：提供多因素认证能力体系，例如账号密码、扫码认证、一键推送、动态口令、人脸识别、短信验证码等，并可扩展认证方式，向业务系统提供统一的认证服务。

**实现行内系统单点登录**：提供适用于不同应用类型，包括但不限于BS、CS、APP、SAAS等应用，对所有应用系统提供单点登录服务。

**构建行内统一门户**：建设轻量级统一认证门户，提供应用中心供用户一站式SSO访问有权限访问的应用系统；建设待办及公告的发布管理模块，统一在门户中查看待办、公告。同时也能提供用户一站式个人信息修改、修改密码、找回密码服务等自助服务。

**安全审计**：集中管理用户、管理员及数据安全等方面的日志审计及图形化报表。

**系统集成**：提供数据同步、认证及单点登录的标准集成能力，同时也可适配异构系统的标准实现集成对接，从而实现行内所有存量或新增系统的接入。

## **业务功能需求**

### **机构、用户、角色**

统一用户管理平台涉及长沙农商银行所有机构、用户和角色。

### **渠道支持及终端分布**

统一身份认证管理平台支持以浏览器方式（BS模式）、客户端方式（CS模式）、移动终端方式（APP、H5等）进行平台访问，接入应用系统的形态包括BS、CS、APP、SAAS等形式。

### **业务功能需求清单**

**2.3.3.1.统一身份治理及管理**

**1.数据源管理**

数据源管理主要目的是把权威的组织用户数据实时同步到统一用户管理平台，计划以人力资源管理系统作为权威数据源，确定用户编码规则及管理范围，完成员工数据治理和全生命周期的系统管理。

平台需支持主流的数据源同步方案，并形成模板化配置，可以快速完成数据源同步工作：

（1）数据库同步：支持从上游系统数据库同步组织用户数据到平台；

（2）API拉取同步：支持通过API方式从上游系统定时同步组织用户数据；

（3）API推送同步：提供组织用户推送API，供上游系统实时推送数据到平台。

**2.组织用户管理**

组织用户管理包括数据存储、组织管理、用户管理等功能。组织管理支持多维组织架构，组织增删改查、迁移、合并等功能。

用户管理支持用户增删改查、数据源状态同步、禁用启用、过期、临时授权等操作。用户类型支持正式员工、临时员工、外部员工、虚拟用户、游客、硬件设备、业务系统等类型，不同用户类型可以赋予不同的生效周期，以及和对应用户组关联赋予不同的应用访问权限。

**2.3.3.2.统一授权管理**

用户应用授权决定用户拥有哪些应用的访问权限，无论是通过统一门户访问还是单独访问应用系统，都需要进行权限判断。

支持用户组授权、用户授权、应用授权三种方式，有效应对批量用户授权、用户同步授权、新增用户授权、新增应用授权等业务场景。

（1）用户组授权：用户组授权按照业务属性对用户进行分组，按照用户组配置用户拥有的应用权限，等同于角色授权，符合RBAC权限模型。是主要授权方式。

（2）用户授权：可以单独对用户进行应用授权，如果该用户拥有相关的用户组权限，那么取并集得到用户最终拥有的应用权限。适用于特殊用户。

（3）应用授权：把应用赋予对应的用户组，因为系统建设时应用是分批次接入，应用授权方式较好的解决了新增应用的授权问题。

**2.3.3.3.统一认证服务**

用户认证提供多种（账户名+密码、扫码认证、一键推送、动态口令、人脸识别、短信验证码等）认证方式供客户选择，替代传统的用户名密码认证，实现用户主账号登录统一门户。

**1.传统密码认证**

传统密码认证支持密码安全策略、密码锁定策略、密码更新、忘记密码与重置密码。密码认证支持公私钥加密机制，防止泄密。

**2.移动认证**

移动认证通过移动设备实现移动免密认证方式，通过设备指纹、软件SE、终端安全防御等核心技术保障认证安全性。移动认证支持以下认证方式，可根据实际情况进行选择：

（1）一键推送：推送认证信息到移动认证APP上，用户进行确认；

（2）扫码：使用移动认证APP进行扫码认证；

（3）软令牌：使用移动认证APP生成软令牌进行认证；

（4）人脸：使用移动认证APP进行人脸认证，需对接人脸识别服务；

**3.应急认证**

在紧急情况下，比如用户忘记携带手机，或者忘记密码，可以通过临时授权码进行认证，管理员在后台可以对特定用户生成临时授权码，临时授权码可以设置有效期。

**4.认证策略**

统一用户管理平台提供单点认证策略、应用认证策略、用户认证策略管理。

单点认证策略包括：

（1）密码认证：支持密码安全策略、忘记密码、重置密码、密码认证加密；

（2）移动免密认证：支持一键推送、扫码、软令牌、短信、人脸；

（3）双因素认证：支持密码认证与一键推送、软令牌、短信、人脸双因素认证组合；

（4）认证分级：支持认证分级，重要应用二次认证。

应用认证策略支持按照应用维度设置认证方式组合。

用户认证策略支持按照用户、用户组设置认证方式组合，支持策略优先级。

**2.3.3.4.统一门户**

统一门户是用户使用入口，提供身份认证，应用单点登录，消息待办、用户自助服务等功能。

**1.单点登录**

用户通过认证后，门户展示用户拥有权限的应用列表，可以按照应用标签分类展示。用户点击应用图标可直接跳转到对应应用，不用再进行身份验证。

应用单点登录是统一门户的主要功能。点击应用图标，可实现单点登录。全部应用支持按点击热度排序，应用访问次数越多排序越靠前，方便用户选择使用常用的应用。

**2.消息待办**

统一门户支持应用待办消息接收和展示，提供待办消息接口供应用系统推送消息。点击待办消息跳转到对应应用系统。可通过与应用对接实时接口实现状态的同步，在应用系统完成任务后向统一用户管理平台发送一个已完成的消息，并且在平台上展示一个当前任务清单，显示哪些已办哪些未办。

**3.账户委托**

管理员或者用户把权限内的应用委托给特定用户，适用于代理他人工作的业务场景。

支持用户本人或管理员将用户A的账号委托给用户B在统一门户登录使用，支持应用账号的委托。B拥有A的账号、特定应用的使用权。支持委托人和管理员解除委托，以及设定有效期定时收回委托。

**2.3.3.5.单点登录**

单点登录被简称为SSO（Single Sign On），实现一次认证、全网通行，是目前比较流行的企业应用整合解决方案。单点登录一般和应用门户进行集成，用户只需要在登录门户时进行一次认证，不需要记忆每个应用系统的密码，提升了工作效率，并减少了密码重置等IT管理工作。另外一方面，单点登录配合强认证、强审计，可以解决认证安全问题。

现实环境中，应用系统有多种形态，比如BS、CS、SAAS、APP，需要根据实际情况采取不同的单点登录技术。

**1.单点登录技术**

单点登录技术主要针对BS应用、CS应用、移动应用三种业务场景给出针对性的解决方案。

**（1）BS应用单点登录：**

1. BS应用单点登录主要分为标准协议支持和密码代填两种解决方案：
2. 统一用户管理平台通过多种技术实现单点登录，可覆盖各种业务场景：
3. 标准协议：依托开源的CAS方案，支持CAS、Oauth、OIDC、SAML、JWT等标准单点登录协议，提供sdk和api供应用系统快速集成，应用系统简单改造。CAS Client会对应用系统登录进行拦截，配合高强度移动认证方式，可以有效提升认证安全性，解决传统密码认证的安全性问题。
4. 密码代填：对于无法改造的应用系统，提供密码代填方案达到单点登录效果，支持Basic、表单、JS脚本等各种BS密码代填技术。

**（2）CS应用单点登录：**

通过密码代填技术可以实现从单点登录门户免密访问CS应用，平台提供CS应用密码代填脚本录制、上传，用户访问CS应用时进行下载安装、绑定账号密码。

**（3）移动应用单点登录：**

移动应用单点登录依托认证移动APP实现，移动认证APP提供应用微门户供移动应用进行集成。移动端单点登录方案采取Oauth方案，后台返回一次一密的token给移动应用，移动应用后台通过token到统一用户管理平台后台获取登录用户信息。

移动应用从桌面上打开时可以调起认证APP进行免密认证，提供原生SDK和Scheme两种集成方案，前者适用于原生APP，后者适用于H5应用。

**2.单点登录方案**

应用有BS、CS、SAAS、移动应用等四种类型，按照上述描述分别使用以下单点登录技术：

（1）自建BS：CAS方案，提供Cas Client供应用集成；

（2）SaaS应用：采用Saml方案，sap应用可以配置外部idp；

（3）CS应用：密码代填；

（4）移动应用：token令牌技术，提供微门户、sdk、scheme等集成方案。

**2.3.3.6.统一审计管理**

**1.审计类型**

统一用户管理平台对管理员行为、用户操作行为、用户认证行为，用户访问行为进行审计，并可以支持对用户业务行为进行风险审计。

管理员行为审计内容包括用户操作审计、权限操作审计、认证策略操作审计、认证设备操作审计：

（1）用户操作行为审计对用户自助操作行为进行审计，包括设备绑定激活、更换设备、修改用户信息和密码、权限申请、账号委托等行为。

（2）用户认证行为审计，对用户认证设备、认证方式、登录时间、登录频度等行为进行审计，发现异常登录认证行为。

（3）用户访问行为审计包括重点应用访问频度、尝试访问没有权限的应用等行为。

（4）用户业务行为审计，是对用户在应用系统内部的操作行为进行审计，需要根据实际情况解决日志采集的问题，比如CAS Client无侵入采集、日志文件实时监控采集、应用网关采集等。

综合用户操作、认证、访问、业务行为，可以有效发现风险异常，打造我行内部的统一用户管理平台。

**2.审计业务**

审计业务包括日志查询、风险报表、风险预警、二次认证等。

（1）支持海量日志存储索引，支持关键信息检索、导出。

（2）风险报表支持对风险事件、风险用户、风险标签、风险规则的统计分析。

（3）风险预警支持通过邮箱、短信等方式向管理员发送风险预警。

（4）对用户登录认证行为进行风险分析，触发高强度二次认证。

**2.3.3.7.后台管理系统**

管理系统提供可视化管理界面，包括用户管理、授权管理、应用管理、认证管理、设备管理，日志查询、风险管理、配置管理、审计管理、系统管理等。

（1）用户管理：包括组织管理、用户管理、属性管理、用户组管理、用户分组策略管理、数据源管理等功能。

（2）授权管理：管理用户应用授权，支持用户组授权、用户授权、应用授权、权限导入、权限审批、基于用户属性自动授权等功能。

（3）应用管理：支持各种单点登录标准协议模板、密码代填模板、双因素认证等模板，可以满足绝大多数的应用接入需求。标准单点登录协议支持CAS、Oauth、OIDC、SAML、JWT等各种协议。

（4）认证管理：对认证策略进行管理、可以按照用户、用户组、应用等维度进行灵活的认证策略设置，满足我行各种业务场景的认证需求。具体支持以下认证策略：

用户名密码认证：可灵活设置密码安全策略；

移动免密认证：设置移动认证方式，易用性好且安全级别高；

双因子认证：灵活组合密码认证和移动认证，安全级别很高；

认证分级：对认证方式进行分级，对应用设置认证级别，当用户认证通过后需要访问更高认证级别的应用时，会触发二次认证，安全级别最高。

（5）设备管理：对用户的移动设备进行管理，展示用户的设备指纹、设备信息，并且可以支持对用户设备进行锁定操作，一旦设备被锁定，用户就无法使用移动认证功能。

（6）日志管理：提供日志审计和统计报表功能，对系统管理日志、用户认证日志、用户操作日志进行审计分析，识别业务风险，便于取证溯源。

（7）风险管理：提供风险规则、风险场景、处置策略、风险预警、风险统计等功能。

（8）配置管理：对系统用户、角色、权限等进行管理，支持管理员分级管理。

（9）审计管理：包括分析维度、风险标签、操作类型、规则模板、规则管理、应用场景、预警、审计报表。

（10）系统管理：包括权限管理、角色管理、用户管理、分级管理。

## **报表需求**

根据内控安全需求，统一用户管理系统需要建立相关的安全审计系统，对用户管理和访问控制中的关键流程、数据进行审计，并提供相关报表查询，具体要求如下：

（1）审计报表应覆盖到统一用户管理、身份认证、授权与访问控制的每个环节；

（2）审计报表应记录应用系统重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统功能的执行等；

（3）相关事件的记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；

（4）建立综合审计展示平台，将审计信息进行集中展现和展示，根据记录数据进行分析，可生成审计报表，并对特定事件，提供指定方式的实时报警。

（5）审计进程必须受到保护，审计记录必须受到保护。

## **标准规范需求**

制定登录认证标准、账号管理标准、权限分配和访问控制标准，以及安全审计标准等方面的安全技术标准。主要包括：身份认证安全技术标准、应用集成技术标准、权限管理技术标准、移动App认证安全标准、应用审计日志技术标准、用户管理办法、系统对接规范等。

## **系统关联需求**

统一用户管理平台建设计划以人力资源管理系统作为权威用户数据源，通过行内ESB企业服务总线与其他业务系统进行服务集成，并与行内零信任网络安全平台对接，实现全终端安全管控。

项目一期计划由厂商协助接入OA、业绩计量、大数据、内容管理平台等十多个使用较为频繁的行内系统，以及信贷系统、柜面前端、ODS等十个全行员工常用的省联社业务系统。

对于行内系统，则需要通过改造实现单点登录接口、组织架构同步接口、权限同步接口；对于省联社或其他无法改造的系统，则使用密码代填的方式实现统一登录。

后续逐步掌握该平台后，自主地将剩余业务系统全部接入统一用户管理平台中。

### **接入行内系统**

|  |  |  |
| --- | --- | --- |
| **序号** | **应用名称** | **使用用户群** |
| 1 | OA协同办公系统 | 内部员工 |
| 2 | 业绩计量系统 | 内部员工 |
| 3 | 人力资源系统 | 内部员工 |
| 4 | 零信任网络 | 内部员工、外部人员、临时人员 |
| 5 | DLP数据安全管理平台 | 内部员工、外部人员、临时人员 |
| 6 | 大数据平台 | 内部员工 |
| 7 | 内容管理平台 | 内部员工 |
| 8 | 电子挎包 | 内部员工 |
| 9 | RPA管理平台 | 内部员工 |
| 10 | 客户财资系统 | 内部员工、外部人员 |
| 11 | ESB企业服务总线及微服务平台 | 内部员工 |
| 12 | 运营工作平台 | 内部员工 |
| 13 | 费控系统 | 内部员工 |
| 14 | 小微信贷 | 内部员工、外部人员 |
| 15 | 理财销售系统 | 内部员工 |
| 16 | 现金调拨系统 | 内部员工 |
| 17 | 凭证调拨系统 | 内部员工 |
| 18 | 网格化营销平台 | 内部员工、外部人员 |
| 19 | 产品定价系统 | 内部员工 |
| 20 | 内部信用评级系统 | 内部员工 |
| 21 | Q支付 | 内部员工 |
| 22 | 账户管理系统 | 内部员工 |
| 23 | JIRA系统 | 内部员工 |
| 24 | 源代码安全检测系统 | 内部员工 |
| 25 | 固定资产管理系统 | 内部员工 |
| 26 | 理财资产管理系统 | 内部员工 |
| 27 | 事后监督系统 | 内部员工 |
| 28 | 查碰库系统 | 内部员工 |
| 29 | 表外不良贷款管理系统 | 内部员工 |
| 30 | 智慧金库系统 | 内部员工 |

### **接入省联社系统**

|  |  |  |
| --- | --- | --- |
| **序号** | **应用名称** | **使用用户群** |
| 1 | 财务管理系统 | 内部员工 |
| 2 | 客户信息管理系统 | 内部员工 |
| 3 | ODS | 内部员工 |
| 4 | 信贷系统 | 内部员工 |
| 5 | 柜面前端 | 内部员工 |
| 6 | 反洗钱系统 | 内部员工 |
| 7 | 冠字号查询系统 | 内部员工 |
| 8 | 总账报表系统 | 内部员工 |
| 9 | 新网银系统 | 内部员工 |
| 10 | 名单监测管理系统 | 内部员工 |

## **建设费用**

统一用户管理平台费用主要来源于三个部分：①统一用户管理平台基础平台费用；②平台搭建和定制化开发费用；③系统集成接入实施费用。通过前期厂商报价和同业调研的情况，价格影响因素主要来源于不同厂商平台价格不同以及接入系统数量不同。

从厂商报价上来看，平台价格从30万到100万不等，功能方面最低价平台也能满足项目基本需求，后期还需POC测试进一步验证，平台搭建和17个左右系统集成费用基本在60万到90万之间，报价总费用在100万到200万之间，由于是初步报价，后期还有下降空间。

而从同业调研情况来看，统一用户管理平台价格普遍在70~150万之间，考虑到厂商建议一期接入系统不宜太多，暂定只接入20个以内的系统，与同业调研接入的系统数量相比要少，费用可以进一步降低。

故统一用户管理平台建设的费用预估在100万。此外，纳入统一用户管理平台管控范围内的系统也可能涉及到改造，这部分费用还需各接入系统另外评估考虑。

# **总体技术需求**

## **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。

（8）系统需保留应急通道，能保证统一用户管理平台无法使用时，其他系统仍能正常登陆。

## **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。

## **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）系统设计需要支持接入我行ESB及微服务平台。

## **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【4000】，并发数不低于【2000】，登录响应时间不超过【1】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【2】秒，系统响应时间最长不超过【2】秒，批处理时间不超过【2】分钟。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100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300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2000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99.999%，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。

## **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，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。

## **系统安全要求**

### **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）。

### **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。

### **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。

### **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。

### **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。

### **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。

### **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。

### **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。

### **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。

### **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。

### **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。

### **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。

### 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）。

### **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。

### **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。

## **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。

## **系统对接要求**

### **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。
4. 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。
5. 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。
6. 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；
7. 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；
8. 在系统升级时，能提供最大程度上的软、硬件投资保护；
9. 确保交易的快速开发过程的质量和效率；
10. 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。

### **行内接口**

1. 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；
2. 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》。
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。
4. 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。
5. 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。
6. 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；
7. 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；
8. 在系统升级时，能提供最大程度上的软、硬件投资保护；
9. 确保交易的快速开发过程的质量和效率；
10. 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。

### **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。

## **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 |

## **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。

## **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。