

长沙农村商业银行股份有限公司

测试服务一体化平台项目

业务需求

**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 1

1.3. 读者对象 2

2. 总体业务需求 2

2.1. 业务目标 2

2.2. 功能树 3

2.3. 业务功能需求 3

2.3.1. 可视化服务 3

2.3.2. 项目管理 4

2.3.3. 需求管理 4

2.3.4. 资源管理 5

2.3.5. 案例管理 5

2.3.6. 缺陷跟踪管理 6

2.3.7. 执行管理 6

2.3.8. 测试报告管理 6

2.3.9. 自动化测试 7

2.3.10. APP自动化测试 8

2.3.11. WebUI自动化测试 10

2.3.12. 仿真挡板服务 12

2.3.13. 性能测试 12

2.3.14. 系统管理 13

2.4. 系统关联需求 14

2.4.1. Jira平台对接 14

2.4.2. Devops平台对接 14

2.4.3. OA平台对接 14

2.4.4. 统一消息中心对接 14

2.4.5. 统一用户管理平台对接 14

2.4.6. 测试工具集成 14

3. 总体技术需求 14

3.1. 系统总体要求 14

3.2. 系统架构要求 15

3.3. 系统性能要求 15

3.4. 系统兼容性要求 16

3.5. 系统安全要求 17

3.5.1. 身份鉴别 17

3.5.2. 会话管理 18

3.5.3. 访问控制 18

3.5.4. 信息交换安全 19

3.5.5. 交易安全 19

3.5.6. 数据安全 19

3.5.7. 组件配置 20

3.5.8. 文件上传安全 20

3.5.9. 密码支持 20

3.5.10. 输入、输出合法性检测 21

3.5.11. 异常处理和日志 21

3.5.12. 备份与故障恢复 21

3.5.13. 抗抵赖与安全审计 21

3.5.14. 安全管理 21

3.5.15. 法律法规特定要求 22

3.6. 系统部署要求 22

3.7. 系统对接要求 23

3.7.1. 省联社接口 23

3.7.2. 行内接口 23

3.7.3. 外部接口 23

3.8. 系统测试需求 24

3.9. 知识转移要求 25

3.10. 知识产权要求 26

# 引言

## 背景

目前我行尚无统一的测试服务一体化平台，在软件开发过程体系中的测试环节缺乏系统级的管理。手工测试、自动化测试及性能测试等都处于单独测试领域各自为战，没有一个对各种类型测试统一管理与监控的全局性抓手。同时，对于测试需求、测试计划、测试案例以及测试环境等的管理并未完全实现线上化，另外，测试数据仍然处于完全依赖测试人员手工准备阶段，未实现测试数据准备的自动化与系统化，各种测试资产都分散在不同的系统中，无法实现对各种测试资产的统一管理与调度，使其发挥更大效力。

随着我行业务及金融科技的蓬勃发展，我行信息系统的规模越来越庞大和复杂，这些信息系统通常具有关联系统众多、关系复杂等特点，测试难度较大。同时，银行同业以及银行与科技金融公司之间的竞争逐步加剧，谁能快速、稳定的推出具有创新性，体验好的产品，就能快速抢占市场，取得先机。测试作为产品研发生命周期的重要一环，已成为银行信息科技领域一项专业工作。

为提升我行开发与测试工作的效率，支撑我行软件产品敏捷开发、持续集成、持续测试、持续交付的开发测试运维一体化建设要求，确保各个系统在充分保证质量的前提下按时上线，我行拟建设功能完整、易学易用、便于扩展的全行统一的测试服务一体化平台。

## 项目概况

通过需求驱动测试，实现从业务需求到测试需求再到测试案例、测试数据准备、测试环境准备、测试执行、缺陷提交与跟踪、回归测试、测试结果展示与分析的全测试流程线上化，对测试进行统一的管理与监控，达到测试流程可双向追踪、测试结果可追溯、测试工具可提供、测试环境可维护的服务目标，涵盖软件开发过程体系中测试相关的内容:

针对现有Jira平台的项目、缺陷资产，做相关资产数据迁移同步；

建设一体化测试服务平台；

针对行内中间节点系统或末端系统的接口自动化测试；

针对不同系统，基于B/S架构的Web自动化测试，基于C/S架构的Windows应用程序的PC自动化测试，基于移动端的Native、微信小程序及H5页面的移动端自动化测试；

针对系统不同的阶段，开展相应的性能测试；

建设符合行内测试实施过程中的自动化测试体系建设及流程优化；

建立自动化测试资产库，提高测试资产的可复用性；

打通DevOps运维平台，实现持续的敏捷开发体系中；

## 读者对象

本文档面向的读者对象为测试服务一体化平台项目相关的技术人员、业务人员、决策层以及高层管理人员等。

# 总体业务需求

## 业务目标

通过平台落地标准化测试流程和规范化质量管理，实现信息化工具的支撑，统一的管理测试工作的实施情况和度量研发工作的质量情况。

通过平台实现测试工作的统一管理、统一测试数据分析。实现对不同测试项目的统一管理；

实现软件项目间的高效协作、降低沟通成本，提升工作质效；

实现外包测试工作和人力的透明化管理；

实现对测试需求、测试计划、测试任务、测试进度、测试资源、测试过程风险、测试评审、测试度量的总体跟踪和描述；

## 功能树



## 业务功能需求

### 可视化服务

一体化测试平台中的可视化服务，通过大盘的形式呈现，具体呈现内容如下：

1、项目统计信息：项目未开始、项目进行中、项目完成、项目完成度，项目资源使用情况；

2、需求统计信息：需求未开始、需求进行中、需求完成；

3、资源情况信息：环境资源使用情况、企业级案例数、企业级缺陷数、人员投入及使用情况；

4、开发质量指标包括：

当前待处理缺陷数：根据缺陷严重程度；

缺陷ReOpen率：根据系统的 缺陷重开数/缺陷总数；

开发人日缺陷率排行：缺陷/开发人日；

采用缺陷率：项目的缺陷/案例；

项目缺陷详情；

缺陷处理动态；

缺陷修复SLA（服务品质协议）排行——采用缺陷解决率：项目的已解决缺陷/缺陷总数；

缺陷收敛趋势图；

各类型缺陷占比；

版本退回详情（缺陷率、缺陷解决率）；

开发处理缺陷效率：开发每人每天处理的缺陷数量；

5、测试质量指标包括：

测试用例总数；

项目测试进度；

测试用例执行率；

项目测试用例类型分布详情；

缺陷有效率；

缺陷QA验证速率；

项目测试用例执行情况；

缺陷逃逸率；

6、缺陷指标包括：

缺陷类型：功能、性能、可靠性、安全性、兼容性、部署

缺陷级别：P0、P1、P2、P3

缺陷修复时长；

### 项目管理

项目负责人、测试经理、系统负责人通过新建项目，添加里程碑计划，创建项目管理项，实现了对测试项目的资源分配、进度管理、质量管理、风险管理及测试项目统计报表功能。

实现对接我行JIRA等项目管理平台实现项目导入功能。

以测试项目为范围，对测试过程的整体进行把控，实现对测试需求、测试计划、测试任务、测试进度、测试资源、测试过程风险、评审、测试度量的总体跟踪和描述。

实现测试报告的输出。

### 需求管理

项目负责人、测试经理、系统负责人创建平台测试需求，关联项目。包括需求项描述、需求类型（技术测试需求或业务测试需求）、测试需求分类（SIT测试、UAT测试或非功能性测试）、测试需求任务分解等内容。

测试需求一经创建，由创建者向测试需求分析人员下发，由测试需求分析人员提交测试设计方法、测试大纲、测试案例、测试执行策略、设计日期等内容，并进入评审环节，由项目负责人、测试经理及评审人员进行评审，通过评审的测试需求状态由审核中转为审核通过。

分解测试需求，按照测试方案建设测试任务，并制定任务负责人，支持任务的导入导出操作。分解后的需求均需要与测试用例进行关联。

### 资源管理

实现测试资源的集中管理，包括各类资源对应的相关管理流程，比如测试环境的申请、使用、释放的处理流程。实现测试资源信息（包括测试硬件资源主机名、台数）、软件资源（包含数据库类型）及人力资源（测试人数等）管理。

人员管理方面实现对测试人员及环境管理员的工作量和工作用时等的统计，对人员的工作情况进行统一的监管，并且形成可量化的形式。

实现对外包商、外包团队、外包人员进行分析和评价。实现外包商测试团队管理，涵盖了供应商、外包人员信息录入和管理。

实现需求说明书、案例库、缺陷库、测试文档等资源入库，入库、修改，资源的入库、修改等操作需要有记录机制，删除操作需要有审核机制。

实现对测试资源的管理，与项目进行关联，展现出当前项目所使用的硬件资源数量，以此明了地看出当前项目实际使用以及项目完成后资源回收的便利性。

### 案例管理

实现对测试案例资产的标准化管理，具体各种类型的案例模板信息需细化；与案例库对接，实现所有类型案例的集中、分类展示；案例合并到基线库需要权限控制；

新增案例时需要存在案例级别、标签、是否自动化、案例类型等选项；在创建案例后的每一次修改均需要记录下修改时间和修改内容。

实现测试案例与系统需求、测试需求、测试缺陷的关联功能，以便其他功能模块对关联信息的查看；增加测试案例回收站功能，操作人员误删除的案例，可以在回收站中恢复。

### 缺陷跟踪管理

实现平台中测试缺陷的集中管理，包括缺陷的创建、流转、关联对象信息的展示等：

提供更加易用的缺陷管理和缺陷流程跟踪的功能；提供缺陷查询的功能，通过检索条件筛选出缺陷数据，并可以生成分析报告(含数据和图形)；

创建缺陷时，用户可选择将缺陷与需求、测试案例等信息进行关联，方便用户根据缺陷查找相关需求和测试案例；

提供图形化的配置，可配置缺陷的流转流程和操作角色功能；

当前缺陷处理人员可以进行退回操作（退回原因必填）；

创建缺陷时，该缺陷关联的系统和人员等信息可以进行模糊查询，辅助缺陷信息的填写；

缺陷信息中可上传附件；

记录缺陷的操作日志。

### 执行管理

实现平台中管理的各类测试案例的执行管理和监控，包括手工测试案例的执行和自动化测试案例的执行，手工测试主要提供标记案例状态、执行备注等功能，自动化测试主要提供执行测试案例、标记案例状态等功能，旨在通过简单的界面操作以减少测试人员除执行案例之外的工作量，同时提供管理者监管测试执行状态的功能。

### 测试报告管理

测试报告模块应涵盖：

1. 项目整体测试总结，测试通过率、测试失败率等；
2. 案例总数量、无效案例数量、已执行案例数量、未完成案例数量；
3. 缺陷总数量、遗留缺陷数量、修复率、缺陷功能模块统计；
4. 被测版本信息；
5. 测试报告可自定义模块；
6. 测试报告支持excel，pdf等格式导入导出；

### 自动化测试

对各种辅助测试开发的工具在平台中实施统一的管理。可以按简单配置方式挂载具有标准接口的外部工具，工具被挂载后，可对外以Web service方式或界面方式提供服务，测试人员不用再在本地安装与配置。

#### 接口自动化测试

1、关联测试项目，实现对测试各接口的调用与模拟

2、支持切换测试项目目的多个被测环境，如SIT环境、UAT环境、准生产环境等。

3、支持测试多种接口协议，如HTTP/HTTPS，RESTful，gRPC，Dubbo等。

4、支持模拟接口异常情况，如重复提交、接口请求发出后网络断开等。

5、接口的层级管理结构目录以测试系统为根节点或者等同节点，在测试系统可以定义层级模块，在其下进行新建接口、复制接口、接口属性对比以及接口字段维护操作。

6、接口用例可以在接口测试中定义并上传，也可从测试管理的测试用例中导入，如导入了测试管理中的测试用例，则需补充该用例的接口url、请求、断言等接口测试基础信息。

7、支持用例同步，接口自动化模块维护的用例可同步到测试管理的测试用例模块中。可通过设置用例标签进行用例筛选。

8、对接口用例各参数、接口用例设置和接口执行情况都有详细描述。

9、支持多接口关联测试，支持接口测试脚本的新增、修改、删除，支持搜索脚本名称及交易名称，支持不同项目的筛选、切换、过滤等

10、支持以任务为维度，选择项目下的案例，可随意调整案例执行顺序，选择或者切换可用环境，并进行环境监督，选择不同的执行机多场景执行任务。设定任务执行策略/重试策略，重试次数等。设置任务结果以邮件形式发送给指定人员，任务结果包括任务执行情况、执行日志、请求报文、响应报文以及验证对比信息等。

11、支持以项目维度查看测试执行情况，支持测试报告定制、在线查看和导出。

12、平台需支持组件是开发、主要组件有报文组件、通讯组件、数据源组件、密码组件、系统函数组件等，可以根据需要变更或新增，最终以组件形式运行在平台中，即实现易变功能插件化，安装运行。

### APP自动化测试

1、所有设备的应用管理，包括查看应用、编辑应用信息、添加应用、删除应用功能。应用列表上方工具栏为筛选功能，可根据筛选条件查找已上传的应用。

（1）支持管理移动端（Android、IOS、鸿蒙OS）应用

（2）支持对应用和依赖文件进行新增、修改、删除操作。

2、支持对不同测试机型进行管理，APP自动化测试平台集成主流的真机，真机画面实时投屏到平台Web端，测试人员可在Web端控制任意真机进行测试。

3、支持测试机资产管理，支持查看上位机的连接情况，支持查看当前上位机下连接的设备信息。

4、支持用例同步。APP自动化模块维护的用例可同步到测试管理的测试用例模块中，可通过设置用例标签进行用例筛选。5、支持可视化界面录制和编写用例。通过脚本录制或拖拽元素控件等方式编写APP自动化测试用例，用例编写完成后可对操作步骤进行编辑。

6、支持Python/Java脚本编写用例。支持主流自动化测试框架，通过编写Python/Java代码实现APP操作。

7、支持查看所有的自动化脚本信息，可对脚本进行管理操作，包括查看脚本信息、编辑脚本等。

8、支持引用自动化测试用例生成测试任务，制定任务执行范围，定制测试执行策略，执行测试任务，查看测试执行情况等。

9、支持主流移动操作平台Android、IOS和鸿蒙OS系统。

10、支持三个主流移动平台的Monkey测试，可测试APP稳定性。

11、支持被测APP管理，如上传APP、查看APP版本号、查看MD5值等，支持保存所有上传的APP和历史测试的APP。

12、支持类似Appium或UIAutomator工具中的元素信息查看功能，可在真机投屏画面点击元素获取元素的xpath、name或id等信息。

13、支持类似Appium或UIAutomator工具中的元素信息查看功能，可在真机投屏画面点击元素获取元素的xpath、name或id等信息。

15、支持对测试失败的用例一键提交缺陷，缺陷需同步到测试管理的缺陷管理模块。

16、质量看板首页展示平台的总项目数、总案例数、总任务数、总设备数以及总通过率。页面中间部分以时间为维度，展示所选时间段内的各个项目的自动化用例执行情况。页面下方以项目为维度，展示所选项目的自动化用例执行情况。

17、具有异常情况处理机制。如弹窗不符合预期、APP崩溃、单个测试用例死循环、wifi断线等情况时，有异常处理机制。

15、支持对测试失败的用例一键提交缺陷，缺陷需同步到测试管理的缺陷管理模块。

16、质量看板首页展示平台的总项目数、总案例数、总任务数、总设备数以及总通过率。页面中间部分以时间为维度，展示所选时间段内的各个项目的自动化用例执行情况。页面下方以项目为维度，展示所选项目的自动化用例执行情况。

17、具有异常情况处理机制。如弹窗不符合预期、APP崩溃、单个测试用例死循环、wifi断线等情况时，有异常处理机制。

1. 支持设备多控，即同时在多部设备上执行同一个脚本。执行结束后，每个设备都有详细的执行情况，包括用例执行情况、失败用例截图、日志信息等。。

### WebUI自动化测试

1、支持B/S架构系统、C/S架构系统（Windows客户端）和H5播放器的Web UI自动化测试。

2、支持对C/S架构系统的增、删、改操作，包括但不限于对应用名称、文件路径、应用版本号、关联驱动的操作。

3、支持用例同步。Web UI自动化模块维护的用例可同步到测试管理的测试用例模块中，可通过设置用例标签进行用例筛选。

4、支持可视化界面录制和编写用例。通过脚本录制或拖拽元素控件等方式编写APP自动化测试用例，用例编写完成后可对操作步骤进行编辑。

5、支持Python/Java脚本编写用例。支持主流自动化测试框架，通过编写Python/Java代码实现APP操作。

6、支持查看所有的自动化脚本信息，可对脚本进行管理操作，包括查看脚本信息、编辑脚本等。

7、支持引用自动化测试用例生成测试任务，制定任务执行范围，定制测试执行策略，执行测试任务，查看测试执行情况等。

8、支持统计自动化测试整体执行情况，记录执行过程详情信息和日志信息，对测试失败的用例截图当前画面保存。测试结束后，支持查看用例执行概况、成功/失败用例数、平均任务耗时等。

9、支持对测试失败的用例一键提交缺陷，缺陷需同步到测试管理的缺陷管理模块。

10、质量看板首页展示平台的总项目数、总案例数、总任务数、总设备数以及总通过率。页面中间部分以时间为维度，展示所选时间段内的各个项目的自动化用例执行情况。页面下方以项目为维度，展示所选项目的自动化用例执行情况。

11、具有异常情况处理机制。如弹窗不符合预期、页面崩溃、单个测试用例死循环、网络中断等情况时，有异常处理机制。

12、Web UI自动化测试兼容主流浏览器：Chrome、Firefox、IE、360浏览器等

### 仿真挡板服务

1、用于适配与我行各类系统、各类产品的配置以及配置产品的管理。包括产品的增删改等操作。

2、具体产品的配置中，可以对产品的仿真规则进行定义和配置。交易定义可以在交易定义配置中对交易的延迟返回进行配置。

3、配置各个系统的环境参数，用于模拟真实模拟银行系统。包括IP、端口、通讯方式、编码方式等关键通讯要素。

4、用于管理不同产品系统的执行与关闭，灵活的控制改产品系统的开启与关闭。

5、执行日志中能对仿真服务执行详细情况进行查询。

6、用于模拟中间系统，代替中间系统对另外两个系统的交互进行转发，并具有中间系统的解析报文，从新拼装转发到对应系统。

7、服务器监控能监测当前仿真服务的资源情况。

1. 支持产品配置。
2. 支持环境配置。

10、支持交易配置。

11、选择需要添加案例和报文的交易，点击新增报文，进行报文的添加。先添加报文模板以及生成报文元素，然后再进行案例以及案例参数的添加。

12、记录测试过程，查看挡板处理的交易的测试结果。

### 性能测试

1、兼容主流Jmeter脚本和Loadrunner脚本。

2、支持将接口自动化测试配置好的接口，作为性能测试脚本，执行性能测试。

3、支持性能测试发压机的资源自动调度与扩容，发压机资源利用率监控和展示。

4、性能测试脚本支持设置并发数、持续时间、断言等常用设置，支持引用外部jar包执行特定操作，支持引用excel或csv文档实现请求参数化。

5、支持混合场景的性能测试，如一个场景包含多个关联接口。

6、支持性能测试结果按测试时间轴查看，而不是只有一个类似于Jmeter聚合报告的最终结果。

7、支持监控关联服务器性能指标，按测试时间轴查看，可对接Prometheus API，可通过模板配置的形式，进行数据编排展示，实现灵活展示个人所属监控数据，如：CPU、MEM、连接数、io、网络带宽、磁盘等数据的展示。

8、支持性能测试结果详细分析，定位性能瓶颈，输出性能测试结果。

9、支持定制测试计划，设置定制器定时触发性能测试任务，测试结束后生成测试报告。

10、支持性能测试服务器资产管理，支持查看服务器配置信息、资源占用情况、版本情况等。

11、支持设置监控项的阈值，超过阈值可配置告警邮件

### 系统管理

实现人员、团队、机构、角色的管理：

实现登录用户可以修改自己的登录密码；不同类型的人员根据角色不同会做出差异化管理；

系统统管理员/测试经理等角色可以建立虚拟测试小组，建立小组的负责人，团队成员等；支持在后续的测试项目管理中以小组为单位进行任务分配；

实现行内机构同步、维护和查询；

实现用户同步、用户信息维护与查询，用户导入、导出、启用、停用；

实现对接行内统一身份证认证和单点登录；

实现角色信息的维护、查询、导入、导出等，权限控制的粒度到按钮级别；

实现系统日志和用户日志查看及管理。用户日志包含但不限于平台各功能、相关人员操作日志。

## 系统关联需求

### Jira平台对接

实现Jira平台等项目管理系统对接，导入项目信息和同步缺陷等信息。

### Devops平台对接

实现对接行内运维平台Devops模块，支持持续集成与持续部署。

### OA平台对接

支持对接行内的OA系统以实现工作流同步。

### 统一消息中心对接

支持实现对接行内消息中心以实现短信、微信、邮件等消息的通知。

### 统一用户管理平台对接

支持对接行内统一用户管理平台以实现组织架构同步，统一登录认证等功能。

### 测试工具集成

包括但不限于以下几类工具：代码扫描工具、性能测试工具、单元测试工具、接口自动化测试工具、APP自动化测试工具、UI自动化测试工具，并提供平台统一的系统登陆界面。采集各工具的测试过程化数据和结论，提供给平台作为管理和报告支持。

# 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、高并发性、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。

## 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。

## 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【1000】，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【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。

## 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、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。

## 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）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》；

（3）项目组负责协调、配合系统设备及相关软硬件的安装调测工作，并解决发现的质量及性能等有关问题。在软件开发过程中出现问题，要在24小时内将处理意见及解决办法上报至管理层。系统测试和验收要符合测试及验收标准；

（4）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；

（5）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；

（6）项目组要提供数据容量规划咨询，设计系统数据备份和恢复策略，在系统中提供手动和自动两种数据备份方式，当系统发生异常时可对数据进行恢复；

## 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）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。

### 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。

### 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 |  |
| 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 |  |

## 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。