长沙农村商业银行股份有限公司

自动化数据建模工具项目需求

**信息技术部**

**2021年08月**

目 录

**[1. 引言 3](#_Toc15161)**

[1.1. 背景 4](#_Toc20097)

[1.2. 项目概况 5](#_Toc484)

[1.3. 读者对象 5](#_Toc20152)

**[2. 总体业务需求 5](#_Toc17656)**

[2.1. 业务目标 5](#_Toc2411)

[2.2. 项目范围及局限性 6](#_Toc26784)

[2.3. 业务功能需求清单 6](#_Toc13381)

[2.4. 系统关联需求 7](#_Toc20231)

**[3. 总体技术需求 7](#_Toc31398)**

[3.1. 系统总体要求 7](#_Toc18453)

[3.2. 系统建设反洗钱标准 8](#_Toc22614)

[3.3. 系统架构要求 9](#_Toc16794)

[3.4. 系统性能要求 10](#_Toc27813)

[3.5. 系统兼容性要求 11](#_Toc22576)

[3.6. 系统安全要求 12](#_Toc11258)

[3.6. 系统部署要求 19](#_Toc6155)

[3.8. 系统对接要求 21](#_Toc23931)

[3.9. 系统测试需求 21](#_Toc28787)

[3.10. 知识转移要求 22](#_Toc19746)

[3.11. 知识产权要求 23](#_Toc30726)

1 **引言**

**1.1 背景**

随着云计算、大数据、人工智能、区块链等技术的持续发展和不断成熟，传统银行和金融机构也在面临着数字化和智能化的转型。科技正催生更多的新应用和商业模式，同时金融的功能也在不断衍变。其中人工智能起到串接互联网、金融、大数据的作用，实现更加智能的精准计算和实时金融，解决“互联网+金融”模式下的诸多痛点，必然会成为银行转型的下一个重要趋势。金融在人工智能的改造和助力下，将不再局限于“互联网+金融”，而是逐步向“互联网+金融+大数据+人工智能”转变。金融科技通过海量的数据、惊人的算力、多样的算法改变了金融机构寻找客户、度量风险、产品定价、创造利润、经营管理的传统模式。

如何能够把握住最新科技发展机遇，积极加强人工智能技术对于商业银行业务发展和管理提升起到重要促进作用，是商业银行数字化转型重大内容。

对此，我行提出金融科技发展三年规划，紧紧围绕“建设有温度的百姓银行”的总体发展愿景，坚持“特色化、轻型化、智能化”的发展方向，以“安全、敏捷、智能、开放”为金融科技发展愿景，逐步提高人工智能能力，构建智能模型全生命周期管理平台和服务配置体系，通过对智能服务的共享复用、对智能服务研发相关角色进行管理，对前台业务提供个性化智能服务的迅速构建能力支持，协同业务部门推出智能营销、智能支付、智能风控、智能消费金融、智能普惠金融、智能客服、智能网点等智能服务。

**1.2 项目概况**

自动化数据建模工具主要是采购全流程的数据建模平台，覆盖数据接入、数据预处理、数据建模、模型发布、模型管理、模型监控等模型的整个生命周期管理，工具需要提供模型设计训练、模型/算法库、模型预测服务、监控服务等一系列能力支持，致力于解决智能应用研发过程中存在的响应缓慢、效率低下问题。为智能客服、智能营销、智能风控、智能运营等智能体系建设提供有力支撑，为全行提供人工智能的标准基础服务。

**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**

自动化数据建模工具的采购目标是通过深度学习框架、机器学习算法库、技术组件、建模和应用流程、智能服务的统一和标准化，逐步沉淀模型资产并实现复用，有效降低模型应用场景门槛、成本，提高数据模型应用场景实现的效率，快速的实现业务交付、为管理和业务赋能。

## **2.2 项目范围及局限性**

自动化数据建模工具与AI中台的机器学习平台在功能上有部分重合，可以看做是机器学习平台建模功能的延伸应用，更加侧重于运用成熟的机器学习或者深度学习模型自动地开发数据模型，模型可解释性更强、业务人员更容易上手。

因此自动化建模工具更侧重于便捷化、高效化的模型开发，对于数据预处理、模型管理等功能实现较为简单。

### **2.3 业务功能需求清单**

**2.3.1.数据源管理**

数据源管理主要目的是把行内数据平台或者其他数据源的数据进行统一管理，平台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：

**2.3.2.数据预处理**

需要提供各类数据的预处理组件，能够支持对接入的数据进行基本探索、数据加工、数据清洗等数据处理操作，以满足建模的数据需求。

**2.3.3.模型开发、训练及评估**

需要兼容各类机器算法和深度学习算法，支持各类建模方式，包括但不限于可视化建模、Notebook、AutoML，可以满足各业务场景的模型的开发，并对开发完成的模型进行训练、验证、评估等以筛选出最优模型。

**2.3.4.模型的发布以及管理**

减少传统模型上线发布中导入、导出、编译等繁琐的手工操作，能够实现模型的一键发布。

需要支持模型导入、导出、上线、下线、删除、检索、审核、资源配置以及权限控制等管理功能，以便后续将全行的业务模型进行统一管理。

**2.3.5.模型的服务及监控**

对于已经完成开发上线的模型需要支持外部应用系统的调用并对调用情况进行监控，支持对已上线的模型明细进行查询，对模型运行状态进行监控。

## **2.4 系统关联需求**

本次自动化建模工具前期需要从省联社系统、行内大数据平台、内容管理平台、ESB等系统接入结构化以及非结构化数据，用于模型开发的数据来源。

同时，后续开发出来的数据模型可以开放服务接口，供行内的信用卡营销、电子挎包、小微信贷、Q闪贷等应用系统进行调用。

**2.5 建设费用**

经过调查同业中的采购情况，本次自动化建模工具采购预算为100万元。

**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）系统设计需要支持接入我行ESB及微服务平台。

## **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【100】，并发数不低于【100】，考虑未来【三】年的发展空间；

（3）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80%；

（4）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；

（5）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；

（6）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。

### 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）。

### **3.6.13 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。

### **3.6.14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**

1. 项目组要负责对接行内大数据平台，支持与其相关系统之间的数据交换等；
2. 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；
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。